



# GI-Edition

## Lecture Notes in Informatics

**Heiko Roßnagel, Christian H. Schunck,  
Sebastian Mödersheim (Hrsg.)**

## Open Identity Summit 2021

**01.–02. Juni 2021  
Copenhagen**

# Proceedings



GESELLSCHAFT  
FÜR INFORMATIK





Heiko Roßnagel, Christian H. Schunck,  
Sebastian Mödersheim (Eds.)

## **Open Identity Summit 2021**

**01. - 02.06.2021**  
**Copenhagen, Denmark**

Gesellschaft für Informatik e.V. (GI)

## **Lecture Notes in Informatics (LNI) - Proceedings**

Series of the Gesellschaft für Informatik (GI)

Volume P-312

ISBN 978-3-88579-706-7

ISSN 1617-5468

### **Volume Editors**

Heiko Roßnagel | Christian Schunck

Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering

Nobelstr. 12, D-70569 Stuttgart, Germany

heiko.rossnagel|christian.schunck@iao.fraunhofer.de

Sebastian Mödersheim

Sebastian Mödersheim

Technical University of Denmark Compute

Richard Petersens Plads, Building 324, Room 180

DK-2800 Kgs. Lyngby, Denmark

samo@dtu.dk

### **Series Editorial Board**

Andreas Oberweis, KIT Karlsruhe,

(Chairman, andreas.oberweis@kit.edu)

Torsten Brinda, Universität Duisburg-Essen, Germany

Dieter Fellner, Technische Universität Darmstadt, Germany

Ulrich Flegel, Infineon, Germany

Ulrich Frank, Universität Duisburg-Essen, Germany

Michael Goedicke, Universität Duisburg-Essen, Germany

Ralf Hofestädt, Universität Bielefeld, Germany

Wolfgang Karl, KIT Karlsruhe, Germany

Michael Koch, Universität der Bundeswehr München, Germany

Peter Sanders, Karlsruher Institut für Technologie (KIT), Germany

Andreas Thor, HFT Leipzig, Germany

Ingo Timm, Universität Trier, Germany

Karin Vosseberg, Hochschule Bremerhaven, Germany

Maria Wimmer, Universität Koblenz-Landau, Germany

### **Dissertations**

Steffen Hölldobler, Technische Universität Dresden, Germany

### **Thematics**

Agnes Koschmider, Universität Kiel, Germany

### **Seminars**

Judith Michael, RWTH Aachen, Germany

© Gesellschaft für Informatik, Bonn 2021  
**printed by** Köllen Druck+Verlag GmbH, Bonn



*This book is licensed under a Creative Commons BY-SA 4.0 licence.*

## Preface

Welcome to the “Open Identity Summit 2021”, which has been jointly organized by the Special Interest Groups BIOSIG within the German Computer Science Society (Gesellschaft für Informatik) and the Technical University of Denmark.

The international program committee performed a strong review process according to the LNI guidelines with at least three reviews per paper and accepted 48 % of the 31 submitted papers as full scientific papers.

Furthermore, the program committee has created a program including selected contributions of strong interest (further conference contributions) for the outlined scope of this conference.

We would like to thank all authors for their contributions and the numerous reviewers for their work in the program committee.

Copenhagen, 22nd of April, 2021

Heiko Roßnagel  
*Fraunhofer IAO*

Christian H. Schunck  
*Fraunhofer IAO*

Sebastian Mödersheim  
*DTU Compute*

## Conference Chairs

Heiko Roßnagel, Fraunhofer Institute for Industrial Engineering IAO  
Christian H. Schunck, Fraunhofer Institute for Industrial Engineering IAO  
Sebastian Mödersheim, Technical University of Denmark Compute

## Programme Committee

Franco Arcieri, Italy  
Arslan Broemme, Germany  
Christoph Busch, Germany  
Victor-Philipp Busch, Germany  
Jörg Caumanns, Germany  
Jos Dumortier, Belgium  
Lothar Fritsch, Sweden  
Walter Fumy, Germany  
Igor Furgel, Germany  
Marit Hansen, Germany  
Olaf Herden, Germany  
Gerrit Hornung, Germany  
Detlef Houdeau, Germany  
Detlef Hühnlein, Germany  
Tina Hühnlein, Germany  
Luigi Lo Iacono, Germany  
Jan Jürjens, Germany  
Ulrike Korte, Germany  
Michael Kubach, Germany  
Andreas Kuckartz, Germany  
Andreas Kühne, Germany  
Sebastian Kurowski, Germany  
Herbert Leitold, Austria  
Peter Lipp, Austria  
Milan Markovic, Serbia  
Tarvi Martens, Estonia  
Gisela Meister, Germany  
Sebastian Mödersheim, Denmark  
Alexander Nouak, Germany  
Sebastian Pape, Germany  
René Peinl, Germany  
Henrich Pöhls, Germany  
Kai Rannenberg, Germany  
Alexander Roßnagel, Germany  
Heiko Roßnagel, Germany  
Christian H. Schunck, Germany  
Rachelle Sellung, Germany  
Jon Shamah, United Kingdom  
Maurizio Talamo, Italy  
Don Thibeau, United States  
Karsten Treiber, Germany  
Tobias Wich, Germany  
Thomas Wieland, Germany  
Alex Wiesmaier, Germany  
Jan Zibuschka, Germany  
Jan Ziesing, Germany  
Frank Zimmermann, Switzerland



## **Hosts and Partners**

### **BIOSIG – Biometrics and Electronic Signatures ([www.biosig.org](http://www.biosig.org))**

The special interest group “Biometrics and Electronic Signatures” (BIOSIG) within GI e.V. is dedicated to the fundamentals, methods, techniques, processes and implementations used to guarantee the authenticity and integrity of entities.

### **NGI TRUST – Next Generation Internet (<https://www.ngi.eu/ngi-projects/ngi-trust/>)**

NGI TRUST supports the development of a human-centric Internet by developing a stronger European ecosystem of researchers, innovators and technology developers in the field of privacy and trust enhancing technologies by supporting third-party projects.

### **mGov4EU – Mobile Cross-Border Government Services for Europe (<https://www.mgov4.eu/>)**

mGov4EU pushes forward the practical use of inclusive mobile Government services in Europe, bringing such services in line with EU citizens’ expectations for safe, resilient and sustainable mobile communication. Innovating electronic identity management, storage of data and the exchange of electronic documents are key elements.

# Table of Contents

## Open Identity Summit 2021 – Regular Research Papers

**Jan Zibuschka and Lothar Fritsch**

*Mapping Identity Management in Data Lakes*.....15

**Radovan Semančík**

*Complexities of Identity Provenance Metadata*.....25

**Giampaolo Bella, Pietro Biondi, Gianpiero Costantino, Iaria Matteucci, and Mirco Marchetti**

*Towards the COSCA framework for “COnceptualizing Secure CARs”*.....37

**Martin Schanzenbach, Christian Grothoff, Hansjürg Wenger, and Maximilian Kaul**

*Decentralized Identities for Self-sovereign End-users (DISSENS)*.....47

**Johannes Kunke, Stephan Wiefling, Markus Ullmann, and Luigi Lo Iacono**

*Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication*.....59

**Daniel Fett**

*FAPI 2.0: A High-Security Profile for OAuth and OpenID Connect*.....71

**Sebastian Vogt and Holger Funke**

*How Quantum Computers threat security of PKIs and thus eIDs*.....83

**Andrés Chomczyk Penedo**

*Self-sovereign identity systems and European data protection regulations: an analysis of roles and responsibilities*.....95

**Lukas Alber, Stefan More, Sebastian Mödersheim, and Anders Schlichtkrull**

*Adapting the TPL Trust Policy Language for a Self-Sovereign Identity World*.....107

**Christopher Ruff, Andrea Horch, Benedict Benthien, Wulf Loh, and Alexander Orłowski**  
*DAMA – A transparent meta-assistant for data self-determination in smart environments*.....119

**Tomasz Kusber, Steffen Schwalm, Dr. Ulrike Korte, and Kalinda Shamburger**  
*Records Management and Long-Term Preservation of Evidence in DLT*.....131

**Michael Kubach and Rachelle Sellung**  
*On the Market for Self-Sovereign Identity: Structure and Stakeholders*.....143

**Michael Kubach and Heiko Roßnagel**  
*A lightweight trust management infrastructure for self-sovereign identity*.....155

**Victor Martinez Jurado, Xavier Vila, Michael Kubach, Isaac Henderson Johnson Jeyakumar, Albert Solana, and Matteo Marangoni**  
*Applying assurance levels when issuing and verifying credentials using Trust Frameworks*.....167

**Lothar Fritsch and Nils Gruschka**  
*Extraction and Accumulation of Identity Attributes from the Internet of Things*.....179

Open Identity Summit 2021 – Further Conference Contributions

**Fabien Imbault, Justin Richer, and Aaron Parecki**

*Managing authorization grants beyond OAuth 2.....*193

**Sebastian Kurowski, Fatma Cetin, and Rudolf Fischer**

*Why should they care? Conceptualizing the challenges of information security training.....*199

**Frank Morgner and Jonas von der Heyden**

*Analyzing Requirements for Post Quantum Secure Machine Readable Travel Documents.....*205

**Harshvardhan J. Pandit, Vitor Jesus, Shankar Ammai, Mark Lizar, and Salvatore D’Agostino**

*Role of Identity, Identification, and Receipts for Consent.....*211

**Vitor Jesus, Catarina Silva, João Paulo Barraca, Gilad Rosner, Antonio Nehme, Muhammad Waqas, and Rui L. Aguiar**

*Permission and Privacy Challenges in Alternate-Tenant Smart Spaces.....*217

**Carsten Schmidt, Robert Krimmer and Thomas J. Lampoltshammer**

*“When need becomes necessity” - The Single Digital Gateway Regulation and the Once-Only Principle from a European Point of View.....*223



**Open Identity Summit 2021**

**Regular Research Papers**



# Mapping Identity Management in Data Lakes

Jan Zibuschka<sup>1</sup>, Lothar Fritsch<sup>2</sup>

**Abstract:** Data lakes are an emerging paradigm for large-scale, integrated data processing within organizations. While it has been noted in earlier work that data governance is central for the successful operation of a data lake, and that privacy is a central issue in such a setting as personal information may be processed, the governance of personal information in data lakes has received only cursory attention. We propose tackling this information using identity management functions and perform a systematic gap analysis based on the FIDIS typology of identity management systems.

**Keywords:** identity management; data lake; privacy; data governance; data protection

## 1 Introduction

Modern organizations experience an influx of digital information from various sources, which they analyze as part of a multitude of business processes, based on the massive computing resources available in contemporary Clouds. These data analytics have become a mainstay of value creation in the information economy [Ma16]. data lakes are quickly becoming the dominant paradigm for comprehensive integration of this data. While there are various implementations and architectures, covering the different relevant business processes to varying degrees [ML16, Na19], in general data lakes facilitate the integration of information from distributed, heterogenous sources within an organization, and allow for performing a wide array of analytics on the information [Gi19]. As the information in data lakes is drawn from diverse, heterogenous sources, in various formats, and may or may not be accompanied by useful annotations [Na19], in its initial state it is more of a “data swamp” [Gi19], with disparate, unconnected information and formats, and may remain so if there is no prudent data governance [GH19].

One important societal challenge of Big Data analytics in general are the privacy issues they induce. Data analytics unleashed on a broad basis of information can lead to insights about a data subject that the data subject may not have foreseen, which will lead to objections down the line [Ma16]. While for dedicated processing of big data in a fully controlled, homogenous environment, various approaches for privacy-preserving analytics exist [Me16], these do not translate to the more decentralized processing

---

<sup>1</sup> Robert Bosch GmbH, Zentralbereich Forschung und Voraentwicklung, Renningen, 70465 Stuttgart, jan.zibuschka@de.bosch.com

<sup>2</sup> Oslo Metropolitan University, Pilestredet 35, 0166 Oslo, lothar.fritsch@oslomet.no



embodied by heterogenous data storage and processing in data lakes. Therefore, privacy engineering for managing personal information on a data lake level would once again focus on data governance of personal information, providing an infrastructure promoting transparency and accountability [Sp19], which are protection goals of the European General Data Protection Regulation (GDPR) [Sp19], and are also commonly used for privacy in data analytics on other continents [We07].

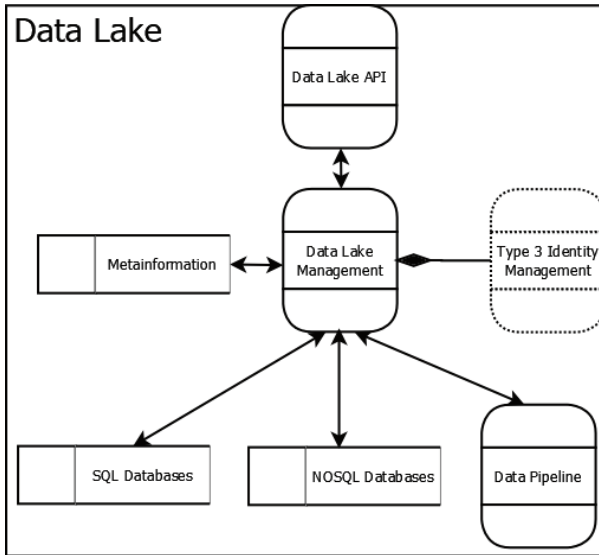


Fig. 1: Structural components of a data lake, proposed identity management

To put it in data lake terminology: we cannot have a data swamp of personal information in an organization but need a more structured approach. The structured processing and transmission of personal information is in the domain of identity management (IdM) systems. While some identity management functions for administration are present in commercial data lakes [K117], and identity management has also been acknowledged as a core function of data lake management systems in research [Na19], there has not, been a systematic investigation of the topic. This contribution aims to fill this gap. Based on an analysis of the flow of personal information in a generalized data lake architecture, we identify key identity management functions in the processing of personal information in a data lake based on the FIDIS (Future of Identity in the Information Society, and EU-funded project<sup>3</sup>) typology of identity management systems [Ba05].

<sup>3</sup> <http://www.fidis.net/>

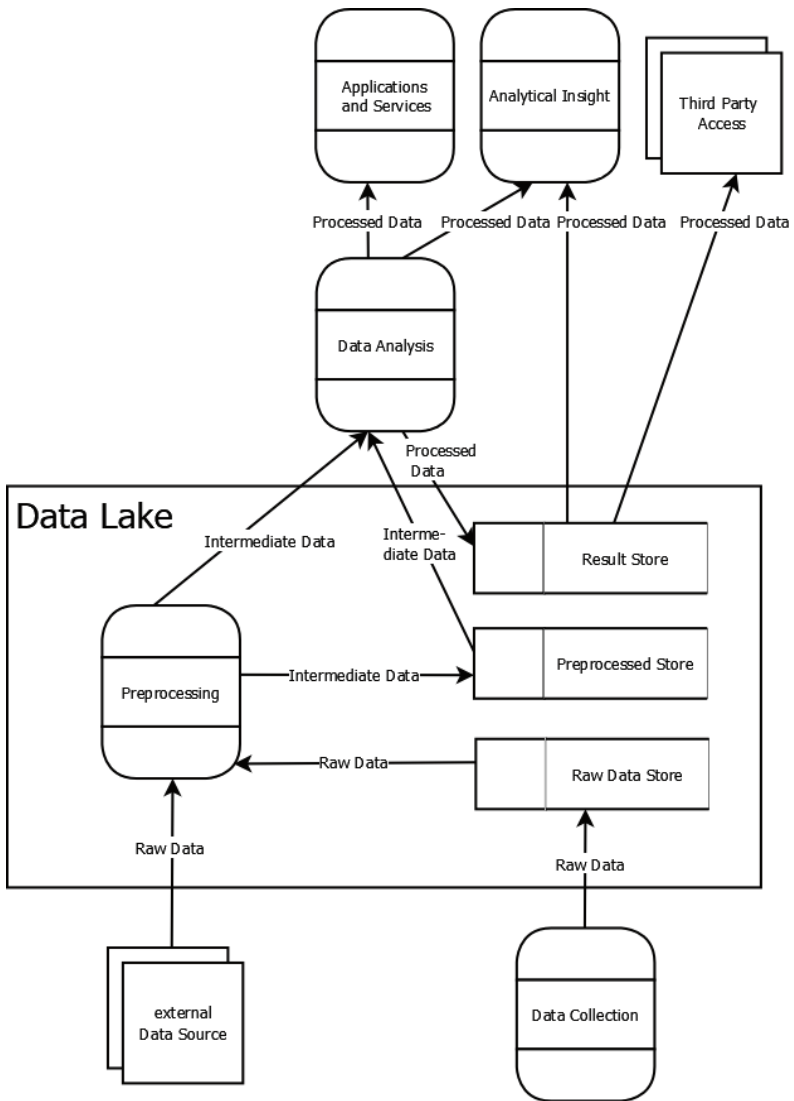


Fig. 2: Data lake reference architecture with personal information flow

## 2 Reference Architecture for Data Lakes

As a basis for mapping identity management in data lakes, we build a simplified reference architecture based the data lake architectures and processes described in related work. Our aim for this architecture for it to be universally applicable and comprehensive with regards to the covered business processes. Firstly, we establish a top-level, structural view of what constitutes a data lake. data lakes comprise various data stores [Na19], including SQL databases, NOSQL databases, and data processing pipelines [GH19] (See Fig. 1). Those data stores are orchestrated by one or several data lake management components, which expose a control interface via an API [Be17]. This data lake management draws on a base of metainformation [GH19] about the underlying data sources. In addition, we map the flow of personal information through a data lake, see Fig. 2. The main structural steps of personal information processing in a data lake are:

1. Personal information may enter such a data lake from external data sources, or from data collection performed by the organization operating the data lake [GH19]. A combination of both approaches is also possible, as externally acquired information may require annotation [GH19]. In any case, the raw data acquired is usually stored in the data lake [Gi19] in an untransformed state [KW18].
2. The information may then be preprocessed in the data lake. Operations that are performed on this level include data extraction and data cleaning [Na19], with the overall aim of bringing the information in a harmonized state fit for further processing. The results of this preprocessing may again be stored in the data lake [Gi19], or may be generated on the fly.
3. Analysis of the information is performed. This step may be performed within the data lake, i.e., in the case of integrated processing pipelines [GH19], or may take place outside of the oversight of data lake management [ML16]. We denote this with a dotted, extended border for the data lake system. Whether the processing is done in the data lake or not, results may be stored there for archival purposes [Gi19].
4. Finally, access to the result of processing may be given to data analysts or services internal to the organization operating the data lake, or to external entities [ML16].

Thus, analysis of the flow of personal information in data lakes can differentiate input, preprocessing, analysis, and output stages of processing. Fig. 2 gives an overview of our data lake reference architecture for analyzing personal information flow.

## 3 Types of Identity Management in Data Lakes

### 3.1 FIDIS Identity Management Typology

In addition to those processing stages, we build on the FIDIS classification of identity management systems [Ba05]. The typology differentiates type 1 identity management systems for account management, that implement authentication, authorization, and access control; type 2 identity management systems for processing of user data by an organization, and type 3 identity management systems that enact user control of their identity information and pseudonyms that are exposed.

A data lake processing personal information would be considered a type 2 identity management system as a whole under this definition. Thus, our contribution is concerned with tracing relevant junctions for the introduction of type 1 and 3 identity management in this overall type 2 identity management structure, and other type 2 identity management structures within the organization that may connect to the data lake.

Overall, type 3 identity management is the main gap identified in our analysis, which is significant, as type 3 identity management most directly addresses legal requirements [Sp19]. Type 1 identity management offers an underlying infrastructure allowing only authorized access, which is necessary for selective transparency and intervenability, and to implement state of the art security. An overview of the position of these components is provided in Fig. 3. The following sections provide some more in-depth discussion of the types of identity management in data lakes.

### 3.2 Type 1 Identity Management

With regards to type 1 identity management components, it is notable that the subjects of the identity management systems can vary quite significantly. Type 1 identity management in data lakes may concern the end user whose personal information is processed, system administrators, data scientists accessing the data lake, or even the organization operating the data lake itself.

This is for example relevant in the integration of external data sources. An external data source may require authentication to access. Then, it be integrated in the data lake using an organizational account representing a link between the organization operating the data lake and the organization operating the external data source on a B2B (business to business) level. Examples include external services offering specialized global information such as weather data, stock market information, or geographic information. The external data sources may, however, also be personal, linked to data lake using an end user account. This may be relevant for individual information such as social network accounts or individual devices and might be accomplished using protocols such as OAuth.

It is notable that type 1 identity management also potentially exists in many of the individual data stores within the data lake, but may not support the authentication needed for processing in the data lake, either being too rigid, not allowing for integrated processing of the data, or not having access to information about the broader processing, such as the accessing entity, that would be needed for a sensible authentication.

This distinction between type 1 identity management for various stakeholder groups is highly relevant in controlling access to the data stored in the data lake. Administrators logging into the underlying systems where the information is stored may get access to it. Analysts of the organization operating the data lake need to be authenticated when accessing the stored information. However, we note the currently documented data lake architectures and management services do not implement any type 1 identity management for the data subject, and therefore cannot offer self-service access, even though it is encouraged by the GDPR [Sp19], specifically regarding access to stored personal information. All in all, data lakes need and, in many cases, already offer on their management layer type 1 identity management for all involved stakeholders, as indicated in Fig. 3.

### **3.3 Type 2 Identity Management**

As already mentioned, the processing of personal information in a data lake as a whole constitutes type 2 identity management in the sense of the FIDIS typology. It is notable that the type 2 identity management in the organization stretched beyond the data lake proper, both into data collection and into further data processing for analytics or services. These steps are also part of our reference architecture for this reason. However, this contribution is concerned with analyzing identity management within a data lake. Data Analytics may be an integral part of a data lake in cases such as integrated data processing pipelines for high throughput Big Data [GH19], bringing this case of type 2 identity management into the scope of our analysis, as depicted in Fig. 3.

### **3.4 Type 3 Identity Management**

While type 3 identity management is part of contemporary data lakes in the form of integration of external data sources that may be under the control of the user, or solely generated by the user [GH19], self-service components in these data lakes do not address the data subject, and instead focus on internal stakeholders, such as data analysts or system administrators [GH19].

While some of the functions associated with contemporary data lake management can constitute type 3 identity management if leveraged by a data subject, such as the ability to identify personal information in a data lake [GH19], the lack of underlying type 1 functions for data subjects makes it unlikely that those functions would ever be used in that way, except when stakeholder roles overlap, e.g., a data analyst is also a data subject.

## 4 Proposed Extension of Identity Management in Data Lakes

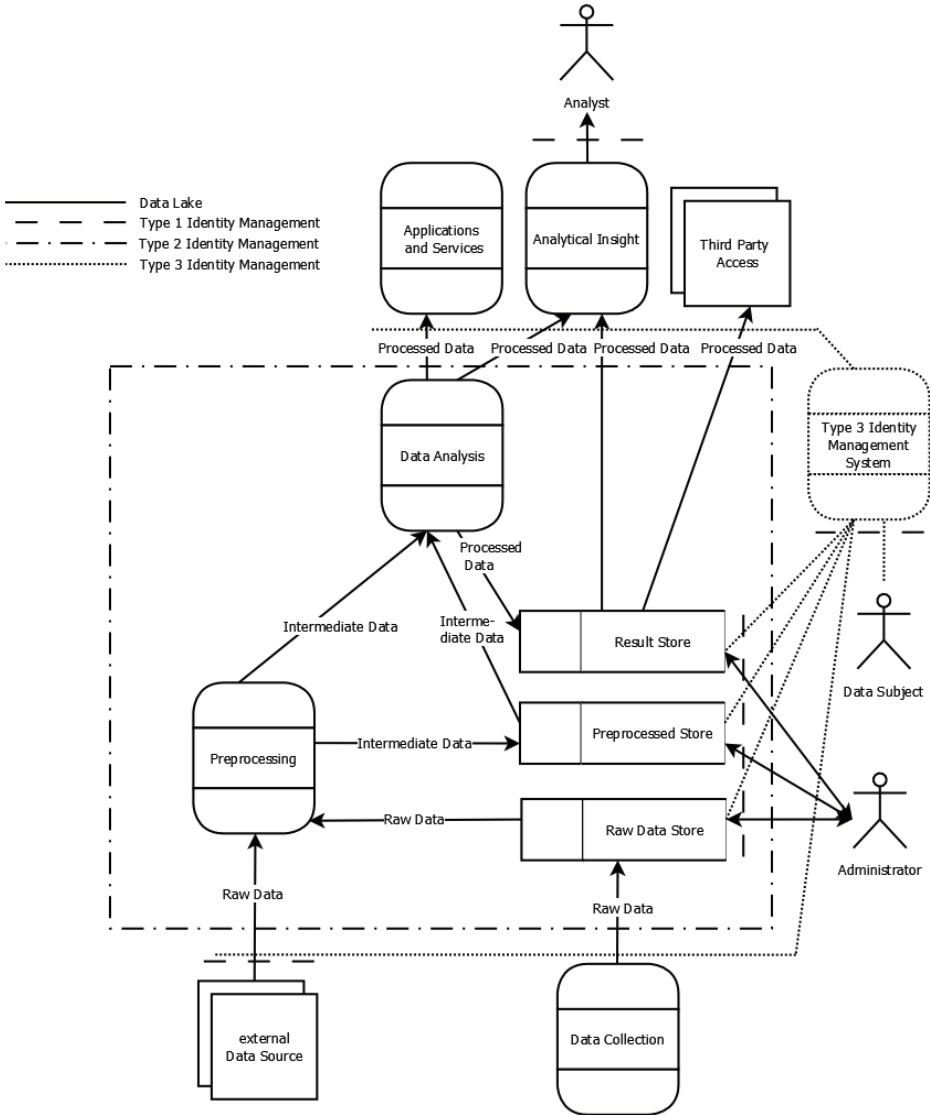


Fig. 3: Identity management in data lakes including proposed type 3 extension

We identify introducing a type 3 identity management component into data lakes, and specifically into data lake management services, as a clear gap of the current implementation landscape. The data lake is linked to data collection, data storage, large-scale data processing, and access to results of such processing by value-added services, analysts, and third parties, and as of such offers excellent opportunities to enact intervenability, transparency, and accountability. Further, this would require type 1 identity management for the data subject linked to the type 3 identity management process, to enable self-service transparency and intervenability.

We propose also linking such a component to the data collection processes, allowing for control of the data flowing into the data lake by the Data subject. Finally, we also propose linking the type 3 identity management to the outbound data flow connecting the data lake to applications, services, and analytics access by data analysts. Such a setup would allow for capturing the data subject's consent for which data is collected in the data lake, and for which purposes this data is used. How to store this consent and interlink inbound and outbound data flows we leave as future work.

## 5 Discussion

In this short contribution, we could only give a very coarse overview of the challenges of privacy and identity management in data lakes. From earlier work, we know that consent management is a very important aspect of implementing privacy in scenarios with multilateral processing of personal information [Ra07, Zi07]. This is even more central in the context of modern data lakes, as the implicit assumption is that data from heterogenous data sources originating from equally heterogenous processing purposes may be integrated. However, this aspect goes beyond the FIDIS typology we build on for this work.

Similarly, we cannot cover the details of authentication to the system. There are several directions for future work in this area. The data subject might be authenticated using federated identity management [Hü10], allowing for cross-domain single sign on and potentially linking to the origin of data in the data lake. That same cross-organizational link may also be established with federated identity management on a B2B level [Hü11]. The data analyst, on the other hand, may require stronger authentication, with might be provided by interoperability of the data lake with a strong authentication infrastructure such as enterprise smart cards [RZ06]. The data analyst may also be given a restricted view of the data, and further privacy protections may be implemented in the system [Gu17]. For example, earlier work has proposed automatically identifying personal information in the data lake [GH19].

It is notable that, from a privacy perspective, interlinking personal information in data lakes is not all bad. The data subject may even benefit from the integration of personal information in a data lake, as raw data, preprocessed information and results of processing, can all be accessed to offer transparency on the level of detail that is most

opportune and understandable. The data subject can also, using identity management functions, potentially control information flowing into the data lake. This includes personal information from both data collection processes of the operating organization and from external data sources. It can also control the use of this information in analytics and services, both internally and at third parties.

All those directions for future work notwithstanding, analyzing identity management in data lakes using the FIDIS typology can make a significant contribution to data governance, as we illustrated in this paper. The reference architecture we also provided may prove useful in the pursuit of any of those possible directions for follow-up. Data lakes are quickly moving from an academic idea to a practical reality. This first contribution could not fully explore the depths of the privacy and identity management challenges that go along with that development. We do, however, encourage future work, which we hope this contribution will inform and motivate.

## Bibliography

- [Ba05] Bauer, M. et al.: FIDIS Deliverable D3. 1–Structured Overview on Prototypes and Concepts of Identity Management Systems, [http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview\\_on\\_IMS.final.pdf](http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf), (2005).
- [Be17] Beheshti, A. et al.: CoreDB: a data lake Service. In: Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. pp. 2451–2454 Association for Computing Machinery, New York, NY, USA (2017).
- [Gi19] Giebler, C. et al.: Leveraging the data lake: Current State and Challenges. In: Ordonez, C. et al. (eds.) Big Data Analytics and Knowledge Discovery. pp. 179–188 Springer International Publishing, Cham (2019).
- [GH19] Gröger, C., Hoos, E.: Ganzheitliches Metadatenmanagement im Data Lake: Anforderungen, IT-Werkzeuge und Herausforderungen in der Praxis. In: BTW 2019. Gesellschaft für Informatik, Bonn (2019).
- [Gu17] Gursoy, M.E. et al.: Privacy-Preserving Learning Analytics: Challenges and Techniques. *IEEE Transactions on Learning Technologies*. 10, 1, 68–81 (2017).
- [Hü10] Hühnlein, D. et al.: Diffusion of Federated Identity Management. *Sicherheit 2010. Sicherheit, Schutz und Zuverlässigkeit*. (2010).
- [Hü11] Hühnlein, D. et al.: Skidentity – Vertrauenswürdige Identitäten für die Cloud. *DA-CH Security*. 296–304 (2011).
- [KW18] Khine, P.P., Wang, Z.S.: Data lake: a new ideology in big data era. In: ITM web of conferences. p. 03025 *EDP Sciences* (2018).
- [KI17] Klein, S.: Azure data lake Store. In: *IoT Solutions in Microsoft’s Azure IoT Suite*. pp. 143–154 Springer (2017).
- [ML16] Madera, C., Laurent, A.: The next information architecture evolution: the data lake



- wave. In: Proceedings of the 8th International Conference on Management of Digital EcoSystems. pp. 174–180 (2016).
- [Ma16] Mai, J.-E.: Big data privacy: The datafication of personal information. *The Information Society*. 32, 3, 192–199 (2016).
- [Me16] Mehmood, A. et al.: Protection of big data privacy. *IEEE access*. 4, 1821–1834 (2016).
- [Na19] Nargesian, F. et al.: Data lake management: challenges and opportunities. *Proc. VLDB Endow.* 12, 12, 1986–1989 (2019).
- [Ra07] Radmacher, M. et al.: Privatsphärenfreundliche topozentrische Dienste unter Berücksichtigung rechtlicher, technischer und wirtschaftlicher Restriktionen. 8. Internationale Tagung Wirtschaftsinformatik 2007 - Band 1. 237–254 (2007).
- [RZ06] Roßnagel, H., Zibuschka, J.: Single-sign-on mit Signaturen. *Datenschutz und Datensicherheit-DuD*. 30, 12, 773–777 (2006).
- [Sp19] Spagnuolo, D. et al.: Accomplishing Transparency within the General Data Protection Regulation. In: Proceedings of the 5th International Conference on Information Systems Security and Privacy. pp. 114–125 (2019).
- [We07] Weitzner, D.J.: Beyond Secrecy: New Privacy Protection Strategies for Open Information Spaces. *IEEE Internet Computing*. 11, 5, 96–95 (2007).
- [Zi07] Zibuschka, J. et al.: Privacy-friendly LBS: a prototype-supported case study. *AMCIS 2007 Proceedings*. Paper 40. (2007).

# Complexities of Identity Provenance Metadata

Radovan Semančík<sup>1</sup> 

**Abstract:** Data provenance information is an important part of personal data protection mechanisms. However, capabilities of existing identity management systems are severely limited when it comes to maintaining and processing data provenance information. This paper describes an effort to design and implement capability to process provenance information in midPoint, an open source identity management and governance system. The solution used value metadata for the purposes of storage and processing of provenance information. Resulting prototype was fully integrated into midPoint code base. The solution dealt with all layers of provenance information processing, from data acquisition to user interface. The prototype uncovered a relation between provenance information and other metadata types, as well as potential use of provenance-enriched metadata in conjunction with data protection mechanisms.

**Keywords:** Identity management, Data provenance, Data modeling, Metadata, Personal data protection


## 1 Introduction

We live in a connected world, where information flows from system to system. This is certainly true for identity information, that moves around the world even more than we would like to admit. Processing of the data does no longer depend only on the content of the data. *Provenance* (origin) [Gy10] of the data has to be considered as well. Provenance of the data may be needed to evaluate trustworthiness of the data, considering aspects such as trust in the source system, declared level of assurance and similar metadata. However, tracking data provenance is crucial for data protection mechanisms as well. Provenance metadata are needed to prove that the data came from a legitimate source and that the data are up-to-date. Data provenance is also closely related to concept of *basis for data processing* [GD16], making provenance a crucial element in evaluating whether we can process particular data at all.

However, there are hidden complexities in processing provenance metadata, complexities that seem to extend to processing of all metadata. The complexities were discovered during work on *Data Provenance Prototype* [MP20a] for midPoint, under the umbrella of midPrivacy initiative [MP21a]. MidPoint [MP21b] is a comprehensive open source identity management and governance platform. The *Data Provenance Prototype* project focused on maintenance of provenance metadata for identity information for data

---

<sup>1</sup> Evolveum s.r.o., Vendelínska 109, Lozorno, 90055, Slovakia, radovan.semancik@evolveum.com,

 <https://orcid.org/0000-0002-4903-1436>

protection purposes, and its prototype implementation in midPoint. Goal of the project was to design a data provenance schema (as metadata schema), and to apply the concept to identity data managed by midPoint.

Due to the limited capabilities of existing identity and access management (IAM) protocols, the goal of the project was focused on "local" provenance information. Existing IAM protocols are currently not capable to convey full, end-to-end provenance information, tracking information lineage from its ultimate source. Therefore, the project was limited to considered provenance from the point of view of a single organization. The goal was to track information provenance from the "previous hop" only, the last external system that provided the information to our organization. Intended result of the project was a practical prototype, maintaining limited provenance information as metadata. Even such a limited provenance information, is still useful for maintaining appropriate data protection mechanisms, which is an ultimate goal of midPrivacy initiative. However, maintaining even such a relatively simple "local" provenance information has proven to be a challenge.

## 2 Metadata Multiplicity Problem

Simply speaking, MidPoint's responsibility is to move identity data between systems. MidPoint can feed identity data from source systems, correlate them, transform them to a common data model, apply policies (such as role-based access control, RBAC), transform data to foreign data models and provision the data to external systems by using a generic connector framework. This is an essential identity management functionality, needed by almost every organization. As midPoint is already in the middle of identity data interchange in the organization, it is a natural point to control policies, including data protection policy. Implementing automated data protection mechanism has been an ambition of midPoint development team for many years. However, there is necessary work on technological foundations, before full data protection mechanisms can be implemented.

MidPoint is a schema-based system, internal data model is based on formal data model definition. The data model can be expressed in XML, JSON and YAML. Data examples in this paper are based on JSON notation based on simplified midPoint schema. For clarity, some examples are shortened to JSON snippets.

Below is an example of pure JSON data, describing a person:

```
{
  "givenName" : "Lawrence",
  "fullName" : "Lawrence Long"
}
```

This data structure can be enriched with metadata using a special notation with @

character:

```
{
  "givenName" : {
    "@value" : "Lawrence",
    "@metadata" : {
      ...
    }
  },
  "fullName" : {
    "@value" : "Lawrence Long",
    "@metadata" : {
      ...
    }
  }
}
```

A naïve design of a data provenance solution would use a simple metadata structure specifying where particular value came from:

```
"fullName" : {
  "@value" : "Lawrence Long",
  "@metadata" : {
    "provenance" : "user entry"
  }
}
```

Obviously, any single value of a data item may come from several sources. In the above example of user's full name, it may be entered manually by the user during registration process. Then the same value may come from the human resource (HR) system, or it may be retrieved from an identity provider in an identity federation. The provenance value must not be simply overwritten when the new information comes, e.g. the user entry value must not be overwritten with HR value when the data are correlated to the HR system. In case of the overwrite we would lose information that the user entered manually, which may be a problem in case that user's employment contract ends and the HR information is removed. In such case we may still want to retain user's name, as it was entered manually outside of the employment context. Therefore we have come to a conclusion that the provenance information has to be multi-valued:

```
"fullName" : {
  "@value" : "Lawrence Long",
  "@metadata" : {
    "provenance" : [ "user entry", "HR" ]
  }
}
```

However, even this solution has proven to be unsatisfactory. The value may be a result combining inputs from several information sources. For example, this particular person may want to be called "Larry" instead of "Lawrence", therefore he changes his given name in his user profile. The system then automatically computes full name by using the user-entered given name and surname that originated in the HR system. Considering this possibility, the provenance metadata become a complex data structure. For simplicity, we will denote this combination using a simple plus sign (+), that is a placeholder for complex data structure used in a real-world system. Naturally, the provenance metadata still need to be multi-valued. The following example illustrates metadata for a value which is a combination of two sources, and at the same time the complete value was obtained from the identity provider acting on behalf of "The Institute":

```
"fullName" : {
  "@value" : "Larry Long",
  "@metadata" : {
    "provenance" : [ "user entry + HR", "The Institute" ]
  }
}
```

The example above provides simplified data structure, the real metadata schemas used in the data provenance prototype project are considerably more complex. Modeling of metadata structures has proven to be a challenge of its own, motivating the design of Axiom [Ax20], a new data modeling language.

However, even this solution can be further improved. Aside from provenance metadata, there are other metadata types. E.g. there are *storage metadata* that describe when was the value stored, when it was updated and so on. There are *assurance metadata* that describe level of assurance or trust in the particular value. There are *transformation metadata*, *process metadata*, *policy-related metadata* and other metadata types. We have found that all the metadata which we need to process in midPoint are tightly bound to a particular provenance. For example, any particular value may have high assurance when it originates in HR system, as such information comes from an employment contract that is checked against identity documents. However, if the same value is entered by the user in a registration form, the level of assurance is likely to be low. It would be incorrect to store only the information about high assurance level, as that may be incorrectly applied to the low-assurance data entered by the user, e.g. in case that the HR record is removed. Therefore both assurance values have to be stored, each of them tightly bound to the provenance metadata. This thinking has been applied in the design of *yield* concept (see below).

Detailed description of this "metadata multiplicity problem" is beyond the scope of this paper. The explanation with detailed examples can be found on the project website [MP20b].

Although we have conducted research of available literature at the beginning of the project, we have not found any mention of this problem in a literature related to identity

management or management of metadata. The fact that *provenance* information (and hence the metadata) have a multi-valued character comes as a natural consequence of provenance character [SPG05]. However, the relation of provenance metadata to all the other metadata types was not obvious (e.g. [MD20]). Therefore, unaware of the problem, we have started the project with a simplistic provenance metadata model, which caused significant re-design and re-engineering later in the project. We find this lack of problem coverage surprising, and it was a partial motivation to author this paper.

### 3 Yield

The design decision in the project was to make the entire metadata structure multi-valued. There is one complete value for all the metadata structures for each individual data source. In midPoint parlance, we use term *yield* to refer to each such source. *Yield* may correspond to external data source, such as HR database, remote identity provider or manual user entry. Yet, *yield* may also represent an internal source, such as mapping that combines data from several sources or a value generator.

Following example shows `fullName` user property with two yields in a very simplified form:

```
"fullName" : {
  "@value" : "Larry Long",
  "@metadata" : [
    {
      "provenance" : {
        ... data are combination of HR and user entry ...
      }
    },
    {
      "provenance": {
        ... data came from The Institute ...
      }
    }
  ]
},
```

Each *yield* may contain a complex data structure that describes fine details about the value. For example, following data structure may provide details how and when particular data were transformed:

```
"fullName" : {
  "@value" : "Larry Long",
  "@metadata" : [
    {
```

```

    "provenance" : {
      ... data are combination of HR and user entry ...
    },
    "transformation" : {
      ... data produced by a dynamic expression in
midPoint ...
    }
  },
  {
    "provenance": {
      ... data came from The Institute ...
    },
    "transformation" : {
      ... data copied directly from the source ...
    }
  }
]
},

```

While *yield* may contain a lot of metadata structures that describe exhaustive details about data, *provenance metadata* still have a prime position among all other details. Provenance metadata work as an identifier, allowing the processor to identify the correct *yield* to work with. E.g., user interface can use provenance metadata to identify the *yield* that describes metadata related to manual user entry, making sure the correct metadata are used or updated. Of course, provenance metadata still describe the origin of data, yet this purpose is almost secondary in this case. For this approach to work, the provenance metadata have to describe data origin on a conceptual level, without excessive details, to allow algorithmic comparison of data provenance information. For example, *midPoint* is using a simple data structure called *acquisition* to represent provenance. The *acquisition* data structure contains a reference to *origin*, which is one of objects in internal *midPoint* database. This *origin* works as a conceptual representation of data source, such as external system, organization or even purely abstract concept as "user entry". The *origin* has two purposes. Firstly, it identifies the logical origin of the data, for the purposes of machine-processing of the metadata. The origin identifies a particular *yield*. Secondly, the *origin* can be used to display the source of data in user-friendly way. This design is illustrated in the following example.

```

"fullName" : {
  "@value" : "Larry Long",
  "@metadata" : [
    {
      "provenance" : {
        "acquisition" : [
          {
            "timestamp" : "2020-06-22T10:52:03Z",

```

```

        "originRef" : {
            ... reference to "User entry" origin ...
            .... indicates data entered by user ...
        }
    },
    {
        "timestamp" : "2020-03-06T23:05:42Z",
        "originRef" : {
            ... reference to "HR" origin ...
            ... indicates data taken from HR Database
        }
    }
]
},
{
    "provenance": {
        "acquisition" : [
            {
                "timestamp" : "2020-08-17T14:45:12Z",
                "originRef" : {
                    ... reference to "The Institute" origin ...
                }
            }
        ]
    }
}
],
},

```

The example describes situation illustrated in the previous section. The value "Larry Long" comes from two sources. First source is a combination of data entered by the user with HR data. Second source is "The Institute" organization.

Conceptualization of the provenance structure does not leave place for excessive details. Additional details can be stored in other metadata structures, such as transformation or storage that can be placed at the same level as provenance structure. Such separation has additional benefit of separating metadata schemas into encapsulated data structures.

```

"fullName" : {
    "@value" : "Larry Long",
    "@metadata" : [
        {

```



```
"provenance" : {
  "acquisition" : [
    {
      "timestamp" : "2020-06-22T10:52:03Z",
      "originRef" : {
        ... reference to "User entry" origin ...
        .... indicates data entered by user ...
      }
    },
    {
      "timestamp" : "2020-03-06T23:05:42Z",
      "originRef" : {
        ... reference to "HR" origin ...
        ... indicates data taken from
        HR Database ...
      }
    }
  ]
},
"storage" : {
  "createTimestamp" : "2020-06-22T10:52:03Z",
  "modifyTimestamp" : "2020-03-06T23:05:42Z",
  ...
},
"transformation" : {
  ... detailed description of data mappings ...
}
},
{
  "provenance": {
    "acquisition" : [
      {
        "timestamp" : "2020-08-17T14:45:12Z",
        "originRef" : {
          ... reference to "The Institute" origin ...
        }
      }
    ]
  },
  "storage" : {
    ...
  },
  "transformation" : {
    ...
  }
}
```

```
    }  
  ]  
},
```

This design was prototyped in midPoint, implemented and integrated in midPoint code-base and released in midPoint 4.2. The prototype reached all layers of the system, from storage to presentation. The prototype was a success, although some challenges and open questions remain.

### 3.1 Variations, Challenges and Further Development

The multi-valued metadata and the concept of *yield* worked very well in midPoint environment. Yet, it is still an open question whether these concepts can work for other systems. E.g. some systems may need single-valued ("global") metadata structures in addition to *yields*, even though we have not identified such need in midPoint. We have also considered an alternative approach that does not require multi-valued metadata. However, in this case the system must allow to repeat the same value of a data item several times. This means that all data items in the system must be (technically) multi-valued, it complicates operations with data, presentation and it is likely to confuse the developers. Even though we have rejected this approach in midPoint, it may still be a feasible solution for other systems.

Comprehensive implementation of data provenance requires non-trivial data structures in the metadata. Modeling of metadata schema was one of the early challenges in the project. However, this challenge was expected. It was addressed by designing Axiom [Ax20], a new data modeling language capable of metadata schema definition. We have decided to design a new data modeling language as our research of data modeling languages revealed no existing solution. The midPoint project had been using W3C XML Schema Definition (XSD) [XSD04] as a data modeling language for almost a decade, gaining considerable experience, especially regarding the limitation of traditional data modeling languages. Although we believe that traditional data modeling languages could be used to model metadata, design and maintenance of such solution is likely to be very difficult. This led to the design and implementation of Axiom, which was an enabler for rich metadata schemas. In hindsight, Axiom was a major factor contributing to the success of data provenance prototype.

Moreover, the project focused on local provenance metadata. Global, end-to-end provenance metadata are likely to be significantly more complex. This was one of the reasons of investing into a modeling language that can support efficient evolution of metadata schemas.

The complexity of data provenance makes it a major challenge to present the provenance information to users. Our project was focused on presenting the information to system administrators, who are expected to handle some levels of complexity. However, even that has proven to be a challenge. The metadata presentation components went through

several design iterations during the project. Even though the final result is acceptable, it is still not ideal. Presenting provenance information to common users is likely to a major user experience challenge.

Data provenance information has a value on its own. However, the full value of the provenance is realized when it is combined with data protection concepts. Data provenance is related to the concept of *basis for data processing* (see Art. 6 of GDPR [GD16]), which is central to the data protection mechanisms. Personal data can be processed only if there is a valid *basis* for their processing. Data for which there is no valid *basis* must be erased. Processing of *bases* such as employment or study may seem straightforward. However, in reality various *bases* for data processing overlap. For example, a person may be both employee and student of the same university, or a contractor and customer of the same company. This complexity is often addressed by the use of *personas*, e.g. segregating student and employee data into separate user accounts. While this approach can be very efficient in some cases, it may also be confusing and uncomfortable for users in other cases. Obviously, there is a value in a system that can properly track many overlapping *bases for data processing* on a single persona.

The concepts of data *origin* (provenance) and *basis for processing* are related, however, they are not equivalent. For example, employee data may originate from the HR system, but they may also be entered by an administrator in emergency situations (e.g. outages). HR data may be manually corrected by the user. Those are three different origins of the data, but we are processing the data on the same basis (employment).

The exact role of the *origin* in the data protection mechanisms is not clear yet. It is clear the concept of *origin* is helpful in demonstrating the data were acquired by lawful means (accountability). However, the *origin* itself is not an entitlement for data processing. Therefore, it is questionable whether *origin* plays an essential role in data erasure, or whether the erasure can be determined using only the *basis*. Such questions are an inspiration for further research.

## 3.2 Conclusion

Data provenance prototype provided valuable insights into practical aspects of identity provenance. The prototype was implemented in midPoint - an established open source identity management system. Therefore the prototype has to fit into an existing ecosystem, adapt to practical limitations of real-world systems. Many of the limitations are arguably given by the design choices made when existing systems were created. However, as many existing systems are built in a similar fashion as midPoint, any identity provenance solution is likely to encounter similar challenges.

Several important lessons were learned during the development and testing of the prototype. Perhaps the most unexpected lesson was the multi-valued nature of metadata. The multi-valued nature of provenance information was no big surprise. However, the fact that this multi-valued character seems to apply to all the metadata was unexpected,

and it caused significant rework during the prototype. It is still an open question whether this is an inherent characteristic of the metadata or whether it is merely a design choice. Either way, there seems to be a major engineering advantage to model metadata in multi-valued fashion, identified by provenance information.

Complexity of data provenance information, and the information associated with it was another major challenge. Even though this challenge was expected, it took significant effort to address it. Existing technology does not provide adequate tools to deal with complex metadata structures. Therefore the solution included design and prototype implementation of a completely new data modeling language: Axiom [Ax20]. Axiom has a native support for influencing the underlying concepts of the data model, dubbed *inframodel* by Axiom authors. New features of Axiom were used to model the provenance metadata, together with other metadata types. The prototype demonstrated that this is a feasible and efficient method to deal with the complexity of metadata structures.

Complexity of the provenance information poses a major challenge to presentation of data provenance to the users. The prototype included a user interface for presentation of provenance information to system administrators. Even though system administrators can deal with complex information, the design of user interface required several iterations. The result is acceptable for the purposes of the prototype. Yet, there is still a significant room for improvement even in the administration user interface. Designing a user-friendly and intuitive user interface for common users is likely to be much more challenging.

The prototype suggests that there may be a close relationship between data, metadata and data protection mechanisms. Most notably, it looks like data protection mechanisms need to use metadata to properly manage data values, especially with regard to *basis for data processing*. It is not clear what is the exact role of data provenance information (beyond its use for accountability). However, it is clear that similar mechanisms that are used to manage provenance information in the metadata can be used to store data protection information.

Overall, the project of data provenance prototype was an engineering project, focused on solving practical problems rather than theoretical ones. Despite that, there were interesting challenges that are worth sharing with the broader community.

Even though the resulting code is just a prototype, it has interesting potential for the future, especially in the area of data protection. The implemented mechanism allows maintenance of metadata for every value of every data item in the system, maintaining separate metadata for every *origin* of that value. E.g. the system can track separate data protection information for a full name value that was entered by the user, and the same value that originated in the human resource system. Similarly, the system can track metadata for each value of multi-valued property, such as data about user's affiliations. This ability is likely to be an essential enabler in fine-grained tracking and management of *basis for data processing*, as given by European data protection regulations. This

seems to be a very promising avenue for future research and development.

### 3.3 Acknowledgements

Author would like to thank all the participants of the project, Katarína Bolemant, Pavol Mederly, Anton Tkáčik, Slávek Licehammer and Igor Farinič. The work of project participants provided an essential material for this paper. We would also like to thank NGI\_TRUST for proving funding for this project, and we would especially like to thank project mentors, Maite Alvarez and Collin Wallis, for their help and encouragement. We would like to express our thanks to open source community and especially all the contributors to midPoint project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the NGI\_TRUST grant agreement no 825618.

### Bibliography

- [Ax20] Axiom, <https://docs.evolveum.com/midpoint/axiom/>, Accessed 27/01/2021.
- [GD16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016.
- [Gy10] Gil, Y. et.al.: Provenance XG Final Report, W3C Incubator Group Report. <https://www.w3.org/2005/Incubator/prov/XGR-prov-20101214/>, 2010.
- [MD20] Metadata 2020, <http://www.metadata2020.org/>, Accessed 27/01/2021.
- [MP20a] MidPrivacy: Data Provenance Prototype, <https://docs.evolveum.com/midpoint/midprivacy/phases/01-data-provenance-prototype/>, Accessed 27/01/2021
- [MP20b] Metadata Multiplicity Problem, <https://docs.evolveum.com/midpoint/midprivacy/phases/01-data-provenance-prototype/metadata-multiplicity-problem/>, Accessed 27/01/2021.
- [MP21a] MidPrivacy, <https://docs.evolveum.com/midpoint/midprivacy/>, Accessed 27/01/2021.
- [MP21b] MidPoint, <https://midpoint.evolveum.com/>, Accessed 27/01/2021.
- [SPG05] Simmhan Y.L., Plale B., Gannon D.: A Survey of Data Provenance Techniques. Technical Report TR618, Department of Computer Science, Indiana University, 2005.
- [XSD04] XML Schema Part 1: Structures Second Edition, <https://www.w3.org/TR/xmlschema-1/>, Accessed 27/01/2021.

# Towards the COSCA framework for “CONseptualing Secure CARs”

Giampaolo Bella,<sup>1</sup> Pietro Biondi,<sup>2</sup> Gianpiero Costantino,<sup>3</sup> Ilaria Matteucci,<sup>4</sup> Mirco Marchetti<sup>5</sup>

**Abstract:** Cyber risks associated with modern cars are often referred to safety. However, modern cars expose a variety of digital services and process a variety of personal data, at least of the driver’s. This paper unfolds the argument that car (cyber-)security and drivers’ privacy are worthy of additional consideration, and does so by advancing “COSCA”, a framework for “CONceptualising Secure CARs” as interconnected nodes of the Next Generation Internet. COSCA adopts an innovative socio-technical approach. It crowdsources drivers’ perceptions on core privacy topics and it classifies the data collected by cars and processed by manufacturers pursuant the General Data Protection Regulation. These steps inform a risk assessment which highlights the more relevant mitigation strategies and cyber security technologies. Finally, COSCA aims at designing novel interfaces to enable drivers to exercise their rights about personal data collection and processing.

**Keywords:** automotive; cybersecurity; framework; privacy

## 1 Introduction

The digital side of innovations in the automotive field has been thriving in the last decade, not just towards the traditional goal of vehicle and passengers’ safety. The inside of cars increasingly integrates infotainment, passengers’ physical preferences, such as on mirror positions, seating configuration and air conditioning setup, as well as non-physical preferences, such as on music to play, preferred numbers to call and on-line payment details, and driver generated data such as driving style and location. The outside perhaps is even more varied, with a number of vehicle-to-vehicle and vehicle-to-infrastructure new application scenarios, and many technologies to support them at various layers, such as Dedicated Short-Range Communications (DSRC) and Wireless Access in Vehicular Environment (WAVE).

While autonomous driving is a compelling ultimate aim, it is not the only one, as it is clear that cars are taking the shape of a unique hub offering drivers and, potentially also

---

<sup>1</sup> Dipartimento di Matematica e Informatica, Università degli Studi di Catania, Catania, Italy. giamp@dmi.unict.it

<sup>2</sup> Dipartimento di Matematica e Informatica, Università degli Studi di Catania, Catania, Italy. pietro.biondi@phd.unict.it

<sup>3</sup> Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy. gianpiero.costantino@iit.cnr.it

<sup>4</sup> Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy. ilaria.matteucci@iit.cnr.it

<sup>5</sup> Dipartimento di Ingegneria “Enzo Ferrari”, Università degli Studi di Modena e Reggio Emilia, Modena, Italy. mirco.marchetti@unimore.it

passengers, a novel or reshaped range of digital services through an integrated user interface and a *sui generis* user experience. For example, cars come with Internet connectivity (via an embedded chipset or a dedicated SIM card) and can download over-the-air updates from the manufacturer. They can also provide services through an app that the driver runs on their smartphone to remotely operate car functions like power doors, sunroof, air conditioning, headlight, horn and even engine start/stop. Additionally, the app enables the driver to remotely locate the car (through the car's onboard GPS) and remotely operate geo-fencing, namely to set an area on a map and be alerted should the car ever exceed that area [AC20].

It becomes fair to claim that cars are progressively resembling computers, hence offering digital services while treating a variety of passengers' personal data and, consequently, attracting various malicious aims.

In this context, we strongly argue that the goal of increasing vehicle safety must be paired up with a similar increase in car security, drivers' privacy and, ultimately, overall passengers' trust in the technologies operating their cars. COSCA is an NGI TRUST H2020 project [CO20] founded on the European forefront of safety and privacy standards for the "driver-vehicle" system in the landscape of connected vehicles [Un20]. COSCA leverages the relevant contributions of the ETSI Cyber [ET20], Human Factors and Intelligent Transport Systems technical committees, in addition to Enisa's recommendations on IoT and Smart Infrastructures [EN20]. The project is also based on major international standards such as the ISO/IEC 27000 series [In18].

The main aim of the COSCA project is to define the COSCA framework for "COncceptualising Secure CARs", which revolves around four main activities and combines them innovatively. The first is an understanding of how drivers and passengers feel about their privacy and what level of trust they pose in their vehicle. The second is a classification of the types of data collected by car manufacturers according to Regulation (EU) 2016/679, the "General Data Protection Regulation" (GDPR) [Eu16]. The third is a risk assessment exercise based on ISO/IEC 27000 series geared towards risks for car safety and drivers' privacy. The fourth and final element is the set of measures for car security such as security protocols and their threat models, as well as the human-computer interfaces to enable drivers to consciously use the systems.

This paper details the four activities and explains the current state of their developments, thus providing a snapshot of where the project stands when it is *half way through its lifetime*. The organisation of the prose is simple. Section 2 outlines the COSCA framework, Section 3 discusses how drivers' privacy concerns and trust perceptions can be leveraged and Section 4 explains what personal data is collected and treated by relevant car brands. This knowledge collectively informs the risk assessment exercise on car security and drivers' privacy conducted in Section 5, while the resulting measures are discussed in Section 6. Finally, Section 7 presents some related work and Section 8 concludes.

## 2 The COSCA framework

The four activities of the COSCA framework are outlined in this Section and expanded in the sequel of the paper.

**Activity 1.** *Crowd-sourcing drivers’ privacy concerns and trust perceptions.* Our framework adopts a socio-technical approach because it bases its contribution on people. This is achieved by leveraging crowd-sourcing to study how real people understand and perceive car security and their own privacy while they drive. We argue that this is innovative and not yet available; for example, the mentioned works about securing communication within vehicles often fail to fully ground the technical details upon drivers’ privacy concerns and trust perceptions.

**Activity 2.** *Classifying car collected data.* While modern infotainment systems come with the usual cumbersome privacy policies that should explain what sort of data will be collected about the driver, this information is not always crystal clear to every driver. Each car may collect specific categories of personal data, some brands may collect more or less sensitive categories and treat them somehow adequately, hence we must dig out such information and evaluate how data is treated. In consequence, the COSCA framework prescribes the analysis of what data relevant car brands collect and treat.

**Activity 3.** *Assessing car security and drivers’ privacy risks per car brand.* The previous elements inform a risk assessment exercise inspired to an ISO/IEC methodology suitably adapted to the risks of car security and drivers’ privacy. The mitigation strategies stemming from the risk assessment suggest and motivate the development of techniques such as security protocols, secure cryptographic key distribution and storage, freshness methods and related threat models. Such techniques find their precise and well grounded motivation as a mitigation of assessed risks.

**Activity 4.** *Devising measures for car security and drivers’ privacy.* There is a stringent need to devise a common set of measures for car security at all levels, from the lowest up to the human-computer interface. Weaknesses may derive not only from the known limitations of old technologies such as the CAN Bus but also from the system’s interaction with the driver. Policies should explain in simple terms the types of data that a car collects from the driver, data on which the car manufacturer may act as data Controller or Processor, perhaps also through appropriate cues.

Figure 1 shows the COSCA framework with its activities and and their interrelations. It can be noted that the first two activities fuel up the third activity. Finally, the third activity determines the fourth activity, and the framework is completed.



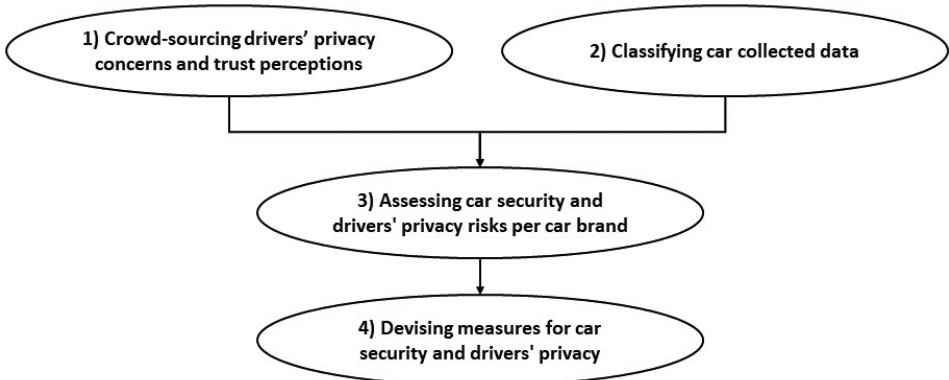


Fig. 1: The four activities in the COSCA framework

### 3 Crowd-sourcing drivers' privacy concerns and trust perceptions

Nowadays, there would be limited use in addressing a problem that drivers did not feel. Despite a few recent headlines on attacks to real cars [VM15], there is limited literature demonstrating how drivers feel about their privacy in their cars and what level of trust they pose e.g. in the interconnected infotainment.

This Section explains the details of activity 1, which prescribes the extraction of people's practical perceptions on (the potential endangerment to their) privacy while they are driving their cars and, at the same time, the trust they place on their vehicles. Such extraction produces a model of privacy and trust, nuanced through the lens of car drivers.

Several steps must be taken. Initially, a questionnaire must be designed with appropriate questions to distil out drivers' privacy concerns and, correspondingly, their trust perceptions. Then, the questionnaire must be submitted to the drivers through crowdsourcing. This is a fundamental step because it allows us to get answers from all over the world, and a valid platform that can be used is Prolific [Pr20]. Finally, the answers of the questionnaires must be studied through statistical analysis in order to derive meaningful correlations [Wi20a, Wi20b].

We completed this work collecting answers from a sample of 1101 respondents, which would be reliable because setting a margin of error of 4% and confidence level of 99% over a large population produces an ideal sample size of 1037 respondents for any population that exceeds 1 million [Qu20]; however, a limitation is that uniformity of distribution of respondents could not be ensured on Prolific. Relevant correlations have arisen through the answers. In particular, most of the participants agree that the systems and technologies implemented in modern cars are increasingly similar to modern computers. Another correlation shows that most drivers disagree that it is necessary for their car to collect their personal data due to the fact that they deem that collection unnecessary to the full functioning of the car. Another correlation shows that a large part of the sample thinks that their data is analysed

and studied by the vehicle systems to evaluate some personal aspects. These correlations highlight privacy concerns.

## **4 Classifying car collected data**

History shows that a poorly designed, interconnected fridge could expose people’s emails [Ne15]. A similar attack could leverage a hacked car to harvest the personal data that the car handles. We must understand and gather what types of data categories cars are collecting — and their manufacturers are treating. Notably, these may even include special categories of data, according to the GDPR, such as religious beliefs and health data.

First, we must build a knowledge base on the current categories of data collected by the major car manufacturers. According to the GDPR, each manufacturer is a data Controller and possibly a data Processor. Manufacturers are therefore responsible for the protection measures they implement on the personal data they collect. To collect this information we can use various ways, such as exercise the right of access with the manufacturer, inspecting and comparing privacy policies or empirically penetrating available cars. This work has been completed about the top ten best-selling car manufacturers of the first quarter of 2019 [Be19] extended with KIA and Tesla. Once data is obtained, we can build metrics regarding privacy policies, such as calculating the level of readability, defining taxonomies based on keywords or noting correlations between car manufacturers. In particular, if special categories under the GDPR are present, then they would require special protection measures as encryption while at rest and in transit.

## **5 Assessing car security and drivers’ privacy risks per car brand**

In all areas of cybersecurity, risks must not be presupposed, they must be assessed. This is especially true for risks affecting car security and drivers’ privacy. A structured, standard risk assessment methodology ought to be used to qualitatively assess such risks, then prioritise them and ultimately mitigate them.

The third activity aims to conduct a cybersecurity risk assessment exercise geared at assessing the risks of car attacks and breaches of drivers’ personal data. Leveraging the outcomes of activity 1 and activity 2, a standard methodology must be tailored to the aims of this activity, yielding the Driver Risk Assessment Methodology (DRAM). This methodology must be then used to conduct the Driver Risk Assessment Exercise (DRAE). In particular, the likelihood parameter will be set considering the outcomes of activity 1, and the impact parameter will be determined by the outcomes of activity 2. Finally, appropriate driver risk mitigation strategies (DRMSs) must be defined, which may include technical measures as well as socio-technical measures to increase people’s understanding and ultimate compliance with the technical measures, such as gamification-enhanced user experiences and specific human training activities.

This work is half-way through. The DRAM is ready, based on ISO/IEC 27005:2018 [In18], also intertwined with other approaches:

- the STRIDE approach [Mi20], to tailor the general security threats to the specific identified assets;
- the threats outlined in premise no.75 of GDPR, such as involvement of “vulnerable natural persons”, to strengthen the account for data protection threats;
- the Guidelines on Data Protection Impact Assessment (DPIA) by the European Article 29 Data Protection Working Party [Eu19], to capture threats specifically inspired to a DPIA exercise.

We have started the DRAE exercise but it is yet to be completed over the twelve car brands, so the DRMSs are yet to be devised.

## **6 Devising measures for car security and drivers’ privacy**

The fourth activity concludes the conceptual development of the COSCA framework for securing modern cars. Inspired by the mitigation strategies produced by the risk assessment exercise from activity 3, this activity covers the technical measures needed for securing in-vehicle communications and all personal data, at rest or in transit, also extending to the human-computer interface and overall user experience.

The first step to take here leads to the relevant technical measures through a systematic classification of all necessary technical elements, such as security protocols, secure cryptographic key distribution and storage, freshness and threat models, followed by the abstract design of their possible combinations. The second step produces the expected socio-technical measures by conducting a systematic classification of interface design methodologies followed by the abstract definition of an appropriate car interface that leverages hypermedia, machine readable privacy terms and GDPR compliance.

This work is still in its early phases. While there is vast literature related to the technical aspect of cyber security and privacy, the design of user-empowering human-computer interfaces appears to be generally neglected. We will tackle this task by conducting an abstract analysis of the user experience by means of tools such as Cognitive Walkthrough. This will guide the use of audiovisual cues to enable drivers to consciously express their informed consent to data processing and thus exercise their rights.

## 7 Related Work

The COSCA framework embraces the key aspects of cybersecurity and privacy in the automotive field, hence it is convenient to organise the related work along the four activities that the framework combines.

### 7.1 Crowd-sourcing drivers’ privacy concerns and trust perceptions

In 2014, Schoettle and Sivak [SS14] surveyed public opinions in Australia, the United States and the United Kingdom regarding connected vehicles. Their research noted that people (drivers as well as non-drivers) expressed a high level of concern about the safety of connected cars, which does not seem surprising on the basis of the novelty of the concept at the time. However, participants demonstrated an overall positive attitude towards connected car technology, with particular interest in device integration and in-vehicle internet connectivity.

Moreover, in 2016, Derikx et al. [De16] investigated whether drivers’ privacy concerns can be compensated by offering monetary benefits. They analysed the case of usage-based auto insurance services where the rate is tailored to driving behaviour and measured mileage and found out that drivers were willing to give up their privacy when offered a small financial compensation.

These works are only loosely related to the crowd-sourcing activity conducted within the COSCA framework because they do not significantly contribute to understanding how drivers “feel” about the security of the cars they drive as well as about how their personal data are treated onboard. It is worth remarking that these matters apply to all modern, interconnected cars. COSCA does not assess the possible inter-relation with incentives such as monetary rewards.

### 7.2 Classifying car collected data

As mentioned above, modern vehicles generate, collect and share a variety of data. Such data can be often associated with a physical person and, therefore, qualify as personal data and must be treated in full compliance with the GDPR.

We have noticed that there is scant literature focusing on protecting drivers’ data. The “CANDY” attack reconfirms how data can be stolen following security weaknesses, which can derive from optimistic network isolation assumptions made at application layer [G.18].

A few works emphasise the overarching problem of how to effectively transmit the contents of a lengthy policy to people. Those wishing to use a service routinely accept the terms of

the service provider without fully understanding them [PLM19]. However, privacy policies in this context are no exception and remain difficult to understand [Wi16].

The literature recalled above reinforces the motivation for the data classification activity conducted within the COSCA framework because no comparative analysis of car manufacturer's privacy policies is available.

### **7.3 Assessing car security and drivers' privacy risks per car brand**

The increasing complexity and connectivity of cars raise the necessity of conducting a security and privacy risk assessment exercise. It is clear that car manufacturers are best positioned to do that exercise because they are fully knowledgeable on the technologies embedded in their cars.

While best practices and recent standards mandate risk assessment processes (e.g. ISO 26262), their outcomes are not publicly available, hence the motivation to do the exercise at end-user level. This is the core of the risk assessment activity within the COSCA framework, which intends to rely solely upon information that the layman can obtain. Therefore, this COSCA activity may only rely on analysing available privacy policies and on conducting empirical tests on how cars operate.

In consequence, an account on the security risks in combination with those on the freedom of people deriving from how their personal data is treated is an original contribution of COSCA.

### **7.4 Devising measures for car security and drivers' privacy**

Recent literature comprises many examples of attacks against modern vehicles, as well as possible defences. Rather than proposing novel defensive techniques, COSCA aims at generalising the main technical countermeasures that are required to protect user's data collected, transmitted and processed by modern vehicles. We remark that this activity includes the design of user-empowering interfaces specifically tailored to the automotive domain. To the best of our knowledge, this aspect has not been analysed before.

## **8 Conclusion**

Modern cars are increasingly interconnected systems, both internally and to an external environment formed by other cars and dedicated infrastructures. Cars also interact more and more tightly with its users, mainly with drivers but sometimes also with passengers. However, users are usually given cumbersome security and privacy policies that should

explain how a car is secured and what types of data it collects about those who use it. We recognise such policies as the essential means that car manufacturers leverage to inform people. While this currently has a variety of limitations in conveying information to people, we conjecture that clarity and effectiveness of privacy policies may become a valuable asset to influence people’s choices of a particular car brand in the future.

In this paper we have presented the COSCA framework that conceptualises secure and privacy preserving cars through the execution of four main activities.

These involve studying whether drivers have privacy concerns and whether they trust the treatment of their personal data by the manufacturers of the cars they drive. Such data must be comparatively understood across a number of relevant manufacturers (ideally all manufacturers) in light of the GDPR. The activities continue with a risk assessment exercise aimed at assessing the cybersecurity of cars from a traditional IT point of view as well as the privacy of drivers from a GDPR perspective. The final activity pertains to socio-technical measures that are motivated by the risk assessment and therefore concerns the design of driver empowering interfaces.

The project is currently underway and we expect the project to contribute to improving the user perception of the drivers by making them aware of the data that is collected, of how they are protected. Furthermore, by defining the Human-Machine Interface we want to allow drivers to exercise their rights over the data processed by the car.

## Acknowledgement

This work has been supported by the COSCA research project [CO20] (NGI TRUST 2nd Open Call (ref: NGI TRUST 2019002)).

## Bibliography

- [AC20] ACKO: , Connected Cars: What is it? Features and Benefits. <https://www.acko.com/car-guide/connected-cars-features-benefits/>, 2020.
- [Be19] Bekker, Henk: , Q1/2019 Europe: Best-Selling Car Manufacturers and Brands. <https://www.best-selling-cars.com/europe/q1-2019-europe-best-selling-car-manufacturers-and-brands/>, 2019.
- [CO20] COSCA Team: , COncceptualising Secure CARs (COSCA) Website. <https://cosca-project.dmi.unict.it/>, 2020.
- [De16] Derikx, Sebastian et al.: Can privacy concerns for insurance of connected cars be compensated? *Electronic Markets*, 2016.
- [EN20] ENISA: , ENISA Good practices for IoT and Smart Infrastructures. <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool>, 2020.

- [ET20] ETSI: , European Telecommunications Standards Institute. <https://www.etsi.org/>, 2020.
- [Eu16] European Union: , General Data Protection Regulation (EU Regulation 2016/679). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>, 2016.
- [Eu19] European Union: , Guidelines on Data Protection Impact Assessment (DPIA). [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611236](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236), 2019.
- [G.18] G. Costantino et al.: CANDY: A Social Engineering Attack to Leak Information from Infotainment System. In: IEEE 87th VTC. 2018.
- [In18] International Organization for Standardization: , Information technology — Security techniques — Information security risk management. <https://www.iso.org/standard/75281.html>, 2018.
- [Mi20] Microsoft: , The STRIDE Threat Model. [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)), 2020.
- [Ne15] Neagle, Colin: , Smart refrigerator hack exposes Gmail login credentials. <https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html>, 2015.
- [PLM19] Pardo, Raúl; Le Métayer, Daniel: Analysis of Privacy Policies to Enhance Informed Consent. In: Data and Applications Security and Privacy XXXIII. Springer, 2019.
- [Pr20] Prolific: , Prolific platform. <https://www.prolific.co/>, 2020.
- [Qu20] Qualtrics: , Determining sample size: how to make sure you get the correct sample size. <https://www.qualtrics.com/experience-management/research/determine-sample-size/>, 2020.
- [SS14] Schoettle, B.; Sivak, M.: A survey of public opinion about connected vehicles in the U.S., the U.K., and Australia. In: ICCVE. 2014.
- [Un20] Union, European: , Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. [https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_202001\\_connectedvehicles.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf), 2020.
- [VM15] Valasek, Chris; Miller, Charlie: , Remote Exploitation of an Unaltered Passenger Vehicle. <http://illmatics.com/Remote%20Car%20Hacking.pdf>, 2015.
- [Wi16] Wilson, Shomir and Schaub, Florian et al.: The Creation and Analysis of a Website Privacy Policy Corpus. ACL, Berlin, Germany, 2016.
- [Wi20a] Wikipedia: , Pearson Product-Moment Correlation. [https://en.wikipedia.org/wiki/Pearson\\_correlation\\_coefficient](https://en.wikipedia.org/wiki/Pearson_correlation_coefficient), 2020.
- [Wi20b] Wikipedia: , Spearman's rank correlation coefficient. [https://en.wikipedia.org/wiki/Spearman%27s\\_rank\\_correlation\\_coefficient](https://en.wikipedia.org/wiki/Spearman%27s_rank_correlation_coefficient), 2020.

# Decentralized Identities for Self-sovereign End-users (DISSENS)

Martin Schanzenbach,<sup>1</sup> Christian Grothoff,<sup>2</sup> Hansjürg Wenger,<sup>2</sup> Maximilian Kaul<sup>1</sup>

**Abstract:** This paper describes a comprehensive architecture and reference implementation for privacy-preserving identity management that bucks the trend towards centralization present in contemporary proposals. DISSENS integrates a technology stack which combines privacy-friendly online payments with self-sovereign personal data management using a decentralized directory service. This enables users to be in complete control of their digital identity and personal information while at the same time being able to selectively share information necessary to easily use commercial services. Our pilot demonstrates the viability of a sustainable, user-centric, standards-compliant and accessible use case for public service employees and students in the domain of retail e-commerce.

We leverage innovative technologies including self-sovereign identity, privacy credentials, and privacy-friendly digital payments in combination with established standards to provide easy-to-adapt templates for the integration of various scenarios and use cases.

**Keywords:** privacy; decentralization; digital sovereignty

## 1 Introduction

The cryptography for secure, privacy-preserving online payments has been known since Chaum's ground-breaking work [CFN90] around 1990. While such digital payments can in theory enable anonymous one-click purchases, in practice online services sometimes require contextual personal information from their customers, the most basic example being a shipping address for delivery.

Furthermore, some of the contextual information may require verification. Today, online services commonly validate contact information like phone numbers or e-mails by sending test messages, burdening users with an extra processing step. Verification becomes even more complex if shops need to satisfy regulatory requirements involving age verification. But not only minors might be interested in supplying false credentials, as governments and other institutions sometimes subsidize eligible citizens such as students, pensioners and the disabled.

While we accept that online services may to some degree have a legitimate need for their users' personal information, we content that the contemporary practice of registering user

---

<sup>1</sup> Fraunhofer AISEC, München, Germany, [firstname.lastname@aisec.fraunhofer.de](mailto:firstname.lastname@aisec.fraunhofer.de)

<sup>2</sup> Bern University of Applied Sciences, Biel/Bienne, Switzerland, [firstname.lastname@bfh.ch](mailto:firstname.lastname@bfh.ch)



accounts prior to receiving online services is an unnecessary and obsolete burden on users. Additionally, with legislation such as the General Data Protection Regulation (GDPR) user information and accounts pose a significant liability for service providers, and setting up and maintaining accounts and associated credentials with the multitude of service providers in existence today is a usability nightmare.

The latter is partially addressed through the use of third-party identity provider services (IdPs). Using an IdP is practical for online services as it delegates the task of verifying and storing personal information while reducing the number of accounts users have to manage. However, the resulting centralization further harms the users' ability to control their data as it becomes easily linkable by the IdP across various life domains. Collecting user data that tracks users' movements across services is a business model that strikes at the core of the right to informational self-determination.

## **1.1 Transforming the role of the IdP**

What is actually needed is a technology stack which gives users a maximum amount of personal control over their digital identities and at the same time relieves service providers from the liability of user data, including payment information. Self-sovereign identity (SSI) management is a way to replace IdPs with a user-centric, decentralized mechanism where data- and access-control are fully under the control of the data subject. In SSI, users are free to create many a priori unlinkable pseudonyms, and ideally they decide which of their attributes they share with which service providers. SSI thus enables users to exercise the right to be forgotten by deleting pseudonyms, which is only meaningful in systems where users can have multiple concurrently useful identities. Attributes can generally be set freely for the various pseudonyms by each user.

As a result, the role of IdPs is transformed: instead of controlling the subject's data, IdPs in SSI are certification bodies that provide attestations for the authenticity of certain attributes. Here, information disclosure can be further minimized using privacy-friendly credentials [CDL16]. Given the possibility of IdPs offering competing certification services, users can pick and choose sets of attested attributes from any number of IdPs. This concept is natural, as the authority over a user's email address is likely different from the authority over the user's employment status, for example.

## **1.2 Objectives**

Our objective is to enable seamless use of online services where users generally do not need any accounts, while improving on the best-case user experience that platforms with accounts can provide. Instead of remembering login information with usernames and passwords, multi-factor authentication, and disclosure of personal information when yet another service

provider’s database is leaked online, users should only authorize to share relevant personal details *while* necessary. GDPR-compliant services would then resolve those personal details only at the time of need without ever storing them, thereby minimizing the chance of inadvertently compromising private information of their users.

Eliminating the online service provider’s data liability should include eliminating the need to store sensitive payment data. Instead of having to outsource payments or to satisfy the non-trivial requirements of the Payment Card Industry Data Security Standard, payments should be processed without revealing any personally identifiable information about the consumer to anyone. As a result, the need for users to enter personal information, credit card data or to pass authorization procedures is completely eliminated — except for logging into their own computer.

We also want to satisfy the practical requirement that back-office business processes related to fulfillment might be executed when the user is not directly interacting with the service. Thus, even though the service is not itself storing a user’s personal data, authorized services must be able to access it even if the user is offline. Finally, we want to maximize compatibility to existing standards where possible, to minimize the migration cost.

### 1.3 Technical contribution

We integrated the self-sovereign identity management system re:claimID [SBS18; Sc20] with the privacy-preserving GNU Taler payment system in a pilot application based on WooCommerce, a widely used online shop based on WordPress. Our Free Software pilot demonstrates how contemporary cumbersome and privacy-unfriendly online shopping processes can be eliminated, improving the user experience, privacy and security of all parties involved. Our reference scenario includes credentials issued by the partners Fraunhofer AISEC and BFH for employees and students, respectively. The Web shop can thus distinguish between “trusted” attributes that are certified by these two IdPs and “untrusted” attributes that are freely chosen by the users.

Our system demonstrates how businesses, users and credential authorities can easily integrate using standard protocols such as OpenID Connect (OIDC), without requiring any a priori registration at Big Tech gatekeepers such as Apple, Google, Facebook or Amazon. The existing OIDC standard already accommodates identity aggregation features necessary in SSI use cases. The resulting architecture enables citizens and businesses to avoid vendor lock-in to those major platform providers without sacrificing usability or privacy. In our system users remain in direct control of their personal data. This is an alternative to the contemporary privacy-unfriendly approaches which either call for governments or Big Tech to “safeguard” personal information storage or access control.

Incidentally, we show that SSI systems can be built without distributed ledger technology (DLT), challenging the common wisdom that DLTs are crucial in this domain.

## 1.4 Unique benefits

This approach offers significant benefits over existing solutions built using other SSI systems such as Sovrin <sup>3</sup> or serto (formerly uPort) <sup>4</sup>.

**No gatekeepers; No vendor lock-in:** Our approach is completely open to issuers and does not impose any registration restrictions (such as registration fees) in order to define domain specific credentials. Further, our system does not impose a consortium-based governance model — which tend to eventually be driven by commercial interests and not consumer interests. Our design enables all participants in the ecosystem to participate without prior onboarding while at the same time being offered full transparency and control regarding their personal data and processes involved. Finally, we try to integrate our technology stacks as much as possible with existing standards in order to facilitate transitioning.

**Support for non-interactive business processes:** At the same time, unlike the SSI systems cited above, our technology offers a way to access user information without online interaction with the user. Offline access of shared identity data is a crucial requirement in almost any business process as such processes often occur after direct interaction with the user. For example, customer information such as billing addresses are required in — possibly recurring — back office billing processes which occur well after interaction with a customer.

**Scalability and sustainability:** Finally, both re:claimID as the SSI system as well as Taler do not suffer from the usual predicament Blockchain-based systems find themselves in: Both systems do not require a decentralized, public ledger. This eliminates the need for consensus mechanisms, which do not scale and are ecologically unsustainable. In fact, we employ decentralization only where it provides the most value and use more efficient technology stacks where needed: re:claimID builds on top of the GNS, which makes use of a DHT, an efficient ( $O(\log n)$ ) peer-to-peer data structure. For payments, GNU Taler uses centralized infrastructure operated by audited and regulated exchange providers and facilitates account-less end-to-end interactions between customers and services where all parties have  $O(1)$  transaction costs.

For a comprehensive discussion and comparison of re:claimID and other SSI systems we refer to [Sc20].

## 2 Background

Our architecture builds on three core technologies, which are introduced in this section.

---

<sup>3</sup> <https://www.sovrin.org>, accessed 2021/02/12

<sup>4</sup> <https://www.serto.id>, accessed 2021/01/12

## 2.1 Classical identity providers

Identities are usually managed through the use of so-called directory services. Traditionally, directory services based on the X.500 protocol family or derivatives such as LDAP are used for identity and organizational information management. While it may not be intuitive at first what name systems such as DNS have to do with identities, efforts such as NameID show how name systems can be used by users to manage pseudonyms and personal information in a decentralized directory.

In most cases, access to identity information through an identity provider is realized using an authorization and authentication service such as SAML or OIDC. Behind every identity provider, there is either a directory service which is used to supply identity information or another identity provider as part of a federation.

In our use case, we presume the existence of identity provider services which follow the traditional approach outlined above. We will show how these services can be used to provision certified attributes in a user-centric SSI architecture.

## 2.2 re:claimID and the GNU Name System

re:claimID [Sc20] is a self-sovereign identity management system developed by Fraunhofer AISEC which uses the GNU Name System (GNS) [SGF20] as a directory service to store credentials and provide authorized parties with access to identity data even when the respective user is temporarily offline.

GNS is an alternative name system developed in the context of the GNUUnet project. It offers secure and decentralized directory storage for identity and personal data. Encrypted name data in GNS is stored in a distributed hash table (DHT). To decrypt the information, one must know a *label* and a *public key*. It should be noted that *these* public keys can be shared secrets and are not exposed by the GNS protocol. GNS enables privacy-preserving name resolution because the peers serving answers do not inherently learn anything about the information they are helping process. GNS is fully decentralized: each user is free to define their own root zone which serves as their trust anchor.

In re:claimID, users manage their identities without the need for a single IdP while at the same time retaining the ability to securely and selectively disclose identity information with other services. Complete transparency, decentralization and elimination of intermediaries are the core value offerings of re:claimID. re:claimID also offers an OIDC compatibility layer which facilitates integration with existing standards-compliant client software.

## 2.3 GNU Taler

GNU Taler is a privacy-preserving payment system using blind signatures to protect the identity of payers. Using blindly signed digital coins to create digital cash was first proposed by Chaum [CFN90]. Taler extends Chaum's work by providing an efficient mechanism to obtain unlinkable change while preserving the income transparency properties of Chaum's original design [Do19]. The resulting payment system is expected to be generally compatible with financial regulation and neutral with respect to central bank's ability to implement monetary policies [CGM].

Taler allows consumers to authorize payments using a single click in their Taler wallet. Two-factor authentication is implicit from the consumer having physical control over the wallet's computing device and the ability to unlock it. Before DISSENS, this account-less single-click shopping experience did not work for physical goods where the shop needs a delivery address, or even for digital goods if they require age verification.

## 3 Architecture

To create a broadly applicable one-click online shopping experience without the need to create and maintain accounts where personal information is persisted with the shop outside of the control of the user, we combine the decentralized, SSI and personal data management system re:claimID with the privacy-preserving GNU Taler payment system as illustrated in Figure 1. Identity providers (such as sovereign states and academic institutions) issue credentials to users. Users manage identities with associated third-party attested credentials and self-attested attributes in a self-sovereign fashion. Users publish their encrypted identity data to the GNS, which serves as a decentralized directory. They can then selectively disclose sets of attributes to relying parties.

### 3.1 Third party identity providers

The design of re:claimID does not require the existence of third party identity providers. Users may self-attest and self-sign attributes. In fact, this can be considered the default and is probably sufficient for many use cases. However, as elaborated in Section 1, there are use cases where a relying party may require an assertion from a trusted third party. We assume that such trusted third parties operate OpenID Provider (OP) services. OPs are assumed to have issued unique user identifiers in the form of email addresses to facilitate the discovery of the OP service through the use of OIDC Discovery [Op21]. This requirement could in theory be relaxed, but OP discovery through this method is the simplest form of discovery within the standard. The OPs are connected to the respective institution's directory, either directly (e.g. LDAP) or through federation (e.g. another upstream OP). The backend architecture of the IdP is irrelevant as long as it exposes OIDC endpoints.

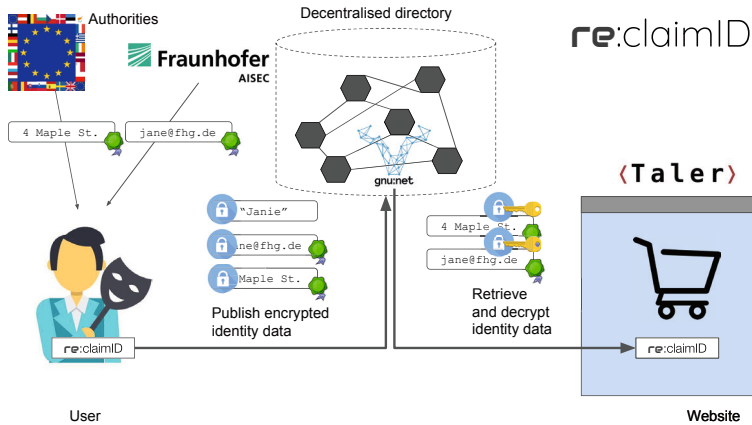


Fig. 1: The DISSENS architecture.

An important caveat for the OP setup is that it must allow re:claimID to request authorization to access user information. For this, the OPs must either have pre-configured a client for re:claimID, or allow for dynamic client registration for the re:claimID redirect URI as a public client. The re:claimID redirect URI is not a central server, but points the browser to the re:claimID web extension which forwards any authorization request to the re:claimID service running on the local device.

In our design, we optionally allow IdPs to provide credentials in a non standards-compliant fashion to re:claimID: Our new API exposed at the IdP allows re:claimID to retrieve a credential which allows the user to selectively disclose *subsets* of the attributes attested in the credential.

### 3.2 User identity management

In our architecture, users can manage any number of pseudonyms with attributes containing their personal information on their own devices. Through re:claimID, attributes basically become records in a zone of GNS. The encrypted attribute data is published in a DHT. When a user interacts with an online service, they can provide the online service a re:claimID “ticket” [Sc20] which grants the service access to subsets of the attributes of a user’s pseudonym. The ticket can be piggybacked within the authorization code of an OIDC authorization flow. It contains the necessary information to find the attributes in GNS. With it, the service can access the data when it is needed, even if the user is offline at the time. It also allows the service to retrieve updates in case the user changes their information. The user can choose to revoke the grant at any time, henceforth preventing the store from resolving attribute data.

From the user’s perspective, interacting with re:claimID is equivalent to interacting with other OPs, with the addition that each user is able to manage multiple pseudonyms. Users can freely add or remove attribute data associated with any of their pseudonyms. They are expected to interact with re:claimID through a browser extension which communicates with a locally running client.

Users can import certified attributes by authenticating with identity providers and extracting certified attributes using the OIDC protocol [Op21]. To do so, users first add an attribute with an email address registered with the third party OP to one of their pseudonyms. The OIDC Discovery protocol [Op21] allows re:claimID to discover the relevant OIDC endpoints. If necessary, re:claimID will attempt to dynamically register an OIDC client at the OP. The user can then initiate an OIDC authorization code to allow re:claimID to retrieve an ID token asserting information about the user.

The user may then add new attributes to their pseudonym and select attribute values from the contents of the ID token. When the user shares attributes which are backed by an ID token, re:claimID will provide the token to the RP as part of the OIDC protocol: As an OIDC OP, it will issue an ID token and provide access to a userinfo endpoint. The payloads will include references to ID tokens issued by third parties as defined in the OIDC specification [Op21] as “Aggregated Claims”. The standard defines how JWTs such as ID tokens can be used within an aggregated claim.

One problem with the concept of aggregated claims in combination with JWTs is excessive disclosure of information. While anonymous credentials such as Camenisch-Lysyanskaya [CDL16] using blind signature schemes such as BBS+ [ASM06] can be used to enable selective disclosure of attributes, such signature schemes are not explicitly defined for the OIDC Aggregated Claims standard. For DISSENS, we have implemented<sup>5</sup> our own C library that supports non-interactive zero knowledge proofs for this use case using pairings on a BLS12-381 curve [Bo17]. With this extension, users can selectively disclose attributes from the credential without invalidating the issuer’s signature. Consequently, the system can selectively disclose only the required information to parties that support this extension.

### 3.3 Service providers

We expect that service providers offer their services through an HTTPS presence on the Internet and utilize an e-commerce platform which supports the use of OIDC identities. This implies that the service is set up with an OIDC relying party (RP) configuration. In particular, the OIDC RP component exposes an OIDC “redirect URI” which is used within a standard authorization code flow. In order to initiate such a flow, the service provider must first register its OIDC RP as a client at the OP service.

---

<sup>5</sup> <https://github.com/Fraunhofer-AISEC/libpabc>

In `re:claimID`, an OIDC RP client is registered by creating a public-private key pair, which establishes a GNS identity that is henceforth identified by its public key. This public key also serves as the OIDC client ID. In order to register the HTTPS redirect URI(s) of its client, the service provider publishes this information in the client's GNS zone. This requires the private key of the identity. The resulting GNS records cryptographically bind the client ID to the client's redirect URI in a way that it is verifiable by the users' `re:claimID` instances.

From the perspective of the service, interacting with `re:claimID` is equivalent to interacting with any other OP with the exception that the OIDC endpoints are split between user and service: The client initiates an OIDC authorization request to the user with an authorization redirect to the user's local OIDC Authorization Endpoint. The user's `re:claimID` instance ensures that the provided redirect URI matches any of the URIs registered in GNS for the respective client ID. Upon authorization, the service receives user information by exchanging the user-provided authorization code at its local OIDC Token Endpoint. This exchange yields an ID Token as well as an access token for use at the local Userinfo Endpoint. The latter allows the service to retrieve fresh and up-to-date information directly from the GNS directory as the code contains the `re:claimID` "ticket" necessary for such a query [Sc20].

Services that require certified attributes need to be configured with the public keys of certification bodies for the respective types of attributes. The establishment of trust in the third party IdP is out of scope of the OIDC standard. We assume that the relying party is configured a priori with a list of trusted institutions. This configuration would typically be a list of domains corresponding to the respective institution's IdPs. This allows the relying party to verify any ID tokens provided by the user through `re:claimID` as part of an Aggregated Claim, typically through the use of a JSON-Web-Key-Set (JWKS) provided by the OP. Alternatively, the relying party could be pre-configured with a key that can be used to verify the signatures of trusted OPs. Note that the method by which the relying party retrieves the key material is independent of the issue of trust: The key material is a means to verify the authenticity of the attestation. Trust establishment into the key material must be done out of band as part of a conscious selection process by the relying party. In order to facilitate trust establishment into a number of entities within a certain consortium or group, trust anchors provided through an X.509 PKI in combination with JWKS are viable.

## 4 Usability survey

We conducted a small usability survey on a pilot setup of DISSENS with seven participants to obtain insights into the usability of the system and derive directions for future improvement. The participants were between 18 and 54 years old and ranged from undergrad and grad students to professionals.



## 4.1 The pilot setup

We setup an OP service connected to the LDAP of the Bern University of Applied Sciences. This enables us to certify attributes based on real-world data about students and employees. The OP was configured with a client for the re:claimID web extension as elaborated in Section 3.1. Users were asked to authenticate using their existing credentials. The OP attested the information found within the directory. The resulting aggregated claims are then stored in the user's GNS zone from where they can be shared via re:claimID with Web sites.

We also created a pilot web shop based on the popular WooCommerce platform <sup>6</sup>. As the platform is based on WordPress, we enabled a third party OIDC plugin and configured a re:claimID OIDC client as outlined in Section 3.3. The plugin initially did not support the aggregated claims feature of the OIDC standard, which is why we implemented this functionality ourselves for the use case and offered our patches upstream <sup>7</sup>. We also implemented a WooCommerce payment extension that added the option to pay with the GNU Taler payment system.

As this survey was conducted during a COVID-19 lockdown, we deviated from our original plan to provide pre-configured workstations and instead opted for the distribution of a virtual machine with a minimal Debian buster image as a base. This image runs on GNU/Linux host systems using QEMUvirtualization. In this image, the required GNUet peer-to-peer software is installed and automatically started. The GNUet REST service gives the host access to the GNUet REST API, allowing the re:claimID extension running in the browser to access the GNUet DHT. We also pre-installed the required plugins ("GNU Taler Wallet" and "re:claimID") in the browser of the virtual machine.

The advantage of this approach is a small and quickly downloadable VM image without a full desktop installation. The disadvantage is that testers needed a working GNU/Linux desktop system to run the setup, which substantially reduced the number of participants we could recruit.

The instructions given to the survey participants are reproduced in the appendix of the extended version of this paper available from the authors.

## 4.2 Results

The results of our SUS questionnaire are promising. From the responses we calculated the following SUS scores, in ascending order: 62,5 (x2), 70 (x1), 77,5 (x2), 80 (x1) and 87,5 (x1). This results in a median score of 77,5 and an average of 73,9. SUS scores above 68 are considered above average <sup>8</sup>.

---

<sup>6</sup> <https://woocommerce.com>, accessed 2021/01/02.

<sup>7</sup> <https://github.com/oidc-wp/openid-connect-generic/pull/255>, accessed 2021/2/12

<sup>8</sup> <https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html>, 2021/02/12

Four participants gave qualitative feedback in the form of free text remarks. One noted that the interfaces were a bit “old fashioned”. Another remark noted that it was necessary to enter credentials on a domain foreign to the institution. This was due to our setup being deployed on an unrelated test domain and would likely not happen in a real world deployment. It shows the importance of domain name familiarity when deploying authentication services.

Another participant noted that it was not clear to them which attributes were required to be attested from the third party and which attributes were acceptable to provide “self-attested” along with the pseudonym. This is actually a shortcoming of the OIDC standard, as it does not offer a way for the relying party to convey this information in a claims request. A related issue was that it was unclear of the relying party would accept attributes issued by other IdPs than the one which was supposed to be used. Both issues could be resolved by having the relying party provide additional metadata along with the claims request. Hence, this may be an area for improvement of the standard.

## 5 Future work and conclusion

While the GNU Name System, re:claimID and GNU Taler have been subjected to extensive standardization work, the same cannot be said for the DHT. Existing RFCs on DHTs do not cover necessary features for GNS, such as in-network block validation and revocation flooding. Thus, additional standardization work is called for to avoid referring the GNUet source code serving as an inadequate substitute for protocol documentation.

Our usability survey provided test subjects with a pre-configured virtual machine image that included some heavy-handed workarounds for problems at the network layer. Today, most computers access the Internet from behind one or more layers of network address translation, possibly further restricted by firewalls and other obstacles. This limits the usable deployment of applications requiring end-to-end connectivity. Modern protocols like WebRTC/ICEwork around these issues using centralized infrastructure providing STUN and TURN services to help consumers that experience connectivity problems. For properly decentralized networking, this centralized infrastructure should be replaced by peers that have found ways to traverse their NAT restrictions helping other peers do the same. This requires integrating STUN/TURN signaling into the peer-to-peer network layer.

Further interface improvement will have to be combined with work on the OIDC standard, as the idea of SSIs in combination with trusted attribute issuers are still in its infancy in that regard. While we did consider the use of the recent W3c DID standard [Re18] together with OIDC, its features do not directly address the shortcomings identified in the OIDC protocol.

We also note that this work proposes to use certification to realize features like age-restricted payments, but such certifications can be socially problematic as they could give too much power to certification authorities that might be better vested with legal guardians. It is conceivable to integrate age-restrictions into Taler by tagging coins with age restrictions

upon withdrawal, effectively providing the power to impose such restrictions to the guardian of the bank account. An open challenge in this context is preserving such age restrictions when Taler renders unlinkable change.

## Acknowledgments

The DISSENS project is funded by the NGI\_Trust program as project number 2.11.

## References

- [ASM06] Au, M. H.; Susilo, W.; Mu, Y.: Constant-Size Dynamic k-TAA. In (De Prisco, R.; Yung, M., eds.): Security and Cryptography for Networks. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 111–125, 2006, ISBN: 978-3-540-38081-8.
- [Bo17] Bowe, S.: BLS12-381: New zk-SNARK Elliptic Curve Construction, Mar. 2017, URL: <https://electriccoin.co/blog/new-snark-curve/>.
- [CDL16] Camenisch, J.; Drijvers, M.; Lehmann, A.: Anonymous attestation using the strong diffie hellman assumption revisited. In: International Conference on Trust and Trustworthy Computing. Springer, pp. 1–20, 2016.
- [CFN90] Chaum, D.; Fiat, A.; Naor, M.: Untraceable Electronic Cash. In (Goldwasser, S., ed.): Advances in Cryptology — CRYPTO’ 88: Proceedings. Springer New York, New York, NY, pp. 319–327, 1990.
- [CGM] Chaum, D.; Grothoff, C.; Moser, T.: How to Issue a Central Bank Digital Currency, Accepted, under pre-publication political review by Swiss National Bank directorate.
- [Do19] Dold, F.: The GNU Taler System: Practical and Provably Secure Electronic Payments, PhD thesis, University of Rennes 1, 2019.
- [Op21] OpenID Foundation: OpenID Specifications, 2021, URL: <http://openid.net/specs/>.
- [Re18] Reed, D.; Sporny, M.; Longley, D.; Allen, C.; Grant, R.; Sabadello, M.: Decentralized Identifiers (DIDs) v0.11, 2018, URL: <https://w3c-ccg.github.io/did-spec>.
- [SBS18] Schanzenbach, M.; Bramm, G.; Schütte, J.: reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption. In: 17th IEEE TrustCom. Pp. 946–957, Aug. 2018.
- [Sc20] Schanzenbach, M.: Towards Self-sovereign, Decentralized Personal Data Sharing and Identity Management, Dissertation, München: Technische Universität München, Dec. 2020.
- [SGF20] Schanzenbach, M.; Grothoff, C.; Fix, B.: The GNU Name System, Oct. 2020, URL: <https://www.ietf.org/archive/id/draft-schanzen-gns-02.html>.

# Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication

Johannes Kunke<sup>1</sup>, Stephan Wiefling<sup>1,2</sup>, Markus Ullmann<sup>1,3</sup>, Luigi Lo Iacono<sup>1</sup>

**Abstract:** Threats to passwords are still very relevant due to attacks like phishing or credential stuffing. One way to solve this problem is to remove passwords completely. User studies on passwordless FIDO2 authentication using security tokens demonstrated the potential to replace passwords. However, widespread acceptance of FIDO2 depends, among other things, on how user accounts can be recovered when the security token becomes permanently unavailable. For this reason, we provide a heuristic evaluation of 12 account recovery mechanisms regarding their properties for FIDO2 passwordless authentication. Our results show that the currently used methods have many drawbacks. Some even rely on passwords, taking passwordless authentication ad absurdum. Still, our evaluation identifies promising account recovery solutions and provides recommendations for further studies.

**Keywords:** FIDO2; Passwordless Authentication; Account Recovery; Fallback Authentication

## 1 Introduction

At least since the COVID-19 pandemic and the inevitable need for work from home solutions for employees [if20, De20], online services and the associated authentication processes have become indispensable. However, this shift in online use also increased attacks on password-based authentication. Credential stuffing, a very successful and scalable attack, where attackers automatically enter leaked login credentials (username and password) on an online service, increased in March 2020 [Ak20]. Similarly, the amount of phishing attacks increased since March 2020 [An20]. To protect against these type of attacks, multiple measures are possible. For online services with a certain amount of sensitive data, risk-based measures to strengthen password-based authentication showed to provide high security with good usability [WDLI20, WDLI21]. Another and even better approach to eliminate attacks on password-based authentication would be to replace passwords with a secure alternative. The FIDO2 Universal Authentication Framework (UAF) standard is a promising solution to implement passwordless authentication. This standard allows strong cryptographic single factor authentication and uses a different asymmetric cryptographical key for each online service [FI17]. Users can provide these keys, e.g., via a security token (also known as the authenticator). The clear advantage of FIDO2 UAF is that users do not have to

---

<sup>1</sup> H-BRS University of Applied Sciences, FB Informatik, Grantham-Allee 20, 53757 Sankt Augustin, Germany  
johannes.kunke@smail.inf.h-brs.de, {stephan.wiefling, markus.ullmann, luigi.lo\_iacono}@h-brs.de

<sup>2</sup> Ruhr University Bochum, Horst Görtz Institute for IT-Security, Universitätsstrasse 150, 44780 Bochum, Germany

<sup>3</sup> Bundesamt für Sicherheit in der Informationstechnik, Heinemannstraße 11, 53133 Bonn, Germany

construct or remember secrets. This is one of the reasons why it is considered to be more usable than classical password-based authentication in some cases [Ly20]. However, users expressed concern about losing service access if the security token becomes permanently unavailable [Ly20, Fa20]. When the token gets unavailable, access to the online services managed with it is no longer possible, since the generated secret keys never left it and thus are only available there. Complicating matters further, the security token stores different secrets for different online services. For this reason, widespread adoption of FIDO2-based passwordless authentication relies on adequate recovery mechanisms.

**Contributions.** We examine 12 account recovery mechanisms in passwordless FIDO2 environments using security and usability metrics evaluated in the literature. Our results suggest that widely deployed account recovery mechanisms need to be replaced with more secure alternatives. We give recommendations on promising account recovery mechanisms. Our work supports service owners and developers on which account recovery mechanism to choose for their FIDO2 implementation. It also supports researchers to select promising account recovery mechanisms for future studies. Overall, we are contributing to the shift from password-based authentication to passwordless FIDO2 authentication on the Internet.

## 2 Evaluation Criteria

To evaluate the various account recovery mechanisms, we introduce a set of criteria established in literature. These criteria are based on those developed by Bonneau et al. [Bo12], Nielsen [Ni94], Saltzer and Schröder [SS75], and Stajano [St11]. We selected the criteria based on their reliability to account recovery mechanisms and frequent citation. Some of these criteria were initially developed for user authentication purposes. However, as account recovery is also a form of authenticating users, it is comparable to classical user authentication schemes [WI20a]. This is further underlined by the fact that the process involved in account recovery mechanisms is also called *Fallback Authentication* [Ja14]. Similar to Bonneau et al. [Bo12], we divided the criteria into three categories *usability benefits*, *deployability benefits*, and *security benefits*.

### 2.1 Usability-Benefits

**(U1) Memorywise-Effortless** [Bo12]: The user does not have to remember an authentication secret. **(U2) Scalable-for-User** [Bo12]: No additional burden is introduced when using the mechanism with hundreds of services. **(U3) Nothing-to-Carry** [Bo12]: The user does not need to carry any additional physical item to use the recovery mechanism at any time. **(U4) Physically-Effortless** [Bo12]: Users do not need to perform any physical activities during the process beyond pressing a button. **(U5) Easy-to-Learn** [Bo12, SS75, Ni94]: The mechanism is intuitively designed and thus easy to learn. **(U6) Match between system and the real world** [Ni94]: The access recovery mechanism is based on real world concepts. The user can operate it intuitively because it is based on real world operations.

## 2.2 Deployability benefits

**(D1) Accessible** [Bo12]: Users must be able to use this mechanism, even with physical limitations. **(D2) Negligible-Cost-per-User** [Bo12]: The financial cost per user must be very low. **(D3) Browser-Compatible** [Bo12]: Mechanism can be used with any standard web browser without installing additional plugins or other software. **(D4) Non-Proprietary** [Bo12]: The mechanism can be used at no additional cost for royalties and are not protected by patents or other trade secrets. **(D5) Implemented** [St11]: The mechanism must be implemented as a practical application. It must not exist only as a theoretical concept.

## 2.3 Security Benefits

**(S1) Resilient-to-Physical-Observation** [Bo12]: Despite observing the user while using the mechanism, attackers fail to successfully legitimize themselves as the user. **(S2) Resilient-to-Targeted-Impersonation** [Bo12]: The attacker can not impersonate the user to the mechanism with background knowledge, which he may be able to obtain, e.g., via social networks. **(S3) Resilient-to-Internal-Observation** [Bo12]: Despite intercepting user input at participating devices, e.g., smartphone or desktop PC, it is impossible for an attacker to imitate the user. **(S4) Resilient-to-Leaks-from-Other-Verifiers** [Bo12]: A user uses other services that use the same or similar mechanism but whose data is made public. The attacker cannot impersonate the user with the obtained data at that service. **(S5) Resilient-to-Phishing** [Bo12]: Attacker is able to fake a legitimate mechanism and convince the user to use the faked version, but cannot successfully impersonate the user to the service with the resulting data. **(S6) Resilient-to-Theft** [Bo12]: Refers to mechanisms that require the factor possession in the form of an object as proof of legitimacy. If attackers gain possession of a user's object, they must not succeed in legitimizing themselves as the user to the mechanism. **(S7) No-Trusted-Third-Party** [Bo12]: The mechanism for checking the authorization of the access recovery process is not based on a third trusted party, which could have been taken over or manipulated by an attacker to become an untrusted party. **(S8) Requiring-Explicit-Consent** [Bo12]: The access recovery mechanism must only be performed with the user's conscious consent. It must never be started accidentally or automatically. **(S9) Unlinkable** [Bo12]: The information processed by this mechanism cannot be used to draw conclusions about what other services a user is using. **(S10) Open** [St11, SS75]: The code or at least the functionality of the mechanism must be openly accessible to everyone. **(S11) Work-Factor** [SS75]: The mechanism should be designed in such a way that an attacker has to invest many resources to falsely successfully legitimize against the mechanism. **(S12) Complete-Mediation** [SS75]: The authorization to use the mechanism must be verified every time. It is not enough to assume that the person that operates the mechanism during an open session is the legitimate user.

### 3 System Evaluation

Based on the criteria, we evaluated 12 account recovery mechanisms described in literature and partly deployed in practice (see Table 1). The mechanisms were selected based on literature research and observed mechanisms on popular online services. To cover all literature as completely as possible, we did forward snowballing based on Lyastani et al. [Ly20], and queried ACM, Springer, and IEEE publication search engines with the keywords FIDO2, account recovery, token loss, authentication, passwordless single factor, and WebAuthn. We further queried the Google search engine with the keywords FIDO2, account recovery, and device loss, to include unpublished mechanisms as well. We discuss a subset of important criteria—due to limited space—for each recovery mechanism below.

		Security Questions	Password	OTP	Pico	Delegated Account Recovery	FIDO2 Backup Token	Identity Card	Advanced Protection Program	Let's Authenticate	Key Copy	Online Recovery Storage	Pre-emptive Syncing
Usability	Memorywise-Effortless	○	○	●	●	○	●	●	●	○	●	●	●
	Scalable-for-User	○	○	●	●	○	○	○	○	●	○	○	●
	Nothing-to-Carry	○	○	○	○	○	○	○	○	○	○	○	○
	Physically-Effortless	○	○	○	○	○	○	○	○	○	○	○	○
	Easy-to-Learn	●	●	○	○	○	○	○	○	○	○	○	○
Deployability	Match System-Real World	●	●	○	○	●	●	●	○	●	●	○	○
	Accessible	●	●	○	○	○	○	○	○	○	○	○	○
	Negligible-Cost-per-User	○	○	○	○	○	○	○	○	○	○	○	○
	Browser-Compatible	●	●	●	○	○	○	○	○	○	○	○	○
	Non-Proprietary Implemented	●	●	●	○	●	●	○	○	○	○	○	○
Security	Resilient-Physical-Observation	○	○	●	●	○	●	●	●	○	●	●	●
	Resilient-Targeted-Impersonation	○	○	○	●	○	●	●	○	○	●	●	●
	Resilient-Internal-Observation	○	○	○	○	○	○	○	○	○	○	○	○
	Resilient-Leaks-from-Other-Verifiers	○	○	○	○	○	○	○	○	○	○	○	○
	Resilient-Phishing	○	○	○	○	○	○	○	○	○	○	○	○
	Resilient-Theft	○	○	○	○	○	○	○	○	○	○	○	○
	No-Trusted-Third-Party	○	○	○	○	○	○	○	○	○	○	○	○
	Requiring-Explicit-Consent	○	○	○	○	○	○	○	○	○	○	○	○
	Unlinkable	○	○	○	○	○	○	○	○	○	○	○	○
	Open	○	○	○	○	○	○	○	○	○	○	○	○
	Work-Factor	○	○	○	○	○	○	○	○	○	○	○	○
Complete-Mediation	○	○	○	○	○	○	○	○	○	○	○	○	

● Criteria fulfilled ○ Criteria not fulfilled **Bold:** Deployed in account recovery practice

Tab. 1: Comparison of account recovery strategies with FIDO2-based passwordless authentication

**Security Questions.** Security questions can be considered as a classical recovery mechanism on online services. They are entered during account registration by the user. If users lose access to their account, they can authenticate themselves to the system by answering the security questions. Typical questions are “*Mother’s maiden name*”, “*Favorite sports team*”, or “*Name of first pet*”. [AJ09][Ra08]. Such security questions proved to be a weak authentication mechanism. Rabkin [Ra08] found that 12% of their studied security questions were solvable on the first attempt using social networks. However, this recovery process is

*Physically-Effortless*. The user does not need to carry any physical object. There is also no additional cost for users to use this mechanism, so *Neglibile-Cost-per-User* is fulfilled. Furthermore, security questions are not resistant to *Resilient-to-Leaks-from-Other-Verifiers*. If the user entered the same question answers on another online service, that service could be compromised. With the information gained from these data breaches, the attacker can impersonate the user on the actual online service.

**Backup Password.** A backup password is stored during registration. If users lose access to their account, they can use this password to regain access. Users must actively enter the password, so it fulfills *Requiring-Explicit-Consent*. However, backup passwords are not *Scalable-for-User*, as users have to remember new passwords for each access recovery mechanism that is based on passwords. It also does not fulfill *Work-Factor*, since attackers can guess simple passwords in a short time [Pa19].

**One-Time Password (OTP).** By proving possession of the OTP, users can authenticate themselves to the system. OTPs can be generated in many ways, e.g., during registration as a list of OTPs, or time-dependent during the recovery process (time-based OTP) [Re19]. The OTP is generated when users start the mechanism, and is communicated to them via another channel. OTPs are *Memorywise-Effortless*, as users do not have to remember a secret. It is also *Browser-Compatible*, since browsers only need to provide a text field, where users enter their OTP. However, it not *Resilient-to-Phishing*, as attackers can trick users into revealing their OTP on a phishing website and replay it on the target website [Gr18, Wi20b].

**Pico.** The Pico ecosystem [St11] consists of a so-called Pico and a Pico sibling. The Pico is an authenticator device, which comes with a docking station. The docking station charges and backs up the Pico. If users lost their Pico, they can connect a new Pico to the docking station and use the Pico sibling of the lost Pico to unlock the backup and transfer the key material of that Pico to the new Pico. Since the access recovery mechanism does not depend on a trusted third party, it satisfies *No-Trusted-Third-Party*. However, users need to purchase several components to use the Pico ecosystem. Therefore, it does not fulfill *Negligible-Cost-per-User*. Also, the mechanism does not fulfill *Requiring-Explicit-Consent* due to the fact that the recovery process starts automatically when the unused Pico, connected to the docking station, and the sibling are nearby.

**Delegated Account Recovery.** Users deposit a token for account recovery at a so-called recovery provider [Fa17]. To restore access, the online service starts a request to the recovery provider. If the user successfully authenticates against the recovery provider, the provider transmits the token back to the online service and recovers access to the user account. The protocol is not *Scalable-for-User* at the moment, as users must enter a recovery provider for each online service they like to register. When the authenticator is lost, users must perform the access recovery process for each online service individually. It is also not *Easy-to-Learn*, since the meaning of authenticating to the recovery provider may not be clear to non-technical users. Beyond that, the protocol does not fulfill *Unlinkable*. The recovery provider could record the online services from which it receives requests for a



particular user. Then, it could authenticate the user and restore access for the user's other online services without the user's consent.

**FIDO2 Backup Token.** The FIDO Alliance recommends to register another FIDO2 security token in addition to the primary FIDO security token [GLS19]. When users lost their primary security token, the second security token can be used to access the account using standard FIDO2 authentication. After that, they can remove the old security token from their account and register a new primary security token. The recovery mechanism has the advantage of being *Memorywise-Effortless*. It is also *Resilient-to-Internal-Observation*, as the authentication challenge requested by the online service is solved within the security token. However, it is not *Scalable-for-User*, since users have to register the backup security token and withdraw the old security token with each online service individually.

**Identity Card.** Citizens in Germany can use their identity card (nPA/eID) as a FIDO authenticator [ij20]. It is possible that other countries' identity cards offer this feature as well [EZ20]. Since every German citizen older than 16 years has to possess such an identity card, it would be possible as a backup authenticator variant. Following that, this recovery mechanism is *Negligible-Cost-per-User*, in contrast to classical FIDO2 backup tokens. Since the identity card is protected with a PIN by default, it is also *Resilient-to-Theft*. However, it is not *Browser-Compatible*, as users need to install special browser plugins or smartphone apps to use this mechanism. It also fails *No-Trusted-Third-Party*, since the eID server must be used in addition to the authenticator and the online service.

**Advanced Protection Program.** Google introduced set of precautions to protect particularly vulnerable user accounts, e.g., those of political activists [Go20]. This includes securing the account with FIDO security tokens as a second factor. As a part of this program, Google also offers the access recovery option. This means that if users lose their security tokens, they can access their account using a device that is still logged in. The account recovery can not be assured *Physically-Effortless*, as the steps to be taken and the amount of required physical effort are not further specified. Therefore, it cannot be ruled out that attackers with person-specific knowledge could carry out a successful attack. Therefore, the mechanism can not reliably fulfill *Resilient-to-Target-Impersonation*. Since the open session is sufficient to restore the account, the mechanism does not fulfill *Complete-Mediation*.

**Let's Authenticate.** The existing FIDO2 scheme is modified to address the access recovery problem [CZ19]. The mechanism provides authentication using certificates rather than public and private keys directly. To do this, a Certification Authority (CA) is introduced into the FIDO ecosystem. For registering with an online service, users need an account at the CA. If the users lose their authenticator, the CA can issue new certificates for the online services they used with the previous security token. The access recovery mechanism is not *Memorywise-Effortless*, as users must authenticate against the CA with a password after losing their authenticator. However, the mechanism is *Scalable-for-User*, because access to all online services is immediately restored using the reissued certificate. The Let's Authenticate paper [CZ19] correctly mentions that no login credentials can be phished.

However, the mechanism is still not *Resilient-to-Phishing*, as the credentials that authenticate the user to the CA could be phished.

**Key Copy.** When using a mobile device as an authenticator, the key material can be transferred from one authenticator to another [Ni18]. In doing so, the security principle that private key material must never leave the authenticator is relaxed. A so-called Owner Identification Service (OIS) ensures that the two devices that are to exchange keys belonging to the user. The recovery mechanism is *Unlinkable*, as it still stores different secrets per online service. It is also *Browser-Compatible*, since it does not require any additional browser functionality. However, it only partially scales for users. Users must periodically perform the key copy mechanism between the two authenticators. Nevertheless, users do not need to register both authenticators on an online service every time. We still attributed *Scalable-for-User*, as users decide how often they perform the key copy mechanism. Since it relies on the OIS, however, the mechanism does not fulfill *No-Trusted-Third-Party*.

**Online Recovery Storage (ORS).** In this mechanism, the user has a primary and a backup security token, and access to a third party ORS [Ta]. The user generates a large number of keys on the backup security token, which the security token signs. The ORS stores the signed keys. During registration on a online service, the primary security token generates a new asymmetric key pair, and sends the public key to the service. Then, the primary security token decrypts a data block from the ORS. In the decrypted data, the primary authenticator adds information of its registration to the new online service. These include a unique app ID and the public key sent to the online service. The access recovery works via newly generated keys and delegations of the backup security token keys via the transfer access protocol [TKC17]. The mechanism is *Scalable-for-User*, as users only need to connect their new security token to the backup security token once to regain access to all of their accounts. Also, it is *Unlinkable*, since the mechanism stores the data block encrypted using the privacy wrapping key on the ORS. Therefore, the information is not traceable to other parties and the user is not traceable. It is not *Browser-Compatible* at the moment, as the concept integrated a non-standardized FIDO protocol message (transfer-access response).

**Pre-emptive Syncing.** The user has a primary and a backup security token in this mechanism [Ta18]. Before the primary security token is registered with an online service for the first time, both primary and the backup security token must be paired over a secure channel. The backup authenticator then generates a sufficiently large number of asymmetric key pairs. To use a new primary security token, the user initiates the Transfer Access Protocol [TKC17] between the new primary and the backup security token. The backup security token informs the new primary security token of the number of key pairs it generated at that time. Then, the new security token generates the same number of asymmetric key pairs and sends the respective public keys to the backup security token. The backup security token delegates each of its private keys to one of the public keys sent by the new security token (see Figure 1). Based on the delegations, the online service can verify that the new primary security token is authorized to access the account. The functionality of this mechanism is very similar to ORS, so the fulfilled criteria can be adopted. In addition,

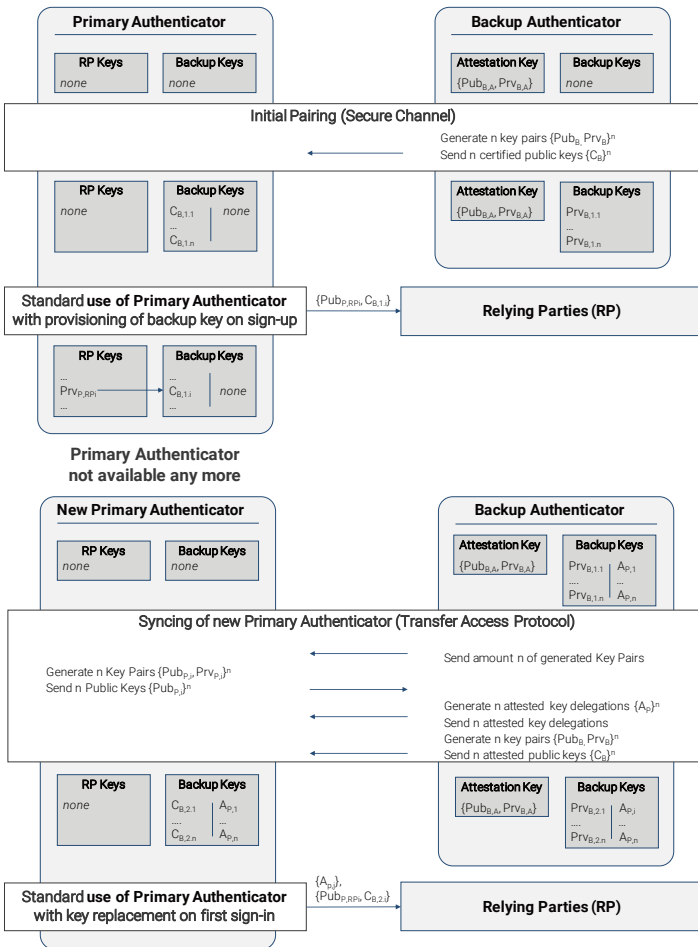


Fig. 1: Replacing a no longer available authenticator with the help of a backup authenticator without a trusted third party based on Pre-emptive Syncing

*No-Trusted-Third-Party* is fulfilled, as the mechanism only requires two security tokens and no third party. The mechanism is also *Unlinkable*, but for a different reason. Pre-emptive Syncing only exchanges the public key parts with the online services. As it does not require a third party, there is no point at which tracing users across online services would occur.

## 4 Discussion

The results confirm that security questions should be avoided at all costs. They performed significantly worse than passwords and provide an attack vector due to publicly accessible

sources. We further discuss a selection of relevant recovery mechanisms based on our results and findings in the following.

**Passwords** are widely used and recognized by users. Based on the evaluated criteria, they also performed quite good. However, users need to remember passwords. Thus, using password-based recovery in a passwordless FIDO2 authentication systems would invalidate the advantages of passwordless authentication. Facebook's **Delegated Account Recovery Protocol** addresses this problem and shows an interest to solve it. However, Facebook itself also has an interest being positioned as a major identity and recovery provider in the future. This can be seen in their initiatives to provide a Single Sign-On solution for other websites [Ka18]. Access recovery using a **FIDO2 backup security token** performed among the best in comparison. Some service providers that offer passwordless FIDO2 authentication also already use this mechanism, since the FIDO alliance recommends this method. The backup authenticator variant with the Identity Card performed slightly worse than the FIDO2 backup variant. For German citizens, this would be a cost-effective alternative with regard to purchasing a second authenticator. A problem, however, is that the Identity Card service would be able to store the online services a user is registered to. Thus, we assume that users will likely reject this method on some online services. The **Online Recovery Storage** mechanism provides a key revocation mechanism. If users lost their primary security token, the ORS can automatically revoke all keys to deny access for attackers. To do this, however, the security tokens used must be able to establish a connection with the ORS. The pre-emptive syncing mechanism does not rely on connecting to a third party. From a cryptographic point of view, the positive aspect of this mechanism is that, in contrast to the key-copy mechanism, the principle that private key material never leaves the security token can still be fulfilled. The disadvantage of this mechanism is the memory and computational load that the security token have to initially carry out once to create the keys.

## 5 Limitations

The results are limited to passwordless FIDO2 single-factor authentication systems only. They can not relate to access recovery mechanisms in the context of two- or multi-factor authentication. We did a heuristic evaluation based on validated metrics in literature. We did not test the FIDO2 recovery mechanisms on real users, and testing all 12 mechanisms in a usability study would be beyond the scope of this research. Nevertheless, our results provide valuable guidance to foster further research on passwordless FIDO2 authentication.

## 6 Related Work

To the best of our knowledge, there are no studies evaluating account recovery mechanisms in terms of passwordless FIDO2 authentication. However, there is related work regarding Fallback Authentication in terms of password-based authentication. Markert et al. [Ma19]

described a study to investigate Fallback Authentication on a long-term. However, they did not show any results to date. Hang et al. [Ha15] studied personal experiences when users had to use account recovery on their smartphone. Based on their results, they recommended to provide multiple recovery mechanisms to address users who fail at one of the schemes. Some of our tested schemes could also provide this solution, e.g., either FIDO2 Backup Token or Identity Card. Ulqinaku et al. [UI20], however, describe a social engineering attack to downgrade FIDO2 2FA. This attack is possible if users are able to choose an alternative authentication method besides the FIDO2 security token. However, this attack does not target the recovery mechanism.

## 7 Conclusion

In order to support user acceptance for passwordless FIDO2 authentication, its recovery mechanisms must be designed effectively. Therefore, we compared 12 account recovery mechanisms regarding their properties for FIDO2 passwordless authentication.

Our evaluation shows that most currently deployed recovery mechanisms performed worse in contrast to ones that only exist in theory to date (see Table 1). Also, knowledge-based access recovery mechanisms nullify many advantages achieved by FIDO2. Therefore, we do not recommend using them. In contrast to them, the FIDO2 backup token mechanism, which also the FIDO Alliance recommends, performed best. To mitigate the still significant usability weaknesses of this mechanism, the pre-emptive syncing mechanism is the most promising variant to provide FIDO2 in passwordless systems with a manageable and secure access recovery. This can achieve the best balance between security, privacy, and usability among all analyzed mechanisms.

In future work, the concept of pre-emptive syncing should be further investigated to address the problem of memory and computational load due to the pre-generated keys on the authenticators. Furthermore, the FIDO Alliance could take up the proposal to adopt the Transfer Access Protocol and the associated Transfer Access Message or concept in its standards. This would allow the two mechanisms, Online Recovery Storage and Pre-emptive Syncing, to become real-world usable mechanisms for access recovery in passwordless FIDO2 environments. In this way, the FIDO Alliance could eliminate the major problem of inadequately standardized access recovery to date and thus increase user adoption of passwordless FIDO2 authentication.

## Bibliography

- [AJ09] Aspinall, David; Just, Michael: Knowledge-Based Authentication: Evaluating and Improving. 2009. <http://groups.inf.ed.ac.uk/security/KBA/CaseforSupport-Aspinall-Just.pdf>.
- [Ak20] Akamai: Credential Stuffing in the Media Industry. [state of the internet] / security, 6(Special Media Edition), July 2020.

- [An20] Anti-Phishing Working Group: Phishing Activity Trends Report (3rd Quarter). 2020.
- [Bo12] Bonneau, Joseph; Herley, Cormac; Oorschot, Paul C. van; Stajano, Frank: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: SP '12. IEEE, May 2012.
- [CZ19] Connors, James S; Zappala, Daniel: Let's Authenticate: Automated Cryptographic Authentication for the Web with Simple Account Recovery. In: WAY '19. 2019.
- [De20] Deloitte: How Covid-19 contributes to a long-term boost in remote working. 2020. <https://www2.deloitte.com/ch/en/pages/human-capital/articles/how-covid-19-contributes-to-a-long-term-boost-in-remote-working.html>.
- [EZ20] Elfors, Sebastian; Zwattendorfer, Bernd: Deploying FIDO2 for eIDAS QTSPs and eID schemes. April 2020.
- [Fa17] Facebook: Delegated Recovery. GitHub, October 2017. <https://git.io/JtVFe>.
- [Fa20] Farke, Florian M.; Lorenz, Lennart; Schnitzler, Theodor; Markert, Philipp; Dürmuth, Markus: "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. In: SOUPS '20. USENIX Association, August 2020.
- [FI17] FIDO-Alliance: FIDO UAF Architectural Overview. February 2017.
- [GLS19] Gomi, Hidehito; Leddy, Bill; Saxe, Dean H: Recommended Account Recovery Practices for FIDO Relying Parties. p. 4, February 2019.
- [Go20] Google: Advanced Protection Program. 2020. [https://landing.google.com/intl/en\\_us/advancedprotection/](https://landing.google.com/intl/en_us/advancedprotection/).
- [Gr18] Gretzky, Kuba: Evilginx 2 - Next Generation of Phishing 2FA Tokens. breakdev, July 2018. <https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/>.
- [Ha15] Hang, Alina; De Luca, Alexander; von Zezschwitz, Emanuel; Demmler, Manuel; Hussmann, Heinrich: Locked Your Phone? Buy a New One? From Tales of Fallback Authentication on Smartphones to Actual Concepts. In: MobileHCI '15. MobileHCI '15, ACM, New York, NY, USA, 2015.
- [if20] ifo Institute: Working from Home and Digitalization in Light of the Coronavirus (2nd Quarter 2020). 2020. <https://www.ifo.de/en/personnel-manager-survey/202008-q2>.
- [ij20] ijon: Versteckte Funktion des nPA – sicherer Login bei Facebook, Google & Co. LOAD, April 2020. <https://www.load-ev.de/2020/04/16/versteckte-funktion-des-npa-sicherer-login-bei-facebook-google-co/> (in German).
- [Ja14] Javed, A.; Bletgen, D.; Kohlar, F.; Dürmuth, M.; Schwenk, J.: Secure Fallback Authentication and the Trusted Friend Attack. In: ICDCSW '14. 2014.
- [Ka18] Karegar, Farzaneh; Gerber, Nina; Volkamer, Melanie; Fischer-Hübner, Simone: Helping john to make informed decisions on using social login. In: SAC '18. ACM, April 2018.
- [Ly20] Lyastani, Sanam Ghorbani; Schilling, Michael; Neumayr, Michaela; Backes, Michael; Bugiel, Sven: Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In: SP '20. IEEE, 2020.

- [Ma19] Markert, Philipp; Golla, Maximilian; Stobert, Elizabeth; Dürmuth, Markus: Work in Progress: A Comparative Long-Term Study of Fallback Authentication. In: USEC '19. Internet Society, 2019.
- [Ni94] Nielsen, Jakob: Enhancing the explanatory power of usability heuristics. In: CHI '94. ACM, April 1994.
- [Ni18] Nishimura, Hideo; Omori, Yoshihiko; Yamashita, Takao; Furukawa, Satoru: Secure authentication key sharing between mobile devices based on owner identity. In: MobiSecServ '18. February 2018.
- [Pa19] Pal, B.; Daniel, T.; Chatterjee, R.; Ristenpart, T.: Beyond Credential Stuffing: Password Similarity Models Using Neural Networks. In: SP '19. IEEE, May 2019.
- [Ra08] Rabkin, Ariel: Personal knowledge questions for fallback authentication: security questions in the era of Facebook. In: SOUPS '08. ACM, July 2008.
- [Re19] Reese, Ken; Smith, Trevor; Dutson, Jonathan; Armknecht, Jonathan; Cameron, Jacob; Seamons, Kent: A Usability Study of Five Two-Factor Authentication Methods. In: SOUPS '19. USENIX Association, 2019.
- [SS75] Saltzer, J. H.; Schroeder, M. D.: The protection of information in computer systems. Proc. IEEE, 63(9), September 1975.
- [St11] Stajano, Frank: Pico: No More Passwords! In: Security Protocols XIX. Springer, 2011.
- [Ta] Takakuwa, Alex: Recovering from Lost Devices in WebAuthn - Online Recovery Storage: store encrypted recovery data online.
- [Ta18] Takakuwa, Alex: . Recovering from Lost Devices in WebAuthn - Pre-emptively syncing recovery keys, 2018.
- [TKC17] Takakuwa, Alex; Kohno, Tadayoshi; Czeskis, Alexei: The Transfer Access Protocol - Moving to New Authenticators in the FIDO Ecosystem. June 2017.
- [UI20] Ulqinaku, Enis; Assal, Hala; Abdou, AbdelRahman; Chiasson, Sonia; Čapkun, Srdjan: Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols. November 2020. <https://eprint.iacr.org/2020/1298>.
- [WDLI20] Wiefling, Stephan; Dürmuth, Markus; Lo Iacono, Luigi: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC '20. ACM, December 2020.
- [WDLI21] Wiefling, Stephan; Dürmuth, Markus; Lo Iacono, Luigi: What's in Score for Website Users: A Data-driven Long-term Study on Risk-based Authentication Characteristics. In: FC '21. Springer, March 2021.
- [WI20a] Weeden, Shane; IBM: Account Recovery is just another Authentication Method. Shane Weeden's Blog, 2020.
- [Wi20b] Wiefling, Stephan; Patil, Tanvi; Dürmuth, Markus; Lo Iacono, Luigi: Evaluation of Risk-based Re-Authentication Methods. In: IFIP SEC '20. Springer, September 2020.

## FAPI 2.0: A High-Security Profile for OAuth and OpenID Connect

Daniel Fett<sup>1</sup>

**Abstract:** A growing number of APIs, from the financial, health and other sectors, give access to highly sensitive data and resources. With the Financial-grade API (FAPI) Security Profile, the OpenID Foundation has created an interoperable and secure standard to protect such APIs.

The first version of FAPI has recently become an official standard and has already been adopted by large ecosystems, such as OpenBanking UK. Meanwhile, the OpenID Foundation's FAPI Working Group has started the work on a the second version of FAPI, putting a focus on robust interoperability, simplicity, a more structured approach to security, and improved non-repudiation.

In this paper, we give an overview of the FAPI profiles, discuss the learnings from practice that influence the development of the latest version of FAPI, and show how formal security analysis helps to shape security decisions.

**Keywords:** Authorization; Authentication; Security; Interoperability

### 1 Introduction

Multi-banking apps and other fintech offerings usually need to access their users' bank accounts in order to retrieve account information and initiate payments. For many years, screen-scraping has been the norm in this area: Apps use their users' online banking credentials to access (directly or via a server) the bank's online banking website through an emulated browser and extract relevant information.

This approach is not only brittle, as it can break easily when elements in the online banking interface change, it is also dangerous: Fintech services get unlimited access to accounts and misuse of the credentials cannot be detected or prevented effectively. From the bank's perspective, this kind of access is largely indistinguishable from phishing attacks.

With PSD2 [Co15] in the European Union and similar efforts in other markets, APIs for account information and payment initiation have been introduced. Nonetheless, some operating modes in these APIs still require the user to enter their credentials into the app or service they are about to use. Besides carrying a similar potential for misuse of credentials as screen-scraping, this trains users that entering their online banking credentials on third-party apps and websites is harmless.

---

<sup>1</sup> yes.com AG, Hafenstrasse 2, 8853 Lachen, Switzerland, mail@danielfett.de



A token-based approach to delegation of authorization, such as the one offered by OAuth 2.0 [Hal12], can ensure that users can give apps and services access to their resources in a controlled and secure way.<sup>2</sup> For open banking use cases such as the one described before, it is, however, not sufficient to just prescribe the use of OAuth 2.0: The IETF standard only defines a *framework* for protocols but leaves a wide range of options in almost all areas of the communication. For a practical use in any larger ecosystem, a *profile* of OAuth 2.0 needs to be defined to ensure interoperability between participants in the ecosystem, to ensure an adequate level of security, and to define a common feature set.

To this end, the OpenID Foundation launched an effort in 2016 to create the *Financial-grade API Security Profile* (FAPI). While initially focussed on financial applications, the standard is agnostic towards the resources to protect and can be used for all kinds of APIs bearing a high inherent risk. Therefore, it has been adopted not only by Open Banking UK<sup>3</sup> and the yes.com open banking scheme<sup>4</sup>, but also by the Consumer Data Right initiative in Australia<sup>5</sup>; an integration in the Norwegian health sector is ongoing.

In this paper, we give a brief overview of the development of and differences between FAPI 1.0 and FAPI 2.0 (Section 2). In Section 3, we introduce the security model underlying FAPI 2.0 and show how it was shaped by formal security analysis. In Section 4 we present the main features of FAPI 2.0 and discuss learnings from practice that have influenced the development. We conclude in Section 5.

## 2 FAPI 1.0 and FAPI 2.0: Overview

FAPI was created by the OpenID Foundation's FAPI working group in order to address the following challenges:

- **Security:** In financial applications, a high level of security must be guaranteed. On its own and without applying further restrictions, OAuth 2.0 is not suitable for high-security applications, as it provides several options that are only secure under moderately strong attacker models [FHK19, FKS16]. FAPI ensures that specific options are selected and extensions are applied which ensure that the resulting protocol is suitable for high-security applications.

---

<sup>2</sup> With OAuth 2.0, a user can give a *client* (app or website) access to their resources at a so-called *resource server*, e.g., a banking API. To this end, the client first redirects the user to an endpoint at the banks *authorization server*, where, in direct communication between the user's browser and the authorization server, the user authenticates to the bank using their regular online banking credentials. The user can then authorize the access by the client, which can be limited in terms of resources that can be accessed, actions that can be performed, and lifetime of the authorization. The user's browser is then redirected back to the client, carrying an *authorization code* in the URL. The client exchanges this code for an *access token* in direct communication with the authorization server's *token endpoint*. With the access token, the client can access the user's resources (e.g., retrieve recent transactions or initiate a payment) at the resource server.

<sup>3</sup> <https://standards.openbanking.org.uk/>

<sup>4</sup> <https://yes.com/docs>

<sup>5</sup> <https://consumerdatastandardsaustralia.github.io/standards/>

- **Interoperability:** FAPI standardizes the protocol features that are used by clients and servers in order to ensure an interoperability between all participants in an ecosystem. This comprises standard OAuth 2.0 features from RFC6749 [Ha12] and RFC6750 [JH12] as well as extensions, such as client authentication via mutual TLS (RFC8705 [Ca20]).
- **Common feature set:** FAPI further ensures that protocol features are available that solve commonly encountered problems in financial ecosystems, for example, the transfer of complex and fine-grained information on the authorization requested by the client. This prevents the creation of individual solutions that lack standardization and support by software vendors.

FAPI 1.0 is defined in two separate profiles, *Baseline* and *Advanced*. The Baseline profile [SJ21a], initially called *read-only*, provides a level of security that is considered sufficient for less-critical operations, such as viewing basic account information. The Advanced profile [SJ21b], initially called *read-write*, aims to provide a high level of security. At the same time, it provides basic features for message-level non-repudiation. FAPI 1.0 has become an official OpenID Foundation standard in March 2021.

The work on FAPI 2.0 has commenced in 2019. Compared to its predecessor, FAPI 2.0 aims to further improve interoperability between FAPI implementations by reducing optionality within the protocol, to provide a broader scope of features, to simplify development for implementers, and to create a well-defined security model. FAPI 2.0 again defines two security levels, but FAPI 2.0 Baseline [Fe21c] provides a higher security level than FAPI 1.0 Advanced with a broader scope of features and easier development. FAPI 2.0 Advanced [Fe21a] additionally provides full non-repudiation, i.e., all relevant protocol messages are signed (see Figure 1). A security model for FAPI 2.0 is defined in a separate document, the *FAPI 2.0 Attacker Model* [Fe21b]. The Baseline profile and the Attacker Model are on track to become so-called *Implementers Drafts* soon.

Medium Security, no non-repudiation	FAPI 1.0 Baseline	
High Security, limited non-repudiation	FAPI 1.0 Advanced	FAPI 2.0 Baseline
High Security, full non-repudiation		FAPI 2.0 Advanced

Fig. 1: Rough comparison of security and non-repudiation levels in FAPI versions.

### 3 Security Model

Through a number of measures, all FAPI profiles achieve a higher level of security than plain OAuth 2.0 can offer.

First of all, less-secure protocol options are forbidden. The prime example is the OAuth Implicit Grant, where an access token is transferred through the user’s web browser. This

mode of operation is forbidden in FAPI, as access tokens are susceptible to a number of attacks in the browser and during transfer [FKS16, Lo20]. As another example, redirect URIs in FAPI must be HTTPS URIs and have to be pre-registered with the authorization server, preventing common vulnerabilities with OAuth redirections [Lo20]. Finally, a major difference to many existing OAuth deployments is also that symmetric client secrets are disallowed in all FAPI profiles except for FAPI 1.0 Baseline.

The second security measure in FAPI is the mandatory use of a selected set of extensions improving the security of OAuth, such as *Proof Key for Code Exchange* (PKCE) [SBA15], which protects authorization codes from misuse.

### 3.1 Lessons Learned from FAPI 1.0

For FAPI 1.0, the selection of security measures was made on a case-by-case basis, based on commonly known best practices and specific attack scenarios.

In previous work [FHK19], we analyzed the security of the then-current draft of FAPI 1.0 in order to analyze whether this process yielded a secure OAuth profile or not. The analysis was based on the *Web Infrastructure Model* (WIM), the most comprehensive formal model of web servers, browsers, and other components of the web to date [Fe18].

For a formal security analysis in general, one or more sets of capabilities of attackers need to be defined, the *attacker model*. The security of (a model of) the protocol can then either be proven against this attacker model, or the analysis reveals an attack on the protocol. Commonly assumed capabilities of attackers in the analysis of network and web protocols are, for example: (1) the capability to participate in the protocol just as a normal user can, (2) the capability to operate an arbitrary number of endpoints (e.g., web servers), and (3) the capability to read and manipulate arbitrary (unprotected) network traffic (the *network attacker model*).

In [FKS16] and [FKS17], we showed security of OAuth 2.0 and OpenID Connect under a network attacker model. For FAPI 1.0, however, a much stronger attacker model was derived from the description of the profile, adding a number of critical attacker capabilities: (3) reading the contents of the authorization request and response, e.g., through a misdirected app-to-app communication on a mobile device, (4) reading the access token, e.g., due to phishing, and (5) controlling the token endpoint, e.g., because it was misconfigured [FHK19].

Parts of this attacker model were explicitly mentioned in the FAPI draft (e.g., phishing), other parts were hinted at by the selection of security measures. For example, hashing the PKCE verifier to acquire the PKCE challenge implies that capability (3) is assumed. With this very strong attacker model, our analysis yielded a number of attacks that were taken into account in later versions of FAPI 1.0. With mitigations in place, the security of FAPI 1.0 was proven in the formal model.

However, the analysis also revealed that reverse-engineering an attacker model from a specification is a complex process. It further showed that an underdefined attacker model can introduce inconsistencies into the specification that can lead to false expectations regarding the security of a protocol. For example, while a hashed PKCE verifier in the authorization request implies a protection against an attacker with capability (3), the *state* value is not protected and an attacker with capability (3) can potentially mount a cross-site request forgery attack against the client.

Therefore, for FAPI 2.0, one goal is to explicitly define a consistent security model. Such a model not only informs security decision in the design process, it also clears the way for easier and more accurate security analyses. Finally, it helps to communicate the precise level of security the specification aims to achieve and can be used by implementers to identify areas where further security measures might be required.

Additionally, some of the security measures in FAPI 1.0 are based on existing OpenID Connect features, necessitating the use of OpenID Connect even if authentication or the transfer of end-user information is not desired and OAuth alone would be sufficient. This can create additional complexity for developers. Another goal for FAPI 2.0 is therefore to make OpenID Connect a fully optional part of the specification and ensuring security with native OAuth features and extensions.

### 3.2 Security Model of FAPI 2.0

The first step in the development of FAPI 2.0 was to create a security model [Fe21b]. It is based on the FAPI 1.0 attacker model identified in [FHK19] described above. It further extends the model by capabilities for an attacker to read requests to and responses from the resource server, and to tamper with responses from the resource server. This was motivated by the fact that these requests often go through reverse proxies that can be manipulated or write log files to less-protected environments.

FAPI 2.0 Baseline and Advanced use the same attacker model, i.e., both must ensure the security and integrity of the authorization (and possibly, authentication) process in the presence of attackers with the described capabilities. Appendix A shows the attacker model for FAPI 2.0.

For Advanced, additional non-repudiation goals are defined: it must be ensured that receivers of protocol messages can prove the origin and integrity of all relevant messages received.

In parallel to the development of FAPI 1.0, the IETF has worked on a document that describes current best practices for OAuth 2.0 deployments [Lo20]. Another goal of FAPI 2.0 is to align its recommendations with those from the IETF.

## 4 Core Elements of FAPI 2.0 Baseline

In the following, we briefly present the main elements that make up FAPI 2.0 Baseline according to the current draft. For the details, refer to [Fe21c]. The Advanced profile is still in early development, in particular regarding the non-repudiation of messages to and from the resource server, which likely requires the development of a new message signing scheme.

FAPI 2.0 is based on OAuth 2.0 as defined in RFC6749 [Ha12] and RFC6750 [JH12]. OAuth may be used in one of two modes, the *Authorization Code Grant* and the *Client Credentials Grant*, where a client accesses a resource on its own behalf. OpenID Connect [Sa] can be used to optionally provide information about the end-user (authentication).

Clients need to authenticate themselves to the authorization server using asymmetric methods, either TLS client authentication as defined in RFC8705 [Ca20] or using a JSON Web Token (JWT) signed using a private key, as defined in OpenID Connect [Sa].

Authorization codes are protected using PKCE [SBA15] and access tokens need to be sender-constrained, i.e., must be bound to a private key only known to the client. This can be achieved by binding the access tokens to a private TLS certificate key as defined in RFC8705 [Ca20] or via Demonstrating of Proof-of-Possession at the Application Layer (DPoP) [Fe20].

To mitigate attacks where an endpoint is misconfigured, as mentioned above, OAuth Server Metadata from RFC8414 [JSB18] must be used. With this extension, authorization servers publish their URLs and other meta information on a predefined URL. This enables an automatic discovery and configuration of the authorization, token, and other endpoints.

To prevent Mix-Up attacks [FKS16], the Authorization Server Issuer Identifier in Authorization Response extension [MzSF21] is used.

Traditionally, OAuth authorization requests contain all information in the parameters of a single URL to which the user's browser is redirected. The information that is transferred includes the kind of access the client requests (expressed as a list of strings in the *scope* parameter) and various security-related parameters. This approach bears three problems: First, the data is neither encrypted nor integrity protected, i.e., the user or malicious code running in the user's browser can read and/or modify the scope or security-critical parameters. Second, there is an upper limit to the length of the data, imposed by the maximum length of a URL. And finally, a list of strings is not expressive enough for complex use cases. For example, a client may want to acquire authorization to initiate a payment of a certain amount of money to a specific bank account using a defined reference text. Custom encodings can be used to circumvent this limit, but these are non-standard and often lack support by software vendors.

To solve these problems, two OAuth extensions were created in the IETF and have become part of FAPI 2.0:

*Pushed Authorization Requests (PAR)* give the client an option to send all data that is normally contained in the authorization request to a special PAR endpoint at the authorization server, using a POST request. Since the data is transferred via a direct, authenticated channel between the client and the authorization server, integrity and confidentiality of all parameters can be ensured. The client receives a unique identifier in response, which can be used in place of the original parameters in the authorization request.

*Rich Authorization Requests (RAR)* are enabled through a new authorization request parameter, `authorization_details`, with a pre-defined, extensible structure. It can be used to transfer complex authorization requirements. While the precise contents of the parameter depend on the ecosystem or scheme it is used in, its fixed structure enables easier software vendor support.

Due to its benefits for security, PAR must be used in FAPI 2.0. RAR is to be used when the scope parameter is not sufficient to solve the use case at hand.

## 5 Conclusion

The work of the FAPI working group fosters the use of OAuth 2.0 and OpenID Connect in large ecosystems. To further support this, the OpenID Foundation has created a comprehensive Conformance Testing Program [Op], which helps to ensure that implementations actually comply to the FAPI specifications.

FAPI 1.0 is in use today, is fully supported by the Conformance Testing Program, and has been shown to be a secure standard.

FAPI 2.0 targets an even higher degree of interoperability by providing a further reduced set of options and covering a broader set of use cases by standard features. FAPI 2.0 uses a new approach to ensuring the security of the protocol by underpinning security-related decisions with an attacker model. This model will also be the basis for future formal analysis efforts to ensure the security of FAPI 2.0.

The FAPI 2.0 Baseline and Advanced profiles are under development at the OpenID Foundation and the working group welcomes feedback from external entities.

## Bibliography

- [Ca20] Campbell, Brian; Bradley, John; Sakimura, Nat; Lodderstedt, Torsten: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens. (RFC 8705), February 2020. <https://rfc-editor.org/rfc/rfc8705.txt>.

- [Co15] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02015L2366-20151223>.
- [Fe18] Fett, Daniel: An Expressive Formal Model of the Web Infrastructure. PhD thesis, 2018. <https://publ.sec.uni-stuttgart.de/fett-phdthesis-2018.pdf>.
- [Fe20] Fett, Daniel; Campbell, Brian; Bradley, John; Lodderstedt, Torsten; Jones, Mike; Waite, David: OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPOP). (draft-ietf-oauth-security-topics-16), 2020. <https://tools.ietf.org/html/draft-ietf-oauth-dpop>.
- [Fe21a] FAPI 2.0 Advanced Profile (Draft), [https://bitbucket.org/openid/fapi/src/master/FAPI\\_2\\_0\\_Advanced\\_Profile.md](https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Advanced_Profile.md).
- [Fe21b] FAPI 2.0 Attacker Model (Draft), [https://bitbucket.org/openid/fapi/src/master/FAPI\\_2\\_0\\_Attacker\\_Model.md](https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Attacker_Model.md).
- [Fe21c] FAPI 2.0 Baseline Profile (Draft), [https://bitbucket.org/openid/fapi/src/master/FAPI\\_2\\_0\\_Baseline\\_Profile.md](https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Baseline_Profile.md).
- [FHK19] Fett, Daniel; Hosseyni, Pedram; Küsters, Ralf: An Extensive Formal Security Analysis of the OpenID Financial-grade API. In: 2019 IEEE Symposium on Security and Privacy (S&P 2019). volume 1. IEEE Computer Society, pp. 1054–1072, May 2019. <https://publ.sec.uni-stuttgart.de/fetthosseynikuesters-fapi-sp-2019.pdf>.
- [FKS16] Fett, Daniel; Küsters, Ralf; Schmitz, Guido: A Comprehensive Formal Security Analysis of OAuth 2.0. In: Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security (CCS 2016). ACM, pp. 1204–1215, 2016. <https://publ.sec.uni-stuttgart.de/fettkuestersschmitz-ccs-2016.pdf>.
- [FKS17] Fett, Daniel; Küsters, Ralf; Schmitz, Guido: The Web SSO Standard OpenID Connect: In-Depth Formal Security Analysis and Security Guidelines. In: IEEE 30th Computer Security Foundations Symposium (CSF 2017). IEEE Computer Society, pp. 189–202, 2017. <https://publ.sec.uni-stuttgart.de/fettkuestersschmitz-csf-2017.pdf>.
- [Ha12] Hardt, Dick: The OAuth 2.0 Authorization Framework. (RFC 6749), October 2012. <https://rfc-editor.org/rfc/rfc6749.txt>.
- [JH12] Jones, Michael; Hardt, Dick: The OAuth 2.0 Authorization Framework: Bearer Token Usage. (RFC 6750), October 2012. <https://rfc-editor.org/rfc/rfc6750.txt>.
- [JSB18] Jones, Michael; Sakimura, Nat; Bradley, John: OAuth 2.0 Authorization Server Metadata. (RFC 8414), June 2018. <https://rfc-editor.org/rfc/rfc8414.txt>.
- [Lo20] Lodderstedt, Torsten; Bradley, John; Labunets, Andrey; Fett, Daniel: OAuth 2.0 Security Best Current Practice. (draft-ietf-oauth-security-topics-16), 2020. <https://tools.ietf.org/html/draft-ietf-oauth-security-topics>.
- [MzSF21] Meyer zu Selhausen, Karsten; Fett, Daniel: OAuth 2.0 Authorization Server Issuer Identifier in Authorization Response. (draft-ietf-oauth-iss-auth-resp-00), 2021. <https://tools.ietf.org/html/draft-ietf-oauth-iss-auth-resp>.

- 
- [Op] Conformance Testing for FAPI Read/Write OPs, [https://openid.net/certification/fapi\\_op\\_testing/](https://openid.net/certification/fapi_op_testing/).
  - [Sa] Sakimura, Nat; Bradley, John; Jones, Mike; de Medeiros, Breno; Mortimore, Chuck: OpenID Connect Core 1.0 incorporating errata set 1. [http://openid.net/specs/openid-connect-core-1\\_0.html](http://openid.net/specs/openid-connect-core-1_0.html).
  - [SBA15] Sakimura, Nat; Bradley, John; Agarwal, Naveen: Proof Key for Code Exchange by OAuth Public Clients. (RFC 7636), September 2015. <https://rfc-editor.org/rfc/rfc7636.txt>.
  - [SJ21a] Financial-grade API Security Profile 1.0 - Part 1: Baseline, [https://bitbucket.org/openid/fapi/src/master/Financial\\_API\\_WD\\_001.md](https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_001.md).
  - [SJ21b] Financial-grade API Security Profile 1.0 - Part 2: Advanced, [https://bitbucket.org/openid/fapi/src/master/Financial\\_API\\_WD\\_002.md](https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_002.md).

## A FAPI 2.0 Attacker Model

The following is an excerpt from the current draft of the FAPI 2.0 attacker model [Fe21b].

FAPI 2.0 profiles aim to ensure the security goals listed above for arbitrary combinations of the following attackers, potentially collaborating to reach a common goal:<sup>6</sup>

### Basic Attackers

**A1 - Web Attacker:** Standard web attacker model. Can send and receive messages just like any other party controlling one or more endpoints on the internet. Can participate in protocols flows as a normal user. Can use arbitrary tools (e.g., browser developer tools, custom software, local interception proxies) on their own endpoints to tamper with messages and assemble new messages. Can send links to honest users that are then visited by these users. This means that the web attacker has the ability to cause, arbitrary requests from users' browsers, as long as the contents are known to the attacker.

Cannot intercept or block messages sent between other parties, and cannot break cryptography unless the attacker has learned the respective decryption keys. Deviating from the common web attacker model, A1 cannot play the role of a legitimate AS in the ecosystem (see A1a).

**A1a - Web Attacker (participating as AS):** Like the web attacker A1, but can also participate as an AS in the ecosystem. Note that this AS can reuse/replay messages it has received from honest ASs and can send users to endpoints of honest ASs.

---

<sup>6</sup> The enumeration is not linear, as some attackers have been merged into others or split up into more detailed models over time.



**A2 - Network attacker:** Controls the whole network (like a rogue WiFi access point or any other compromised network node). Can intercept, block, and tamper with messages intended for other people, but cannot break cryptography unless the attacker has learned the respective decryption keys.

Note: Most attacks that are exclusive to this kind of attacker can be defended against by using transport layer protection like TLS.

### **Attackers at the Authorization Endpoint**

The attackers for the authorization request are more fine-grained than those for the token endpoint and resource endpoint, since these messages pass through the complex environment of the user's browser/app/OS with a larger attack surface. This demands for a more fine-grained analysis.

**A3a - Read Authorization Request:** The capabilities of the web attacker, but can also read the authorization request sent in the front channel from a user's browser to the authorization server. This might happen on mobile operating systems (where apps can register for URLs), on all operating systems through the browser history, or due to Cross-Site Scripting on the AS. There have been cases where anti-virus software intercepts TLS connections and stores/analyzes URLs.

**A3b - Read Authorization Response:** The capabilities of the web attacker, but can also read the authorization response. This can happen e.g., due to the URL leaking in proxy logs, web browser logs, web browser history, or on mobile operating systems.

### **Attackers at the Token Endpoint**

**A5 - Read and Tamper with Token Requests and Responses:** This attacker makes the client use a token endpoint that is not the one of the honest AS. This attacker can read and tamper with messages sent to and from this token endpoint that the client thinks as of an honest AS.

Note: When the token endpoint address is obtained from an authoritative source and via a protected channel, e.g., through OAuth Metadata obtained from the honest AS, this attacker is not relevant.

### **Attackers at the Resource Server**

**A7 - Read Resource Requests and Responses:** The capabilities of the web attacker, but this attacker can also read requests sent to and from the resource server, for example because the attacker can read TLS intercepting proxy logs on the RS's side.

**A8 - Tamper with Resource Responses:** The capabilities of A7, but this attacker can also tamper with responses from the resource servers (e.g., a compromised reverse proxy in front of the resource server).



# How Quantum Computers threat security of PKIs and thus eIDs

Sebastian Vogt<sup>1</sup> and Holger Funke<sup>2</sup>

**Abstract:** Quantum computers threaten the security of asymmetric cryptography and thus the heart of a PKI - used for example to protect electronic data in passports. On the one hand, there are already promising candidates for post-quantum secure algorithms, but these also have disadvantages (stateful and / or with significantly larger public keys or signatures). On the other hand, there are some application areas for which a PKI should use post-quantum secure procedures as soon as possible. What is the situation regarding PQC in the market for secure, electronic identification (e.g. electronic travel documents)? What needs to be done to prepare electronic travel documents for a post-quantum world?

**Keywords:** post-quantum cryptography, PQC, quantum-safe, eID, electronic travel document, passport

## 1 Introduction

So-called quantum computers are subject of research for many years. These computers are not working with usual physics but are using quantum phenomena like superpositions or entanglement. Certain computational problems can be solved much more efficiently on a quantum computer than on a classical computer.

Some of these computational problems are integer factorization and calculating discrete logarithm. Both problems can be solved efficiently on a large-scale quantum computer with Shor's algorithm, which has been invented by Peter Shor in 1994 [Sh94]. Hence, the currently widespread asymmetric algorithms RSA (security is based on hardness of integer factorization) and elliptic curve cryptography (security is based on hardness of calculating discrete logarithm) can be easily attacked if an attacker has access to a large-scale quantum computer.

Moreover, Lov Grover invented Grover-algorithm in 1996, which is able to search in an unsorted database of size  $N$  in square root  $N$  iterations [Go96]. Therefore, symmetric cryptographic algorithms can be attacked with Grover's algorithm on a large-scale quantum computer. However, this will only halve the bit security of symmetric algorithms, so that one can avert this attack by doubling the bit security, e.g. use AES-256 instead of AES-128.

---

<sup>1</sup> secunet Security Networks AG, Division Homeland Security, Essen, [sebastian.vogt@secunet.com](mailto:sebastian.vogt@secunet.com)

<sup>2</sup> secunet Security Networks AG, Division Homeland Security, Paderborn, [holger.funke@secunet.com](mailto:holger.funke@secunet.com)

Type	Algorithm	Classical bit security	Quantum bit security	Quantum attack
Asymmetric	RSA 2048	112	0	Shor's algorithm
	RSA 3072	128		
	secp256r1	128		
	secp521r1	256		
Symmetric	AES 128	128	64	Grover's algorithm
	AES 256	256	128	

Tab. 1: Impacts of quantum computers on bit security

Based on quantum threat timeline report 2020, more than 50% of the experts think that it is unlikely (less than 5%) that the quantum threat will occur within the next 10 years. However, more than 50% of the experts believe that it is 50% or more likely that quantum threat will occur within the next 15 years [MP21]. Hence, if data shall be protected for more than 10 or 15 years, one should already consider how to encrypt or sign them quantum-safe today.

Substantial technological progress in development of quantum computers, as well as the above-mentioned Shor algorithm, raised the need for new asymmetric cryptographic algorithms. Hence, the National Institute for Standard and Technology (NIST) started a process for the development and standardisation of quantum-safe asymmetric algorithms in 2016 [NI16]. Initially the community was asked for proposals of quantum-safe algorithms. Those algorithms have been evaluated in multiple rounds, each of them consisting of a reduced list of candidates. At the end of this process there will be new asymmetric algorithms, which are believed to be secure against attackers with access to both: quantum and classical computers.

In July 2020 NIST announced the end of round two with three remaining third-round finalists as well as three alternative candidates for digital signature algorithms. Moreover, there are four third-round finalists as well as five alternative candidates for public key encryption resp. key establishment algorithms [AI20].

As it's getting clearer and clearer, which quantum-safe digital signature algorithms might be standardised soon, it is important to start working on the integration of these new algorithms into protocols and applications. This paper discusses how a PKI can issue quantum-safe certificates and why quantum computers threaten the security of eIDs. On the one hand, for the most promising quantum-safe algorithms the applicability for PKI is analysed and on the other hand, different ways for transition to quantum-safe certificates are discussed, which includes hybrid ways to combine classical, i.e. RSA or ECC, and quantum-safe algorithms. Furthermore, a prospect of necessary steps, which have to be done before quantum-safe algorithms can be fully used in PKI, is outlined.

## 2 Post-Quantum Signature algorithms

Several proposals for quantum-safe signature algorithms have been invented. They rely on completely different mathematical principles and they have different characteristics, e.g. statefulness, large signatures or large public keys.

First of all, some stateful hash-based signature algorithms are believed to be quantum-safe. The security of these algorithms relies on the security of the underlying hash function. Two of these algorithms are eXtended Merkle Signature Scheme (XMSS) [Hu18] and Leighton-Micali Hash-Based Signatures (LMS) [MC19]. They have already been standardised in RFC 8301 resp. RFC 8554. Both algorithms are stateful and thus, for each state only one signature is allowed to be calculated. This also implies that the total amount of signatures for one key pair is limited (based on the chosen parameter set this might be around one thousand or one million signatures).

Both XMSS and LMS can in general be used for a PKI. However, for each use case it needs to be precisely evaluated if a hash-based signature scheme is suitable. The Certification Authority (CA) itself is a system in a controlled environment and thus, it should be possible to maintain the state of a hash-based signature scheme appropriately, although the limited amount of signature might be a challenge for certain PKIs if a CA has to issue a lot of certificates. In such a case one should evaluate whether one of the other candidates for quantum-safe signature algorithms might be a better choice.

Besides these two signature algorithms, which are already standardised, several other proposals for quantum-safe signature algorithms have been submitted to NIST process. These candidates rely on different mathematical principles, like lattices or multivariate polynomials. In the following, the three third-round finalists of NIST process will be described and evaluated for their suitability to be used in a PKI.

CRYSTALS-DILITHIUM is a lattice-based signature scheme [Du18]. Its security relies on the hardness of Module Learning With Errors (MLWE) and Module Short Integer Solution (MSIS) problem. Both public keys and signatures are roughly 1-2 KB large and hence relatively balanced, however, a little bit larger than for RSA scheme. Key generation, signing and verification of signatures are very efficient. Based on NIST report on second round, this scheme is slightly favoured compared to the other lattice-based finalist FALCON, since implementation of signing in FALCON algorithms is complex and might lead to security issues, i.e. revealing of private key [AI20].

FALCON is a lattice-based signature scheme as well [Fo18]. Security of this scheme relies on the hardness of Short Integer Solution (SIS) problem over NTRU rings. Public keys and signature sizes are slightly smaller than for DILITHIUM and overall FALCON has the smallest sum of public key and signature size of all quantum-safe signature schemes in NIST process. Key generation is slower than for DILITHIUM, however, signing and signature verification are very efficient. NIST stated that one of these two lattice-based signature schemes will be most likely selected as the primary post-quantum

signature scheme [A120].

Both DILITHIUM as well as FALCON generally are good candidates to be used in a PKI. Since both have larger public keys and signatures than currently used RSA and ECC algorithms, certificates will get larger as well. Thus, for each use case it needs to be evaluated if these larger certificates are still suitable.

Another third-round finalist of NIST process is Rainbow, which is a multivariate signature scheme [DS05]. Signature size is very small and both signing and verification of signatures is very fast. However, public keys are very large (approximately 150 KB). Hence, this scheme might not be used in a PKI, since certificates would be too large. Nevertheless, Rainbow is one of the third-round finalists of NIST process, since NIST wants to offer a quantum-safe signature scheme for applications that does not need to send keys often but could benefit from small and fast signatures [A120].

We can already expect that the lattice-based signature algorithm, which will be selected after round three of NIST process, i.e. DILITHIUM or FALCON, will most likely be the primary signature scheme for quantum-safe PKIs in the future. Besides this lattice-based scheme, we can expect that XMSS or LMS will be used for certain use cases in a PKI, especially in the near future, before NIST process is finished.

Algorithm	Public key size (in bytes)	Signature size (in bytes)
DILITHIUM	1472	2701
FALCON	897	652
Rainbow	157800	66
XMSS	64	2500
LMS	56	2512
RSA-2048	256	256
Secp256r1	32	64

Tab. 2: Overview of public key and signature sizes of some quantum-safe signature algorithms compared to RSA and ECC

### 3 Integration of Post-Quantum signature algorithms in PKI

Experts are discussing several variants how post-quantum signature algorithms could be integrated into a PKI. Of course, the simplest variant is to just replace the current RSA or ECC algorithm with a post-quantum signature scheme. Besides, there are different variants for hybrid use of pre- and post-quantum algorithms. This chapter describes different variants how a PKI could integrate post-quantum algorithms.

#### 3.1 Quantum-safe Certificates

This variant simply uses a quantum-safe signature algorithm instead of the currently

used RSA or ECC algorithms. This ensures that these certificates are safe against an attacker who has access to a classical as well as a quantum computer.

A disadvantage of this approach is that every application, which needs to verify these certificates, has to migrate to post-quantum algorithms until a specific deadline. Hence, this does not ensure a smooth transition. Moreover, it might turn out in a few years, that the chosen post-quantum scheme can be attacked by either an attacker with access to a classical or quantum computer. In that case the whole PKI would need to be replaced. Another threat could be that even if the algorithm itself is secure, it is a difficult task to develop secure implementations of an algorithm. Either the implementation itself could be attacked or in terms of side channel attacks.

However, there are advantages of this approach as well. First of all, current standards would not need to be changed, only the list of allowed signature algorithms for a specific use case, e.g. like in ICAO Doc 9303 [IA15], would need to be updated. Moreover, size of certificates would increase, but it would not additionally increase, because there are two signatures and two public keys contained.

### 3.2 Hybrid Certificates

This variant combines both a pre- and post-quantum algorithm. On the one hand, there are two signatures in the certificate, one which is created by a classical signature algorithm and one which is created by a post-quantum signature algorithm. On the other hand, there are also two public keys in the certificate. To be able to store the additional signature and public key in the certificate, the international standard ISO/IEC 9594-8 proposed three X.509 extensions: Alt signature algorithm, Alt signature value and Subject Alt public key [IS20b]. However, ISO/IEC 9495-8 does not define to verify both signatures, but only one of them. Hence, this does not strictly fulfil requirements of a hybrid approach. This approach is illustrated on the left-hand side of Fig. 1.

It is best to create these new X.509 extensions as uncritical. This ensures that applications which are not yet able to process them, can still process the hybrid certificates based on the pre-quantum algorithm. This provides an elegant way for a smooth transition to post-quantum cryptography.

There is at least one additional variant for a hybrid approach to combine a pre- and a post-quantum algorithm. This variant does not use additional X.509 extensions, but just concatenates the second signature after the first signature in the same signature blob. The same will be done for both public keys respectively [OP21]. This approach is actually described for even more than two signatures and public keys, however, since size of certificates increases with each new signature and public key, the combination of one pre- and one post-quantum algorithm is the only practical choice. This is illustrated on the right-hand side of Fig. 1.

This variant implies that all applications, which would like to use these certificates, are



already able to process the used post-quantum algorithm and moreover, they need to be able to parse the signature and public key blob into the corresponding two signatures, respectively two public keys. Hence, this variant does not allow a smooth but rather abrupt transition to post-quantum cryptography.

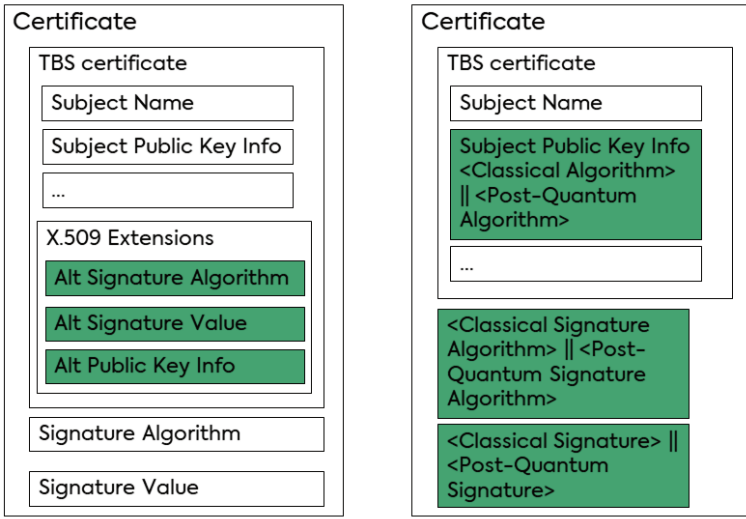


Fig. 1: Hybrid certificates variant 1 (on the left-hand side) and variant 2 (on the right-hand side)

Both variants ensure that these certificates are safe against an attacker who has access to a classical as well as a quantum computer.

A drawback of both variants is that they contain two signatures and two public keys in the same certificate, which enlarges the certificates significantly compared to the currently used ones.

### 3.3 Parallel Hierarchies

Another variant to combine pre- and post-quantum algorithms for certificates is the use of parallel hierarchies. One PKI hierarchy uses a classical algorithm, e.g. RSA or ECC, while the other PKI hierarchy uses a post-quantum algorithm. Each entity, i.e. each CA and each End-Entity, gets two certificates, one of each hierarchy. This approach is illustrated in Fig. 2.

As long as the classical algorithms can still be assessed as secure, certificates from that classical hierarchy will be used. Optionally, certificates from post-quantum hierarchy can already be validated additionally. As soon as the quantum threat becomes real, only certificates from post-quantum hierarchy will be used. From that time on, each entity will only get new certificates from post-quantum hierarchy.

One advantage of this approach is, that classical algorithms can still be used, as long as the quantum threat is not yet real. However, each entity is already equipped with a quantum-safe certificate, which enables them for the transition to post-quantum cryptography. Hence, this approach does not need an abrupt migration but ensures a smooth transition. Another advantage of this approach is, that each certificate only stores one signature and one public key, so that these certificates are not as large as the hybrid certificates.

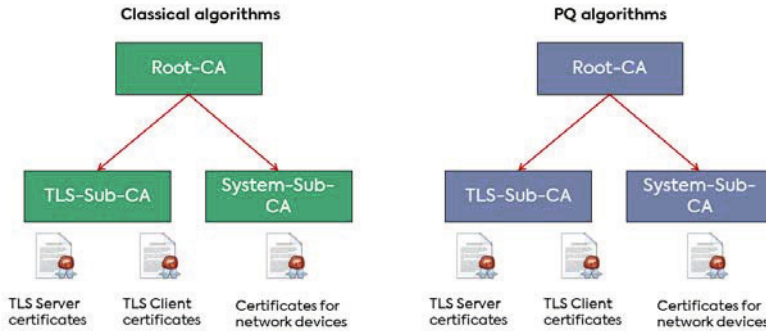


Fig. 2: Parallel PKI hierarchies

### 3.4 Comparison of different approaches

In the previous subsections different approaches to integrate post-quantum algorithms into certificates have been described. If both signatures are validated in the hybrid approach of subsection 3.2, it is the most secure approach, while just replacing the current algorithms with post-quantum ones as described in subsection 3.1 requires the fewest changes of existing standards. The approach of parallel hierarchies is the most balanced one. The different pros and cons are shown in Tab. 3.

Approach	Advantages	Disadvantages
Quantum-safe certificates	<ul style="list-style-type: none"> <li>- Only few changes of standards and applications/devices</li> <li>- Only moderate increase of certificate size</li> </ul>	<ul style="list-style-type: none"> <li>- Abrupt migration for all applications at the same time</li> <li>- No fall back in case security or implementation issues are discovered for quantum-safe algorithms in the future</li> </ul>
Hybrid certificates (variant 1)	<ul style="list-style-type: none"> <li>- Smooth transition to quantum-safe certificates</li> <li>- Combines security of pre- and post-quantum algorithms</li> </ul>	<ul style="list-style-type: none"> <li>- Needs changes of standards (e.g. RFC 5280 [Co08]) to store and verify two signatures and two public keys in a certificate</li> <li>- Size of certificates increases</li> </ul>

		the most
Hybrid certificates (variant 2)	- Combines security of pre- and post-quantum algorithms	- Abrupt migration for all applications at the same time - Needs changes of standards (e.g. RFC 5280 [Co08]) for two signatures and two public keys in a certificate - Size of certificates increases the most
Parallel hierarchies	- Only few changes of standards and applications/devices - Smooth transition to quantum-safe certificates - Only moderate increase of certificate size	- PKI software needs to be changed to manage parallel hierarchies

Tab. 3: Comparison of different approaches for quantum-safe certificates

#### 4 Impacts on eIDs

Once available, quantum computers will be able to solve certain calculations much faster than today’s computers, threatening security algorithms such as RSA and ECC. Various popular protocols like Transport Layer Security (TLS), S/MIME or PGP use cryptography based on RSA or ECC to protect data communication between computers. In this context smart cards play an important role. Smart cards have limited resources and cannot solve large key sizes. A typical smart card, that is used in an eID, has available memory around 80 Kbyte which makes the usage of large PQC resistant key sizes impossible. Another challenge – especially for eID – is the long lifetime of these documents: a usual ePassport has a lifetime of ten years. During these ten years a fundamental change of cryptographic protocols in the field is impossible.

In the field of eID the International Civil Aviation Organization (ICAO) and the German Federal Office for Information Security (BSI) have specified several cryptographic protocols that are used in eID and similar documents. ICAO has specified these protocols in Doc 9303 [IA15] and BSI in the technical guideline TR-03110 [Fe15]. A typical use case of these protocols is to sign the stored data to assure the integrity and authentication. An ePassport includes electronic information (e.g. holder information like name and birthday but also a facial image and fingerprints). This information is signed by a document signer key which is certified by the country signing certification authority (CSCA). CSCAs are root CAs whose self-signed certificates are uploaded into the ICAO public key directory (ICAO PKD) that is similar to an PKI for international exchange of these certificates. The corresponding signer keys are short-term usage keys to sign the electronic information but need to remain secure for the entire lifetime of the

ePassport. This procedure – called Passive Authentication (PA) – uses protocols for signature generation and verification of certificates based on protocols that are affected by quantum computers. ICAO Doc 9303 requires in part 12 the usage of RFC 4055 [Sc05] which specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1\_v15. A compromise of this digital signature scheme would mean fake passports and identities could be easily created. That would certainly be a nightmare for States and their border controls.

To assure that only authorized States are able to read sensitive information like fingerprints another protocol is used in context of ePassports called Extended Access Control (EAC). One key role of EAC is Terminal Authentication (TA), where the reading terminal must authenticate itself against the ePassport. And again, TA is based on certificate chains that must be verified by the chip in the ePassport. In [Fe15] you can find the algorithms and key sizes that are currently used in the field and again you can see vulnerable algorithms based on RSA like RSA-v1-5-SHA-256 and RSA-PSS-SHA-256 or ECC-based like secp256r1 or BrainpoolP512r1.

Besides signing data, the encryption and decryption of the communication between the reader and the ePassport is affected by quantum cryptography. The popular protocol Password Authenticated Connection Establishment (PACE) currently uses AES with a key size of 128 bit. As you can see in table 1, this key length is also not quantum-safe.

The trend from smart card based eID documents to mobile and virtual eIDs based on smartphones or wearables might turn out as a solution for the limitations described [Fu20]. But these mobile devices also use a kind of smart card (e.g. Secure Elements (SE) or eUICCs) as a secure hardware token to assure higher eIDAS levels of assurance.

Additionally, these problems are not limited to the area of eID. Smart cards are used in various domains like banking, health, access control etc. Most of these smart card applications are based on the international standard ISO/IEC 7816 [IS20a]. The working group behind this standard (ISO/IEC JTC1/SC17 WG4 “Generic interfaces and protocols for security devices”) recognized this risk and established in 2020 an ad-hoc working group to focus this challenge. The issue of this working group is to identify the concerned algorithms and key size and replace them by PQC-safe algorithms. With this new working group, a first step is done to migrate the eID-ecosystem to a PQC-safe era. But there might be new challenges during this migration, like new side channel attacks of new algorithms or more expensive smart cards.

## 5 Outlook

Even though the quantum threat is not yet real the transition to post-quantum cryptography should already start today. Most of the data should be secure for 10 or 15 years. Moreover, there are use cases like IoT, in which devices usually have a lifetime of more than 15 years and do not have any possibility to change the cryptographic

mechanism, once the devices are in place. Since most experts estimate a probability of 50% or higher that large-scale quantum computers will be available in 15 years, we should already start the transition to quantum-safe algorithms now.

However, before a PKI can issue quantum-safe certificates, there is still a long way in terms of standardisation and migration. First of all, before further standardisation can take place, the NIST process needs to be finished, except for use cases for which the use of stateful hash-based algorithms is suitable. Afterwards the selected algorithms will be standardised and other standards, which defines cryptographic algorithms for specific use cases (like ICAO Doc 9303 [IA15] or BSI TR-03110 [Fe15]), might adopt them. Moreover, standardised object identifiers (OIDs) need to be defined for those algorithms as well as for stateful hash-based algorithms. Transitions of other cryptographic algorithms, e.g. from DES to AES or from MD5 and SHA-1 to SHA-2, have shown that standardisation of new algorithms and migration of applications usually takes several years or even a decade.

Meanwhile, for some use cases, which are a closed system, transition to post-quantum cryptography can already be started or at least tested. One of these use cases is authentication of firmware updates. German BSI already recommends using stateful hash-based signature schemes for this use case [Fe20]. Since some vendors of Hardware Security Modules (HSM) are already offering these signature algorithms, hardly anything is left to be done before this use case can be implemented quantum-safe.

In our opinion, there is also a strong need to evaluate whether stateful hash-based signature algorithms are suitable for CSCA and Document Signer certificates. Michele Mosca introduced a very picturesque way to evaluate if there is an urgent need for transition to post-quantum cryptography for a specific use case [Mo18]. One needs to take the following three questions into account:

1. How long should your data remain confidential? This is denoted as X.
2. How long will it take to deploy post-quantum cryptography? This is denoted as Y.
3. How long will it take to build a cryptographic relevant quantum computer? This is denoted as Z.

If the sum of X and Y is shorter than Z there is time left to start the transition to post-quantum cryptography. If the sum of X and Y is larger than Z there is a serious security problem. This approach is illustrated in Fig. 3.

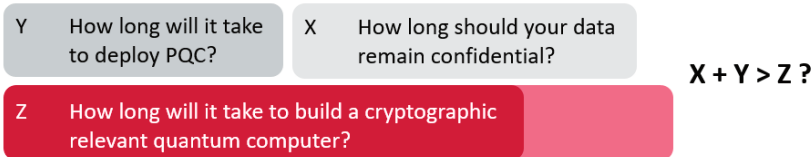


Fig. 3: Do we have to act now?

For the use case of CSCA PKI we know that X is 13 years. As we discussed in Chapter 1 we can assume Z to be 15 years and this is already a rather optimistic interpretation of quantum threat timeline report 2020 [MP21]. This shows that Y should not be larger than two years. Even if ICAO Doc 9303 [IA15] were changed today to use quantum-safe signature algorithms for CSCA and Document Signer certificates from now on, migration of CSCA systems and renewal of corresponding certificates would take more than two years. However, the longer it takes until CSCAs are quantum-safe, the more likely it becomes that passports may not be secure for their whole lifetime of ten years.

Are stateful hash-based signature algorithms suitable for CSCA and Document Signer certificates? Firstly, CSCA and Document Signers are used in a controlled environment so that it should be possible to maintain the state and do not use one state for more than one signature. Secondly, at least the parameter set for about one million signatures should provide enough signatures for that use case. Since these algorithms are believed to be quantum-safe, it is possible to use the approach of quantum-safe certificates as described in Section 3.1 for CSCA PKI hierarchy.

We conclude that there is a strong need for a fast transition to a quantum-safe CSCA PKI hierarchy and that the CSCA PKI hierarchy is suitable for the use of stateful hash-based signature algorithms.

A similar evaluation of the usage of stateful hash-based signature algorithms for PKI hierarchies of other eIDs should be done. However, as discussed in Chapter 2 there are limitations for the usage of stateful hash-based signature algorithms, i.e. number of signatures and statefulness. Hence, migration of PKI hierarchies for other eIDs to post-quantum cryptography might only be possible after NIST process is finished.

## Bibliography

- [AI20] Alagic, G. et al.: Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8309, US National Institute of Standards and Technology, 2020, DOI: <https://doi.org/10.6028/NIST.IR.8309>.
- [Co08] Cooper, D. et al.: Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. IETF RFC 5280, 2008
- [DS05] Ding, J.; Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme, International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, 2005.
- [Du18] Ducas, L. et al.: Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems: 238-268, 2018.
- [Fe15] Federal Office for Information Security (BSI): Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, 2015
- [Fe20] Website: Federal Office for Information Security (BSI): Migration zu Post-Quanten-

- Kryptografie, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf>, accessed: 13/02/2021.
- [Fo18] Fouque, P. et al.: Falcon: Fast-Fourier lattice-based compact signatures over NTRU, Submission to the NIST's post-quantum cryptography standardization process 36, 2018
- [Fu20] Holger Funke: Digital and mobile Identities. In (H. Roßnagel, C. Schunck, S. Mödersheim, D. Hühlein, ed.): Open Identity Summit 2020, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020
- [Go96] Grover, Lov: A fast quantum mechanical algorithm for database search, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996
- [Hu18] Huelsing A et al.: XMSS: eXtended Merkle Signature Scheme. IETF RFC 8391, 2018
- [IA15] ICAO: Doc 9303 Machine Readable Travel Documents, 7<sup>th</sup> edition, 2015
- [IS20a] ISO: ISO/IEC 7816 Identification cards — Integrated circuit cards, 2020
- [IS20b] ISO: ISO/IEC 9594:8 Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks, 2020
- [MC19] McGrew, D.; Curcio, M.; Fluhrer, S.: Leighton-Micali Hash-Based Signatures, IETF RFC 8554, 2019
- [Mo18] Mosca, M.: Cybersecurity in an era with quantum computers: will we be ready?, IEEE Security & Privacy 16.5: 38-41, 2018
- [MP21] Website: Global Risk Institute, <https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/>, accessed: 13/02/2021.
- [NI16] Website: National Institute for Standard and Technology: <https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms>, access: 13/02/2021.
- [OP21] Ounsworth, M.; Pala, M.: Composite Keys and Signatures For Use In Internet PKI draft-ounsworth-pq-composite-sigs-04. IETF Internet-Draft <https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/>, 2021.
- [Sc05] J. Schaad, B. Kaliski, R. Housley, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF RFC 4055, 2005.
- [Sh94] Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th annual symposium on foundations of computer science, IEEE, 1994.

# Self-sovereign identity systems and European data protection regulations: an analysis of roles and responsibilities

Andrés Chomczyk Penedo  <sup>1</sup>

**Abstract:** Decentralized identity systems have taken a key role in the identity management landscape. Self-sovereign identity management systems have promised to return control over identity to individuals. However, these promises still need to be assessed against the existing regulatory framework. As identity attributes can be considered personal data, rules such as the General Data Protection Regulation are applicable. The existing legal literature has still not delivered an analysis of who is a controller and who is a processor in the context of a self-sovereign identity system for the process of identity creation. As such, the purpose of this contribution is to tackle this challenge.

**Keywords:** digital identity, self-sovereign identity, identity management, data protection, privacy.

## 1 Introduction

Decentralized systems have taken the centre stage in the identity management landscape in the last couple of years [B119, Ab16, A116]. Although identity can be considered as a human right [A118], it is also possible to consider that the elements that compose an identity, as noted by Wang and De Filippi [WD20], are also personal data. With the rise of decentralized solutions for identity management, several legal scholars have devoted themselves to the analysis of the legal and regulatory compliance of such systems [WD20, Fi19, Wa18]. However, their analysis has focused mainly on whether blockchains and private distributed ledgers, that provide the technical infrastructure for these systems, can be compliant with data protection regulations. In this respect and to the best of our knowledge, an analysis, from a data protection perspective, of how these systems operate is still missing. Therefore, this contribution seeks to address this point.

---

<sup>1</sup> Vrije Universiteit Brussel, Department of Interdisciplinary Studies of Law (Metajuridica), Law, Science, Technology and Society (LSTS) Research Group, Pleinlaan 2, Elsene, Brussel, 1050,

andres.chomczyk.penedo@vub.be,  <https://orcid.org/0000-0002-6820-999X>

The author has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 813497.



## 2 Identity, digital identity, and the case for self-sovereign identity

Identity can be characterized as “(...) an experience of the essential consistency and continuity of the self in time and space, as well as observations and acknowledgments of existence by others” [DG18]. Identity is built upon information that allows an individual to separate itself from the rest of society and individualized itself above the whole. While there are certain aspects of an individual’s identity that might be possible to construct on a solitary basis, a considerable portion of it is built upon interactions between the individual and third parties.

### 2.1 Identity’s legal framework

The information that constitutes an identity “(...) is a collection of individual attributes that describe an entity and determine the transactions in which that entity can participate” [Ab16]. In this respect, Wang and De Filippi [WD20] argue that following the definition of personal data provided by Article 4.1<sup>2</sup> General Data Protection Regulation<sup>3</sup> (“GDPR”), the attributes of identity could be deemed as personal data. Moreover, Al Tamimi [A118] mentions that it is also possible to consider identity to be protected as a human right<sup>4</sup>.

### 2.2 What is a digital identity and its relevant legal framework?

As Kim Cameron points out, a digital identity is a set of statements that a digital subject makes about itself or another digital subject [Ca05]. These digital subjects can be either a natural or legal person as well as a thing -mainly hardware-, such as an IoT sensor. These statements are called claims, i.e., an assertion regarding the veracity of something which is usually under discussion or doubt, and are associated with a digital subject using an identifier. In this regard, and following Wang and De Filippi [WD20], if these statements are related directly or indirectly to an identified or identifiable natural person, then they would be considered as personal data.

---

<sup>2</sup> “ (...) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (...)”

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

<sup>4</sup> While his research focuses solely on European case law and regulations, his approach applies to other regional human rights systems that protect the same aspects of identity, such as the Latin American system organized, mainly, under the San José de Costa Rica Treaty as well as national regulations. Al Tamimi focuses on the rights to private life, religious freedom, and free association which are present in the San José de Costa Rica Treaty under articles 11, 12, and 16, respectively. Moreover, other rights provided in this international treaty could also serve as a base for the protection of human identities such as the right to a name or the right to a nationality in articles 18 and 20, respectively.

However, identifiers are not directly linked to claims but instead are stored in a credential, which in return can have one or more declarations [A116] and even regarding one or more digital subjects [Ca05]. Using these identifiers, it is possible to distinguish an entity from the rest. Identifiers should fulfil two fundamental requirements for them to be effective and useful: identifiers should be unique and limited in amount per field [WD20]. To achieve this, centralization has long been the answer to make identity systems useful in their purpose [A116].

### **2.3 What is self-sovereign identity and its relation to identity's legal framework?**

The process of creating a digital identity depends on how the identity system is designed; most of the current systems rely greatly upon the interaction with a centralized entity that acts as an identity provider, as Allen remarks [A116]. As such, users were and still are, vulnerable to actions that could compromise either the confidentiality, the integrity, or the availability of the information since their data, i.e., the attributes that are part of their identities, is controlled by other entities.

To solve the perils that centralization poses, the idea of self-sovereign identity (“SSI”) systems was proposed by Christopher Allen in his paper titled “The Path to Self-Sovereign Identity” [A116]. This idea puts the individual at the centre of an identity system and all actions related to identity need to be authorized by that person by consenting to that data processing activity. Giannopoulou and Wang argue that SSI systems are “(...) rooted in the belief that individuals have the right to an identity independent of reliance on a third-party identity provider, such as the state or any other central authority” [GW20].

Within this context, Allen, building upon previous work, put forward 10 principles that SSI systems should follow to be considered as such, namely: (i) existence; (ii) control; (iii) access; (iv) transparency; (v) persistence; (vi) portability; (vii) interoperability; (viii) consent; (ix) minimalization; and (x) protection. Several of the principles that Allen proposes are aligned, if not expressly recognized, with data protection principles and rights provided for by the GDPR and similar regulations. While compliance with data protection principles is mandatory for any identity management system, SSI systems can leverage the fact that their development has started after the enactment of regulations such as the GDPR. Therefore, their design and implementation can already be made following these principles rather than adapting and adjusting to them. In this respect, legal scholars, such as De Filippi and Wang [Fi19], and different reports drafted regarding SSI systems, mainly from the European Union Blockchain Observatory and Forum [B119], have also recognized that SSI systems could become an important tool, if properly deployed, to enhance and foster the rights and safeguards prescribed in data protection regulations, such as the GDPR.

Controllers could leverage the SSI system to achieve compliance with the data protection regulations. For example, the SSI system might have a template where the mandatory

information of Article 13 GDPR, or any other relevant data protection regulation, could be provided before any data collection takes place. Also, SSI systems developed with the privacy by design principle in mind could help to achieve a proper informed consent<sup>5</sup>, following the requirements set by the Article 29 Working Party (“WP29”) and the European Data Protection Board (“EDPB”) [Gu20a]. Moreover, SSI system developers proclaim that these systems could foster data subject’s rights exercise although no evidence has yet been produced regarding this.

Beyond the identity creation process, the use of the data associated with that identity constitutes a data processing activity that is subject to data protection regulations. If an individual is requested for certain information regarding its identity to provide a service, that activity triggers the applicability of, for example, the GDPR. If the SSI system works properly, the individual would have greater control over how their data is used because they will know in greater detail which data was requested as well as for which purposes but compliance with GDPR still is necessary for the data processing activities carried out by the relying parties on such identity.

The use of blockchain and distributed ledger technologies is not necessary for the development of an SSI system although its use is aligned with some of the guiding principles stated by Allen [GW20]. However, if these technologies are used, then all identified issues, and proposed solutions, regarding data protection regulations should also be considered to make the system and its use compliant with the GDPR

### **3 How are roles in an SSI system assigned under European data protection regulations?**

Recital 79 GDPR states that “[t]he protection of the rights and freedoms of data subjects (...) requires a clear allocation of the responsibilities under this Regulation (...)”. The question proposed in the headline is, therefore, of the uttermost importance and should be the starting point for any debate around how the SSI system should comply with European data protection regulations or any other piece of legislation related to data protection.

The answer to this question could help policymakers, practitioners, and academics in addressing other data protection-related issues regarding SSI systems. Identity management systems are complex; there are several data processing activities taking

---

<sup>5</sup> Since a great deal of importance is placed on fostering consent-based interactions through SSI systems, it is possible to further overload data subjects with consent requests, albeit in a different format, that could result in a situation not that different from the current crisis that consent is undergoing or, even worse, further deepen it, as well as causing information fatigue [SC14]. Following with this, information, according to the existing interpretation from authoritative bodies [Gu18], needs to be tailored in several manners: from timing to wording as well as structure, keeping always in mind the intended audience. SSI systems proclaim that, through them, data subjects can have complete knowledge about how and who will make use of their data. However, the effectiveness of this mechanism for this purpose still needs to be tested.

place at the same time and, often, they are interconnected [Ab16]. To properly answer this question, it is possible to differentiate between the roles performed for the creation and operation of digital identities, mainly credentials and identifiers, and, on the other hand, the roles of the infrastructure used to operate the SSI system. Since the latter has been addressed by legal scholars, see e.g. [Fi19], focus for this contribution shall be placed on the former. Moreover, and as mentioned above, the specific usage of an identity created and operated through an SSI system can also be analysed under the lens of data protection regulations, but that analysis is beyond the purpose of this contribution.

### **3.1 Roles in the creation and operation of a digital identity within an SSI system**

SSI systems do not function statically as they are intended to operate relying upon a horizontal model of equality between all participating actors [Wa18]; in this regard, it is possible to say that SSI systems intend to escape the hierarchical relationship with which the GDPR, and many other similar regulations, was conceived, i.e., the controller/data subject structure. By looking into some of the most relevant projects and technical standards under development [DI20] and taking into consideration the previously mentioned principles, it is possible to outline some common features among SSI systems to answer the proposed question.

In this regard, and for this contribution, the following operational structure for the identity creation process of a hypothetical SSI system is proposed: (i) any individual might make claims about themselves and add such claims into a credential issued by them; (ii) individuals and legal entities might make claims about other individuals and add such claims into a credential issued by them; (iii) the credential might be held by a different entity than the individual that the credential refers to; (iv) the credential is stored in a medium under complete control of the holder (v) individuals are allowed to self-issue identifiers, in particular, decentralized identifiers; and (vi) a verifiable data registry using a public distributed ledger is used for facilitating the managing of identifiers and claims. The proposed structure could be used by both trusted identity providers as well as individuals interacting on a peer-to-peer basis.

### **3.2 Who can be a controller in an SSI system?**

Identifying the controller within the context of certain data processing activity is of the uttermost importance since “(...) they are the primary bearers of the obligations set by such law towards data subjects” [Kr20]. To answer this first question, it is possible to start with the definition of data controller provided by Article 4.7 GDPR<sup>6</sup>.

---

<sup>6</sup> “(...) means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its

To interpret this concept, EDPB has recently published the update to WP29's Opinion No. 1/2010 regarding the concepts of controller and processor in the GDPR [Gu20b]<sup>7</sup>. As it is pointed out in that guidance, there are 5 core elements to the concept of controller: (i) the entity that determines the processing; (ii) the actual determination of the processing; (iii) whether the determination is done solely or jointly with other; (iv) which purpose and means are determined; and (v) the determination of the process itself. WP29 characterized the role of the controller by stating that it was the entity that dictated the information lifecycle, from its collection to its destruction [Op10]; although this characterization with those exact words is missing in EDPB's guidelines, the idea remains present due to the relevance of the determination.

The process of determining who is a controller demands a fact-based answer where a considerable number of factors play into account [Kr20]. SSI systems intend to put people in control of their identity. Following EDPB's criteria, the information lifecycle would be dictated by the individual, i.e., the purposes and means for processing personal data would be selected by a person. In this context, the only one legally authorized to arrange the creation, maintenance, and operation of a digital identity would be that individual. As mentioned above, EDPB follows closely the criteria set forth by WP29 and expands upon it due to recent developments in the caselaw from the Court of Justice of the European Union ("CJEU")<sup>8</sup>.

Regarding the first criteria, Article 4.7 GDPR allows for natural persons to be controllers; therefore, an individual might be considered as such. Being able to determine a processing activity implies that an entity has influence, either legal or factual, to choose why data are processed. In this respect, an individual meets both criteria. Identity is a right that is recognized to an individual and only that individual is legally authorized, unless a specific provision applies to the case such as the case of parents over their children, to act over such identity. On a factual basis, only that person should be in the position to decide about their own identity.

As for the last two criteria -the purposes and means, and the processing itself- the EDPB elaborates on the ideas drafted by WP29. In this regard, EDPB upholds that purposes and means, from a data protection perspective, constitutes why and how a data processing activity takes place; therefore, to qualify as controller, it is necessary to choose the objective for which data shall be processed and, also, the technological resources that shall be used to that end [Gu20b]. However, not all means are equally important and, as

---

nomination may be provided for by Union or Member State law (...)"

<sup>7</sup> As of the date hereof, the document is still under public consultation period and changes could occur.

<sup>8</sup> In this respect, we are referencing to the following cases: Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV., ECLI:EU:C:2019:629 (Court of Justice of the European Union (Second Chamber) 2019); Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta, ECLI:EU:C:2018:551 (Court of Justice of the European Union (Grand Chamber) 2018); and Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388 (Court of Justice of the European Union (Grand Chamber) 2018).

such, only those that could be deemed as essential would be important enough to meet the standard to qualify as controller [Gu20b].

Nevertheless, individuals are in the perfect position to choose why their identity data becomes part of a credential and then, attach it to a decentralized identifier -determination of purposes- and it is up to them the selection of the tools, i.e., picking a platform, selecting a wallet to store credentials, etc., that would be essential to this activity -determinations of means-. Finally, as for the processing itself, data subjects would be the ones choosing whether to enrol in this identity management solutions and, as such, determining the activity to be performed upon their data.

However, and as the literature points out, if an individual merely processes their personal data, then the GDPR -as well as any other data protection regulations based upon it or with a similar structure- would not be applicable; this is because data protection regulations, such as the GDPR, need the existence of two separate entities that act as controller and data subjects, respectively, to be applicable, see e.g. [Kr20]. It is appropriate to ask and try to answer whether an individual is a controller, therefore rendering the inapplicability of the GDPR or similar data protection regulations, or if other entities involved in these data processing activities, would-be controllers.

As for the first question, while it is possible for an individual to become a controller of personal data and the case law from the CJEU seems to be inclined in the direction of expanding the consideration of individuals as controllers [Ed20], it is not so clear that data subjects can become controllers of their data. In a sense, as Bygrave and Tosoni point out, the whole purpose of data protection regulations is “(...) to protect others’ interest (i.e., those of data subjects), not their own (...) In essence, it would seem logical that a controller must be some party other than the data subject” [BT20a]. As such, at least what respect to the identity creation process under analysis herein, individuals would not be considered as controllers regarding their own identities. The WP29 pointed out that the assignment of the role of the controller should be to help data subjects to have a clear entity to demand their rights [Gu20b]. In this regard, a question that could be asked is if the shift of controllership to an individual, i.e., traditional data subject in any other identity system, is acceptable or not, but this falls beyond the scope of this contribution.

It is possible to wonder if other entities, including other individuals, can be controllers in the identity creation processes. In contrast to the situation presented above, the alternation needed to trigger the applicability of the GDPR exists. Therefore, any other person who intends to do that -create and operate a digital identity- would incur into a data processing activity as it would be determining purposes and means. However, an individual might be a controller but could be exempt from complying with the GDPR. In this regard, Article 2.2.c.<sup>9</sup> GDPR -the personal or household exemption- could be used in certain situations. For example, a legal representative of a child could be considered as a

---

<sup>9</sup> “(...) 2. This Regulation does not apply to the processing of personal data: (...) (c) by a natural person in the course of a purely personal or household activity; (...)”

controller as the individual, i.e., the child, would not be processing its data to construct its identity but instead, this would be done by a third party, e.g., their legal representative. This exemption needs to be interpreted when it is applied to a particular case. To do so, it is possible to rely on Recital 18 GDPR<sup>10</sup>.

According to it, it shall be necessary to pay particular attention to the legal relationship between the individuals involved in the processing activity to address the type of data protection relationship which they will have. In other words, and as Recital 18 GDPR states, if the bond between controller and data subjects does not imply a commercial or professional relationship, the personal or household exemption would be applicable. Legal literature commenting on the existing caselaw of this exemption under the former European data protection directive, whose wording is mimic by the GDPR and therefore its analysis relevant to it, is inclined in this respect [Kr20]. In this sense, a parent managing the digital identity of their child may fall within the household exemption while the management of digital identity by the guardian of an insane would not and, therefore, it would be a controller that shall need to comply with the GDPR.

Generally, it is possible to conclude that the individual would not be considered a data controller regarding the issuance of their credentials. When it comes to the issuance of credentials and the association of such credentials to a decentralized identifier for those with whom it shares a family bond, the household exemption would be applicable. As for other entities that process personal data related to an individual's identity, that processing operation would constitute a data processing activity that would imply considering that entity as a controller as it is defining purposes and means.

### **3.3 Who can be a processor in an SSI system?**

While the core data processing activity in an SSI system would be the operation of credential issuance and pegging to a decentralized identifier, it is possible to mention that other activities are secondary to that: from the validation of claims to the storage of credentials or their presentation. However, the main shared characteristic among these is that none of them, in principle, implies the determination of purposes and means. Any entity conducting those activities could be considered as a processor. As EDPB denotes, “[t]he role of a processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context (...) In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means (...)” [Gu20b].

---

<sup>10</sup> “This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.”

As for this second question, it is possible to follow the same path as before by relying on the definition of data processor as prescribed in Article 4.8 GDPR<sup>11</sup>. EDPB rightly points out that what matters to determine if an entity is a processor is a decision of by a controller -in this case the individual- to delegate into a third-party certain processing activity per its instructions, i.e., there needs to be some act of delegation by the controller in favour of the processor [Gu20b]. As Bygrave and Tosoni mention, to consider an entity as a processor, there needs to be an entity acting as a controller to impose processing conditions [BT20b]. However, if the processor, going against the mandate given by the controller, determines for what and how will data be processed, then that entity would have crossed the threshold and would become a controller [Op06].

If the controller is not the data subject or an individual that can rely on the exemption provided for in Article 2.2.c, there is no doubt that the full extent of the GDPR applies and that the processor would have to comply with the GDPR. However, if the data subject or an individual that can rely on that exemption is the controller, does the processor still has to comply with the GDPR? The fact that the controller is exempt from complying with the GDPR does not imply that exemption should be extended to the processor as the exception must be interpretive restrictively and as it only covers the controller, as noted by Recital 18 GDPR [Kr20].

Certain regulated activities, such as the services covered by the eIDAS Regulation<sup>12</sup>, have a logical connection with SSI systems [Al20]. The question of how the eIDAS Regulation should be applied to the SSI system is on itself a topic that exceeds this contribution and one which there is no answer yet from authoritative bodies. Nevertheless, it is possible to ask if a trust service provider can be considered as a processor for the controller or whether it is a controller due to the determination of purposes and means. The literature is inclined towards considering trust services providers as controllers as a trust service provider is the sole responsible for how its business shall be run, i.e., it is the one that determines purposes and means for the processing of data [Ts16]. However, given that within an SSI system context, data processing activities are constraint to what the individual allows, trust service providers would have their autonomy severely limited but also due to what the developers of the software have permitted within the code over which an SSI system runs.

### 3.4 Are the developers of an SSI system controllers, processors, or something else?

Software developers are in a particular situation in *peer-to-peer* solutions<sup>13</sup>. Therefore, it

---

<sup>11</sup> "(...) the natural or legal person, public authority, service or other body that processes personal data on behalf of the controller (...)".

<sup>12</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

<sup>13</sup> In the field of decentralized finance, there is an ongoing discussion on whether developers have to comply with applicable financial regulations if they can be considered as the prime responsible for it [Va19].



is possible to ask if developers are determining means and purposes from a data protection perspective in the case of an SSI system. Although software developers through their code condition and limit what users can do with the software in question by only making it useful for certain activities done in a certain way, such limitation is not sufficient to consider that purposes and means have been selected for the user. For example, none would even think about considering Microsoft as a controller over users for the provision of a copy of Word installed on a home computer. Users of SSI systems are free, first, to use them and, second, to select which attributes of their identity would be uploaded.

However, if developers operate in any manner the SSI system, this argumentation falls short as there is some form of determination of processing activities as well as purposes and means. As such, a middle ground solution could be considering the existence of a joint controllership with the data subject. The CJEU has already ruled in certain cases that individuals can be joint controllers with other, either persons or legal entities [Ed20]. The trouble with this approach is twofold. On one hand, the fact that the individual cannot be the controller of their data is still on the table, as noted above. On the other hand, and according to EDPB, joint controllership must result from a converging decision, i.e., the purposes and means selected by each entity have a symbiotic relationship between each other and result in a single larger data processing activity [Gu20b]. This solution might be relevant for those cases where the controller is someone besides the person that their credentials refer to, as described above.

Developers could be considered as data processors by proving resources to the individual to carry out all activities related to the creation and maintenance of the credential. In this regard, as pointed out by Recital 18, software developers might be processors. As for guidance on this matter, the EDPB has not addressed the situation in their guidelines regarding the concepts of controller and processor; the only piece of advice given by EDPB that could be somehow used for further interpretation is provided as an example of an IT consultant that incidentally process personal data and where the entity that request the provision of such software development activity assumes any liability arising from such performance by a third party [Gu20b].

## 4 Conclusions

Decentralization and peer-to-peer relations have shaken regulations as most of our legal systems are structured around the identification of an accountable entity. In the case of existing European data protection regulations, the question regarding how SSI systems can reach compliance, if possible at all, with them is still an open question. While these types of identity management systems are intended to foster users' control over their identity personal data, the actual details on how to implement them in a compliant manner demand further analysis and, most important, guidance from authority bodies.

In this contribution, some insights were provided for this endeavour regarding the process of identity creation: (i) individuals can build and operate their own identity and would not be data controllers of such process; (ii) individuals and legal entities building and operating other people identities can be both data controllers or processors, depending on the situation, although in certain cases exempt from having to comply with these regulations, as in the case of parents for their children identity; and (iii) SSI systems developers would most likely be exempt from the application of data protection regulations as data controllers or processors unless they engage in building or operating those identities in any manner whatsoever.

Although the discussion is still open, there is one thing that is clear among the overall uncertainty: any action taken needs to put individuals at the front and avoid making existing, functioning, and tested pieces of regulation not applicable. In this respect, any SSI system should keep its focus on the founding principles of them: individuals should be able to seek legal remedy against any wrongdoing over their identity and not putting burdens on them.

## Bibliography

- [Ab16] A Blueprint for Digital Identity. World Economic Forum, Aug. 2016.
- [Al16] Christopher, Allen. The Path to Self-Sovereign Identity. *Life With Alacrity*, 25 Apr. 2016, <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>, date accessed February 15, 2021.
- [Al18] Yussef, Al Tamimi: Human Rights and the Excess of Identity: A Legal and Theoretical Inquiry into the Notion of Identity in Strasbourg Case Law. *Social & Legal Studies*, vol. 27, no. 3, pp. 283–98, June 2018.
- [Al20] Ignacio, Alamillo Domingo. How EIDAS Can Legally Support Digital Identity and Trustworthy DLT-Based Transactions in the Digital Single Market. European Commission, Apr. 2020.
- [Bl19] Blockchain and Digital Identity. EU Blockchain Observatory and Forum, 2 May 2019.
- [BT20a] Lee, A., Bygrave, and Luca, Tosoni. Article 4(7). Controller. *The EU General Data Protection Regulation (GDPR) A Commentary*, edited by Christopher, Kuner et al., 1st ed., Oxford University Press, pp. 145–56, 2020.
- [BT20b] Lee, A., Bygrave, and Luca, Tosoni. Article 4(8). Processor. *The EU General Data Protection Regulation (GDPR) A Commentary*, edited by Christopher, Kuner et al., 1st ed., Oxford University Press, pp. 157–62, 2020.
- [Ca05] Kim, Cameron. *The Laws of Identity*. May 2005.
- [DG18] Dragana, Deh and Danica Glodović: The Construction of Identity in Digital Space. *AM Journal of Art and Media Studies*, vol. 16, pp. 101–11, 2018.
- [DI20] Decentralized Identity, <https://github.com/decentralized-identity/decentralized-identity.github.io/blob/master/assets/map-of-adjacent-orgs-and-specs--sept-2020--one->

- [sided.pdf](#), date accessed February 15, 2021.
- [Ed20] Lilian, Edwards, et al. Data Subjects as Data Controllers: A Fashion(Able) Concept? Internet Policy Review. *policyreview.info*, <https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400>, date accessed April 9, 2021.
- [Fi19] Michèle, Finck. Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?, European Parliament, 2019.
- [Gu18] Guidelines on Transparency under Regulation 2016/679. WP260 rev.01, Article 29 Working Party, 11 Apr. 2018.
- [Gu20a] Guidelines on consent under Regulation 2016/679. 05/2020, European Data Protection Board, 2 Sept. 2020.
- [Gu20b] Guidelines on the Concepts of Controller and Processor in the GDPR. 07/2020, European Data Protection Board, 2 Sept. 2020.
- [GW20] Alexandra, Giannopoulou and Fennie, Wang. Self-sovereign identity. Glossary of distributed technologies. Internet Policy Review. *policyreview.info*, <https://policyreview.info/glossary/node-1524>, date accessed April 9, 2021.
- [Kr20] Herke, Kranenborg. Article 2. Material Scope. The EU General Data Protection Regulation (GDPR) A Commentary, edited by Christopher, Kuner et al., 1st ed., Oxford University Press, pp. 60–73, 2020.
- [Op06] Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). WP128, Article 29 Working Party, 22 Nov. 2006.
- [Op10] Opinion 1/2010 on the Concepts of ‘Controller’ and ‘Processor’. WP 169, Article 29 Working Party, 16 Feb. 2010.
- [SC14] Bart, W., Schermer, and Bart, Custers. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. *Ethics and Information Technology*, vol. 16, no. 2, p. 12, June 2014.
- [Ts16] Niko, Tsakalakis, et al. What’s in a Name: The Conflicting Views of Pseudonymisation under EIDAS and the General Data Protection Regulation. *Gesellschaft für Informatik*, 2016, pp. 167–74.
- [Va20] Peter, Van Valkenburgh. Electronic Cash, Decentralized Exchange, and the Constitution. *CoinCenter*, Mar. 2019.
- [Wa18] Kai, Wagner, et al. Self-sovereign Identity A position paper on blockchain enabled identity and the road ahead. Identity Working Group of the German Blockchain Association, 23 Oct. 2018.
- [WD20] Fennie, Wang and Primavera, De Filippi: Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, vol. 2, p. 28, Jan. 2020.

# Adapting the TPL Trust Policy Language for a Self-Sovereign Identity World

Lukas Alber,<sup>1</sup> Stefan More,<sup>2</sup> Sebastian Mödersheim,<sup>3</sup> Anders Schlichtkrull<sup>4</sup>

**Abstract:** Trust policies enable the automated processing of trust decisions for electronic transactions. We consider the Trust Policy Language TPL of the LIGHT<sup>est</sup> project [Mö19] that was designed for businesses and organizations to formulate their trust policies. Using TPL, organizations can decide if and how they want to rely on existing trust schemes like Europe’s eIDAS or trust scheme translations endorsed by them. While the LIGHT<sup>est</sup> project is geared towards classical approaches like PKI-based trust infrastructures and X.509 certificates, novel concepts are on the rise: one example is the self-sovereign identity (SSI) model that enables users better control of their credentials, offers more privacy, and supports decentralized solutions. Since SSI is based on distributed ledger (DL) technology, it is a question of how TPL can be adapted so that organizations can continue to enjoy the benefits of flexible policy descriptions with automated evaluation at a very high level of reliability.

Our contribution is a first step towards integrating SSI and the interaction with a DL into a Trust Policy Language. We discuss this on a more conceptual level and also show required TPL modifications. We demonstrate that we can integrate SSI concepts into TPL without changing the syntax and semantics of TPL itself and have to add new formats and introduce a new built-in predicate for interacting with the DL. Another advantage of this is that the “business logic” aspect of a policy does not need to change, enable re-use of existing policies with the new trust model.

**Keywords:** Trust policies, Accountability, Security, LIGHTest, eIDAS, SSI

## 1 Introduction

Automated trust decisions are an essential component of many business and government processes. When Alice sends an electronic transaction to Bob, the latter must verify Alice’s signature on the transaction, in particular, that it is the person claimed here and it is legally binding. That, in turn, relies on trust in the organization that certified Alice in terms of a credential or in an organization that translates this trust in some way. Bob’s prerogative is to determine his policy, i.e., which issuers or trust schemes to trust and what requirements to ask from Alice.

---

<sup>1</sup> Graz University of Technology, Inffeldgasse 16a, Graz, Austria lukas.alber@iaik.tugraz.at

<sup>2</sup> Graz University of Technology, Inffeldgasse 16a, Graz, Austria stefan.more@iaik.tugraz.at

<sup>3</sup> Technical University of Denmark, DTU Compute, Richard Petersens Plads, Bygning 324, 2800 Kongens Lyngby, Denmark samo@dtu.dk

<sup>4</sup> Aalborg University Copenhagen, Department of Computer Science, A.C. Meyers Vænge 15, 2450 Copenhagen SV, Denmark andsch@cs.aau.dk

The trust verification system introduced by the LIGHT<sup>est</sup> project [BL16] enables this: a high level of assurance, a rich and flexible Trust Policy Language (TPL), and automated policy verification. In this context, the term *transaction* is used in a quite liberal way: it can include, for instance, a bid in an auction house or a simple login at an online system.

The Trust Policy Language was introduced by Mödersheim et al. [Mö19] inspired by existing concepts of trust policy systems [BFG10; DD10; GN08; He00; LFG99]. Using a policy language is obviously more flexible and declarative than rules hard-coded in an implementation. TPL is in particular based on logic-programming and uses a Prolog-style syntax and semantics, allowing to separate “business logic” from lower-level aspects of the evaluation like interfacing with trust servers.

Centralized trust and identity management approaches represent an attractive target for criminals and cyber war [Fr20]. Furthermore, storing identity data in centralized data silos increases the likelihood and impact of data breaches [Be17; Be20; Th17]. For this reason, in recent years, more decentralized trust management architectures caught the research community’s attention.

Our goal is to integrate support for such modern identity solutions with TPL and trust policies in general. We focus on two concepts: distributed ledgers (DL) and self-sovereign identity (SSI). DLs decentralize storage and governance helps to mitigate issues like a single point of failure, split-world attacks, and the loss of identity retention [Ko20]. SSI describes the concept of storing identities decentralized at the owner, also called holder, instead of centrally at an identity provider. The SSI community furthermore introduced several concepts regarding credentials [SLC19] and identities [Re21; SS20] while ensuring interoperability, privacy, and decentralized storage by combining SSI with DLs and other promising technologies (e.g., zero-knowledge proofs).

In this paper, we present a vision of bringing LIGHT<sup>est</sup>’s world of automated trust decisions together with novel concepts of SSI and DLs. Our contribution is to show how this integration can be made without changing the syntax and semantics of TPL itself. That has several advantages. First, the tools based on TPL do not need substantial modification: the logical evaluation stays the same, and only new modules for the interfacing with the DL and parsers for new document formats are needed. Indeed, the connection of the theorem prover  $RP_X$  that provides LIGHT<sup>est</sup> trust decisions with an independent verification does not require any changes. Second, a policy’s “business logic” does not have to change either. That makes it possible to formulate policies accepting classical eIDAS credentials and modern SSI-credentials in a uniform way, making the lower level only a “technology-choice”.

The rest of this paper is structured as follows: In Sect. 2 we give an overview of DL and DL-based Trust Management, SSI, and TPL. We discuss our position on extending TPL for the DL/SSI world in Sect. 3 and show the extension by example in Sect. 4. We discuss the support of additional SSI concepts and conclude the paper in Sect. 5 with an outlook into a concrete implementation.

## 2 Background

**Distributed Ledger (DL)-based Trust Management** A distributed ledger (DL) is a decentralized data storage model. The data is stored redundantly at several distributed nodes maintained by different entities, improving resilience. Each node preserves independent control, and they agree on a common state by running a consensus protocol [Xi20]. A DL is often referred to as “blockchain”, although it indicates a subset of the ledger technology. Access-wise, DLs support a large spectrum of models, mostly grouped and described by the terms public, private, permissionless, and permissioned [Zh18].

The **Self-Sovereign Identity (SSI)** community aims to replace centralized or federated identity concepts [ZZS14] with a decentralized model, i.e., keeping the identity in the holder’s sole possession [Ab17]. In the SSI model, a user creates a **Decentralized Identifier (DID)** for its identity [Re21; SS20] and publishes it by defining a DID document (DIDoc) containing the DID, a corresponding public key, and other application dependent information. That is often done using a DL.

The vision of SSI is that any party can certify attributes of any other party, e.g., a higher education institution can accredit graduation to a student, or an interior ministry can attest someone’s date of birth. For such certifications it is common to use the **Verifiable Credentials (VCs)** data model [SLC19]. This specification defines a generic way of packaging claims and the corresponding issuing authority in a signed JSON document.

**Trust Policy Language (TPL)** In a previous publication [Mö19], we introduced TPL to enable service providers to flexibly define and run an automated process for deciding when to accept a transaction, e.g., based on whether the signatures and certificates that come with the transaction are sufficient for the service providers to consider the transaction’s sender trustworthy. TPL was initially created in the context of the LIGHT<sup>est</sup> project [BL16; Ro17; Wa19].

A TPL policy is a list of Horn clauses in the syntax of Prolog. Each Horn clause is in the form  $p(t) :- q_1(u_1), \dots, q_n(u_n)$ . meaning: if all the  $q_i(u_i)$  are true, then also  $p(t)$  is true. We refer to the Horn clauses as rules. A set of rules of the form  $p(t) :- q_1(u_1), \dots, q_n(u_n)$ . for the same  $p$  defines the *predicate*  $p$ . Rules can be evaluated in the same way as Prolog would: To see if a query  $p(s)$  succeeds, find a suitable rule; e.g. the above  $p(t) :- q_1(u_1), \dots, q_n(u_n)$ . if  $s$  and  $t$  can be unified. Then apply the resulting unifier to all  $q_i(u_i)$  and evaluate them; if the evaluation for the subqueries evaluates to success, then we say that the original query also evaluated to a success. If that is not the case, then try again with the next suitable rule if any such exists. The subqueries are evaluated in the same way by recursion, except for the case where a  $q_i$  is a so-called built-in predicate, i.e., a predicate that interacts with, e.g., servers or formats. In that case, the interaction is performed, which either results in a success or a failure. We notice that the rules define the policy in a positive way: the transaction is rejected

if and only if in every applicable rule at least one of the conditions is not met. For a policy where the above procedure takes too long, we reject the transaction based on a timeout.

TPL features built-in predicates which essentially wrap context-specific discovery and verification logic. In the LIGHT<sup>est</sup> context that includes all the interactions with Europe's eIDAS and comparable trust schemes. The Automated trust discovery and the verification of trust status information use DNSSEC [Ar05] for security and authenticity protection. Therefore, the application of TPL in LIGHT<sup>est</sup> focused on centralized PKI, although means for a trust translation between different trust schemes have been presented. For a more in-depth description see our previous publication on the topic [Mö19]).

### 3 Concept

In this section, we introduce our vision of an SSI extension to the TPL system. We give an overview of the process flow typical in the SSI world to create and register an identity, acquire credentials of identity attributes, provide them with legal value, and use these credentials to authenticate at service providers (SPs). At the same time, we show how this flow integrates into the TPL infrastructure. Further, we discuss the policy system's functionalities and show the extensions needed to support the described SSI model. Finally, we conclude the chapter with a discussion on the consequences concerning accountability of integrating TPL with SSI.

#### 3.1 Step by Step Flow

To derive qualified identity credentials for our purpose in SSI, we utilize the process introduced by Abraham et al. [Ab20]. A holder (user holding a credential) needs to generate a decentralized identifier (DID), and a corresponding DID document, let the DID document get registered at a DL, and acquire legal identity credentials. Only then the holder can attempt to authenticate herself to a service provider (cf. Fig. 1).

To **generate a DID**, the holder first generates a public/private key pair. From the public key, they derive a decentralized identifier (DID) that can refer to them as the holder in a privacy-friendly way. The holder can then choose what credentials she wants to obtain for this DID, e.g., one certifying only their birth date.

To **acquire credentials** for their identity attributes, the holder first authenticates at an Identity Provider (IdP) such as their government's E-ID system. Additionally, the holder needs to prove the ownership of their DID to the IdP. That is done by initiating a challenge-response protocol with the IdP using the holder's DID keys. The IdP then uses the public key from the transmitted DID document to verify the signature that resulted from the challenge-response. After the holder has successfully proven the ownership, the IdP system generates various identity credentials. Each of those credentials contains one of the holder's identity attributes.

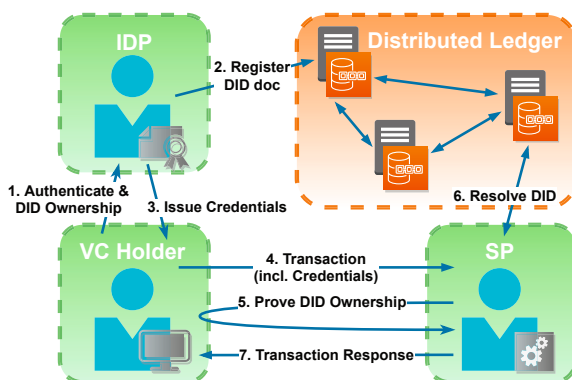


Fig. 1: Architectural overview of our concept. After retrieving credentials from the identity provider (IdP), the VC Holder sends an electronic transaction (including the verifiable credentials) to the service provider (SP) and proves ownership of their DID. The service provider then uses an Automated Trust Verifier (ATV) to interpret the TPL policy, resolve the DID document using a DL, and forms an automated trust decision about the transaction.

The VCs are bound to the holder by adding their DID as a credential subject. The IdP system signs the credentials and sends them to the holder. The IdP also adds the holder's DID documents to the DL, enabling retrieval by all other nodes.

Using SSI, a holder can now **authenticate to a service provider** with the registered DID and the obtained identity credentials. First, the holder provides one or more identity credentials to the service provider, which the service provider can use for authentication. The holder also provides additional transaction information, signed with the secret key corresponding to their DID. The holder also proves their DID ownership to the service provider by including a challenge provided by the SP in the signed transaction. To verify the signature on the transaction, the service provider discovers and retrieves the holder's DID document from the DL and uses the contained public key. To ensure a qualified issuer issued the holder's identity credentials, the service provider needs to **authenticate the issuer**. In our case, the issuer is the IdP. That ensures that the IdP is indeed a qualified issuer and that it indeed signed the credentials. If this authentication succeeds, the service provider trusts the attributes contained in the credentials.

In LIGHT<sup>est</sup> this authentication uses a trust infrastructure, e.g., the eIDAS trust scheme. To that end, the service provider uses an automated trust verification system (ATV). The ATV uses TPL to interpret the holder's policy that enables the definition of custom trust rules. TPL's built-in predicates allow specifying queries to servers that the ATV must perform.

**Adding SSI Support:** To support the SSI model, we introduce the new built-in predicate `resolveDID`. With this predicate, users can create policies that use information stored on the



DL (cf. Sect. 3.3). Further, we add support for several SSI data-structures by introducing new TPL *formats* for each of them (cf. Sect. 3.2).

We show that all necessary modifications can be made within the extensible built-in predicate and formats system of TPL. Hence, no syntax changes are needed, and formal properties of TPL and the accountability of policy evaluations are not weakened, as shown in Sect. 3.4.

### 3.2 New TPL Formats

In TPL, the concept of formats is used to connect policies with parsers that extract values from complex data formats and ensure compliance with data schemas [Mö19]. These values can be concrete numbers, constants, or of some format themselves. The `extract` predicate is used in a policy to extract values, e.g. we write `extract(Form, certificate, Certificate)` to extract a certificate from a form into the variable `Certificate`. The special key `format` is used to specify what format we expect, e.g. we write `extract(Certificate, format, x509)` if we require the certificate to be an x509 certificate. Consequently, to make additional data used in SSI accessible in TPL, we introduce two new formats:

`ssi_credential` is the format for Verifiable Credential (VC). The format contains the VC's fields and supports verification of the VC's signature. For example, if we have a VC with a `birthday` attribute, we can directly call `extract(Credential, format, ssi_credential)`, `extract(Credential, date_of_birth, Birthdate)` to extract the birthdate to the variable `Birthdate`. This is only an example: different formats for different *VC contexts* can exist.

`ssi_diddoc` is the format for DID Documents. It contains names from the name-value of the DID Document. For example, if we want to access a corresponding public key, we specify `extract(DIDDoc, format, ssi_diddoc)`, `extract(DIDDoc, pk, PK)`. Similar to the `ssi_credential` format, for each context different a DID document format may exist, supporting different versions of the DID specification (such as `w3id.org/did/v1`).

### 3.3 New TPL Predicate

Built-in predicates wrap functionality that is executed by the ATV and not inside TPL, such as lookups and signature verifications. Built-in predicates may return their result in the variables that have been passed to the call (output parameters). For our extension to SSI, we introduce one additional built-in predicate:

`resolveDID(DID subject, min_blockage, out: DID document)` takes three arguments: The first argument is the DID to resolve. The second argument specifies the minimal age of the block. On call, the ATV will try to look up the DID document at the DL and, on success, return the result to the last argument's variable. If a ledger-based system (like in this paper) is used, the block age parameter can be seen as a choice of assurance level regarding the

DID document because a young block could be dropped as the blockchain grows, while an older block is more established and is unlikely to drop out. That means the higher number we choose, the more sure we will be that the block is not dropped.

### 3.4 Verification and Accountability

In [SM20] we investigated how we can formally verify aspects of trust decisions and make them accountable: for instance, in case a business transaction enters a legal dispute, it is valuable to have a precise argument available consisting of all data, especially involved credentials, and the policy rules upon which a decision was made.

Obviously, there are several problems that such a package cannot solve. First, the author of a trust policy may have made a mistake so that the trust policy does not truly reflect the business or organization's needs. Second, there may be problems in the implementation, like an overflow problem in a document parser. Third, especially when we look at an electronic document decades in the future, today's cryptographic algorithms like signature schemes may be broken. Fourth, when retrieving trust information from a server, it may be later impossible to prove that this server indeed gave a particular answer at the time of the policy decision. Here distributed ledger technology can give an advantage (and partially also with respect to the third problem) because it has interesting archival properties since as long as all but the few latest blocks are undisputed, we can reconstruct the state at every given point in time. Moreover, due to the distributed nature, we do not rely on a single party (that could, e.g., be hacked or out of business). However, with the distributed ledger technology come also different problems, most notably, a policy decision is made with respect to a block that has not yet "aged" sufficiently and is ultimately not included in what becomes the accepted chain of blocks. For this reason, we add the `min_blockage` parameter to the new `resolvedDID` predicate to specify which block age is required for relying on an entry.

A problem we can solve concerns the correct implementation of trust policy's semantics in the decisions of the automated trust verifier ATV. Suppose, due to a bug, the ATV accepts a transaction that should be rejected according to the policy semantics. Building on the paper by Schlichtkrull; Mödersheim [SM20] results in a solution to this problem: the ATV records a *proof certificate*, i.e., a package consisting of a set of relevant facts about the transition, the state of the world at the given time, and the policy; then one can *check* if the acceptance indeed logically follows from the policy using an independent and verified software tool named  $RP_X$  introduced by Schlichtkrull et al. [SBT19; Sc20]. It is extremely unlikely that a logical mistake in the ATV decision process gets erroneously accepted by this "independent pair of eyes". In particular, we have no semantic gap, as the semantics of TPL rules can directly be formulated as first-order sentences, and thus in the native language of  $RP_X$ . Since this logical deduction is independent of the concrete technology (like formats and cryptography) that implements the facts, it works immediately with the extensions of TPL for SSI and DL.

## 4 Age Verification Example

We now give an example of the concept introduced in Sect. 3. To illustrate the concepts, we use a social online platform for teenagers. In this fictional platform, teenagers can join without revealing their legal identity, but they need to be in their teens (older than 12, not older than 18) to ensure only teenagers participate in the discussions. Since other identity attributes of the teenagers are not relevant, it is sufficient to provide an *age credential*. This age credential only contains the date of birth of the teenager and no further information.

The age credential is a VC containing the user's DID as subject and the date of birth encoded in the credential's `credentialSubject` field. To add (legal) value to the credential, a qualified issuer must issue it. A government authority or a similar trusted institution can be a legitimate issuer for such claims.

```
accept(Form) :-
    extract(Form, format, registrationFormat),

    extract(Form, birth_credential, Credential),
    extract(Credential, format, ssi_credential),
    extract(Credential, date_of_birth, Birthdate),
    calculateAge(Birthdate, Age), Age >= 13, Age <= 18,

    extract(Credential, dIDsubject, DIDsubject),
    extract(Credential, dIDissuer, DIDissuer),

    get_DIDdoc(DIDsubject, PKu, DIDDocSubject),
    verify_signature(Form, PKu),
    get_DIDdoc(DIDissuer, PKi, DIDDocIssuer),
    verify_signature(Credential, PKi),

    check_issuer(DIDDocIssuer).

get_DIDdoc(DID, PK, DIDDoc) :-
    resolveDID(DID, 3, DIDDoc),
    extract(DIDDoc, format, ssi_diddoc),
    extract(DIDDoc, pk, PK), verify_signature(DIDDoc, PK).

check_issuer(DIDDocIssuer) :-
    extract(DIDDocIssuer, trustScheme, TrustSchemeClaim),
    trustscheme(TrustSchemeClaim, trustedTrustScheme),
    trustlist(TrustSchemeClaim, TrustListEntry),
    extract(TrustListEntry, pubKey, PKi),
    verify_signature(DIDDocIssuer, PKi).
```

List. 1: TPL policy sketch for our exemplary age verification use case

## 4.1 Example Policy

We show an example policy in List. 1 corresponding to the age verification use case (cf. Sect. 4). A user sends a transaction containing a registration request `registrationForm` to the discussion platform. The discussion platform uses the given policy and an automated verification tool to assess if the user is in the right age span to be admissible to the platform.

The input parameter passed to the TPL interpreter (`Form`) contains the registration request, signature, and credential of the user. After ensuring the incoming transaction has the correct format, it checks the user's age by extracting the date of birth from the birth credential. Then it uses the predicate `calculateAge` to derive the user's age before it verifies if the age is within the specified range. We omit a concrete explanation of the `calculateAge` predicate since it is of no interest to this discussion.

Next, the built-in predicate `extract` is used to retrieve the DID of the sender (credential subject) and of the credential's issuer. These two DIDs are then used with the new built-in predicate `resolvedDID` (cf. Sect. 3.3) to retrieve the DID documents of the two entities. This step also takes the minimum age of the DID document into account, as specified by the second parameter. Each DID document contains a public key corresponding to DID, which is first used to verify the DID document itself. Further, the sender's key is used to verify the transaction, and the issuer's key to verify the credential. If all those checks succeed, there is a valid trust chain between the issuer and the registration request. The interpreter proceeds to authenticate the issuer itself. In our example, we authenticate the issuer in `check_SSI` using a common `LIGHTest` authentication flow [Wa19] and a trust scheme `trustedTrustScheme`, showing that both centralized and decentralized world can be used together in one policy.

## 5 Future Work

### 5.1 Towards an implementation

We have shown that TPL's extensibility supports novel trust and identity management concepts like SSI. To give more insights into this adaption's consequences and explore further extensions or modifications to the TPL language, we propose implementing the stated concepts following an agile approach. Doing so supports the verification of the stated concepts while at the same time keeping up with the ongoing development of SSI concepts to ensure compatibility. Given that the first version of TPL is currently interlocked with the `LIGHTest` toolchain, we propose a more stand-alone implementation, enabling other projects to use the TPL interpreter. Nevertheless, `LIGHTest` provides powerful concepts which are essential to TPL. It is unavoidable and reasonable to keep building on these concepts. Finding the middle ground might be challenging.

## 5.2 Outlook

In this section we discuss further possibilities and future work in the intersection of distributed trust management and trust policies.

**Issuer accreditation** While authentication of a credential is performed by resolving and retrieving the signer’s DID document and verifying the credential’s signature, a DL is not always used to authenticate the signer or their respective issuer. On the one hand, if a consortium of qualified entities operates the ledger, the fact alone that a DID is registered on the DL provides legal value to the DID. The same is true for (identity) credentials registered on such a “qualified ledger” – as only qualified entities can add credentials to the DL, the registration alone acts as a certification of the credential’s content. Thus, authentication of issuers can be achieved by supporting the respective discovery means using a DL.

On the other hand, if the used ledger is a public ledger such as the commonly used “Ethereum mainnet”, other means are needed to define which entities represent qualified trust (service) providers or otherwise relevant entities. In the end, it depends on the service provider’s local rules, laws, and other regulations which issuers are trusted by them. So it makes sense to anchor these rules in a trust policy. For instance, the service provider could define all qualified trust service providers as defined by their existing and trusted trust scheme to act as SSI (credential) issuers. In the example shown in Sect. 4, we sketch out how such a definition of a trusted scheme could be integrated into a TPL trust policy. To extend this (centralized) trust scheme-based authentication framework, we propose to support decentralized frameworks such as those realized by a smart contract-based web of trust [Mo21].

**Privacy-preserving features** In our example (cf. Sect. 4), even the date of birth provides more information than needed. The only relevant information is the 1-bit of information whether a person is in the defined age-range. Thus, more privacy could be added by supporting, e.g., range proofs, which we intend to do in a later version of TPL.

## Acknowledgments

This work was supported by the European Union’s Horizon 2020 Framework Programme for Research and Innovation under grant agreements No. 871473 (KRAKEN), No. 959072 (mGov4EU), and No. 830929 (CyberSec4Europe), as well as the Sapere-Aude project “Composec: Secure Composition of Distributed Systems”, grant 4184-00334B of the Danish Council for Independent Research.

## References

- [Ab17] Abraham, A.: Whitepaper: Self-Sovereign Identity, tech. rep., 2017, visited on: 10/16/2020.
- [Ab20] Abraham, A.; More, S.; Rabensteiner, C.; Hörandner, F.: Revocable and Offline-Verifiable Self-Sovereign Identities. In: TrustCom. IEEE, pp. 1020–1027, 2020.
- [Ar05] Arends, R.; Austein, R.; Larson, M.; Massey, D.; Rose, S.: DNS Security Introduction and Requirements. RFC 4033/, pp. 1–21, 2005.
- [Be17] Berghel, H.: Equifax and the Latest Round of Identity Theft Roulette. *Computer* 50/12, pp. 72–76, 2017.
- [Be20] Berghel, H.: The Equifax Hack Revisited and Repurposed. *Computer* 53/5, pp. 85–90, 2020.
- [BFG10] Becker, M. Y.; Fournet, C.; Gordon, A. D.: SecPAL: Design and semantics of a decentralized authorization language. *J. Comput. Secur.* 18/4, pp. 619–665, 2010.
- [BL16] Bruegger, B. P.; Lipp, P.: LIGHT<sup>est</sup> - A Lightweight Infrastructure for Global Heterogeneous Trust Management. In: Open Identity Summit. Vol. P-264. LNI, GI, pp. 15–26, 2016.
- [DD10] Dong, C.; Dulay, N.: Shinren: Non-monotonic Trust Management for Distributed Systems. In: IFIPTM. Vol. 321. IFIP Advances in Information and Communication Technology, Springer, pp. 125–140, 2010.
- [Fr20] Fritsch, L.: Identity Management as a target in cyberwar. In: Open Identity Summit. Vol. P-305. LNI, Gesellschaft für Informatik e.V., pp. 61–70, 2020.
- [GN08] Gurevich, Y.; Neeman, I.: DKAL: Distributed-Knowledge Authorization Language. In: CSF. IEEE, pp. 149–162, 2008.
- [He00] Herzberg, A.; Mass, Y.; Mihaeli, J.; Naor, D.; Ravid, Y.: Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers. In: IEEE S&P. IEEE, pp. 2–14, 2000.
- [Ko20] Koa, C.-G.; Heng, S.-H.; Tan, S.-Y.; Chin, J.-J.: Review of Blockchain-Based Public Key Infrastructure. In: Cryptology and Information Security Conference 2020. P. 20, 2020.
- [LFG99] Li, N.; Feigenbaum, J.; Grosf, B. N.: A Logic-based Knowledge Representation for Authorization with Delegation. In: CSFW. IEEE, pp. 162–174, 1999.
- [Mö19] Mödersheim, S.; Schlichtkrull, A.; Wagner, G.; More, S.; Alber, L.: TPL: A Trust Policy Language. In: IFIPTM. Vol. 563. IFIP Advances in Information and Communication Technology, Springer, pp. 209–223, 2019.
- [Mo21] More, S.; Grassberger, P.; Hörandner, F.; Abraham, A.; Klausner, L. D.: Trust Me If You Can: Trusted Transformation Between (JSON) Schemas to Support Global Authentication of Education Credentials. In: IFIP SEC. IFIP Advances in Information and Communication Technology, In press, Springer, 2021.

- [Re21] Reed, D.; Sporny, M.; Longley, D.; Allen, C.; Grant, R.; Sabadello, M.: Decentralized Identifiers (DIDs) v1.0, W3C Working Draft, W3C, Jan. 20, 2021, URL: <https://www.w3.org/TR/2021/WD-did-core-20210128/>.
- [Ro17] Roßnagel, H.: A Mechanism for Discovery and Verification of Trust Scheme Memberships: The Lightest Reference Architecture. In: Open Identity Summit. Vol. P-277. LNI, Gesellschaft für Informatik, Bonn, pp. 81–92, 2017.
- [SBT19] Schlichtkrull, A.; Blanchette, J. C.; Traytel, D.: A verified prover based on ordered resolution. In: CPP. ACM, pp. 152–165, 2019.
- [Sc20] Schlichtkrull, A.; Blanchette, J.; Traytel, D.; Waldmann, U.: Formalizing Bachmair and Ganzinger’s Ordered Resolution Prover. *J. Autom. Reason.* 64/7, pp. 1169–1195, 2020.
- [SLC19] Sporny, M.; Longley, D.; Chadwick, D.: Verifiable Credentials Data Model 1.0, W3C Recommendation, W3C, Nov. 19, 2019, URL: <https://www.w3.org/TR/2019/REC-vc-data-model-20191119/>.
- [SM20] Schlichtkrull, A.; Mödersheim, S.: Accountable Trust Decisions: A Semantic Approach. In: Open Identity Summit. Vol. P-305. LNI, Gesellschaft für Informatik e.V., pp. 71–82, 2020.
- [SS20] Sporny, M.; Steele, O.: DID Specification Registries, W3C Note, W3C, June 2020.
- [Th17] Thomas, K.; Li, F.; Zand, A.; Barrett, J.; Ranieri, J.; Invernizzi, L.; Markov, Y.; Comanescu, O.; Eranti, V.; Moscicki, A.; Margolis, D.; Paxson, V.; Bursztein, E.: Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials. In: CCS. ACM, pp. 1421–1434, 2017.
- [Wa19] Wagner, G.; Wagner, S.; More, S.; Hoffmann, M.: DNS-based Trust Scheme Publication and Discovery. In: Open Identity Summit. Vol. P-293. LNI, GI, pp. 49–58, 2019.
- [Xi20] Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y. T.: A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Commun. Surv. Tutorials* 22/2, pp. 1432–1465, 2020.
- [Zh18] Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H.: Blockchain challenges and opportunities: a survey. *Int. J. Web Grid Serv.* 14/4, pp. 352–375, 2018.
- [ZZS14] Zwattendorfer, B.; Zefferer, T.; Stranacher, K.: An Overview of Cloud Identity Management-Models. In: WEBIST (1). SciTePress, pp. 82–92, 2014.

# DAMA – A transparent meta-assistant for data self-determination in smart environments

Christopher Ruff<sup>1</sup>, Andrea Horch<sup>2</sup>, Benedict Benthien<sup>3</sup>, Wulf Loh<sup>4</sup> and Alexander Orłowski<sup>5</sup>

**Abstract:** Global sales of AI-based smart voice assistants and other smart devices are increasing every year. Smart devices are becoming ubiquitous, including living and workspaces. These spaces often have very high privacy requirements, like living rooms, bedrooms or meeting rooms in office environments. Users of smart devices have security and privacy concerns regarding personal data collection, data storage and the use of such data by the devices and the providers. These concerns are aggravated by a lack of transparency by the device manufacturers. As a result, users have limited possibilities to make an informed decision due to missing information or interfaces. While this leads to limited trust regarding the security and privacy of smart devices, for most users, the practical benefit dominates. The project DAMA wants to address user's security and privacy concerns by creating transparency and regulating the smart devices in connection with the respective context (e.g. when users are alone at home or when they have visitors). For this purpose, the project is developing a "meta-assistant", an assistant that regulates other AI-based assistants and other smart devices. It uses artificial intelligence (AI) for context detection and device regulation. The regulation processes are based on established ethical guidelines, which are adjusted to the project context.

**Keywords:** Smart Home, Smart Office, Smart Speaker, Privacy.

## 1 Introduction

The use of smart speakers like Amazon Echo or Google Home for services like music streams or search engines or to control other smart devices within a Smart (Home) environment via voice command are becoming more and more popular every year. According to [Br20a], global sales of Smart Speakers increased from 32.8 Million in 2017 to 86.5 Million, and were estimated to reach 91.3 Million by 2019. In a survey, introduced in [Br20b], 1.000 Germans indicated where they use their smart speakers in their Smart Homes. The result shows that the top four rooms equipped with smart speakers are the following: 67% living room, 53% kitchen, 44% office room, 43% bedroom. The survey of [Xu2020] shows the most popular functions of smart speakers. The top three functions are (1) asking general questions (55%), (2) getting information like weather, travel or

---

<sup>1</sup> Fraunhofer IAO, Identity Management, Nobelstr. 12, Stuttgart, 70569, christopher.ruff@iao.fraunhofer.de

<sup>2</sup> Fraunhofer IAO, Identity Management, Nobelstr. 12, Stuttgart, 70569, andrea.horch@iao.fraunhofer.de

<sup>3</sup> Fraunhofer IAO, Identity Management, Nobelstr. 12, Stuttgart, 70569, benedict.benthien@iao.fraunhofer.de

<sup>4</sup> Internationales Zentrum für Ethik in den Wissenschaften (IZEW), Wilhelmstr. 19, Tübingen, 72074, wulf.loh@izew.uni-tuebingen.de

<sup>5</sup> Internationales Zentrum für Ethik in den Wissenschaften (IZEW), Wilhelmstr. 19, Tübingen, 72074, alexander.orłowski@uni-tuebingen.de



sports updates (45%) and (3) the use of in-built music streaming services (35%). Home automation ranked on place seven (18%). The survey also states that at the end of 2019 an average U.S. home owned 9.2 connected devices. The most popular devices in the survey were phones, desktop and tablet computers, streaming boxes and sticks, connected TVs, gaming consoles, smart speakers, watches and thermostats. These surveys show that the use of smart speakers and other smart devices becomes more and more commonplace and the number of devices in use increases year by year.

Through the use of and interaction with Internet of Things (IoT) devices, a large amount of data is generated. Since personalized services are a central component here, the identification of the respective users creates profiles that contain a variety of personal data, from daily schedules, personal preference up to medical issues and biometric data used for identification [Wa2018]. As applications of smart devices in one's own home concern a specially protected private space, the trade-offs between the need for privacy protection on the one hand, and access to modern IoT technology on the other, are difficult not only from a data protection standpoint, but also from an ethical one [Hu2018]. Risks arise not only from consciously shared data, but also from reconfiguration with other existing data sets. These so-called *derivable data* [Gh2016] enable conclusions to be drawn about individuals far beyond their intended use. These possibilities are likely to undermine informational self-determination, i.e. in this case the possibility of users to control their shared data.

Due to the multitude of devices, the intransparency of data collection and processing, as well as the inconsistent and insufficient regulatory schemes, an understanding of the impact on privacy is often difficult to comprehend, even for experts. Therefore, DAMA seeks to empower users to regain their informational self-determination by giving back control over the devices and thus over the collected data. Regulatory efforts such as the General Data Protection Regulation (GDPR) address some of these issues. However, there are still gaps here [Wa2018], that prevent users from making informed privacy decisions as well as gaining adequate control over the privacy settings on their IoT devices. DAMA addresses this gap in the current legislation in order to create a possibility for users to use IoT devices in a self-determined way.

These issues not only concern legal and ethical challenges of IoT and Smart Home applications, but also user trust. A consumer study published in [HFA20] investigated the security and privacy concerns of smart home users concerning the smart devices in their homes. The results show a lack of transparency of the smart devices regarding data collection, data storage and the use of data by the devices and their providers. According to the study, the consumers are afraid of e.g. that their households are profiled, that the providers could sell their data, or that the government or someone from outside could get access to the data. The perceived lack of transparency may lead to a loss of confidence regarding the technology. The study also mentions that some of the users take simple and non-technical mitigation actions regarding their concerns, which do not have much effect, due to limited technical options or the lack of technical expertise. The lack of technical options can be traced back to the fact that most multi-agent systems in Smart Homes are

closed systems, which use miscellaneous protocols, interfaces and standards as stated in [Fi2020]. Additionally, devices like smart speakers exhibit false detections regarding the wake word, thus being triggered without the user uttering the wake word [Sc2020]. Especially in situations subjectively considered as intimate, these false triggers confuse and unsettle the users and may lead to a loss of trust in the technology.

The research project DAMA (Data Autonomy Meta-Assistant) is addressing the users' needs as described above. The project aims to ensure privacy and informational self-determination - and thereby create trust - by developing a meta assistant called DAMA. This assistant will regulate the devices within the Smart Home environment in accordance with the respective context (e.g. resident is alone, resident has visitors) as well as depending on the sensors and functions of the devices. In order to secure privacy and increase trust, the meta-assistant will also be able to regulate itself, e.g. by turning off its own speech recognition. In order to maximize transparency, the meta-assistant informs the users about the privacy context DAMA has determined (alone, visitors, etc.), and which devices/sensors are currently active. The users also have the possibility to access this information at any time by asking DAMA. The respective context will be identified by using machine learning on sensor data and user input. The regulation will consider ethical aspects in order to enhance privacy, informational self-determination, and transparency for the users of Smart Home environments.

## 2 Related Work

The High-Level Expert Group on AI of the European Commission presented ethics guidelines for a trustworthy artificial intelligence (AI), which can serve as a starting point for the design of trustworthy AI systems [EU2019] like smart speakers or other smart devices. However, the report provides little guidance on how to implement the explicability of AI systems. In addition, DAMA makes use of the guidelines of the German Ethics Council on Big Data and AI [DE2017]. They go a little bit into more detail on how to establish control, transparency, and traceability for users, as well as conditions for explainability.

Large companies often have guidelines and policies to improve the trustworthiness of their AI products. Examples are the guidelines for AI of the Telekom [Fu2018], the baselines for AI of SAP [Ma2018] or the ethical AI principles of Microsoft [Bo2019].

In addition, there are different national and international initiatives for AI ethics standards, such as the IEEE P70xx series of ethical technology standards [Ci2019].

A practical approach to create trust for consumers of IoT devices is given in [Ca2021]. The authors describe a privacy and security label for IoT devices to enable consumers to make well-informed choices when they select an IoT device for their applications. The label informs consumers e.g. about included sensors, the data storage on the devices and in the cloud and the groups, the data collected by the device is shared with. Another

initiative is [AI2020], in which a group of scientists and standardization experts made a first effort to move AI ethics “from principles to practice” and create an AI ethics label as well as introduce the idea of criticality levels for AI applications.

The goal of the EU project uTRUSTit (2010-2013) was to provide understandable security and trustworthiness feedback to the users of IoT devices in order to create transparency and trust. As described in [Ho2012] the project developed an overview of data sent by the smart devices, like device or network information and personal data. The overview is displayed on a mobile device like a mobile phone or tablet in a comprehensible and user-friendly manner.

The project PAPAYA (PlATform for PrivAcY preserving data Analytics) [Pa2021] develops dedicated privacy preserving data analytics modules in order to enable users of devices and applications, which use third-party processors to analyse the user’s data, to get valuable information about the processed data.

Several research projects created a good set of Transparency Enhancing Technologies (TETs) which provide users with all necessary information about their data being stored, processed, exchanged and used by applications and devices. This data also includes private information of the users like voice or sensor data collected by smart devices in Smart Home environments. An overview of such technologies and tools is given in [Ja2013].

The BlockIT project introduced in [Lo2018] describes a blockchain-based solution for privacy preserving translucent data sharing on a smart IoT-aided grid by using smart contracts to regulate the interactions between the nodes in the grid. The blockchain provides transparency concerning the transactions and a wallet of pseudonyms offers a solution to preserve data privacy.

### **3 Objectives**

The main objective of the DAMA project is to create more transparency and privacy for users of Smart Home applications and thereby increase their trust in the technology. To reach this goal, different context levels with different privacy settings are introduced. They describe typical situations in smart environments (use cases), for example: the resident of a Smart Home is alone or the resident has visitors. The devices within the smart environment are then configured and regulated automatically according to the respective context level that the users explicitly or implicitly set. The regulation can entail the activation or deactivation of specific devices or sensors in order to assure the user’s privacy needs and informational self-determination within the given situation. The users are notified about the deactivation and activation of devices or single sensors, which also helps to increase the transparency of the whole system. Additionally, users can retrieve the information about the status of all smart sensor devices at any time and check whether they are active or not, by using the assistant’s intuitive user interface. The algorithms and AIs in DAMA will detect the context of a situation and control the devices and

configuration. In addition to the regulation of the other devices within the smart environment, DAMA also regulates itself, including a trustable, complete shutdown, to assure the adequate privacy level in situations of very high privacy needs.

## 4 Context Levels and Use Cases

The context levels are a convenient and practical way to regulate the Smart Home and its different applications. By changing context levels, it is easy for the users to react to a situational change without having to interact with all the different devices. At the same time, the user is given full control over the various devices while DAMA also displays the collected data by the devices. To make this an even more seamless user experience, DAMA will be able to automatically detect privacy patterns in user's behavior and sets context levels accordingly through a ML algorithm.

Three basic modes can be distinguished for the context levels:

- 1) Maximum functionality: all devices of the Smart Home / Smart Office are activated (context level 1).
- 2) Intermittent customizable modes - only certain sensors, displays and devices are activated; this depends on the respective situation and existing devices (context level 2-9).
- 3) Maximum privacy: all Smart Home / Smart Office devices are switched off. In addition, DAMA's microphones and speech recognition are deactivated (context level 10).

The second category is a compromise between functionality and privacy, depending on the user's preferences for a given situation. It is therefore not a single mode, but various customizable context levels are possible. By giving DAMA control over the other applications and their sensors, and letting the user self-define the context levels and when they are applied, the project maximizes the user's informational self-determination. The user can define for herself what constitutes an "appropriate flow of information" [Ni2010: 114] within her home. At the same time, the user receives status information about the active applications / sensors, which increases her informational self-determination [Lo18a]. In addition, the information about the data flows and uses provides her with the opportunity to make an informed decision whether and what data it opts to share in return for functionality [Lo2021].

For this, it is important to distinguish between sensors (for example, Alexa's microphone) and displays (for example, calendar entries on a smart mirror). The different context levels allow users to either hide their private data from visitors, e.g. the personal calendar displayed on a screen or a smart mirror. In addition, it allows them to protect their own and their visitor's privacy from datafication by the smart devices.

In the project, we identified different use cases, which represent different situations in which ideal-typical demands for privacy and functionality are raised. This allows us to

elaborate and define the different context levels. The aim of these use cases is to create a solid basis that shows the usefulness of the system to enhance privacy and informational self-determination (proof of concept). In addition, a demonstrator will be developed that covers typical settings, but also is limited to certain idealized assumptions about intended use and usage environment. Based on this foundation created in the DAMA project, further use cases and requirements can be realized in the future, addressing a larger variety of usage environments as well as unintended usage. The development of DAMA also includes analyses of the range of various sensors. Specifically, the extent to which devices in adjacent rooms or on other floors can also collect data is examined.

The use cases identified by the project are:

- Use Case 1 - Resident comes home
- Use Case 2 - Resident gets a visitor in the evening
- Use Case 3 - Resident has a visitor with a child
- Use Case 4 - Craftsman or service provider must enter the flat

We will use a short example to explain the function of the context levels: After work, the resident of the Smart home comes into the house with a colleague. DAMA recognizes that the resident is not alone and therefore does not automatically switch to the mode that is usually selected for the end of the day: by playing a relaxation playlist and DAMA reading out private messages. Instead, DAMA switches off the private displays. In course of the evening, the conversation turns to important developments in the company that should not be made public, so the occupant switches to context level 10 "maximum privacy" - all devices and DAMA itself are switched off.

## 5 Technical Environment

The technical implementation of the AI prototype (meta-assistant DAMA) is work in progress. DAMA will be integrated into an existing Smart Home / Smart Office laboratory in the office building of the Fraunhofer IAO in Stuttgart. The laboratory is spatially divided into a *Smart Home section* and a *Smart Office section* as shown in Figure 1.



Fig. 1 - Smart Home / Smart Office laboratory

The Smart Home section includes devices like a smart fridge, a smart couch, a smart couch table, a smart mirror and a smart TV. Fig. 1 shows the Smart Home laboratory and some of its devices. The Smart Office section includes devices like a Microsoft Surface Hub coffee table, a projector, a smart coffee machine and various environment-sensors, measuring things as e.g. the air quality, humidity or the air temperature in the room.

## 6 The Meta-Assistant »DAMA«

In the following, the technical concepts and architecture of the DAMA system components are detailed. The overall technical concept of the DAMA system can be viewed as a layered architecture, as seen in Fig. 3.

### 1. Context Detection Layer

The context detection layer includes all the components that gather information via sensory systems, like microphones in voice assistants, environmental sensors but also AI powered algorithms coupled with computer vision.

The basis for context detection is to derive information about who and how many people are present in the current smart home (or office) environment that the DAMA assistant has access to. As DAMA is designed to maximize privacy, the system will use minimally privacy-invasive detection technology and avoid biometrical recognition, such as face,

voice, iris recognition etc. Currently, the system uses computer vision, based on OpenCV and machine learning to detect people entering the smart home. Cameras are located in less private areas like the entrance focusing only a small area and also only from above. The AI only tries to recognize people coming or leaving and does not record any biometrical information. Data processing is done locally.



Fig. 2 - Detecting people entering the home using computer vision

This will be coupled with other systems such as infrared cameras and light barriers. The sensor systems are chosen to only collect the minimal amount of data necessary to tell whether someone is present in the smart. To identify the residents and their closer friends or partners, we are using MAC-scanners to identify smart phones of registered users to allow more fine tuned privacy settings. All devices can be switched off.

In order to solve the dilemma of introducing more sensors into the smart home to enhance privacy and informational self-determination, the DAMA system will focus on transparency. In general, it will only collect the information needed to identify the context (privacy by design) and avoid re-identification. The system is designed to run locally without sharing information with external servers. Furthermore, the system itself will shut down if requested by the user.

## 2. Controller

In the controller layer, the data and information collected by the various sensors and devices are collected and processed. Based on the user configuration, including the setting of different context levels, the DAMA Assistant's business logic is responsible for the processing and control of the devices in the Smart-Home through the Actor-Layer.

This layer will have a web-based user interface than can be shown on smart-TVs as well

as other devices. To streamline and simplify connection to a variety of smart devices, smart home controllers are connected to the DAMA Assistant as well and are used where the devices support the required protocols. In the final version, data connection between devices and the controller will use TLS encryption to safeguard against tempering of the information sent.

3. Actors

The actor layer consists of all the smart devices the DAMA Assistant can control and regulate. The modular structure of the system will allow various devices and setups to work with minimal integration effort.

4. Transport layer

The DAMA Assistant needs to interoperate with a lot of devices and information sources, so an efficient bi-directional communication infrastructure is required. The MQTT [HTS08] protocol is lightweight, robust and as such capable to handle our requirements. Implementations of MQTT Clients are available for all major platforms and programming languages. While it can handle different communication scenarios, the publisher/subscriber using a MQTT-Broker as an intermediary is used in our context.

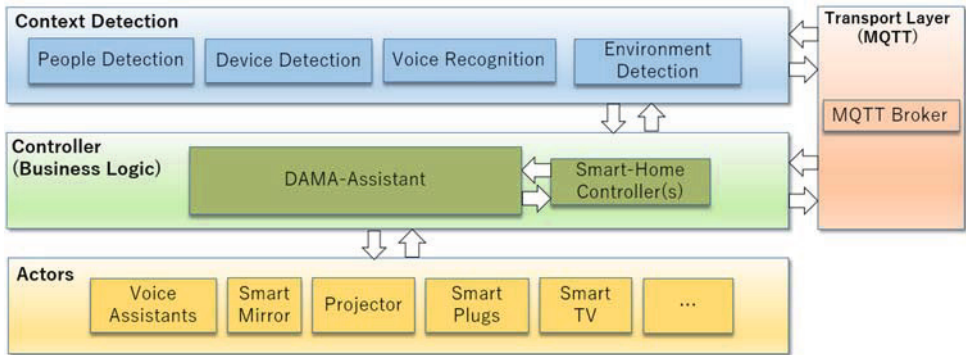


Fig. 3 - DAMA System Architecture

5. User Interface

The user interface is designed to address the needs of ordinary residents without a lot of technical knowledge. The system will be controlled via an intuitive user interface that allows registering new users, their respective smart device environment and their desired privacy context levels.

To facilitate the setup for less technically inclined users, default settings will be provided, based on a general classification of devices in terms of their possible impact on privacy. For the classification of devices, a privacy impact assessment is necessary. As common standards for classification are still in development, the classification will be based on a survey of existing approaches and criteria as of the “IT-Gütesiegel” certificate initiative



of the German state government and the privacy and security label [GI14]. This and other sources are taken into account to create a project internal privacy matrix to structure this classification.

The DAMA backend logic is contained in several python scripts. Users can either call a web application to authenticate and change the context level directly, or it can be changed by sensors located inside the trusted smart environment. The MQTT Protocol is again used for the communication between DAMA, actors and sensors. Changes made to the context level are stored in a database with a timestamp and the used method for later reference.

## 7 Conclusion and Future Work

In this paper, we presented the underlying technical and ethical concept of a meta-assistant that is able to mitigate the privacy challenges that the use of smart assistants inevitably introduce, such as voice assistants and other smart devices that gather, display and share personal and potentially sensitive information in our living and work spaces. We tackle this problem by defining privacy related context levels, based on ethical values and assessments, which are subsequently implemented in a technical system that regulates said devices in terms of activity and data handling according to the current context.

By using these concepts, many of the challenges of dealing with a multitude of individual smart devices and their settings are hidden from the users, which in turn can assess on a much more abstract level, which privacy requirements they have for a given situation.

One of the challenges is the regulation of devices that do not allow users to have fine-grained control over said devices and do not provide interfaces to regulate them. While the DAMA assistant tries to use provided application interfaces when possible, lesser accessible devices are controlled by means of cutting power supply, shutters for visual devices or blocking network traffic. If interfaces allow, more fine-grained settings are possible, i.e. to activate or de-activate only part of the full functionality of the devices - for user-controlled periods.

The here presented system allows the user to exercise control and transparency over the multitude of smart devices while also enabling users to respect and cater to the needs of guests and visitors in terms of their privacy concerns, as well as their own. The work on the DAMA assistant is ongoing. In future work, privacy contexts and privacy settings are to be increasingly set by using machine learning to identify potentially privacy sensitive situations and automatically suggest the best system settings accordingly in more complex user scenarios.

## 8 Acknowledgement

We thank and acknowledge the Baden-Württemberg Stiftung for financing the DAMA

project. For more information, please visit: <https://www.bwstiftung.de/>.

## Bibliography

- [AI2020] AI Ethics Impact Group: From Principles to Practice – An interdisciplinary framework to operationalise AI ethics, VDE/Bertelsmann, <https://www.ai-ethics-impact.org/>, accessed 12/02/2021.
- [Bo2019] Böhm T.: Künstliche Intelligenz und Ethik: Warum KI ethische Prinzipien braucht, um ein Erfolg zu werden, <https://news.microsoft.com/de-de/ethik-prinzipien-kuenstliche-intelligenz/>, accessed 04/02/2021.
- [Br20a] Brandt, M.: Smart Speaker-Absatz - Amazon - Nummer 1 mit knappem Vorsprung, <https://de.statista.com/infografik/20675/geschaetzter-weltweiter-smart-speaker-absatz/>, accessed 26/01/2021.
- [Br20b] Brandt, M.: Smart Speaker - Wo Alexa und Co. im Einsatz sind, <https://de.statista.com/infografik/20414/orte-an-denen-smart-speaker-genutzt-werden/>, accessed: 26/01/2021.
- [Ca2021] Carnegie Mellon University: IoT Security & Privacy Label, <https://www.iotsecurityprivacy.org/>, accessed: 28/01/2021.
- [Ci2019] Cihon P.: Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development, [https://www.fhi.ox.ac.uk/wp-content/uploads/Standards\\_FHI-Technical-Report.pdf](https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_FHI-Technical-Report.pdf), accessed 04/02/2021.
- [DE2017] Deutscher Ethikrat: Big Data and Health – Data Sovereignty as the Shaping of Informational Freedom. 2017.
- [EU2019] European Commission, High-Level Expert Group on AI: Ethics Guidelines for Trustworthy Artificial Intelligence, <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, accessed 04/02/2021.
- [Fi2020] Firouzi R., Rahmani R., Kanter T.: An Autonomic IoT Gateway for Smart Home Using Fuzzy Logic Reasoner, *Procedia Computer Science*, Vol. 177, pp. 102-111, 2020.
- [Fu2018] Fulde V.: Guidelines for Artificial Intelligence, <https://www.telekom.com/en/company/digital-responsibility/details/artificial-intelligence-ai-guideline-524366>, accessed 04/02/2021.
- [Gh2016] Ghiglieri, M., Hansen, M., Nebel, M., Pärschke, J.V., Fhom, H.S.: Smart-TV und Privatheit. Bedrohungspotenziale und Handlungsmöglichkeiten. Hg. v. Forum Privatheit. 2016.
- [GI14] IoT, Security & Privacy Label, Carnegie Mellon University, <https://www.iotsecurityprivacy.org/>, accessed: 13/04/2021.
- [HFA20] Haney J. M., Furman S. M., Acar Y.: Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges, *HCI for Cybersecurity, Privacy and Trust*, pp. 393-411, 2020.

- [Ho2012] Hochleitner C., Graf C., Unger D., Tscheligi M.: Making Devices Trustworthy: Security and Trust Feedback in the Internet of Things, Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Volume 4, 2012.
- [HTS08] Hunkeler, U.; Truong, H. L.; Stanford-Clark.: "MQTT-S — A publish/subscribe protocol for Wireless Sensor Networks," 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08), Bangalore, India, 2008, pp. 791-798, doi: 10.1109/COMSWA.2008.4554519.
- [Hu2018] Hummel, P.; Braun, M.; Augsburg, S.; Dabrock, P.: Sovereignty and Data Sharing. ITU Journal: ICT Discoveries, Special Issue No. 2, 23 Nov. 2018.
- [Ja2013] Janic M., Wijbenga J. P., Veugen T.: Transparency Enhancing Tools (TETs): An Overview, 2013 Third Workshop on Socio-Technical Aspects in Security and Trust, New Orleans, LA, USA, 2013, pp. 18-25, doi: 10.1109/STAST.2013.11.
- [Lo18a] Loh, W.: A Practice-Theoretical Account of Privacy, in: Ethics & Information Technology 20/4, pp. 233-247, 2018.
- [Lo18b] Lombardi, F.: An IoT data sharing dilemma: Transparency or Translucency?, <https://medium.com/cybersoton/an-iot-data-sharing-dilemma-transparency-or-translucency-9cd85ca278c3>, accessed 06/04/2021.
- [Lo2021] Loh, W.: Social Pathologies of Informational Privacy, in: Journal of Social Philosophy, forthcoming.
- [Ma2018] Machmaier C.: Die Grundsätze für Künstliche Intelligenz von SAP, <https://news.sap.com/germany/2018/09/ethische-grundsätze-kuenstliche-intelligenz/>, accessed 04/02/2021.
- [Ni2010] Nissenbaum, H.: Privacy in context: Technology, policy, and the integrity of social life, Stanford Law Books, Stanford, 2010.
- [Pa2021] PAPAYA Project: PAPAYA project website, <http://www.papaya-project.eu/>, accessed 06/04/2021.
- [Sc2020] Schönherr L., Golla M., Eisenhofer T., Wiele J., Kolossa D., Holz T.: Unacceptable, where is my privacy? Exploring Accidental Triggers of Smart Speakers, arXiv.org, 2020, <https://arxiv.org/abs/2008.00508>, accessed: 04/02/2021.
- [Wa2018] Wachter, S.: Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, in: Computer Law & Security Review, 34 (3), 436-449, 2018, DOI: 10.2139/ssrn.3083554.
- [Xu2020] Xu, C.: The Smart Speaker Frenzy and Why It's Happening, <https://www.comscore.com/ger/Insights/Blog/The-Smart-Speaker-Frenzy-and-Why-Its-Happening>, accessed 26/01/2021.

# Records Management and Long-Term Preservation of Evidence in DLT

Tomasz Kusber<sup>1</sup>, Steffen Schwalm<sup>2</sup>, Dr. Ulrike Korte<sup>3</sup>, Kalinda Shamburger<sup>4</sup>

**Abstract:** DLT improves decentralized business models and transactions from supply chain or cryptocurrencies to shared mobility, electronic registries or proof of origin. The planned enhancement of European Blockchain Service Infrastructure approximately 2021-2022 is expected to accelerate these developments based on a scalable, standardized framework. Like any infrastructure or IT-system used for business relevant transactions also in DLT is has to be possible to make decisions and processes evident against 3rd parties such as courts, auditors or regulative authorities. This leads to the challenge to fulfil requirements on a valid records management acc. to current standards [IS20b] [IS16] as well as to preserve the evidences of electronic records as long as they are needed according to current regulations and standards [eIDAS] [ETS19b] [VDG]. Based on international standardization the authors are taking part in, this paper focuses on the challenges and requirements for records management and preservation of evidence in DLT as well as possible solutions and needs for further standardization.

**Keywords:** DLT, blockchain, eIDAS, long-term preservation, digital evidence, blockchain security, records management

## 1 Introduction

In the last years Distributed-Ledger-Technology (DLT) and its most famous representative blockchain generated a real hype in particular the well-known use case Bitcoin. After the bitcoin crash in 2019 first doubts about the real capacity of DLT occurred. In this context standardization on DLT increased and industry as well as public sector used the chance to enable the technology for high-regulated industries with corresponding requirements on records management and trust [Le17]. Basically, DLT is a decentralized distributed peer-to-peer network of technical nodes for data exchange and transaction execution. According to [IS20a] a distributed ledger is in this case shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism. The consensus mechanism ensures that all transactions are valid and unaltered. Its manner depends on the type of DLT so that the well-known prejudice that DLT implies unacceptable high energy need is only valid for some consensus mechanisms e.g. Proof of Work, other ones are much more efficient especially those ones in DLT with restricted access rights e.g. BFT, Proof of Authority, Proof of Stake etc. [IS20b]. DLT networks allow the transfer of data or value from one party to another without having intermediates involved. Once written to the ledger the transactions are immutable, mainly based on hash protection of data

---

<sup>1</sup> Fraunhofer Institute for Open Communication Systems, Kaiserin-Augusta-Allee 31, 10789 Berlin, Germany

<sup>2</sup> msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany; Convenor ISO Tc 46 Sc 11 JWG 1

<sup>3</sup> Federal Office for Information Security. Heinemannstr. 11,-13, 53175 Bonn, Germany

<sup>4</sup> msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany

stored on the chain. Any transaction can reliably be tracked on the chain [Ko20], [IS21]. If the factual distributed data set or transactions are bundled in sequential linked blocks it is called a blockchain – a special kind of DLT. The blocks can also include the hash of the previous block and so build the mentioned hash-protection [IS20b] and a so called “timestamp”. This DLT-“timestamp” has to be differentiated from timestamps acc. to [RFC3161], defined in [eIDAS] and related standards [EN319421] due to its lack of a trustworthy source of time, missing creation and validation of digital signatures by trust service provider and missing Proof of Existence created by 3<sup>rd</sup> party instead of the system, here DLT, itself. The hash-based integrity protection of each block is based on Merkle-trees [Ko20] [Xu19]. In comparison to the original ideas of blockchain, DLT does not mandatorily require the elimination of an operator or consortium providing the distributed network, this depends on the kind of DLT which can be distinguished regarding the access rights and transparency of the transactions. In public DLT everybody can view all transactions and data so there is full transparency, in private DLT only authorized users are allowed, similar conditions apply concerning execution of transactions. In permissionless DLT every user is allowed to validate and persist transactions, in permissioned DLT it depends on the access rights who has the authorization to do so. Furthermore, DLT is differentiated concerning data storage, on chain if data are stored on the ledger or off-chain if data are only represented by hash in DLT. At minimum the transaction documented by ledger records or referred records acc. to [IS20b] are stored on chain together with hash values of the related off-chain records. Due to performance limitations and privacy reasons e.g. [GDPR] off-chain storage is currently widely used [Ko18], [An18]. In summary, DLT can be characterized as distributed system which derives its trust from the immutability due to cryptographic protection and integrity, as well as the consistency (not completeness) check by the consensus mechanism so that any unauthorized alteration will be transparent and, at best, no central authority or intermediary is needed. This also means that DLT is typically only useful in distributed ecosystems with more than 2 parties involved where distribution is reasonable and the parties typically do not trust each other, so that trust in the technology seems to be necessary [An18], [Wer18].

Currently the European Union is improving the European Blockchain Service Infrastructure as a pan-European DLT-network with a focus on use cases like e.g.:

- Notarization or data validation
- Self-sovereign identity
- Digital proofs or evidences
- Electronic registries and tokenization
- Cross-industry trade platforms or data exchange platforms

In most cases the DLT acts as a transaction layer or in case of SSI also as an anchoring layer where the records will mostly be stored off-chain, only anonymized or pseudonymized equivalents e.g. DIDs in SSI are on-chain. Together with scalability also trustworthiness and security shall be improved within [EBSI] until 2022.

Regardless of these properties and goals there are some challenges to use DLT in regulated industries with typically extensive documentation requirements and a burden of proof associated with retention periods between 5 and 100 years, some only starting after decades depending on a future event. This leads to the question how DLT could fulfill the

requirements for a valid records management, which ensures the authoritativeness of records to achieve compliance with burden of proof and documentation requirements. Associated with this is the preservation of evidence to make transactions and records evident against 3<sup>rd</sup> parties such as courts, regulative authorities etc. for as long as the records are needed [Ko18], [Di21], [We18]. Against this background the paper shows the main areas of action focused on records management, evidence preservation and related questions.

After the introduction in the first chapter, the second chapter of this document summarizes the legal and technical requirements of evidence of electronic records and long-term preservation. The third chapter explains unsolved, open challenges in DLT in connection with records management and preservation of evidence under the perspectives of privacy [GDPR], and the missing crypto stability [ET19a] in connection with long-term preservation of evidence in DLT. Chapter 4 provides a feasible solution to preserve the authenticity and integrity of on-chain and off-chain records in connection with their evidence by combining DLT with a Preservation Service pursuant to [eIDAS] and [TR-ESOR] in order to archive long-term crypto stability and preservation of evidence in DLT.

## **2 Fundamental Requirements for Evidence of Electronic Records and Long-Term Preservation**

### **2.1 Legal Requirements**

The [eIDAS]-regulation which came fully into force in July 2016 provides a Europe-wide mandatory legal framework for digital identities and trust services. It enables trustworthy digital transactions between public administrations, companies and citizens with or without DLT. [eIDAS] contains two main parts: digital identities and trust services. Concerning identities [eIDAS] currently only defines requirements on identity of natural and legal entities. The levels of assurance from high to low according to Art. 8 [eIDAS] and [2015/1502] define graded security requirements on identity-verification-procedures (LoA). Any notified eID has to be accepted by any public administration. Along with digital identities [eIDAS] also defines trust services. In the context of records management especially creation, validation and preservation of electronic signatures, seals, timestamps have to be recognized. Cryptographic electronic signatures or seals make the authenticity and integrity of electronic records evident against 3<sup>rd</sup> parties, a (qualified) timestamp gives a valid Proof of Existence (PoE) and evidence for the time of transactions. In all cases a successful validation and preservation is necessary. Any at least advanced signature, seal or timestamp from each qualified trust service provider has to be accepted and validated by any public administration. Based on a valid as well as technology neutral standardization framework [eIDAS] also ensures acceptance and interoperability of trust services [eIDAS]. Currently [eIDAS] is under revision so that new trust services e.g. regarding SSI or DLT might arise. Furthermore, different industry-specific requirements have to be mentioned in context of records management such as [EASA] Part 21 in aerospace, [FDA] or [GxP] in pharma and chemicals or anti-money laundering laws in banking or in the public sector. All of them require the proof of authenticity, integrity and

traceability of electronic records against 3<sup>rd</sup> parties for as long as those records are needed. Considering these decade-long retention periods, the legislators defined obligations for long-term evidence preservation and qualified preservation services in Art. 34 and 40 [eIDAS] as well as § 15 [VDG] in Germany. The [GDPR] defines requirements on the confidentiality of personal data in electronic records and digital transactions [GDPR]. Apart from appropriate technical and organisational measures to protect the confidentiality of personal data especially the evidence for consent of the affected person, the obligation to inform (Art. 13+14) as well as the rights of the affected person have to be taken into account [We18].

## **2.2 Documentation and Technical Requirements**

### **Records Management**

In accordance with applicable law and international standardization e.g. [IS16], [IS20b] a valid records management with or without DLT provides the necessary processes, roles and responsibilities, governance and technical solutions for the management of electronic records which provide the evidence for business transactions. Essential characteristics are the authenticity, integrity and traceability of electronic records as well as their availability and transferability. These inherent properties have to be ensured and preserved as long as the records are needed. This requires the availability and transferability of the records – so their evidence based on the records themselves and their useability acc. to retention requirements e.g. readability, analysability etc. Records fulfilling these requirements are called authoritative records and their authoritativeness, so their authenticity, integrity and traceability, has to be preserved until the end of the retention period. A system creating, capturing, storing records until disposition, is called record system [We18] [IS16] [IS20]. So, if DLT is used in high-regulated industries where typically a valid records management is necessary, it acts as a record system and so has to fulfil the requirements on record systems and records management [IS16], [IS21a]. In DLT with on-chain and off-chain storage the evidence for a transaction needs the transactions records which are stored on-chain and the corresponding off-chain records for a valid records management [VL17], [IS21a].

### **Long-Term Preservation**

Cryptographical measures such as (qualified) electronic signatures and seals from qualified trust service providers [eIDAS] enable the non-repudiation and thus unique evidence of the authenticity of records as well as their integrity by trusted 3<sup>rd</sup> party. There is no trust by self-confirmation as done by DLT, only by proof and therefore by trust services [NIST], [Ko20]. Together with a qualified timestamp they also allow a valid PoE at the given time. DLT inherent cryptographical protocols do currently not fulfil the requirements on (qualified) signatures, seals or timestamps [eIDAS] and have to be enhanced with addition of eIDAS-compliant trust services needed to provide genuine verifiability of digital transactions as well as a PoE in DLT and the legal effects (equivalent to handwritten signature) of (qualified) e-signatures pursuant to [eIDAS]. This effectively requires the combination of DLT with trust service providers acting like a “trusted gatekeeper” to enable DLT for trustworthy digital transactions as it is currently also

required by first standards [Ko20], [DI21]. Cryptographical signature techniques (e.g. seals, signatures, timestamps, and evidence records) also enable the preservation of evidence of the records without losing the negotiability of the records [UN17]. That requires that measures regarding long-term preservation must focus on the record itself and not on the system or infrastructure in which they are stored [Sc17], [IS12], [KSH14]. Preservation of evidence over decade-long retention periods is currently executed by preservation mechanisms based on cryptographic measures by re-signing and rehashing of (qualified) signatures/seals in combination with a qualified electronic timestamp or evidence records pursuant to RFC4998 [GBP07] “in spite of obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or of the loss of the ability to check the validity status of public key certificates” [ET19b]. Utilization of Merkle Hash trees acc. to RFC4998 ensures an efficient approach as illustrated below.

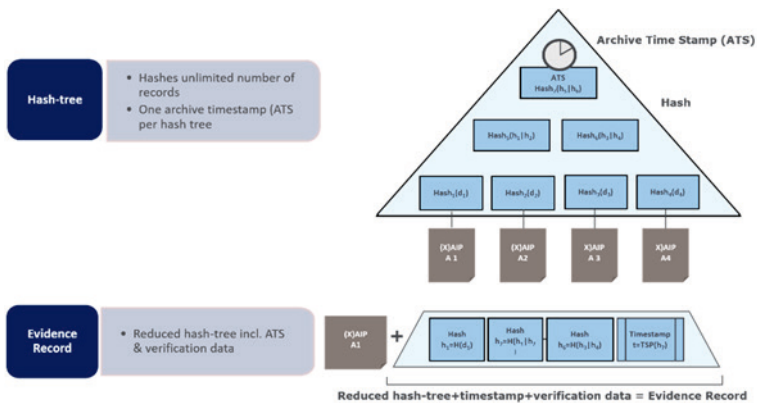


Figure 1: Hash-Tree and Evidence Record acc. to RFC 4998/6283

This procedure was adopted for (qualified) preservation services acc. to Art. 34 and 40 [eIDAS] by standards like [ET19b] [ET20a] for the service provider and in Germany [TR-ESOR] for the used preservation product. Since version 1.2.1 the [TR-ESOR] whose main content was adopted in [ET19b] and [ET20a] for European preservation services, is fully compliant to [eIDAS] and since version v1.2.2 it provides full interoperability to European ETSI standards. The [TR-ESOR] defines a reference architecture for evidence preservation service as well as container formats of self-contained archival information packages which contain all necessary information (metadata, content, credentials) to preserve evidence of electronic records and the records themselves. In addition to preservation of evidence also the traceability and availability of electronic records as well as the reliability of the transaction in which it was created have to be preserved, also in case of DLT. A comprehensible approach ensures both – the preservation of evidence and information of electronic records using well-defined processes and self-contained information packages in a trustworthy digital archive based on established international standards [IS12], [Sc17], [KoSH14].



### 3 Challenges in Records Management and Preservation of Evidence in DLT

Since currently there are no standardized measures in DLT to fulfil privacy requirements according to the [GDPR], it is recommended to store electronic records off-chain, if possible. In this case, only the transaction records remain on the chain. This leads to a complexity in the operation of DLT because the link between on-chain and off-chain records has to be preserved for as long as the records are needed. Another challenge stems from the fact that there are no standardized measures to preserve the information itself, i.e. its availability or technical interpretability over a retention period of 10, 20 or more years. To make the authenticity and integrity of on-chain records (e.g. transactions) evident towards 3<sup>rd</sup> parties, it is necessary to ensure crypto agility and the preservation of the evidence of records, and to renew the underlying hash protection in the light of technical improvements in cryptanalysis, and to couple it with a valid proof of existence including utilisation of state of the art hash-algorithms [ET19a] [SOGIS], [DI21], [Ko20], [Ya18]. A typical DLT application implies the storage of the relevant data (at minimum transaction records) in a dedicated transaction object (e.g. Tx01 on Figure 2) directly on the chain, possibly linked to off-chain records. The transaction records are protected by a Merkle-tree (by using the hash algorithm H), which's root (e.g. HR<sub>1</sub>) is placed in the block header (e.g. B<sub>1</sub>H) and together with the tree constitutes a single block (e.g. B<sub>1</sub>) on the chain [NA08]. On the other hand, the block header together with the tree constitutes a single block (e.g. B<sub>1</sub>) on the chain [NA08].

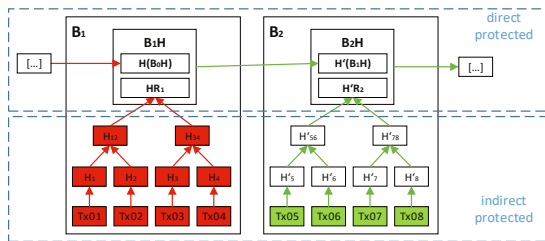


Figure 2: A sample of a blockchain with on-chain and off-chain storage – rehashing issue.

In case the used hash algorithm H (see block B<sub>1</sub>) is about to become weak, a hash algorithm change has taken place and the new block B<sub>2</sub> is using the new stronger hash algorithm H', which means sufficient protection (because directly hashed with H') for B<sub>2</sub> and the header of B<sub>1</sub> (pointed at with green arrows), but not for the Merkle-tree of B<sub>1</sub> (because only indirectly hashed with H' – actually only root of the tree) and all blocks before B<sub>1</sub> (red marked parts). It means, it is not definitely excluded, that possible manipulation of those transaction data remains undetected, which means, that the integrity protection and further the evidence preservation of those data is irrevocable lost. This also means that there is no long-term crypto stability in DLT currently as well as no PoE acc. to state-of-the-art technology as needed for burden of proof [We18], [eIDAS]. In order to preserve the evidence of the “red marked data” a suitable mechanism has to be applied to refresh the hash values of the all relevant data stored on and perhaps referenced from the chain as well as to provide a valid proof of existence. So, measures for crypto-stability and

preservation of evidence in DLT have to focus their actions on DLT.

### 4 Possible Solution

As mentioned above the hash protection in DLT is using Merkle-trees similar to preservation of evidence acc. to current standards in [ET19b], [ET20a] and [TR-ESOR]. This is the key for possible solutions. As mentioned in chap. 1 transaction records are always stored on-chain but any other records e.g. content etc. may also be stored off-chain and only referenced. As a direct implication of such an approach, an additional level of indirection is created, “double indirect protection” (see Figure 3). It means, the issues discussed in section 3 apply a fortiori.

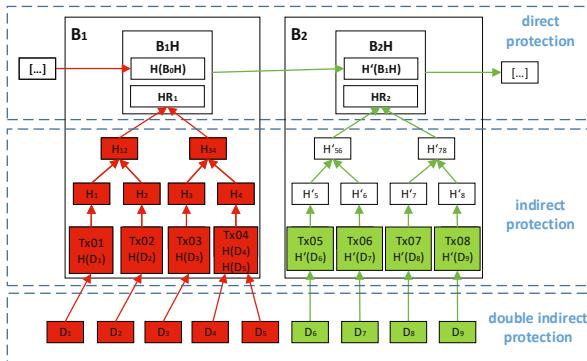


Figure 3: Blockchain example with off-chain transaction data and rehashing issue.

Due to the weakness of the hash algorithm H, which has been used in the block B1 and before the next block, B2 is using a stronger hash algorithm H'(typical blockchain rehashing approach). In such a case all the information hashed directly with H' is still sufficiently protected (marked green), but the parts of the chain, which have not been directly hashed with H', became weak (marked red) – the evidence would be lost [eIDAS], [VDG]. In order to keep the evidence on the whole chain, the approach of a “logical blockchain”, which based on the evidence record method described in RFC4998 [GBP07], has been developed. The RFC4998-method of the evidence preservation is purely based on the Merkle-trees and does in particular support the rehashing mechanisms. By using this approach, the whole blockchain data will be protected by a dedicated RFC4998-enabled tree. Following Figure 4 depicts the approach of “logical blockchain” by using the example of the blockchain illustrated in Figure 3.

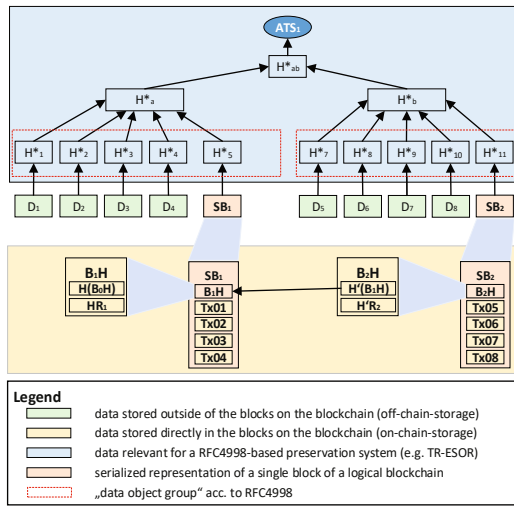


Figure 4: “Logical” blockchain

Every single block from the chain (here B<sub>1</sub> and B<sub>2</sub>) has to be slightly prepared in advance and suitably submitted to the RFC4998-based system. The following steps have to be performed:

1. A serialized replication of a block on the chain (serialized block, e.g. SB<sub>1</sub> on Figure 4) has to be created by the DLT for every single block to be protected on the RFC4998-based system. The serialized block does contain the data of the single block (especially the transaction data with the hash references on the external documents, but also the header and the hash tree) stored in a well-defined manner. The hash from the referenced off-chain records are renewed in this step.
2. For every block the serialized block (e.g. SB<sub>1</sub>) and (optional) a collection of the referenced documents (e.g. D<sub>1</sub>, D<sub>2</sub>, D<sub>3</sub>, D<sub>4</sub> and D<sub>5</sub>) build so called data object groups acc. to RFC4998.
3. Depending on the implemented approach by the preservation service to be used, it is possible either to submit the whole data object group built in step 2, or only the suitable hash value list, containing a hash of every single object in the group to the preservation service [TR-ESOR], [ET20a].
4. The preservation service internally builds the Merkle-tree and seals it with an archive-timestamp (e.g. ATS<sub>1</sub>).
5. The preservation service provides a unique id (AOID<sup>5</sup>) for every submitted data object group, which has to be stored for further purposes.
6. By using the received AOID it is possible to obtain the corresponding evidence record for the protected block incl. referenced off-chain records (e.g.  $ER_1^* = \{ \langle [ (H^*_1, H^*_2, H^*_3, H^*_4, H^*_5, H^*_6), (H^*_b) ], ATS_1 \rangle \}$ <sup>6</sup>).

<sup>5</sup> AOID – Archive Object ID

<sup>6</sup> An evidence record with one archive timestamp chain, reduced hash tree for data object group of SB<sub>1</sub> and a corresponding archive time stamp ATS<sub>1</sub>.

In case the hash algorithm of the preservation service (here  $H^*$ ) is about to lose its security suitability, the rehashing operation acc. to RFC4998 (see [GBP07], chapter 5.2) shall be applied in advance (by using a new hash algorithm e.g.  $H^{**}$ ) including the replicated block and sends notification to the DLT to rehash the off-chain-records referenced from the transaction records. This means it is an interaction of preservation service, DLT and off-chain storage. The resulted rehashed hash tree will preserve the evidence of the whole block data (on- and off-chain records). In order to perform the rehashing operation, the preservation service has to have access either to every corresponding data or its new hash value (see step 3 above). The renewed (rehashed) evidence record for a particular block, can be obtained by providing the corresponding AOID (see step 5 above) directly from the preservation service (e.g.  $ER_{11}^{**} = \{ \langle [ \{ (H^{**}_1, H^{**}_2, H^{**}_3, H^{**}_4, H^{**}_5, H^{**}_6), (H^{**}_b) \}, ATS_1 ] \rangle, \langle [ \{ (H^{**}_1, H^{**}_2, H^{**}_3, H^{**}_4, H^{**}_5, H^{**}_6), (H^{**}_b) \}, ATS_2 ] \rangle \}^7$ ). Even if the data of  $B_1$  is protected by a weak algorithm  $H$ , the possible manipulation of it could be easily detected by verifying the corresponding evidence record, respectively  $ER_{11}^*$  or  $ER_{11}^{**}$ . The provided solution makes use of 3 components, the preservation service, the DLT and the data storage with the off-chain records. The preservation service ensures the preservation of evidence acc. to [ET20a], [ET19b], [TR-ESOR] and the crypto-stability of the DLT as transaction- and or anchoring layer itself. The DLT represents the distributed application and contains the transaction records, the storage contains the off-chain records. To make a transaction evident the authenticity and integrity of on-chain transaction records as well as the linked off-chain records are needed [Ve16], [Ve17], [IS20], [IS21]. Picture below shows the interaction.

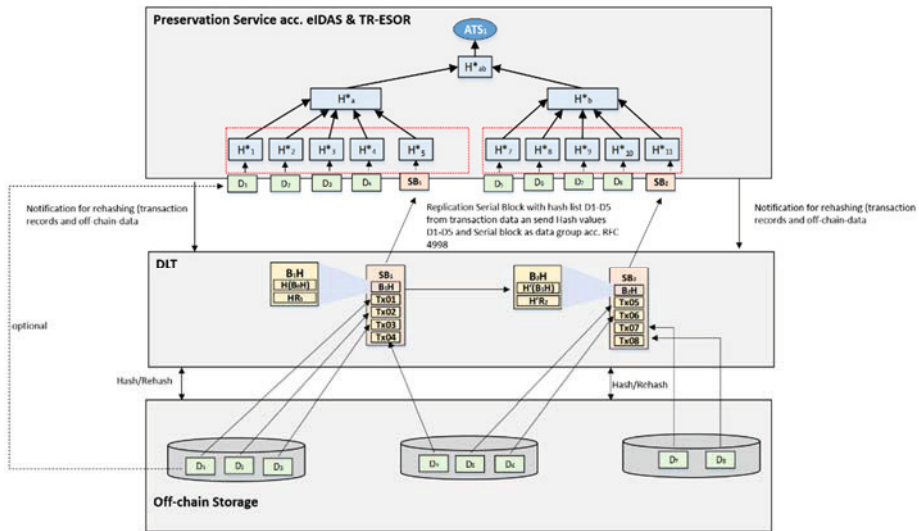


Figure 5: Solution example

<sup>7</sup> An evidence record with two archive timestamp chains, corresponding two reduced hashed trees of SB<sub>1</sub>, one with  $H^*$  and another one with  $H^{**}$  and two corresponding archive time stamps for every chain,  $ATS_1$  respectively  $ATS_2$ .

## 5 Conclusion and Needs for further Research

The utilisation of DLT increases also in regulated industries. This leads to the need for fulfilling burden of proof and documentation requirements so to achieve requirements on a valid records management as well as evidence against 3<sup>rd</sup> parties. Currently there are some challenges in DLT to reach legal verification needs as they are common in regulated environments such as deletion, portability or change of records but also evidence for authenticity, integrity and reliability of on-chain and off-chain records. With supplement of trust services acc. to [eIDAS] some challenges may be solved. But concerning decade-long retention periods the crypto stability, preservation of evidence and preservation of especially on-chain records themselves seem to be some of the main critical challenges for a wider DLT-utilisation. The approach mentioned in chap. 4 provides a feasible solution to preserve the authenticity and integrity of on-chain and off-chain records and so their evidence and to achieve crypto stability in DLT. De facto it probably must be done for each node.

This requires further technical standardization on DLT. Main requirements are the ability to create the serial block with all transactions from the block it contains including new hashes of the referenced off-chain records, the replication of the serial block to the preservation service including hash list of related off-chain records, receive and send notifications from and to the preservation service in case of rehashing to ensure the rehashing of off-chain records linked to the transactions in the serial block. A valid standardization should develop a generic solution which can be assessed and adopted for at minimum the leading DLT protocols e.g. Ethereum, Hyperledger Fabric, Hyperledger Indy (used for SSI) and Corda. The example described in the paper will be input for international standardization efforts in ISO and CEN, where the authors are taking part in.

## 6 Bibliography

- [An18] Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2017
- [BSI19] Federal Office for Information Security (BSI): Towards Secure Blockchains. Concepts, Requirements, Assessments. 2019.
- [DI21] DIN TS 31648: Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain. 2021.
- [DN21] UNE 71307-1 "Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. N72 CEN/CENELEC JTC19, Brussels 2021
- [EBSI] EBSI, European Blockchain Services Infrastructure, <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI>, accessed: 30/03/2020.
- [eIDAS] Regulation (EU) No 910/2014 of the European Parliament and of the Council - of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. eIDAS, 2014.
- [ESSIF] European Self-Sovereign-Identity Framework <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505734>

- [ET19a] ETSI: TS 119 312 - V1.3.1 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. 2019.
- [ET19b] ETSI: TS 119 511 - V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques. 2019.
- [ET20a] ETSI: TS 119 512 - V1.1.2 - Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services. 2020.
- [ET20b] ETSI Group Report 003. Permissioned Distributed Ledger (PDL). Application Scenarios
- [ET21] ETSI Group Report 004. Permissioned Distributed Ledgers (PDL) Smart Contracts. System Architecture and Functional Specification. 2021
- [EU18] Blockchain and the GDPR. EU Blockchain Observatory and Forum. Version 1.0. Brussels 2018
- [GBP07] Gondrom, T.; Brandner, R.; Pordesch, U.: Evidence Record Syntax (ERS), IETF RFC 4998. 2007
- [GDPR] Regulation (EU) 2016/ 679 of the European Parliament and of the Council - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation). GDPR, 2016.
- [IS12] ISO 14721:2012 Space data and information transfer systems - Open archival information system (OAIS) - Reference model, 2012.
- [IS16] ISO 15489-1:2016 Information and documentation - Records management - Part 1: Concepts and principles, 2016.
- [IS20a] ISO 22739:2020: Blockchain and distributed ledger technologies - Terminology, 2020.
- [IS20b] ISO 30300:2020 Information and documentation — Records management. Core concepts and vocabulary
- [IS21a] ISO/WD TR 24332 Information and documentation - Blockchain and DLT and records management: Issues and considerations, 2021.
- [IS21b] ISO/DIS 23257 Blockchain and distributed ledger technologies — Reference architecture. 2021.
- [JSG11] Jerman, A.; Saljic, S.; Gondrom, T.: Extensible Markup Language Evidence Record Syntax (XMLERS). IETF RFC 6283. 2011.
- [KHS14] Korte, U.; Hühnlein, D.; Schwalm, S.: Standards for the preservation of evidence and trust. Proceedings Archiving 2014, Springfield 2014, S. 9-14.
- [Ko18] Korte, U. et al.: Langfristige Beweiserhaltung und Datenschutz in der Blockchain, DACH-Security 2018. S. 177-191 Frechen 2018.
- [Ko20] Korte, U. et. al.: Criteria for trustworthy digital transactions – Blockchain/ DLT between eIDAS, GDPR, Data and Evidence Preservation. OpenIdentity Summit 2020. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2020 S. 49-60
- [Le16] Lemieux, V. L.: Trusting records: is Blockchain technology the answer? In Records Management Journal, 2016, 26; S. 110–139.

- [Le17] Lemieux, V.: A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. 2017 IEEE International Conference on Big Data (Big Data). DOI: 10.1109/BigData.2017.8258180
- [Me80] Merkle, R. C.: Protocols for Public Key Cryptosystems. In: 1980 IEEE Symposium on Security and Privacy. IEEE, Oakland, CA, 1980. S. 122-134.
- [NIST] NIST Special Publication 800-207. Zero Trust Architecture. 2020
- [OE17] OECD Digital Economy Outlook 2017. Organisation for Economic Co-operation and Development OECD, Paris, 2017.
- [RFC3161] Adams, C. et al.: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). IETF RFC 3161. 2001.
- [Sc17] Schwalm, S.: A service for the preservation of evidence and data – a key for a trustworthy & sustainable electronic business. Open Identity Summit 2017. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2017 S. 131-144
- [Schu19] Schütz, A. et al.: Blockchain für Entwickler. Das Handbuch für Software Engineers. Grundlagen, Programmierung, Anwendung. Bonn 2019
- [SM17] Sato, M.; Matsuo, S.'i.: Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography. In ICCCN: 26th International Conference on Computer Communications and Networks (ICCCN) July 31-August 3, 2017, Vancouver, Canada. IEEE, Piscataway, NJ; 2017, S. 1–8.
- [SO16] SOG-IS Crypto-Evaluation Scheme - Agreed Cryptographic Mechanisms-1.0. 2016.
- [TR-ESOR] Federal Office for Information Security (BSI): BSI Technical Guideline 03125, TR-ESOR – Preservation of Evidence of Cryptographically Signed Documents.v.1.2.2, <https://www.bsi.bund.de/EN/tr-esor>, 2019
- [UK16] UK Government Chief Scientific Adviser: Distributed Ledger Technology: beyond blockchain, 2016.
- [UN17] UN United Nations Commission on International Trade: UNCITRAL model law on electronic transferable records. United Nations, New York, 2017.
- [VDG] Vertrauensdienstegesetz. VDG, 2017.
- [We18] Weber, M. et al.: Records Management nach ISO 15489. Einführung und Anleitung. Beuth Verlag, Berlin, 2018.
- [Wer18] Werbach, K.: The Blockchain and the New architecture of Trust. Massachusetts Institute of Technology. 2018
- [Xu19] Xu, X. et. al.: Architecture for Blockchain Applications. Cham 2019
- [Ya18] Yaga, D. et al.: Blockchain technology overview. National Institute of Standards and Technology, Gaithersburg, MD, 2018.
- [Yak18] Yakubov et.al.: A Blockchain based PKI Management Framework. NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium. April 2018 DOI: 10.1109/NOMS.2018.8406325
- [Zi18] Zile, Kaspar et. Al.: Blockchain Use Cases and Their Feasibility. Applied Computer Systems May 2018, vol. 23, no. 1, pp. 12–20. doi: 10.2478/acss-2018-0002

# On the Market for Self-Sovereign Identity: Structure and Stakeholders

Michael Kubach<sup>1</sup> and Rachelle Sellung<sup>1</sup>

**Abstract:** For SSI solutions to make a significant impact, they need to be designed to cater to the requirements of the market to be adopted. Therefore, this paper proposes a structure of the market for SSI solutions, analyses its stakeholders, and surveys its current state.

**Keywords:** Self-sovereign identity, SSI, digital identity, decentralized identity, identity management, market, eID, stakeholders, trust, network effects

## 1 Introduction

The digital identity market remains a market with massive growth potential [Di19]. Given its potential, it makes sense that new technologies come along to take on the challenges. In the last years, Decentralized and Self-Sovereign identity (SSI) solutions have claimed to transform identity management. However, in order to transform the identity solutions market, one needs to understand and address market and stakeholder requirements.

In an emerging context, SSI is a term frequently used for blockchain-based identity management approaches. Yet, it is not always applied consistently. This paper follows the definition according to [Mü18], who summarized that a Self-sovereign identity management system allows users to fully own and manage their identity without having to rely on a third party.

In order to design SSI solutions that make an impact by reaching a significant share through adoption by users who can only then take back control of their identity data, we also need to take on a market perspective. However, users will only adopt, if those solutions are adopted by service providers/relying parties as well – and there might be other parties having a stake this process. Therefore, we will have to analyze the market structure for SSI solutions in general and in particular the stakeholder structure. This analysis serves as the basis for further research and recommendations on SSI that go beyond the often prevailing technological and privacy-oriented focus.

This paper explores the market structure of the SSI market in chapter 2. Building on that, in chapter 3 it adds a stakeholder analysis of the market. In chapter 4, it gives a brief overview of the current market offerings for SSI projects. Finally, in chapter 5 a conclusion of the paper is provided.

---

<sup>1</sup> Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, Germany, [firstname.lastname@iao.fraunhofer.de](mailto:firstname.lastname@iao.fraunhofer.de)



## 2 Market Structure

The literature on SSI considering a whole market and/or service provider perspective is scarce. So far, research seems to focus on technology development and on the supply side of identity management – repeating a pattern that has already been observed in Federated Identity Management (FIDM) [Ro14]. Based on the experience with Federated Identity Management as well as web identity management (WIM), we argue that the whole market has to be taken into account – supply as well as demand side. WIM approaches like Facebook Login that provide a clear value for End Users, Service Providers and Identity Providers have been widely adopted, while alternative approaches, even though they were technically sound and privacy friendly do not play a significant role on the market (CardSpace, Uprove, and Attribute Based Credentials) [UP20, Zi16].

Our market analysis builds on the previous work by [ZR12] and their model for the WIM market. The relationship between users and relying parties (service providers using the WIM) is heavily influenced by indirect network effects. One can observe a two-sided market where the “chicken or egg”-problem is apparent: When no services are supporting the WIM, it is not useful for the user. On the other hand, when no users have adopted the WIM yet, service providers’ motivation to implement it is quite minimal as there are no users that it can reach thorough the WIM. For a user to gain meaningful reduced sign-on capabilities across the web, a system has to be widely adopted, and its underlying protocol implemented by a wide range of service providers. An important aspect was already highlighted by [ZR12]. Relying parties seem to be scarce even for existing protocols: CardSpace (preinstalled in Windows Vista), and OpenID (AOL alone contributed 60 million accounts), had a huge user base – but were not widely adopted by relying parties. Today, with the Germany national eID we can observe a similar (non-)development: almost every German citizen above 16 years has it in his pocket, but barely anyone uses it as there are no service providers supporting it<sup>2</sup>.

One can observe that the utility for both sides in the WIM market significantly depends on the adoption of the WIM-Technology on the other side. This induces indirect network effects with positive feedback: if more service providers adopt a WIM system, more users will adopt, and the other way around. The presence of indirect network effects also identifies WIM as a two-sided market. Such a market serves two distinct types of customers, who depend on each other in some important way. Their joint participation makes the system more valuable to each. This means that there are indirect network externalities between the two different customer groups [Evan03]. One would expect that for SSI or other types of blockchain-based identity management systems this aspect of the market structure is similar because, just as in the case of WIM, we usually have a User accessing a Service Provider using the IdM-System where both, the User as well as the Service Provider need to adopt the IdM-System.

---

<sup>2</sup> Additional reasons might be that (1) it can only serve as alternative means of authentication, as most service providers do not focus solely on German citizens, and (2) it initially required special card readers.

The relationships towards the identity provider are mainly dominated by trust issues in the WIM market – principal-agent trust between users and identity provider and interorganizational trust between relying party and identity provider. Several authors have argued that insecurity and trust issues can make identity management systems fail, as users might be unwilling to delegate the handling of their personal identity information to someone (the identity provider) if they do not trust him. This has led to a strong focus on research and development on security as well as privacy for IdM-Systems [ZR12]. However, this trust is his subjective perception and not a completely objective decision based on the technical features of the identity management system. Research has also shown the limited influence of technological solutions on user’s trust perceptions with disposition to trust and institutional trust being important factors [MCK02, ZR12].

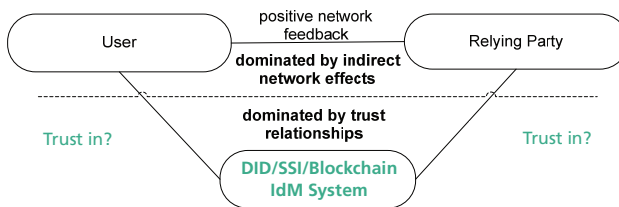


Figure 1: Structure of the SSI market as extension of [ZR12]

In fact, for the average end user it is very difficult to assess whether a certain security solution is technically well-designed, secure, privacy friendly and should thus be trustworthy. As [ZR12] have shown, asymmetric information about the security and/or privacy of an IdM-System is a problem that might lead to market failure. The relationship between identity provider and end use resembles one of a principal (end user) and its agent (identity provider). This makes it challenging for identity providers (agents) as market participants with high standards in terms of quality (i.e., security and privacy) as users cannot value these against identity providers offering solutions with lower quality standards but apparent value to the user (this could be ease of use, lower/no price, large base of Service Providers etc.). This challenge remains in the market for SSI or other blockchain-based IdM-Systems. However, depending on the particular implementation of the IdM-System, there might not be a specific organization acting as identity provider. Calling the trust relationship principal-agent trust might therefore seem inappropriate, even though the challenges appear quite similar (it may even be more difficult for the user to assess the quality and trustworthiness of the SSI or other blockchain-based IdM-System as there is not a single provider and the whole system is even more complex). Trust in technology could be an important aspect. There are, however, SSI-Solutions like Sovrin’s (<https://sovrin.org/>) that are governed by a foundation. Sovrin and its branded wallet could appear to the average end user as something like a service provider. In this case, something pretty close to the WIM-model might even be appropriate.

The relationship between relying party and identity provider for WIM is described by [ZR12] as dominated by interorganizational trust. Apparently, the authors expect that relying parties are more capable to assess the trustworthiness of an identity provider

objectively. The information asymmetry does not seem to play such an important role. This might be the case for relying parties with sufficient IT-competence but seems less likely for firms like start-ups or small shops. However, the relying party as organization has to trust the identity provider as organization to act in its best interest. This is of course dependent on the power relationship between both organizations as well as the institutional framework, the possibility to observe violations and to sanction them etc. For SSI Systems, there is no identity provider as a single organization. Therefore, we cannot speak of interorganizational trust here – except for the Sovrin case (or similar ones) as mentioned above. Trust in technology is similarly important as above, as the complexity of SSI system certainly exceeds the IT-competence of many relying parties.

Concluding, regarding the market structure there doesn't appear to be fundamental differences between classic web identity management (WIM) and the newly proposed SSI approaches. One can still observe a multi-sided market that is subject to indirect network effects and influenced by trust relationships. The chicken and egg problem of getting enough service providers for end users while at the same time requiring a large user base to be attractive to service providers persists. For the average end user and smaller businesses as service providers with limited IT-security expertise the trust relationship in the SSI market might be even more complex as it is unclear who the counterparty actually is and what to do in case of problems.

In summary, there are three main challenges that the market faces regarding SSI solutions. First, the challenge of trust management. As described by [Ku20], there is an absence of a natural trust anchor for DLT based digital identities. For example, the problem that SSI-based solutions face is addressing “How can one trust that the credential issuing entity is who they claim to be?”. The answer to this could be to add a gate keeper or a centralized governance layer, however, in turn this could be argued to defeat a key reason to use SSI solutions in the first place. Potentially, a decentralized trust architecture such as proposed at [Wa17] could be a way forward here. Second, the aforementioned challenge of network effects that every identity management system aiming at broader adoption faces with the resulting chicken and egg problem. Third, the challenges of establishing viable business models for all relevant stakeholders as also referenced by [Ku13].

### **3 Stakeholder Analysis**

Building on the method of a stakeholder analysis, we further analyze the requirements and interests of the different actors in the SSI ecosystems that have to be considered for the market to be sustainable. The most common definition of the term stakeholder goes back to [Fr84]. Hence, an organization's stakeholder is, a group or individual who influences or is influenced by the achievement of organizational goals. Pouloudi and Whitley [PW97] clarify this definition for an information systems context as those actors (persons, groups or organizations) involved in the development process, whose actions influence or are influenced by these factors, both directly and indirectly, in the development and use of a

system. For further analysis, and to address their requirements specifically, stakeholders can be subdivided into groups, which in turn pursue similar demands or can influence the success of the project in different ways. Different categorization approaches have been presented, e.g. by Cotterell and Hughes, [CH95], Sharp et al. [SFG99], and Sillitti and Succi [SS05]. It is clear that those stakeholder categorizations, when viewed individually, each have clear gaps. However, these generic groups of stakeholders proposed in the literature can serve as a starting point to identify stakeholder groups that are relevant for the success of SSI ecosystems. Therefore, we combine those categorizations into one that seems suited for this specific context.

First, we differentiate between two main stakeholder groups: direct participants of the ecosystem and such actors that are only indirectly involved in its daily business. We call the first group “Active Stakeholders” and the second group “Enabling Stakeholders”.

Active Stakeholders						
Users						ID-/Credential-/Trust Providers
End-Users (Subjects/Holders)	Service Provider/Relying Parties (Verifiers – Companies and other Organizations)					National eID Providers / Systems
Organizations	B2B	B2C		e-Government/ Administration	Humanitarian / Development Organizations	IT-/Platform-Corporations-IDs
End-Users (Consumers)	Intraorganizational	Online	Offline	Local / District Level	Focusing on Refugees	ID-Service Providers/-Platforms
End-Users (in Organizations)	Interorganizational (federated)	Large Portals / Platforms	Public Transport	State Level	Focusing on Development / Persons w/o ID	SSI-/DIdM -Startups / Organizations
Refugees		Medium eBusinesses	Travel / Hotels	Federal / National Level		other Credential-Providers (Issuers)
Persons without Legal Proof of Identity		Smaller eBusinesses / Startups	Banking / Financial Services	EU		Trust Service Provider
		Banking / Financial Services	(Car) Sharing / Rental	Supranational		

Figure 2: Active Stakeholders in the SSI Ecosystem

Figure 2 depicts the Active Stakeholders as main group in the SSI ecosystem. Active stakeholders can be split into the two types of Users of identity services, whom would be interested in a specific use case that requires an identity service rather than in the identity service itself, and ID-/Credential/Trust Providers. Those two Active Stakeholder groups, the Users and ID-/Credential/Trust Providers, are actively involved in the everyday processes in the ecosystem, e.g., by issuing credentials operating ID-Systems or taking on another role in the ecosystem. In these stakeholder roles, those actors have a high economic interest in the sustainable success of the ecosystem (ID-/Credential Providers) or derive some other kind of direct value from it, e.g., as it supplies them with a secure and easy to use digital identity. With that in consideration, active stakeholders are of high relevance for the value creation in the ecosystem, and thus for the SSI business models.

ID-/Credential/Trust Providers provide digital IDs or components or related services in the ecosystem. In this stakeholder role, the focus is not on them using digital identity or trust services themselves. The types of organizations and interests of these stakeholders may differ significantly. Nevertheless, a viable business model remunerating the effort they put into the ID ecosystem needs to be developed for all of these entities. With certain restrictions, this even applies to National eID Providers/Systems operated by governmental institutions. In addition, this group includes: IT-/Platform-Corporation-IDs (for example, Google Login, Apple ID, Facebook Login, etc.), ID-Service Providers/-Platforms (Verimi, Yes, etc.), SSI-/DIDM-Startups/Organizations (Sovrin/Evernym, Jolocom, etc.), other Credential-Providers (Issuers, such as Mobile Connect, or even Universities etc.), and finally Trust Service Providers (Schufa, etc.).

The User stakeholder-group, that contains persons or entities making use of digital identities in some form, is divided further into End-Users that are actually using services in the ecosystem (also known as Holders or Subjects – depending on the perspective and use case) and Service Providers/Relying Parties (also Verifiers) that are usually companies and organizations offering a specific service that requires trust or identity information.

Regarding the End-Users (Subjects), who use their digital identity themselves in the ecosystem, we would like to focus in this paper on the identities of natural persons. These are to be distinguished from the digital identities of organizations, legal entities, and in the context of the Internet of Things (IoT), identities of things/devices, e.g., for sensor data. Identities of natural persons are further differentiated into End-Users (Consumers) and End-Users (in organizations), e.g., identities/accounts for employees, since different requirements and interest are of relevance here. Refugees and persons without legal proof of identity are also currently a much-discussed use case for secure digital identities that have high requirements for privacy and trust, but also for international and interorganizational interoperability.

Service Providers/Relying Parties that use digital IDs can be grouped into four categories according to use case: (1) B2B applications, (2) B2C applications, for (3) e-Government/Administration, and (4) Humanitarian/Development Organizations.

In B2B applications, organizations might use digital IDs internally to identify their employees (this is sometimes referred to as B2E - business to employee), for example as a basis of their access rights management. Since today's distributed value chains increasingly involve direct collaboration in digital processes across organizations, this identification of employees is also necessary there – which in turn creates additional challenges (relating also to Federated Identity Management) [Ku14].

B2C applications can be further differentiated into online or offline applications on the basis of their provision. Here, too, different requirements and framework conditions apply.

Online applications are provided, for example, by Large Portals or Platforms. Their requirements and capabilities (financial capacity, IT expertise, etc.) differ significantly from those of Medium-Sized eBusinesses, which in turn must be distinguished from

Smaller eBusinesses / Startups. Banks / financial service providers have special requirements as well – this illustrates that even more types of stakeholders are emerging here, which would have to be differentiated on the basis of the use cases and their specific requirements, so that this list cannot be exhaustive.

For offline applications, only exemplary use cases are listed as well. These include Public Transport, Travel/Hotels (Tourism), Banking/Financial Services, and (Car)Sharing or Rental. In contrast to online use cases, the particular challenge here is that the digital ID (usually stored on the smartphone) must also be suited for verification in the "offline environment". NFC interfaces or QR codes are often used here – forms of visual verification may also be possible.

e-Government / Administration is a stakeholder group that is often in the particular focus of publicly funded digital identity research projects. Here, there is a particular need to digitize processes; at the same time, these organizations are often subject to particularly high requirements regarding the legal security and Levels of Assurance (LoA) of digital identities. This overview is oriented at the federal structure of the German state and its integration into the EU – of course it could easily be adjusted for other national contexts. As stakeholder groups or levels, we identify: municipalities on the Local / District Level, Länder on the State Level, Bund on the State / Federal Level, and the EU (an important player with the eIDAS regulation, among other things). Supranational institutions and agreements (e.g., on digital passports, visas and apostilles) may also have an influence on the development and success of digital identities, which is why they are also listed here.

Finally, there is the group of Humanitarian/Development Organizations. Here, we can differentiate between organizations with a focus on refugees, such as the UNHCR, and others with a focus on development and persons without legal proof of identity in general (the World Bank being very active here).

While Enabling Stakeholders (as shown in Figure 3) are not actively involved in the daily business of a SSI Ecosystem and in this role are neither users nor providers of identity services or components, they are still relevant for its overall success as they are indirectly involved in various forms as can be seen in the following.

The enabling stakeholder group is separated further into “Developing Stakeholders” and “Framing Stakeholders”. The first group consists of actors that are developing the technology and standards required for the ecosystem (e.g., SSI/DidM Startups, ID-Technology Companies and Large IT-Corporations). Thus, those stakeholders have an interest in the success of the technology and need to generate some kind of revenue to cover their costs for R&D. Some of those stakeholders could take on the role of an active stakeholder at the same time, when they also operate SSI components, but this does not always have to be the case. Hence, the business model of those stakeholders can differ from the one of active stakeholders.

The second group of Enabling Stakeholders are “Framing Stakeholders”. Those actors set the framework conditions for the SSI Ecosystem without actively using or developing the

actual technology and its components. However, through the development of basic technologies (Research Organizations) or forming the regulatory framework (Regulatory/Legislative Bodies), overseeing data protection regulations (Data Protection Institutions), influencing public discussions and the legislative process (Civil Society and Multipliers) and so on, they can be a significant success factor for the ecosystem. Their direct economic interest and investment in the SSI Ecosystem is, however, quite low and, hence, their relevance for the business models in the ecosystem limited.

Enabling Stakeholders	
Developing Stakeholders	Framing Stakeholders
SSI/DIdM-Startups	Research Organizations
ID-Technology Companies	Regulatory / Legislative Bodies
Large IT-Corporations	Data Protection Institutions
Organizations/ Foundations (e.g. Hyperledger)	Civil Society
Standardizing Bodies	Multipliers

Figure 3: Enabling Stakeholders in the SSI Ecosystem

In order to achieve market success, SSI solutions need to address the requirements of all relevant stakeholders in a specific use case – and not just focus on a single group i.e., the consumer. The relevant stakeholders’ priorities rely on what value creation is gained from a solution. For example, value creation could be having increased usability, security or privacy benefits, greater convenience, or financial benefits depending on the requirements of each respective stakeholder.

#### 4 Brief Overview of the Current Market Offerings for SSI

Due to the novelty of the basic technology, the market for SSI is in a state of dynamic movement. An exhaustive overview of all market offerings currently available or in development is therefore hardly possible. Nevertheless, there have been a few recent papers aiming to summarize and analyze various aspects of SSI solutions or projects and trying to give an overview of the current market situation and maturity.

Dunphy and Petitcolas [DP18] focus their analysis on three solutions (uPort, ShoCard, Sovrin). Regarding usability, they conclude that all of those projects have an “unclear usability and user understanding of [...] (the) privacy implications.” What they completely disregard in their analysis is a comprehensive stakeholder perspective, in particular of the service providers’. They only evaluate the solutions regarding the “laws of identity” that

solely focus on the user [DP18]. This goes in line with publications of SSI projects that mainly present the benefits in security and privacy for the user while disregarding that service providers have to implement those solutions for users being able to use them.

In an extensive analysis, [Ku19] surveyed 43 approaches to blockchain-based identity management from the enterprise and ecosystem perspective. He applies an impressive set of 12 compliance and liability criteria, 32 end-user experience criteria, and 29 technology, implementation, integration and operations criteria. Quantitative properties such as performance are not included, what he justifies with the low level of maturity of the solutions available. In conclusion, he finds very different levels of maturity and only few solutions that could compete with traditional approaches. Overall, business models are lacking (see also section 2 and 3), so are compliance and enterprise-grade aspects (liability, revocation) and usability.

A recent overview [DT20], analyzed the “most relevant” (without defining this further) SSI solutions regarding the 10 principles of SSI [Al16]. The SSI solutions included in this evaluation were: uPort, Sovrin, ShoCard, IDchainZ, EverID, LifeID, SelfKey, Civic, TheKey, and Bitnation. From this analysis, 8 categories of challenges were derived. Two technical challenges: (1) challenges related to the use of blockchain, and (2) challenges in the context of key management. Six non-technical issues: (1) transfer from legacy systems, (2) lack of regulatory systems adjusted for SSI, (3) lack/immaturity of standards leading to interoperability issues, (4) adoption by users of all sides, (5) accessibility through vulnerable and/or disadvantaged persons, and (6), complex behavior of actors required to adopt the solution. Many of the challenges identified in this analysis go in line with our findings in sections 2 and 3, as well as the analysis of [Ku20].

For this paper we have also reviewed a collection of SSI projects to gain an impression of the current state of the market. Figure 4 presents an overview as of January 2021.

SSI Projects reviewed in 2021		
Connect.Me	IKosmos BlockID	Spherity
Uportlandia	Blockpass	Onfido*
Jolocom SmartWallet	Knownmenow	Yoti*
Bloom-Secure Identity	Nuggets	Shocard
Meeco	SelfKey	HelixID
Keepin	Confidare	Blockcerts
Iden3	Civic Secure Identity	Estatus
Onto	mySaveID	OneIdentity
Lissi	Authenteq*	Trinsic
		MAX-Wallet

Figure 4: Overview of SSI Projects at start of 2020 and 2021

In order to be integrated, the projects needed to meet the following requirements: They needed to have a working prototype (available on request) or even be available as a desktop version or from the Android or Apple app store. Projects marked with an asterisk are not solely decentralized / blockchain based wallets but claim to be SSI approaches. At the start of 2020, 23 projects were identified. In an update of the analysis in January 2021,



we could add six projects to the list. It appears that these projects are still in the early and agile stages of development, where even the more advanced projects are still undergoing frequent, noticeable changes or even remove essential features such as key backups.

After reviewing all the forementioned digital wallets, a use case analysis was conducted. We assume that the use cases an SSI solution proposes are those where it assumes to be able to create the most value. In Figure 1, an overview is given of the six key use cases that those solutions present as valuable areas for the application of their product. We also counted, how often a respective use case was proposed in our sample (# Proposed). This could serve as an indicator for the areas on which SSI currently the focuses the most. Of the 29 reviewed projects, the identity verification (19 projects) and exchange of information (20 projects) use cases were proposed the most often.

Use Case	Description	# Proposed
<b>Identity Verification</b>	e.g., public safety enforcement, university, job, doctor's office, pharmacy	19
<b>Document Verification</b>	ID, Green Card, Social Security Card, medical insurance card, driver's license, insurance coverage, employment card, city ID, college transcripts, university diploma, credit score, drug prescription, credit card, public transport ticket, membership (e.g., museum)	16
<b>Application for Services</b>	Applying for citizenship, job, loan/credit, etc.	8
<b>Single Sign-on</b>	Apps, websites, social media, bank account, car renting, games, IoT devices	13
<b>Exchange of Information</b>	Payment, data, person check (renting a room, buy or sell items, date online), exchanging cryptocurrency, multiple forms (auto-fill), token trading	20
<b>Electronic Signatures</b>	Signing of documents with a qualified electronic signature	6

Figure 5: Overview of use cases proposed by SSI solutions

While the Identity Verification, Document Verification, and Exchange of Information Use Cases were proposed by the majority of the reviewed projects, these use cases particularly face the beforementioned trust management challenge. While, as an example, Identity Verification might be a use case that doesn't occur daily for the average user, Exchange of Services and especially Single-Sign-On could be more relevant from this perspective. Generally, our analysis could indicate that the use cases are not driven by the respective business potential and added value for the end user and other stakeholders, but rather by technical feasibility and potential to showcase adherence to the SSI principles. One could cast doubt, whether this is enough for the adoption of the technology by the stakeholders.

## 5 Conclusion

Overall, SSI solutions that aim to make an impact, need to take on a market perspective to meet the requirements of all relevant stakeholders. The understanding of the market as

well as the stakeholder structure and not only the technical challenges are crucial for the adoption of these solutions. With this understanding, one can design solutions that provide value for all relevant stakeholders, overcoming the “chicken or egg”-problem, to achieve wide adoption. These fundamental steps are needed in order to reach market success for new SSI solutions – and only those with market success can actually be used, and then protect the sovereignty of peoples’ identities.

This paper aimed to serve as a basis for further research and development for SSI solutions. We pointed out challenges resulting from the specific market structure – such as the network effects and the complex trust relationship. Moreover, we argued that the SSI ecosystem consist of a number of stakeholders whose specific requirements need to be met – not just those of the end user. We presented a generic map of those stakeholders of the SSI ecosystem – distinguishing active and enabling stakeholders. This can serve as a starting point for a use case-specific stakeholder analysis. The overview of the market that was based on recent literature and our own survey revealed that the current market offerings still have significant challenges to overcome. The analysis of the other authors goes pretty much in line with our analysis here. The market and its offerings are still immature and under heavy development.

Future work could take this market structure and stakeholder analysis as a basis to be expanded by further qualitative and quantitative empirical studies on the needs and requirements of real stakeholders, e.g., service providers, and end users regarding SSI. Regarding this, we see it as important to highlight that non-technical aspects are as important as technical functionalities. User experience, functioning trust management and viable business models are as relevant for the success of SSI as are zero knowledge proofs.

## 6 References

- [Al16] Allen, C.: The Path to Self-Sovereign Identity., <https://github.com/ChristopherA/self-sovereign-identity>, accessed: 05/02/2020.
- [CH95] Cotterell, M.; Hughes, Bob: Software project management: International Thomson Computer Press, 1995.
- [Di19] MarketsandMarkets: Digital Identity Solutions Market Size, Share and Global Market Forecast to 2024., <https://www.marketsandmarkets.com/Market-Reports/digital-identity-solutions-market-247527694.html>, accessed: 21/02/2020.
- [DP18] Dunphy, P.; Petitcolas, F.: A First Look at Identity Management Schemes on the Blockchain 2018. In: IEEE Computer and Reliability Societies, 2018.
- [DT20] Dib, O.; Toumi, K.: Decentralized identity systems: Architecture, challenges, solutions and future directions. In: Annals of Emerging Technologies in Computing Bd. 4, Nr. 5, pp. 19–40, 2020.
- [Ev03] Evans, D.: The Antitrust Economics of Two-sided Markets. In: Yale Journal on Regulation Bd. 20, Nr. 2, pp. 235–294, 2003.

- [Fr84] Freeman, R.E: *Strategic Management: A Stakeholder Approach*. Cambridge: Ballinger Publishing Co, 1984.
- [Ku13] Kubach, M.; Roßnagel, H.; Sellung, R.: Service providers' requirements for eID solutions: Empirical evidence from the leisure sector. In: Hühnlein, D.; Roßnagel, H. (Hrsg.): *Open Identity Summit 2013 - Lecture Notes in Informatics (LNI) - Proceedings*. Bonn, pp. 69–81, 2013.
- [Ku14] Kubach, M. et.al.: ENX ID – An Architecture for Practical and Secure Cross Company Authentication. In: Hühnlein, D.; Roßnagel, H. (Hrsg.): *Open Identity Summit 2014, Lecture Notes in Informatics – Proceedings*: Köln, pp. 109–120, 2014
- [Ku19] Kuperberg, M.: *Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective*. In: *IEEE Transactions on Engineering Management*, 2019.
- [Ku20] Kubach, M. et.al.: Self-sovereign and Decentralized identity as the future of identity management? In: *Open Identity Summit 2020 - Lecture Notes in Informatics (LNI) - Proceedings*. Bonn: Köllen Druck + Verlag GmbH, 2020, pp. 35–47, 2020.
- [MCK02] McKnight, D H.; Choudhury, V.; Kacmar, C.: Developing and validating trust measures for e-commerce: An integrative typology. In: *Information systems research* Bd. 13, Nr. 3, pp. 334–359, 2002.
- [Mü18] Mühle, A. et.al.: A survey on essential components of a self-sovereign identity. In: *Computer Science Review* Bd. 30, pp. 80–86, 2018.
- [PW97] Pouloudi, A.; Whitley, E.: Stakeholder identification in inter-organizational systems: gaining insights for drug use management systems. In: *European journal of information systems* Bd. 6, Nr. 1, pp. 1–14, 1997.
- [Ro14] Roßnagel, H. et.al.: Users' willingness to pay for web identity management systems. In: *European Journal of Information Systems* Bd. 23, Nr. 1, pp. 36–50, 2014.
- [SFG99] Sharp, H.; Finkelstein, A.; Galal, G.: Stakeholder identification in the requirements engineering process. In: *Proceedings. Tenth International Workshop on Database and Expert Systems Applications. DEXA 99*, pp. 387–391, 1999.
- [SS05] Sillitti, A.; Succi, G.: Requirements engineering for agile methods. In: *Engineering and Managing Software Requirements*: Springer, pp. 309–326, 2005.
- [UP20] U-Prove., <https://www.microsoft.com/en-us/research/project/u-prove/?from=https%3A%2F%2Fresearch.microsoft.com%2Fen-us%2Fprojects%2Fu-prove.>, accessed: 2020-09-25.
- [Wa17] Wagner, S. et.al.: A mechanism for discovery and verification of trust scheme memberships: The LIGHTest Reference Architecture. In: *Open Identity Summit 2017, Lecture Notes in Informatics (LNI), Lecture Notes in Informatics (LNI)*. Bd. P277. Bonn: Köllen Druck + Verlag GmbH, pp. 81–92, 2017.
- [Zi16] Zibuschka, J.; Hinz, O.; Roßnagel, H.; Muntermann, J.: *Zahlungsbereitschaft für Föderiertes Identitätsmanagement*, Baden-Baden, 2016.
- [ZR12] Zibuschka, J.; Roßnagel, H.: Stakeholder Economics of Identity Management Infrastructures for the Web. In: *Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012)*. Karlskrona, Sweden, 2012.

# A lightweight trust management infrastructure for self-sovereign identity

Michael Kubach<sup>1</sup> and Heiko Roßnagel<sup>1</sup>

**Abstract:** Decentralized approaches towards digital identity management, often summarized under the currently popular term Self-sovereign identity (SSI) are being associated with high hopes for a bright future of identity management (IdM). Numerous private, open source as well as publicly funded research initiatives pursue this approach with the aim to finally bring universally usable, trustworthy, interoperable, secure, and privacy friendly digital identities for everyone and all use cases. However, a major challenge that so far has been only rudimentary addressed, is the trust management in these decentralized identity ecosystems. This paper first elaborates this problem before presenting an approach for a trust management infrastructure in SSI ecosystems that is based on already completed work for trust management in digital transactions.

**Keywords:** Self-sovereign identity, SSI, digital identity, decentralized identity, identity management, IdM, trust, trust frameworks, trust schemes, trust lists, IT-security, eID, eIDAS

## 1 Introduction

Despite of years of research and development, the availability of different technical approaches and eIDAS creating a stable EU level regulatory framework, establishing trust for secure digital identities remains a challenge in practice. With a few exceptions (e.g., Austria, Estonia), the wider adoption (including by private sector service providers) of identity solutions with high levels of assurance has remained limited. Instead, the market is dominated by web and cloud identities with low assurance levels, mainly provided by big transatlantic platform corporations. Worries exist, that this lack of secure digital identities could slow down the digitalization of the European society and economy. Moreover, there is the real risk that European digital sovereignty is in danger if big international platform corporations take over control of digital identities and trust management as they have done in such areas as smartphone operating systems, social media platforms, web search and cloud services. Solving the challenge of trust and secure digital identities is therefore an important task for the digital sovereignty and the cohesion of the European single market. The increasing importance of digital identities for things/devices only tightens the situation. This analysis is reflected in several initiatives that have been brought on track in the recent months, such as the European Commission's vision for a European Digital Identity [ON20, St20] and similar initiatives by the German government [DI20].

Regarding the technological basis for secure digital identities, so-called Self-sovereign

---

<sup>1</sup> Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, Germany, [firstname.lastname@iao.fraunhofer.de](mailto:firstname.lastname@iao.fraunhofer.de)

identity approaches are favoured by many, calling them “the next evolutionary step in the development of digital identities” [DE20], the future of digital identity [Si18] etc. and marketed as easy to roll out and ready for productive use (e.g. [PR20]). All four R&D projects that were recently selected for the final phase of the German “Schaufenster Sichere Digitale Identitäten” (Showcase Secure Digital Identities), receiving in total over 40 million EUR in governmental funding, build mainly on SSI [SH21].

Surfing the wave of the blockchain hype, the term and respective projects have emerged from blockchain/Distributed Ledger Technology (DLT)-based and other decentralized identity solutions. While not always used consistently, these approaches usually aim to allow users to fully own and manage their digital identity without having to rely on a third party. The DLT is used to build a decentralized Public Key Infrastructure (PKI). End users usually manage keys and credentials for their digital identities in smartphone application “wallets” [Le20, Mü18]. The privacy-focused vision and term SSI are rooted in the *Ten Principles of Self-sovereign Identity* postulated by [Al16]. It can be noted, however, that SSI has since been gradually emancipating itself from the blockchain context and there have been proposals for SSI-approaches not relying on blockchain/DLT [Sm21].

However, despite the high hopes that are placed in SSI-technology, it still has to overcome significant challenges before a wide adoption seems possible. Some of these apply to all types of IdM solutions. Those are the complicated multi-sided market with non-interoperable solutions that leads to a “chicken or egg” problem, the creation of sustainable and balanced trust relationships between identity providers, relying parties and users [ZR12], and creating sustainable business models in IdM ecosystems [Ku13] with generally low willingness to pay of users and preferences of convenience often overtaking privacy and security concerns [Ro14]. Most IdM solutions have so far not been particularly successful in solving these challenges. In addition to that, SSI, due to its particular approach and still relative immaturity, faces some distinct challenges. In a previous paper [Ku20] we have summarized those as into four main aspects: (1) Immaturity of the technology without established standards: Building solutions while SSI technologies and standards are still under development and evolving rapidly, (2) Usability and User Experience: Self-administration of digital identities and private keys for non-technical users, (3) Transparency vs. unlinkability: Reliable and transparent revocation of SSI based credentials and claims, and (4) Trust management: Absence of a natural trust anchor for DLT-based digital identities. Those four challenges and the aforementioned general ones coincide well with the eight challenges identified by [DT20] in a recent review of decentralized identity systems.

In this paper we want to focus on just the set of challenges that is related to trust management. This is not meant to disregard the importance of the others, but for trust management we can build on previous work in a research project for a different, but similar use case to propose an approach that might be valuable for SSI.

The remainder of the paper is structured as follows. Next, we will analyse the trust-related challenges in SSI in greater detail (chapter 2) and address relevant related work on these

topics (chapter 3). Then, we will present our approach to trust management in SSI (chapter 4), before concluding the paper.

## 2 Some trust-related challenges in Self-sovereign identity approaches

SSI approaches put a high emphasis on the user's control over their data. In the Principles of Self-sovereign identity [A116], the interests of other stakeholders of the identity ecosystem are not considered. Data is to be freed from the siloes of service providers and dependence on trusted third parties is to be minimized. It is expected that this is going to foster trust into the technology by end users and eventually foster adoption of the technology through them. To achieve this, the most prominent SSI approaches only store non-personal data on public blockchains and build on components such as Decentralized Identifiers (DIDs) [DE21], Verifiable Credentials (VCs) [VR20] with Zero Knowledge Proofs that allow for highly privacy-friendly solutions [Le20]. While this is certainly an important aspect for the adoption, we certainly cannot dismiss the trust requirements of the other relevant stakeholders in the identity ecosystem that are also essential for the adoption of an identity technology [ZR12]. Here, the relying parties (RP) also known as service providers (SP) are of particular importance, as they offer services that end users might want to access with a somehow provided and managed digital identity. In the following, we address trust-related challenges of SSI that are especially relevant from a service provider's perspective. First, we will turn to the challenge of the root of trust in SSI solutions. Second, we will focus on the challenge to manage complex trust-relationships between multiple actors/ organizations on different levels in an automated manner, so that the solution is scalable in practice.

### 2.1 Absence of a natural trust anchor

Establishing a chain of trust in SSI approaches remains a major challenge. How can it be assured that the credential issuing entity is in fact the entity that it claims to be? How can partners in a digital interaction be certain that a public key really belongs to the claimed entity? This challenge is illustrated in the simplified example depicted in Figure 1. In this SSI architecture, following basic SSI principles, credentials can be issued by anyone: any *Bank* or *Fake Bank* can issue a credential about the solvency of Tom (holder)<sup>2</sup>. It is cryptographically easy to verify for *Web Shop* (service provider/relying party/verifier) whether the solvency credential was really issued from *Bank* or *Fake Bank* to Tom and

---

<sup>2</sup> The "solvency credential" here simply serves as a handy example for this illustrative use case. There are certainly other ways for *Web Shop* to ensure to get paid. However, this use case example aims to illustrate how there is a need for identity attributes or credentials to be issued by parties that can be trusted by service providers and how this trust can be established in a scalable manner while leaving the trust decision with the verifiers.

has not been tampered or revoked.

The credential issuers *Bank* or *Fake Bank* are not involved in the proof of solvency by Tom to the *Web Shop*, so the privacy of Tom is protected. The question that remains is what happens if *Fake Bank* is a fraudulent service posing as *Bank* that just issues solvency credentials to anyone? How can the *Web Shop* assess the trustworthiness of the issuing *Bank* and/or the Level of Assurance of the Credential? How can this process be automated so that it is scalable?

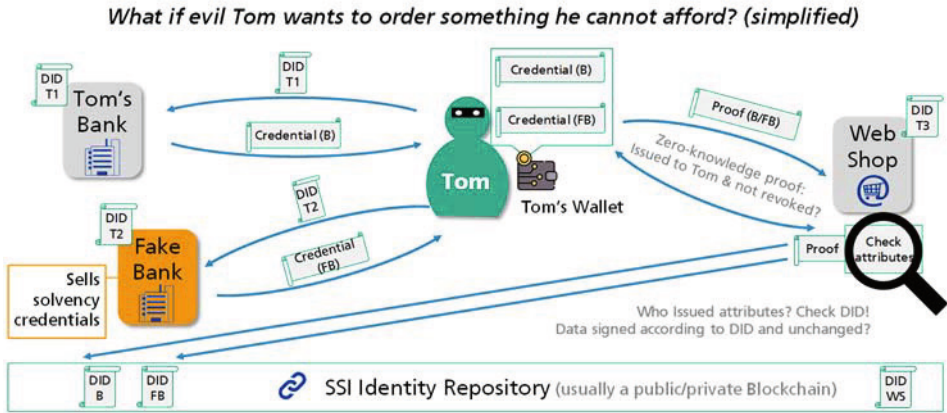


Figure 1: The Challenge of the Root of Trust in SSI solutions

## 2.2 Automated trust management

Digital identity and associated trust information is increasingly exchanged between organizations. This follows from several developments that are likely to take off even more in the future. People work on premise and increasingly remotely in project-teams consisting of members of multiple organizations, assisted by smart Internet of Things (IoT)-devices, and linear production chains have evolved into complex value networks. Identity and trust information is needed to secure these processes, protect intellectual property etc. SSI seeks to support this by opening up identity and data silos between separate organizations and independent platforms. This requires technical interoperability through standards, but also advanced trust management capable of dealing with different trust levels and roots of the participating entities in a scalable manner.

Hence, automatization of trust management processes could be an important step to achieve efficient trust management in many use cases and might be actually a requirement to leverage the full potential of SSI. Otherwise, scalability would be limited as efforts to manage trust manually raise too fast when trust domains, organizations, devices etc. increase beyond a certain simple level. This requires however, that trust policies can be expressed in a formalized way and it requires tools that can verify transactions against

those policies in an automatic fashion.

### 3 Previous and related work

So far, SSI approaches do not explicitly contain trust management approaches. The current focus is more on technical interoperability through standardization of interfaces and protocols (Decentralized Identifiers (DIDs) [DE21], Verifiable Credential types [VR20] etc.). Work on trust of verifiers focuses on the trust of verifiers in the cryptographic integrity of credentials while preserving the holder's privacy [Yo21] – certainly an important aspect, but not enough. Nevertheless, some approaches are worth considering, could be built on previous work from other contexts and are increasingly being recognized by important SSI players such as the Trust over IP Foundation and EBSI ESSIF.

One approach to trust in SSI would be to introduce centralized governance layers and trust frameworks with trust anchors and/or trust intermediaries. This could potentially increase trust in certain use cases. However, such would contradict the decentralized aspect of SSI and one of its main arguments, moving from an open ecosystem to one with a dominant stakeholder (or cartel) acting as gatekeeper. Hence, we would fall back to the reliance on central trusted third parties.

A different approach could be to just stick to a decentral model and reliance on the market to decide about the trustworthiness of actors. One could expect that in the long term, trustable actors would prevail – if they are able to build a sustainable business model. However, we would have to face re-occurring problems with fraudulent actors in this model – as illustrated in the example above. Fake banks could always re-enter the market<sup>3</sup>. Automation of processes would become quite difficult. And in the end, we could end up with few powerful players dominating the market. Quite similar to the current situation regarding web identity management. The market approach could therefore lead to a low level of trust and/or promote an oligopoly that is hostile to innovation (as it makes it very difficult for new small players/start-ups to gaining a foothold in the market).

A compromise between these two extreme approaches could be to rely on traditional hierarchical solutions for trust management such as hierarchical PKIs. There, a trust root issues certificates for certification authorities who again issue certificates to customers. This forms a chain of trust from the root of trust to the leaf certificates. However, the process of certification usually requires substantial time and effort, might not be scalable and flexible enough for the large number of entities in future use cases (i.e., Internet of Things) while also lacking advanced automated management functions needed for large scale interorganizational or cross domain/region etc. application areas. Furthermore, this approach requires that both parties (holder and verifier) accept the same trust root.

---

<sup>3</sup> It would even be possible to automate the re-entry process, which would allow the Fake Bank to register a new DID every time their old one is exposed and removed.



The Trust over IP foundation has also recognized the need for “strong evidence of the credibility and authority of the issuer making claims” [IN20]. They propose to rely on the chain of trust that results from hierarchical approaches, but instead of setting up a new PKI for the identity system, they promote the use of existing already established Trust Schemes and Trust Ecosystems. This is a very pragmatic approach, that only requires that the verifier considers the trust root of the used trust scheme/ecosystem to be authentic and trustworthy.

The SSI eIDAS Bridge could be seen as one such instance of the proposal by Trust over IP and a hierarchical PKI. It is an approach to make eIDAS available as a trust framework for the SSI ecosystem. On the one hand it assists the issuer in signing a verifiable credential. On the other hand, the verifier is assisted by verifying the issuer’s advanced or qualified electronic signature (if the issuer is a natural person) or seal (if the issuer is a legal person) that are attached to the verifiable credential in form of a linked data signature. This approach is currently developed in an EU H2020 NGI ESSIF Lab project [ES21c]. However, it has to be noted that this specific approach follows a quite narrow goal: it can only integrate SSI with one trust framework which is eIDAS. eIDAS is just one of several existing trust frameworks (others for example being the Pan Canadian Trust Framework, the Trust Scheme of Turkey etc.) and eIDAS is focused on the trust domain of national legal electronic identification and trust services in the European context. The relevance of eIDAS for the private sector has so far been rather limited. Other trust domains and the private context cannot be integrated through the SSI eIDAS Bridge (which is of course also not its goal).

The EU-funded project LIGHTest takes this idea one step further. Initially focused on electronic transactions in general, they provide a standardized way that allows operators of trust schemes to publish all the relevant information about their trust scheme using DNSSEC [Wa17]. This provides a great advantage, because it allows the verifier to also check the identity of the trust scheme operator following the DNSSEC chain of trust up to the already established and globally accepted trust root of DNSSEC. LIGHTest also provides the means to automatically verify transactions using a so-called Automated Trust Verifier (ATV), that collects all relevant information and verifies transactions against the trust policy of the verifier. Therefore, it is possible for the verifier to more easily integrate new trust domains and to verify transactions in an automatic fashion. Section 4 describes how this approach can be leveraged to establish trust in SSI ecosystems.

Automation of trust management in supporting verifiers of verifiable credentials and interoperability between trust domains is also being picked up. The Policymen Project in the EU H2020 NGI ESSIF Lab [PO21] is developing a middleware with APIs for verifiable credential issuers, holders, and verifiers. The policy management tool should allow service providers to specify policies for access to their resources using a graphical interface. Moreover, a publicly accessible policy registry is envisioned to store different syntactic policies and a conversion server to convert policies between different syntactics of various SSI ecosystems.

## 4 Proposing the TRAIN approach as a lightweight trust management infrastructure for Self-sovereign identity

The situation and challenges as described in section two, that are currently not fully addressed by the related work, as described in the previous section, can be summarized as:

- 1.) Credentials can basically be issued by anyone. Every service provider/verifier can individually decide for him/herself whether the issuer is deemed trustworthy given the information available. No intermediary, other third party or gatekeeper is required in this process. This is an important and aspired aspect of the decentralized, open architecture.
- 2.) In some, more or less sensitive use cases (e.g. online shopping, employers reviewing diplomas), verifiers highly profit from support when having to decide whether certain credential issuers are trustworthy.
- 3.) Certain schemes and standards, for example regarding the Levels of Assurance (LoA) behind certain credentials would allow for automated decision making and could ease the handling of credentials from different issuers and more trustable.

In the following, we present an approach to address these challenges. It is based on the work of the EU H2020 research project LIGHTest [LI21] that is currently being developed further for the application in the SSI context in the EU H2020 NGI ESSIF Lab<sup>4</sup> project TRAIN (TRust mAnagement INfrastructure) [ES21b].

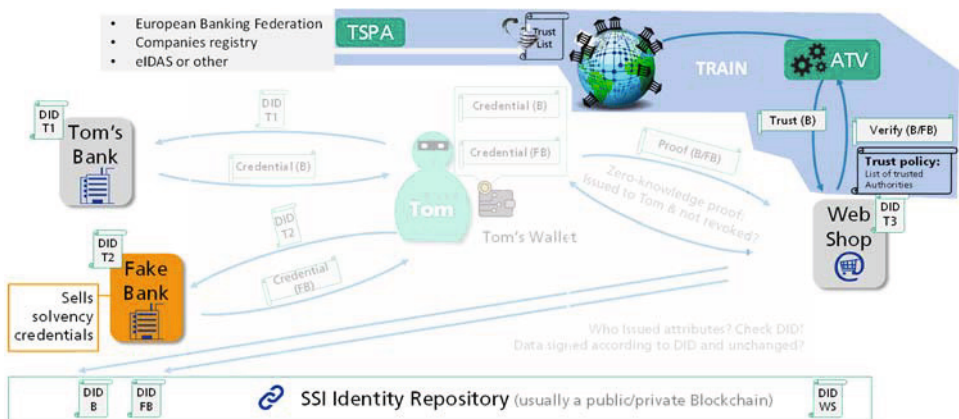


Figure 2: TRAIN as a lightweight trust management infrastructure for Self-sovereign identity

Figure 2 gives an overview of the architecture. It illustrates how the TRAIN component is introduced into the simplified SSI architecture already known from the scenario in section

<sup>4</sup> eSSIF-Lab is an EU-funded project and aims at advancing the broad uptake of Self-Sovereign Identities (SSI) as a next generation, open and trusted digital identity solution for faster and safer electronic transactions via the Internet and in real life (<https://essif-lab.eu/>).

2.1. The TRAIN project is currently working to integrate it into the more sophisticated EBSI ESSIF Framework [ES21a].

Using TRAIN, *Web Shop* as verifier can decide to seek external support to assess the trustworthiness of solvency credentials issued by banks not known to him. Thus, the verifier defines in a Trust Policy one or multiple trusted authorities to accept for certain transactions – e.g., over a certain financial threshold. Based on the Trust Policy, the Automatic Trust Verifier (ATV) component verifies if any Bank that has issued the solvency credential is listed in one of the corresponding Trust Lists of Trusted Authorities accepted by the Web Shop. Such a list could for example be published by a banking federation or another industry association. These are the so-called Trust Scheme Publication Authorities (TSPAs) that operate standard DNS Name Servers with DNSSEC extension. Such a server can publish multiple trust lists under different sub-domains of the authority's domain name. Alternatively, the Web Shop could require eIDAS certificates and refer to eIDAS Trusted List.

As mechanism for the discovery and verification of trust scheme memberships, TRAIN makes use of the global, well-established and trusted infrastructure of the internet Domain Name System DNS (using DNSSEC) as trust root. This approach has been developed and validated in several pilots of the LIGHTest project (for the general context of trust for digital transactions). For the reference architecture of this approach please refer to [Wal7].

Compared to the alternative approaches sketched out above in section 3, TRAIN still follows a decentral approach. The final trust decision remains with the verifiers that can decide whether to rely on other authorities to transparently support them. Central gatekeepers are avoided and everyone still being able to issue credentials, just as everyone can easily publish their own trust lists as TSPA. While allowing for this, TRAIN introduces a transparent and trustable infrastructure that supports participants of the SSI ecosystem to define which issuers they deem trustable – or who can support them in this decision and under which circumstances and automate this process. Verifiers are supported in setting up self-defined Trust Policies that define certain credentials/certificates that are issued by specific entities that are incorporated in specific trust lists are deemed trustworthy. Hence, the focal point of trust remains with the verifier. The trust lists are published by TSPAs that operate Trust Schemes. A Trust Scheme comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled entities in a given domain of trust. Thus, it is transparent how issuers got included in the Trust List of a certain Trust Scheme. TSPAs can be governmental institutions, but also any other organizations like businesses or other non-governmental institutions. Thus, if a verifier decides that external support for a trust decision is needed, it refers to the TSPA of its preference. Moreover, issuers can signal their trustworthiness by committing to a certain Trust Scheme to be included into certain Trust Lists. Finally, credential holders profit from a trustable and still dynamic ecosystem with low barriers for new entrants. TRAIN adds a flexible trust layer to SSI, enables scalable and automated trust management and is fully in line with the open and decentral SSI approach.

## 5 Conclusion

To fulfill the promise for a bright future of identity management, SSI solutions urgently need to solve the trust management issues that we outlined in section 2, particularly regarding the trust anchor and automation. The emphasis of SSI on protecting the privacy of the holder and the overall decentralized approach have created a situation in which the verifier can find itself in a disadvantageous situation. However, the verifier is a stakeholder that also has to be motivated to adopt SSI as identity solution – as has the user. Hence, the valid interests of the verifier as provider of valuable service cannot be neglected.

In the currently limited SSI approaches, the verifier might be forced to make a decision on whether or not to trust a credential presented by the holder without the means to verify if this credential is reliably and trustworthy. As outlined in section 2, cryptographical verification is not enough, if you are not able to assess if the source is genuine and trustworthy. Approaches to address this issue range from central governance layers with dominant stakeholders as gatekeepers to approaches that fully rely on the market to govern itself. Hierarchical approaches could be a viable compromise between these extremes but require all parties to accept a common root of trust – which is not a realistic scenario in many cross-domain and/or international use cases. This particular drawback, however, can be solved by leveraging existing trust schemes and ecosystems and by providing a standardized way to publish their trust-relevant information. The TRAIN project follows such an approach to provide a trust management infrastructure for SSI. This is an important first step for providing the necessary credibility to make SSI also attractive for relying parties.

The TRAIN approach is currently working to transfer knowledge and components developed and focused in LIGHTTest to the SSI ecosystem. Currently, it focuses on fundamental interaction with verifiers and is developing the respective API. However, the SSI ecosystem is in dynamic development and standards are only currently forming and there is currently no universal interface to issuers available. In general, TRAIN faces the challenge of achieving enough momentum for being picked up by enough issuers and verifiers. Here, it faces a two-sided market with network effects. If enough verifiers would integrate the solution, it would also be attractive for issuers – and vice versa. Making it as easy as possible for both sides to integrate the solution by building on the emerging standards in SSI and also facilitating the enrolment process of issuers through a respective API, making it easy for verifiers to formulate policies by adjusting the policy authoring tool developed in LIGHTTest [WO21], sharpening the value position and making the approach more known in the SSI ecosystem – e.g. through further work in EBSI ESSIF – will be important next steps on the roadmap for TRAIN.

## 6 References

[A116] Allen, C.: The Path to Self-Sovereign Identity., <https://github.com/ChristopherA/self->

- sovereign-identity, accessed: 05/02/2020.
- [De20] INATBA: Decentralized Identity: What is at Stake? INATBA Position Paper : INATBA Identity Working Group, 2020.
- [De21] W3C: Decentralized Identifiers (DIDs) v1.0. <https://www.w3.org/TR/did-core/>. - accessed: 09/02/2021.
- [Di20] Bundesregierung: Digitale Identität - Personalausweis im Smartphone und mehr. <https://www.bundesregierung.de/breg-de/aktuelles/digitale-identitaet-1824658>. - accessed:0802/2021.
- [DT20] Dib, O.; Toumi, K.: Decentralized identity systems: Architecture, challenges, solutions and future directions. In: *Annals of Emerging Technologies in Computing* Bd. 4, Nr. 5, pp. 19–40, 2020.
- [Es21a] EBSI ESSIF Lab: eSSIF-Lab Functional Architecture | eSSIF-Lab. <https://essif-lab.pages.gnet.gr/framework/framework/docs/functional-architecture>. accessed: 23/02/2021.
- [Es21b] ESSIF Lab Project: eSSIF-TRAIN by Fraunhofer-Gesellschaft | ESSIF-LAB. <https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/>. accessed: 23/02/2021.
- [Es21c] SSI eIDAS Bridge Project: ESSIF-Lab / infrastructure / VALIDATED-ID / SEB\_project\_summary. [https://gitlab.gnet.gr/essif-lab/infrastructure/validated-id/seb\\_project\\_summary](https://gitlab.gnet.gr/essif-lab/infrastructure/validated-id/seb_project_summary). accessed: 01/03/2021.
- [In20] Trust over IP Foundation: Integration with Established Trust Ecosystems - Guidance Deliverable, 2020.
- [Ku13] Kubach, M.; Roßnagel, H.; Sellung, R.: Service providers' requirements for eID solutions: Empirical evidence from the leisure sector. In: Hühnlein, D.; Roßnagel, H. (Hrsg.): *Open Identity Summit 2013 - Lecture Notes in Informatics (LNI) - Proceedings*. Bonn, pp. 69–81, 2013.
- [Ku20] Kubach, M. et.al.: Self-sovereign and Decentralized identity as the future of identity management? In: *Open Identity Summit 2020 - Lecture Notes in Informatics (LNI) - Proceedings*. Bonn: Köllen Druck + Verlag GmbH, 2020, publisher: Gesellschaft für Informatik eV, pp. 35–47, 2020.
- [Le20] Lesavre, L. et.al.: *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*: National Institute of Standards and Technology, 2020.
- [LI21] LIGHTest. <https://www.lightest.eu/>. accessed: 23/02/2021.
- [Mü18] Mühle, A. et.al.: A survey on essential components of a self-sovereign identity. In: *Computer Science Review* Bd. 30, pp. 80–86, 2018.
- [On20] DG CONNECT: Online European Digital Identity Roundtable: Clear message in favour of a secure e-Identity for all Europeans!. <https://ec.europa.eu/digital-single-market/en/news/online-european-digital-identity-roundtable-clear-message-favour-secure-e-identity-all>. accessed: 08/02/2021.
- [PO21] Policyman Project: ESSIF-Lab / business / PolicyMan / PolicyMan\_project\_summary. [https://gitlab.gnet.gr/essif-lab/business/policyman/policyman\\_project\\_summary](https://gitlab.gnet.gr/essif-lab/business/policyman/policyman_project_summary). -

accessed: 01/03/2021.

- [Pr20] Products - Evernym's Verifiable Credential Platform. <https://www.evernym.com/products/>. - accessed: 09/10/2021.
- [Ro14] Roßnagel, H. et.al.: Users' willingness to pay for web identity management systems. In: European Journal of Information Systems Bd. 23, Nr. 1, pp. 36–50, 2014.
- [Sh21] Showcase programme "Secure Digital Identities". [https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere\\_Digitale\\_Identitaeten/sichere\\_digitale\\_ident.html](https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html). accessed: 28/02/2021.
- [Si18] Simons, A.: Decentralized digital identities and blockchain: The future as we see it. <https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/>. accessed: 05/02/2020.
- [Sm21] Smith, S. M.: Key Event Receipt Infrastructure (KERI). In: arXiv:1907.02143, 2021.
- [St20] Stolton, J.: EU leaders to call for an EU electronic ID by mid-2021. <https://www.euractiv.com/section/digital/news/eu-leaders-to-call-for-an-eu-electronic-id-by-mid-2021/>. accessed: 08/02/2021.
- [VR20] W3C: Verifiable Credentials Data Model 1.0. <https://www.w3.org/TR/vc-data-model/>. - accessed: 06/02/2020.
- [Wa17] Wagner, S. et.al.: A mechanism for discovery and verification of trust scheme memberships: The LIGHTest Reference Architecture. In: Open Identity Summit 2017, Lecture Notes in Informatics (LNI), Lecture Notes in Informatics (LNI). Bd. P277. Bonn: Köllen Druck + Verlag GmbH, pp. 81–92, 2017.
- [WO21] Weinhardt, S.; Omolola, O.: Usability of Policy Authoring Tools: A Layered Approach. In: 2021 — ISBN 978-989-758-359-9, pp. 301–308, 2021.
- [Yo21] Young, K.: Verifiable Credentials Flavors Explained, Linux Foundation Public Health: Linux Foundation Public Health, 2021.
- [ZR12] Zibuschka, J.; Roßnagel, H.: Stakeholder Economics of Identity Management Infrastructures for the Web. In: Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012). Karlskrona, Sweden, 2012.



# Applying assurance levels when issuing and verifying credentials using Trust Frameworks

Victor Martinez Jurado<sup>1</sup>, Xavier Vila<sup>2</sup>, Michael Kubach<sup>3</sup>, Isaac Henderson Johnson Jeyakumar<sup>3</sup>, Albert Solana<sup>2</sup>, Matteo Marangoni<sup>1</sup>

**Abstract:** Technical interoperability of the issuance, presentation, and verification of verifiable credentials (VC) across domains of trust is a current challenge for self-sovereign identity. We present an approach incorporating different levels of assurance and trust domains in an eIDAS compliant way. This is illustrated through a use case with real-world relevance: the issuance and cross-border usage of the European Health Insurance Card.

**Keywords:** eIDAS, self-sovereign identity, SSI, trust, trust frameworks, verifiable credentials

## 1 Introduction

When providing electronic services in a cross-border context, providers should have in place practices, policies, and other controls to provide assurance and evidence to the governor bodies of different trust schemes that effective practices are in place. The whole ecosystem benefits from this practice since consumers (holders, verifiers) can rely on the authorities and on the applied trust schemes to provide the needed assurance on the services consumed. The eIDAS regulation [Eu14] provides a such framework for determining the assurance levels of electronic identification schemes. However, eIDAS is focused on the EU, while many other domains of trust exist and even more could be defined. Hence, it would be advantageous if individuals or groups (industry organizations, NGOs, etc.) of verifiers could define for themselves their required trust standards and refer to self-defined trust schemes or schemes defined by other trustable entities besides the EU.

This paper describes the concept jointly developed by SICPA, Validated ID, and Fraunhofer in the EU NGI ESSIF Lab [ES21], demonstrating the issuance, presentation, and verification of verifiable credentials (VC), incorporating different domains of trust. Firstly, we demonstrate how we can leverage the SSI-eIDAS Bridge to provide legal confirmation of the identity of the issuer (using a Qualified Electronic Certificate) and a legal basis for attributing a VC to an issuer (by using electronic seals); and secondly, we propose the TRAIN approach as means to verify that an issuer was authoritative to issue a VC (by integration in a trust scheme infrastructure) so it can be trusted by the verifier. The use case chosen to illustrate this concept is the European Health Insurance Card.

---

<sup>1</sup> SICPA SA, Av. de Florissant 41, 1008 Prilly, Switzerland, [firstname.lastname@sicpa.com](mailto:firstname.lastname@sicpa.com)

<sup>2</sup> Validated ID, C/ Aragó 179, 08011 Barcelona, Spain, [firstname.lastname@validated.id](mailto:firstname.lastname@validated.id)

<sup>3</sup> Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, Germany, [firstname.lastname@iao.fraunhofer.de](mailto:firstname.lastname@iao.fraunhofer.de)



The concept combines the following building blocks: (1) An interoperable issuance, presentation, and verification application that can support multiple protocols, credential types, and did-methods. (2) An SSI-eIDAS bridge component, providing legal confirmation of the identity of the issuer by incorporating the Issuer's advanced or qualified electronic signature or seal. (3) A Trust Management Infrastructure (TRAIN), providing a globally applicable means to verify conformance of the issuer to a certain policy and trusted scheme, fostering the trustworthiness of the electronic transaction.

The paper is structured as follows. Chapter 2 presents the EHIC use case that illustrates our approach. Subsequently, chapter 3 depicts the generic solution architecture with its elements. Chapters 4, 5, and 6 give details on our main components: the SICPA Bridge, the SSI-eIDAS Bridge and the TRAIN infrastructure. Finally, we come to a conclusion, point at open issues and lay down our next steps in chapter 7.

## 2 The European Health Insurance Card (EHIC) use-case

**The problem:** The EHIC scheme allows EU citizens to obtain free medical care or in some cases at a local rate if they are visiting countries that take part in the scheme [Eu21]. The EHIC scheme covers emergency treatment and certain pre-existing medical conditions. EHIC fraud occurs when visitors claim for treatments under EHIC when they are not entitled to do so. The main fraud types in this category are (1) False Application: This relates to someone who has intentionally made a fraudulent application for a European Health Insurance Card, and (2) False Use: This relates to someone using a European Health Insurance Card who has no entitlement to do so.

**High-level approach:** We would like to leverage the eIDAS framework to provide a substantial assurance level on the issuer's identity, both when holders and verifiers receive and validate the EHIC credential or presentation. We regard VCs as an appropriate technology for the use case, as it provides flexibility and decentralization. First, enhance the trust between issuers, holders, and verifiers, secondly solve the Just in time issuance problem in Identity systems (verifier no longer has to contact the issuer). Citizens (holders) can keep control and ownership over their digital EHIC, deciding what information they want to disclose, sharing only the required data to whom they wish to disclose it. (currently, various available cryptography techniques can be used to achieve selective disclosure or data minimization, i.e. Zero-Knowledge Proofs). At the same time, we want to minimize false use by applying different trust frameworks (private health insurance providers as valid issuers, holder-specific entitlements, etc) on the verification of the EHIC credential and related entitlements.

**Goals:** The goals of our approach are to (1) demonstrate the issuance of EHIC by health insurance providers, applying eIDAS framework, (2) demonstrate the verification of EHIC by cross-border healthcare providers to ensure entitlements are valid, and (3) apply country/healthcare specific trust frameworks to ensure false use is mitigated.

**Stakeholders, Roles, and Components:** The following table (*Figure 1*) gives an overview of the relevant stakeholders and their roles in our exemplary use case, mapped to the components of our solution architecture.

Stakeholders	Role	Component
National Health Insurance Provider	Issuer of EHIC, issuer of entitlements, payer	Issuance service, SSI-eIDAS bridge
Healthcare provider	Verifier of EHIC, provider of service, payee	Verification service, TRAIN ATV, SSI-eIDAS bridge
Citizen	Holder, consumer of healthcare service	Wallet
National Government	Accreditation of National Health Insurance Providers	TRAIN TPA
EU	Provides trust framework for cross-border usage of EHIC	TRAIN TSPA

Figure 1: Stakeholders, Roles, Components

### 3 Architecture

Our architecture defines the following components, while Figure 2 below gives a high-level, generic overview of the intended architecture context for this concept.

**A) Holder/Wallet:** This is the software that is able to request/store/manage the user's VCs, and possibly related artifacts such as DIDs and cryptographic keys.

**B) Issuance application backend:** Logic associated with preparing VC data for a Holder with issuing credentials.

**C) Issuance application backend Front-end:** Renders to the user's agent software, helping them obtain the credential and navigate the Issuer business logic.

**D) VC Issuer HTTP API Service:** An implementation of the VCs Issuer HTTP API that is capable of generating VCs with a qualified electronic seal attached to it.

**E) Verification application backend Front-end:** Renders to the user's agent software, requesting them a Verifiable presentation and navigating the Verifier business logic.

**F) VC Verification HTTP API Service:** An implementation of the VCs Verifier HTTP API that is capable of verifying VCs / Presentation, verifying qualified electronic seals, and verifying conformance of the issuer to a certain policy and trusted scheme.

**G) SSI-eIDAS bridge:** Enhance the legal certainty of the VC issued, by incorporating the issuer's advanced or qualified electronic seal. For details see chapter 4.

**H) TRAIN:** Provides a global trust infrastructure that can be used to verify conformance of the issuer to a certain policy and trusted scheme. For details see chapter 5.

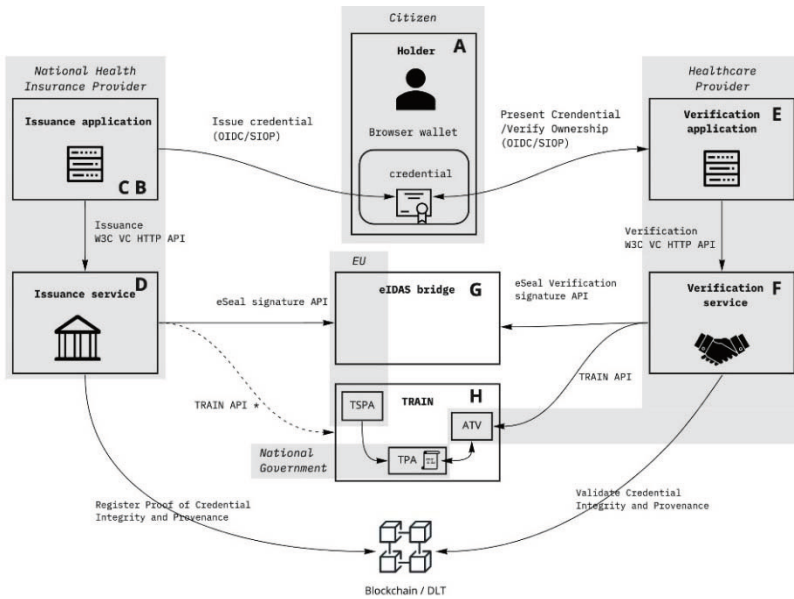


Figure 2: Proposed Architecture and with Stakeholders

### 3.1 Scope and Process

In order to achieve practical interoperability and build an end-to-end use-case from issuance to verification, the scope of the work has been limited. The VC-data model [VR20] is rendered using [JSON-LD] with the usage of linked data proofs [LD-PROOF] [Li20a]. The protocol used to transfer credentials between issuer - wallet - verifier is OIDC (see more details 3.3 Connectors). The scope of TRAIN in this use case is to verify whether a certain Credential Issuer (identified via DID) is enrolled in a certain Trust Scheme (identified via DNS Hostname) as required by the Verifier in a Verifier Policy. Both, the enrolment process of the issuer in the Trust Scheme, as well as the formulation of a (dynamic) Verifier Policy are for now out of the scope of this concept. Finally, did:key is the only did method supported in this use-case. The process is as follows:

1. Enrolment of the Issuer as a Trust Schema member by a Trust Scheme Operator (Trust Scheme Publication Authority or Trust Publication Authority) via Train (out of the scope of this current version, manual installation step)
2. Holder connects with the Issuer and requests a credential via OpenID.
3. Holder authenticates with his wallet, using it as a Self-Issued OpenID provider.
4. Issuer generates credential, signs and e-seals it, and sends to wallet back via OpenID.
5. Presentation Request by the Verifier to the wallet using OIDC.
6. Presentation Submission to the Verifier website by the wallet using OIDC.

7. Cryptographic Verification of the presentation by Verifier.
8. Verification of the seal by SSI-eIDAS bridge.
9. Verification of conformance of the issuer to a certain policy that is defined by the verifier through check of integration in a certain trusted scheme by TRAIN.

### 3.2 European Health Insurance Card Vocabulary Specification

For this concept, we have specified a Linked Data vocabulary for asserting VCs related to European Health Insurance Card (EHIC) information, such as Insurance number, Country, ID number of the insurance carrier. It is published at [MM21].

### 3.3 Connectors

We are using OpenID to connect the wallet with both the Issuer and the Verifier when issuing credentials and when presenting them.

**OpenID Connect Credential Provider:** OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables relying parties to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User. In this project we extend the role of an OpenID Provider from being the provider of simple identity assertions into being the provider of credentials, as defined at [Lo21]:

1. The Holder acting as an OpenID Client sends a Credential Request to the Credential Provider that is acting as an OpenID Provider (OP).
2. The Credential Provider authenticates the End-User and obtains authorization.
3. The Credential Provider responds with a Credential.

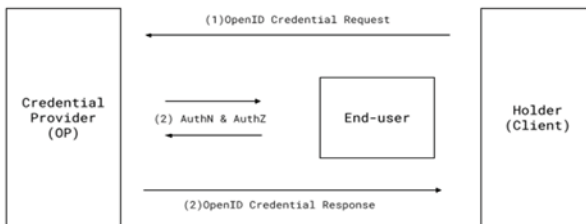


Figure 3: OpenID Connect Credential Provider

**Self-Issued OpenID Provider – SIOP:** OpenID Connect supports Self-Issued OpenID Providers (Self-Issued OPs, or SIOPs) [Op20]. These are personal OpenID Providers (OPs) that issue self-signed ID tokens, enabling portability of the identities among providers. We propose to use the wallet as a SIOP when interacting with the Issuer and

the Verifier during the authentication process and to provide the required EHIC credential.

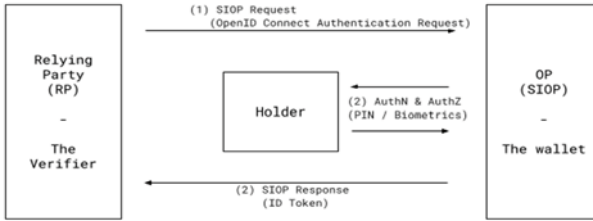


Figure 4: Self-Issued OpenID Provider - SIOP

## 4 SICPA bridge

**Business problem:** While the current state of the art in SSI is being driven by global open standards, this does not automatically guarantee practical interoperability between different implementations using a variety of protocols, credential types, and DID-methods. True interoperability is critical in preventing vendor and technology platform lock-in. This is of special importance to buyers that are essential in the market adoption of SSI systems. In addition, true interoperability is also key for adoption by holders, who i.e. should not have to worry about wallet management in order to facilitate different issuers or verifiers.

The consequences for businesses will be a higher cost structure to support different approaches (comparable to the iOS vs Android dilemma for developers) and to cope with a lack of flexibility and inability for systems to interoperate due to vendor lock-in. On the market side, application providers face a slow adoption rate and a limited subscriber base.

**Solution approach SICPA bridge:** The SICPA bridge enables trusted online peer-to-peer interactions based on interoperable distributed ledger technologies (DLTs), peer-to-peer (P2P) interactions across multiple did-methods, using standardized VCs. It provides a set of APIs to enable the usage of decentralized identifiers (DIDs), DID-communication, and VC exchange. From these building blocks, implementers can build issuance and verification services in a manner that is agnostic to any particular DID network, credential exchange protocol or credential type.

SICPA proposes the following technological building blocks for issuance and verification of VCs, that will enhance interoperability in the SSI ecosystem and lowers the barrier to adoption for all stakeholders in the market.

**DIDComm and CHAPI protocol support:** An Issuance and verification service that supports both DIDComm [De21], as well as the Credential Handler API (CHAPI) [Cr20b]. Supporting both protocols will increase the freedom of choice in wallets for the holder.

**AnonCreds and [JSON-LD] credential type support:** Integration of [JSON-LD] signing and verification in the Aries code-base [Hy19]. Providing both AnonCreds [LZ19]

and [JSON-LD] [JS20c] standards will greatly enhance the interoperability across the overall ecosystem and enable true portability of VCs

**Support for multiple DID-methods:** Native support for multiple issuers and verifier DID-methods in Aries. Offering multiple did-methods (e.g. did:sov, did:ala, did:eth) for issuers and verifiers will enable broad support across the ecosystem.

## 5 SSI-eIDAS bridge

The SSI-eIDAS bridge is a component that proposes to enhance the legal certainty of any class of VC, by incorporating the issuer’s advanced or qualified electronic signature (if the issuer is a natural person) or seal (if the issuer is a legal person). Qualified certificates, defined under articles 28 (natural persons) and 38 (legal persons) of the eIDAS Regulation, can be used to confirm the identity of the natural or legal person. In the case of the electronic seal, Article 3 (29) of eIDAS Regulation defines the electronic seal certificate as “*an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person*”.

Trustworthiness in a VC is linked to the issuer’s DID: Verifying an issuer’s identity is paramount, as there is no binding of a DID to a real-world natural or legal person per se.

The eIDAS regulation will evolve to be more technologically neutral and inclusive so that some of the benefits of using SSI can be achieved (fine-grained and specific attribute-based credentials, privacy improvements through selective disclosure, protocols for data sharing), but this will take time. The main role of the eIDAS Bridge is thus to assist (1) Issuers, in the process of signing/sealing a VC, and (2) Verifiers, in the last mile of the verification process, to help identifying the natural or legal person behind an issuer’s DID.

### 5.1 Technical solution description

From a technical perspective, this electronic signature or seal is attached to the VC in form of a linked data signature, a special class of a linked data proof, according to [Li20a]. A linked data signature is a type of linked-data proof [LD-PROOF] consisting of information about the signature, parameters required to verify it, and the signature value itself. All of this information is provided using linked data vocabularies such as the security vocabulary [SECURITY-VOCABULARY], [Th21]. An example of the resulting proof follows, where a new proof type, 2020 CADES RSA Signature Suite, has been defined:

```
"proof": {
  "type": "CadESRSASignature2020",
  "proofPurpose": "assertionMethod",
  "created": "2019-08-23T20:21:34Z",
  "verificationMethod": "did:factom:5d0dd...3d99ef#MIIIE...suIcuV",
  "proofValue": "-----BEGIN PKCS7----- iG9wDQYLK... -----END PKCS7-----"
}
```

In any case, this linked data proof is verified using the issuer’s qualified certificate; which must be resolvable and accessible to any relying party. To this end, different options are available. The certificate can be directly available in the `verificationMethod` of the proof structure or linked in the DID document of the issuer where it could be directly published or pointing to an online repository where the certificate could be published. Any person receiving a VC is able to lookup the DID, and then resolve the DID to get the DID Document; with the DID document, it is possible to access the qualified certificate contained in this repository, thus having access to the verified identity of the issuer.

## 5.2 eIDAS regulation discussion

As discussed in [Do20], “*the electronic seal must serve as proof that an electronic document has been issued by a legal entity, providing certainty about the origin and integrity of the document*”, but it does not mean that it can be used by the legal entity for “*all legally binding actions, especially in accordance with the rules of representation of the different types of legal entities*”. When using electronic seals to issue VCs it should be checked that its use does not conflict with national legislation. Regarding the use of qualified and non-qualified electronic seals, “*the eIDAS Regulation establishes a legal norm of non-discrimination of the electronic signature different from the qualified electronic signature, which also extends to the unqualified electronic seal*”. This is shown in article 35 (1) of the eIDAS Regulation which indicates that “*an electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals*”.

On the other hand, when a qualified seal is used, as per Article 35 (2) of the eIDAS Regulation, it “*shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked*”, and also it benefits from cross-border recognition, per Article 35 (3), since “*a qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States*”. The identification of the natural or legal person, which is the main purpose of digital certificates, is used to support the signature or advanced electronic seal by confirming the identity of the person concerned. The certificates are used thus to “authenticate” the identity of the natural or the legal person. Finally, it should be noted that in any case, the certificates must be issued by a Qualified Trust Service Provider, “*in compliance with the corresponding legal requirements applicable to an advanced or qualified electronic signature or seal*”.

## 6 TRAIN

TRAIN is a lightweight trust management infrastructure for an open ecosystem of stakeholders and trust schemes. The train approach allows for the flexible definition,

consideration, publication of trust lists and verification of trust schemes compliance (e.g., eIDAS including LoAs or other Trust Schemes that can also be application/industry-specific) with different Levels of Assurances (LoA), using DNS as a root anchor. TRAIN aims to leverage this to support SSI infrastructures through a global trust infrastructure that can be used to verify the trustworthiness of issuers. The trust layer enables actors to verify the root of trust of certificates used to sign credentials. It is not dependent on a hierarchical CA infrastructure. The component builds on the infrastructure developed in the EU project LIGHTest ([www.lightest.eu](http://www.lightest.eu)). Its trust layer is flexible: individual parties can define their own trust policies, manage, and publish them. TRAIN is fully in line with the open and decentral SSI approach and complements other approaches.

The trust management architecture that is made possible by TRAIN enables secure, trustable digital interactions. At the same time a classical hierarchical CA-type structure is avoided – so is fraud, chaos, and the pure dominance of the economically strongest actors in the system. Individuals or groups (industry organizations, NGOs, etc.) of verifiers can define for themselves the trust standards they require. Issuers can publish to what standards they comply. The system is open, but standards for trust are transparent, as the trust schemes and lists can be published. TRAIN adds a flexible trust layer to be used by verifiers to define their required level of trust. No central authority is established, everyone can issue certificates, but TRAIN facilitates individual trust decisions. Trust standards such as Trust Schemes (eIDAS, Pan Canadian Trust Framework, but also self-defined schemes and policies) can be integrated.

The two main components of the TRAIN infrastructure are briefly explained in the following.

## **6.1 Publication of trusted issuance services**

The two types of publication authorities of the TRAIN Infrastructure are Trust Scheme Publication Authorities (TSPA) and Trust Publication Authorities (TPA). A TSPA is the higher-level component which is to develop and publish different trust schemes in the TRAIN infrastructure. A trust scheme comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled entities in a given domain of trust. For example: In the European Health Insurance Card use case, the European Commission is the TSPA and develops its own trust scheme.

A TPA in TRAIN is responsible for maintaining a list of trusted issuance services for credentials. Issuance services that meet the requirements of the trust scheme of the specific TSPA can be included in its trust list. Thus, it is transparent how issuance services get to be included in the trust list of a certain trust scheme. In our simple use case example, a TPA is operated by each individual national EU member country's government or National Health Insurance Provider (or another institution – depending on the national specifics). This TPA is then responsible for including the different insurance providers of the respective country in the trust list if they adhere to the guidelines of the trust scheme



issued by the European Commission. All the approved issuance service's DIDs will be published by the TPA on a trust list in the trust infrastructure. Since the TRAIN infrastructure uses the DNS as a root anchor, the hostname of the trust publication authority will have to be integrated in the credential in the form of a Domain Name. This is required to resolve the corresponding trust scheme from the credential. For example: When a national health insurance provider is the issuance service of the credential, and EHIC is the trust scheme publication authority, it will be published as EHIC.eu in the TRAIN Infrastructure.

Any trust scheme with any type of LoAs structure can be formalized and published through TRAIN. By adding an issuance service's DID to a trust list, the issuance service can be integrated into different trust schemes of TSPAs. The trust list is published under the corresponding trust scheme. For the use in an SSI infrastructure, the model of TS 119 612 – ETSI for trust lists was extended, so that the trust list can accommodate the DID of the issuance service which is used to resolve DID documents. It is important to note that multiple TSPAs/TPAs can be set up under the TRAIN infrastructure to scale globally and to cater different domains of trust. This gives verifiers the flexibility to subscribe to different trust lists and schemes based on different regions, preferences or use cases. Verifiers decide which TSPAs to use.

## **6.2 TRAIN infrastructure component for the verification service**

The verification service of the verification application has an additional API to TRAIN to perform an external verification of the credential based on the hostname of the TPA and the DID URI of the issuance service using an API request. As a first verification step, TRAIN performs a DNSSEC request of the hostname to verify the chain of trust with the root DNS. Subsequently, a query is made using the hostname to locate the corresponding pointer mapped to trust scheme and trust list. Then, the pointer of the trust list is queried to fetch the details of the issuance service DID. The DID obtained from the trust list is used to verify the issuer service DID from the credential. By doing so, the inclusion of this specific issuance service in the trust list of the specific TPA can be verified and the verification service will receive the verification results. Various trust schemes with different LoAs can be queried based on the respective requirements.

## **7 Conclusion**

Decentralized identity uses cryptography to allow individuals to create and control their own unique identifiers. They can use these identifiers to obtain VCs from different stakeholders and prove the integrity and authenticity of these credentials to relying parties. However, for use-cases where individuals share their information across trust domain boundaries, providers should have in place the needed practices, policies, and other controls that apply regardless of such differences. With our concept, we have

demonstrated technical interoperability of the issuance, presentation, and verification of VCs incorporating different levels of assurance and trust domains in an eIDAS compliant way. Furthermore, the European Health Insurance Card (EHIC) is presented as an example to illustrate how, by providing a common framework, different participants in an ecosystem can increase trust. The presented concept builds bridges between Decentralized identity and trust / legal frameworks, showing how decentralized identifiers and VCs could be used as a base to provide trust to electronic services in a cross-domain ecosystem.

Some open issues and areas for future work remain. As of now, the initial enrolment of the issuer via publication of the issuer DID in the trust publication authority (TPA) is a manual process. As an improvement, this governance process could be supported through an API to enable some form of automation. Moreover, the creation of verifier policies is currently a manual process that doesn't provide a good user experience - particularly for verifiers without programming knowledge. Hence, a user-friendly verifier policy management tool with a graphical user interface building on work in LIGHTest [WO21] and/or in ESSIF-Lab [PO21] should be integrated into the concept.

As mentioned in this paper, the trust publication authority's hostname is included as a claim in the credential in the form of a Domain Name. This step is needed since TRAIN uses the Domain Name System (DNS) as a root anchor, and as an issuer, their DID can be published in multiple trust publication authorities (TPA).

We acknowledge that further exploration is needed to improve the proposed solution. One line of work could be to publish DIDs in the DNS for discovery on an hostname's base, as discussed in [MKS20]. A verifier based on their verification policies could determine if the given issuer belongs to one of the Trusted List of the trust publication authorities configure in the verification policies. By doing so, not only we will avoid the inclusion of the extra claim in the credential, but it would allow us to define the identifier of the issuer as a URI instated of only a DID, as specify in the VC data model. As of per today, there are no eIDAS Qualified Trust Service Providers that provide SSI-eIDAS Bridge services. Someone implementing a qualified SSI-eIDAS Bridge service would need to integrate a remote qualified e-sealing service to benefit from cross-border recognition and presumption of correctness of the origin of that data as stated in Article 35 (2) of the eIDAS. Finally, due to the constraints of the format of the conference, our presentation focusses on a technical approach to trust in SSI. It is important to highlight that this needs to be complemented by legal and regulatory development efforts, such as [Do20].

## Bibliography

- [Cr20] W3C: Credential Handler API 1.0. [w3c-ccg.github.io/credential-handler](https://w3c-ccg.github.io/credential-handler). accessed: 01/03/2021.
- [De21] Decentralized Identity Foundation: DIDComm Messaging Specification. [identity.foundation/didcomm-messaging/spec/](https://identity.foundation/didcomm-messaging/spec/). accessed: 01/03/2021.

- [Do20] Domingo, I.: SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market, 2020.
- [ES21] ESSIF-LAB | ESSIF-LAB: Help Shape a Safe and Secure Next Generation Internet GENERATION INTERNET. [essif-lab.eu/](https://essif-lab.eu/). - accessed: 01/03/2021.
- [Eu14] European Parliament: Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union (Regulation Nr. 910/2014). Brussels, Belgium: European Parliament, 2014.
- [Eu21] European Commission: European Health Insurance Card. [ec.europa.eu/social/main.jsp?catId=559&langId=en](https://ec.europa.eu/social/main.jsp?catId=559&langId=en). accessed: 01/03/2021.
- [Hy19] Hyperledger/aries-rfcs. [github.com/hyperledger/aries-rfcs](https://github.com/hyperledger/aries-rfcs). accessed: 01/03/2021.
- [JS20] W3C: JSON-LD 1.1. [w3.org/TR/json-ld11/](https://w3.org/TR/json-ld11/). accessed: 01/03/2021.
- [Li20] W3C: Linked Data Proofs 1.0. [w3c-ccg.github.io/ld-proofs/#linked-data-signatures](https://w3c-ccg.github.io/ld-proofs/#linked-data-signatures). accessed: 01/03/2021.
- [Lo21] Looker, T. et al.: OpenID Connect Credential Provider. [mattglobal.github.io/oidc-client-bound-assertions-spec/](https://mattglobal.github.io/oidc-client-bound-assertions-spec/). accessed: 01/03/2021.
- [LZ19] Lodder, M.; Zundel, B.: Anonymous Credential Protocol - Hyperledger Indy HIPE documentation. [hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0109-anoncreds-protocol/README.html](https://hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0109-anoncreds-protocol/README.html). accessed: 01/03/2021.
- [MKS20] Mayrhofer, A.; Klesev, D.; Sabadello, M.: The Decentralized Identifier (DID) in the DNS. [datatracker.ietf.org/doc/draft-mayrhofer-did-dns/?include\\_text=1](https://datatracker.ietf.org/doc/draft-mayrhofer-did-dns/?include_text=1), accessed: 01/03/2021.
- [MM21] Marangoni, M.; Martinez Jurado, V.: European Health Insurance Card v0.1. [essif-lab.pages.grnet.gr/interoperability/eidas-generic-use-case/](https://essif-lab.pages.grnet.gr/interoperability/eidas-generic-use-case/). accessed: 2021-03-01.
- [Op20] OpenID Foundation: `openid / connect / openid-connect-self-issued-v2-1_0.md` — Bitbucket. [bitbucket.org/openid/connect/src/master/openid-connect-self-issued-v2-1\\_0.md](https://bitbucket.org/openid/connect/src/master/openid-connect-self-issued-v2-1_0.md). accessed: 01/03/2021.
- [PO21] Policyman Project: ESSIF-Lab/business/PolicyMan\_project\_summary. [gitlab.grnet.gr/essif-lab/business/policyman/policyman\\_project\\_summary](https://gitlab.grnet.gr/essif-lab/business/policyman/policyman_project_summary). accessed: 01/03/2021.
- [Th21] W3C: The Security Vocabulary. [w3c-ccg.github.io/security-vocab/](https://w3c-ccg.github.io/security-vocab/). accessed: 01/03/2021.
- [VR20] W3C: Verifiable Credentials Data Model 1.0. [w3.org/TR/vc-data-model/](https://w3.org/TR/vc-data-model/). accessed: 06/02/2020.
- [WO21] Weinhardt, S.; Omolola, O.: Usability of Policy Authoring Tools: A Layered Approach. In: 2021 — ISBN 978-989-758-359-9, pp. 301–308, 2021.

# Extraction and Accumulation of Identity Attributes from the Internet of Things

Lothar Fritsch<sup>1</sup> Nils Gruschka<sup>2</sup>

**Abstract:** Internet of Things (IoT) devices with wireless communication provide person-relateable information usable as attributes in digital identities. By scanning and profiling these signals against location and time, identity attributes can be generated and accumulated. This article introduces the concept of harvesting identifiable information from IoT. It summarizes ongoing work that aims at assessing the amount of person-relatable attributes that can get extracted from public IoT signals. We present our experimental data collection in Oslo/Norway and discuss systematic harvesting, our preliminary results, and their implications.

**Keywords:** IoT; profiling; identification; identity attributes; privacy

## 1 Introduction

The goal of this article is an assessment of how much measureable person-realteable IoT devices are. Detected devices and their re-identifiability, linkability, tracability and potential for placement in contexts such as private addresses will provide opportunities for collection of personal data and for identification.

Internet of Things (IoT) devices are omnipresent nowadays not only in professional environments like industrial production or smart cities, but also as personal devices. Many household devices are nowadays “smart” devices that are communicating via wireless communication protocols like IEEE 802.11 (commonly called Wi-Fi), Bluetooth, ZigBee or Z-Wave. This applies especially to home automation (like smart bulbs) and home entertainment equipment (like TVs or speakers). Also, outside our home we are surrounded by IoT devices. Modern cars not only offer Bluetooth communications (typically for hands-free phone calls), but also span a Wi-Fi access point. And even when just walking (or using public transport), personal IoT devices follow us. In addition to the smart phone, which more or less everyone uses, many people carry wireless headsets/headphones, fitness trackers or smart watches.

All these devices are constantly transmit signals and it is very easy for an adversary to scan the communication from a safe distance and to analyse the scan results later or even in

---

<sup>1</sup> Oslo Metropolitan University, Dept. of Computer Science, Oslo, Norway Lothar.Fritsch@oslomet.no

<sup>2</sup> University of Oslo, Dept. of Computer Science, Oslo, Norway nilsgrus@ifi.uio.no

real time. Although nearly all communication is nowadays encrypted and most protocols contain mechanisms to obfuscate the sender, many devices (like TV or headsets) do not make use of these methods and simply broadcast their identifier. Also, research has shown that, even if mechanisms like MAC randomization are active, it is still possible to profile the communications signals and identify the sending device. And this allows in many cases to learn the behaviour of the owner (like “is at home”) or even track him with high accuracy.

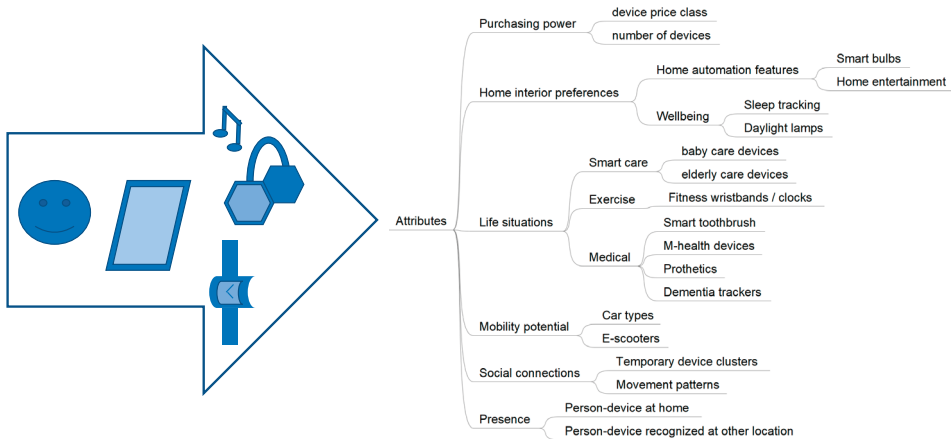


Fig. 1: IoT attributes (examples) available from IoT devices.

In this paper, we will show how personal attributes (examples shown in Fig. 1) can be retrieved from IoT environments of personal devices by scanning their presence and by recognizing what kinds of devices they are. We introduce the concept of IoT-extracted identity attributes, describe several proof-of-concept-measurements, and propose an approach for systematic collection and mapping of such attributes in order to enrich digital partial identities.

## 2 Background

The potential for identity data extraction from smart environments has been identified in 2006 by the SWAMI project. In its final report, in chapter three, four dark scenarios for sensing environments are summarized that envision data collection by ambient systems [Wr08]. Its vision has now developed into ubiquitous sensing infrastructure. For Android apps, it has been shown that systematic access to smartphone data can provide partial identity information to app ecosystems [MF20; PH10]. Such profiling against IoT devices’ publicly broadcast radio signals could deliver similar identity attributes. Possibilities for clandestine identification, location tracking and eavesdropping on individuals carrying such communication terminals, by exploiting functionalities available in the wireless communication protocols and their implementations [An19].

We present a set of attacks that allow an attacker to link a Wi-Fi device to its owner identity. We present two methods that, given an individual of interest, allow identifying the MAC address of its Wi-Fi enabled portable device. Those methods do not require a physical access to the device and can be performed remotely, reducing the risks of being noticed. Finally, we present scenarios in which the knowledge of an individual MAC address could be used for mischief [Cu13]. By profiling device network addresses, it will be possible to distinguish devices, follow them over space and time, and to correlate them to each other. It will be possible to extract which other devices or networks they exchange messages with, too. From a database, it will be possible to look up past observations for the devices. In addition, presence of certain devices will indicate presence of people or their absence.

The classification of mobile consumer devices through information provided by their wireless communication interfaces has been demonstrated successfully. Using this opportunity, the type of device can get recognized. A demonstrator was presented in [VG13]. By adding device type information, it will be possible to infer specific context attributes, such as purchasing power (device price), specific interests (fitness performance monitoring) or specific infrastructure (such as home automation). Similar insights about the side channel information gained from profiling RFID tags for business intelligence was discussed in [Fr09]. The consideration of location information adds context information [Fr08] that can enrich or even create new attributes.

Many sensing approaches focus on Wi-Fi device profiling and tracking based on passive and active discovery probe requests [CKB14]. Here, frequent probing reveals device characteristics. In particular, passive identification techniques for sensing without the sensed devices involved in the protocol are useful in the context of attribute extraction [Bh19]. When sensing nodes collaborate as a sensing network over a larger geographic area, tracking of mobile devices and profiling of their movements is possible. This feature is used in indoor navigation applications. However, it has been discovered to be able to track recognizable smart cars through their Wi-Fi interfaces, too [BZ19].

Finally, the application of forensic analysis and visualization of devices and their movements can generate insights that may lead to qualified identity attributes added [TLT16]. The mapping of a device to a place of living and to a place of work is one obvious source of direct identity information. Classification of whereabouts from geographical metadata, proximity to other devices—stationary or mobile—and the analysis of stationary equipment in private homes can easily generate attributes.

### 3 Data collection

As a proof-of-concept, we ran several small data collection campaigns. Their purpose was the demonstration of the availability of identity attributes from IoT devices. In an exploratory series of data collection experiments, we used the WIGLE<sup>3</sup> scanning app for Android

---

<sup>3</sup> <https://www.wigle.net>

devices as a data collection sensor. We planned a series of small experiments. Google Earth was used for visualizing geographical plots of the data.

By analyzing scans of wireless device communication, we accumulate IoT-extracted personal identity attributes that enhance our knowledge about the device owner.

### **3.1 Results**

In initial random scanning during daily movements, we learned that several vendor's television sets, and home entertainment equipment (Apple TV, Android TV, local cable TV providers' boxes) were easily identified in abundance. The same holds for various wireless audio speakers, smart light bulbs, an occasional smoke detector or wireless dimmer. Even a smart electric toothbrush was observed. Mobile phones and headsets were met in most places. We collected data in four targeted locations:

1. in a multi-floor, dense urban housing area in central Oslo;
2. in a villa district with free-standing houses with large gardens (Fig. 2);
3. on a highway-crossing pedestrian bridge targeting passing cars (Fig. 3);
4. by a footpath in a urban park that leads to a childcare facility (Fig. 4).

Below, we summarize our findings.

#### **3.1.1 Urban housing area**

We collected both Wi-Fi and Bluetooth information. However, in this article we focus on the collected Bluetooth data. In the multi-floor housing area located central in Oslo, a very large number of devices was found. Mobile phones, headsets, electric scooters from competing scooter pools, vehicle entertainment systems, television sets and set-top boxes were present in abundance. Wireless speakers and other audio equipment frequently was detected. Also, an occasional smart lamp was found in the sample. However, due to the density of housing, the mapping of devices to apartments required triangulation, advances to specific windows and tours around the next corner in order to observe weakening signals. Passing traffic—including public busses filled with passengers with smartphones, headsets and other devices—polluted the measurements. An effort targeting passing cars in this environment was given up due too many passing pedestrians.

### 3.1.2 Villa district

As a complementary approach to the dense urban center, we approached a villa area in Oslo's Holmenkollen district where spacious gardens surround houses. Due to fencing, we moved at a distance to the buildings. We noticed the presence of more contemporary cars, of smart home devices, televisions, fitness wristbands, wireless audio equipment and phones and tablet devices. The geography made mapping of the devices to houses relatively easy by traversing the property on roadside. We noticed a house that had devices named after rooms, as shown in Fig. 2. We saw a fitness wristband in a house where the lights were on, which possibly indicated the presence of a tenant. In the villa district, the mapping of wireless devices to property should be a task of low effort, due to large spaces in-between houses, low traffic and low number of passersby. It should be a relatively easy task to harvest network addresses, SSIDs and device fingerprints for named persons through their addresses in this environment.

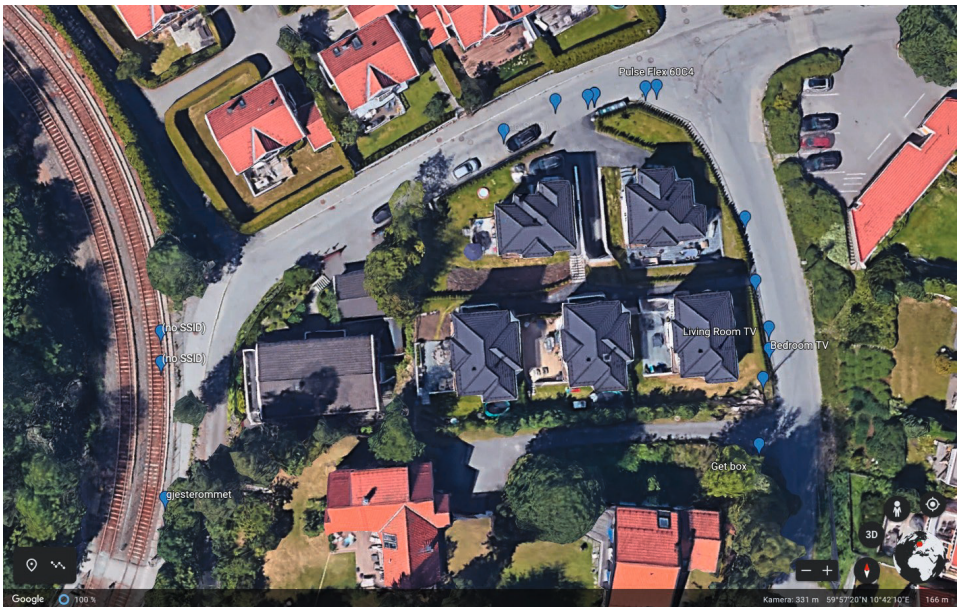


Fig. 2: A housing area with devices named Living Room TV, Bedroom TV and Guestroom, together with a pulse clock indicating presence of a person.

### 3.1.3 Highway pedestrian bridge

To evaluate the observability of car equipment, we sampled Oslo's ring road ("Ring 3") from a pedestrian bridge. Cars pass at 60km/h in two lanes in both directions. We were able



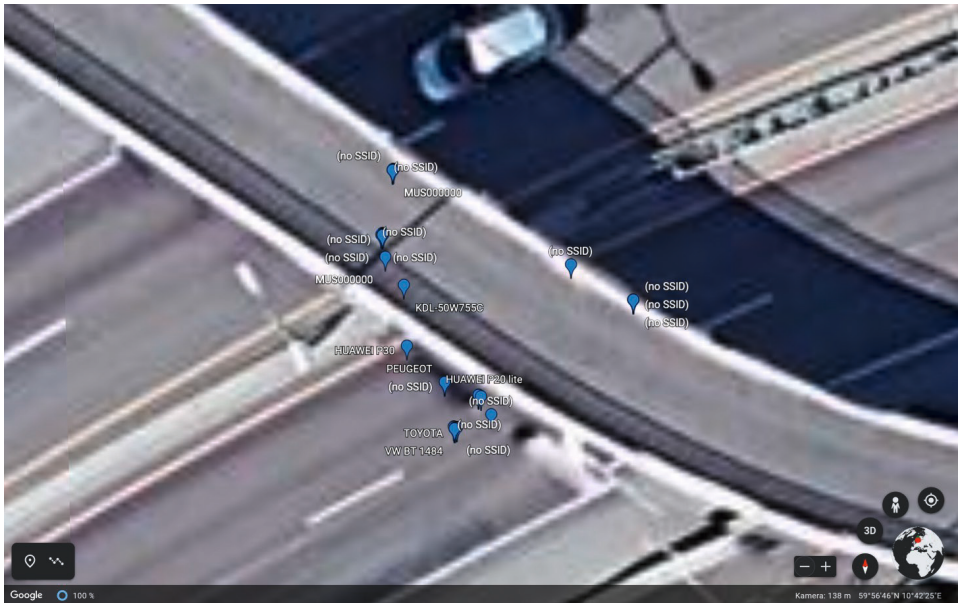


Fig. 3: Captured driving cars at 60-80 km/h from bridge over highway (Bluetooth): Toyota, Peugeot and Volkswagen. Other devices are likely hands-free devices and headsets.

to capture many wireless/hands-free devices, some of them named after the car make. There were even Wi-Fi networks with car brand names in their SSID. In addition to the cars, we picked up various smartphones and tablets (see Fig. 4). It should therefore be relatively easy to track the car communication interfaces and the driver/passenger phones with a database.

### 3.1.4 Footpath through park to childcare facility

A last measurement was a stationary placement of a probe in a window next to a footpath on the edge of a public park in Oslo. The path leads to a childcare facility, and leads, in addition, to a bus stop in the area. It is well-used by pedestrians and bicyclists at daytime. Over an interval of three days, passing devices were captured. We sampled phones, headphones, fitness wristbands, smart speakers, GPS navigators, an occasional electric scooter and other devices (see Fig. 4). Interestingly, by looking up the brand names from our log file in online shops, we were able to assess the monetary value of the devices, as shown in Tab. 1. We detected well-known products on a market price scale ranging from 70€ to 500€ sales value from persons passing by our position.



Fig. 4: Data collection about headsets on walkway along a park towards a childcare facility

Garmin Fenix 5x	500€	Bose quite comfort 35	230€
Jabra evolve2 65	200€	Sony WH-H900N h.ear	200€
Jabra Elite 85h	200€	Jabra Elite 75t	140€
Adidas R headphone	130€	Jabra Elite Active (65)	100€
Jabra Elite 45h	70€	Huawei P smart 2019	70€

Tab. 1: Detected devices and their approximate value (online purchase prices in Norway in 2021)

### 3.2 Issues

We met several issues that require further attention when capturing data.

**Discoverable devices and hidden devices** Paired and hidden devices are more challenging as sources for identity attributes. They do not advertise device names, do not interact with unpaired devices, and may use network address and device ID obfuscation techniques (see below). Such devices may therefore lack from a measurement sample when comparing or accumulating device status on a timeline.

**Changing device identifiers** Frequent changes of MAC addresses (as used in Apple devices) and randomness plus encryption as used in Bluetooth do hinder re-identification

or might create false positives<sup>4</sup>. However, profiling operating system behavior and individual protocol implementation, devices can still get profiled [BLS19] with certain effort.

**Positioning against addresses or points of reference** Location is not very precise without further equipment, such as DGPS receivers. As seen in Fig. 4, stationary measurements have a 30–50m inaccuracy in urban space. Radio waves in addition reflect from buildings and other objects. Precise mapping of stationary devices into smaller spaces, such as apartments, will require multiple measurements or triangulation.

**Dimensions of measurement** It will require several measurements over a time span in order to decide whether a device is static in a location, or whether it is mobile. Differentiation between such devices will require several data points or continuous measurement. Device fingerprinting may be necessary against changing network addresses.

**Ethical issues** The easy availability of traceable personal devices in private spaces and around moving human beings poses threats to safety, privacy and health. Abusive applications include surveillance, stalking, assault, intrusions, commercial exploitation such as price discrimination, risk for theft, burglary, robbery or personal targeted assault. Andreas Pfitzmann warned against person-specific bombs that explode when certain person's RFID passport walks by [Pf07].

## 4 Approach for elaborate identity attribute extraction

We propose the following approach for collecting IoT attributes (see Fig. 5). Sensing of wireless communication can be executed by stationary sensors (e.g., mounted at lampposts at popular locations), by mobile sensors (e.g., attached to urban buses) or by a sensor network. A typical instance of the last category would be a large community collecting data using either their smart phones or some special equipment. The WIGLE community mentioned in the previous section is a well-known example for such a crowd-based sensor network.

All these sensors scan for wireless signals and collect header information from the link layer, e.g., Wi-Fi probe requests or Bluetooth advertisements, but potentially also from higher protocol layers. Typical information that can be gathered are network addresses (e.g, MAC or SSID) and device names (e.g., Bluetooth name). As mentioned before, it is not always possible to extract identifiers directly from the scanned data, but in most cases it is possible to profile a signal source and re-identify it, when it appears again at a later point in time. This aforementioned information is enriched with meta-data such as timestamp and the current location of the sensor. Additionally, with a combination of multiple readings from

---

<sup>4</sup> See Bluetooth LE Privacy, <https://www.bluetooth.com/blog/bluetooth-technology-protecting-your-privacy/>, accessed 2020-02-26.

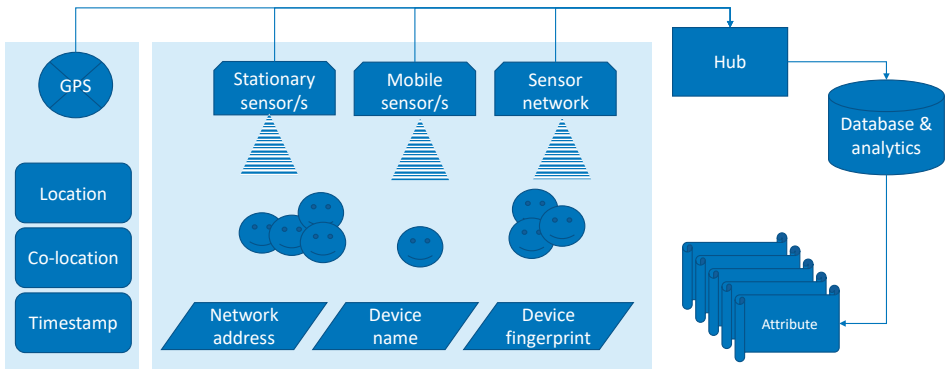


Fig. 5: IoT attribute sensing approach.

the same source, the sender's location can be calculated and stored. However, when storing the signal strength this can also be done later during the analysis phase.

The collected and stored data can then later be analyzed and further attributes can be derived. Here are some typical types of analysis that can be performed.

**District profiling** Regarding the sum of all collected scan results from a larger area can lead to interesting conclusions in many different aspects. Looking at the number of TVs or other media equipment gives an indication on the number of households or even residents. An analysis of the value of all scanned devices allows derivation of a district's socioeconomic status. In addition, the type of mobile devices can indicate the usage of an area. An example is a large number of fitness trackers on a popular jogging route.

**Traffic observation** Our experiment has shown that Bluetooth and Wi-Fi devices in cars can be scanned even when the car is driving by (with moderate speed). Nowadays, not all cars are fitted with such wireless equipment, but this will become more and more in the near future. This kind of scan allows for example analysis of traffic density (traffic jams) or characteristics of traffic (types of cars). As it is easily possible to identify a specific car and re-identify it later or at a different location also analysis of traffic flows are possible. Especially the last one is much harder with "traditional" traffic surveillance cameras, as it requires license plate recognition, which is expensive, error prone and does not conform to privacy regulations in many countries.

**Home surveillance** In sparsely populated areas like villages but also suburbs the location of a wireless device indicates uniquely to which house it "belongs". This allows surveillance of this house regarding the deployed IoT devices, the current status of inhabitants, visitors or trespassers. This information can be used for example as additional authentication factor for smart locks or for triggering a burglar alarm

system. However, it can obviously also be used for malicious actions (like described in Section 3.2).

**Person tracking** The fingerprint of all devices typically carried by a specific person is in most cases unique. Thus, once a link between this device fingerprint and the person is established the person is traceable. This link can be created for example by a treacherous device identifier (e.g., “Mike’s iPhone”) together with other publicly available information or observing entering to which home the devices (and therefore the person) return in the evening. Tracking a person can be used for smart locks in houses or cars or flexible charging of public transport. However, it also poses a huge privacy treat to this person (like described in Section 3.2).

This list of use cases is of course not exhaustive. We plan to examine other possible applications in future work.

## 5 Conclusion

In this paper, we proposed an approach for identity attribute extraction from personal IoT devices using a network of sensors. We demonstrated the feasibility of data collection, which showed availability of identity attributes directly from device properties, or from their spatial or temporal context. However, data quality is of varying levels and can get greatly improved with additional measures.

In future work, we will research further analysis possibilities using machine learning methods. We plan to look into new applications for attributes extracted from wireless IoT sensing data. Possible use cases might range from additional authentication factors in security models through facility and people management applications up to enhancing consumer surveillance through harvested attributes.

On the other hand, we will carefully analyze possible threats posed by the availability of attributes and the ease of tracing devices and their owners. This may lead to unintended exploitation on all levels of severity, such as surveillance of persons, targeted theft, burglary or kidnapping, assault (e.g. from stalkers) or as targeted liquidations based on device identification, up to weaponization of IoT and the obtained data in acts of cyberwar [FF18].

## References

- [An19] Andersen, M.: Identification, Location Tracking and Eavesdropping on Individuals by Wireless Local Area Communications, MA thesis, Norwegian University of Science and Technology (NTNU), 2019.

- [Bh19] Bhaskar, N.: A survey of techniques in passive identification of wireless personal devices and the implications on user tracking, tech. rep., Department of Computer Science, University of California San Diego, 2019, URL: [https://cseweb.ucsd.edu/~nibhaska/papers/RE\\_paper\\_19.pdf](https://cseweb.ucsd.edu/~nibhaska/papers/RE_paper_19.pdf).
- [BLS19] Becker, J. K.; Li, D.; Starobinski, D.: Tracking anonymized bluetooth devices. Proceedings on Privacy Enhancing Technologies 2019/3, pp. 50–65, 2019.
- [BZ19] Bruegger, B. P.; Zwingelberg, H.: Location Services can systematically track vehicles with WiFi access points at large scale, tech. rep., Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), 2019, URL: <https://uld-sh.de/LStrack>.
- [CKB14] Cunche, M.; Kaafar, M.-A.; Boreli, R.: Linking wireless devices using information contained in Wi-Fi probe requests. Pervasive and Mobile Computing 11/, pp. 56–69, 2014, ISSN: 1574-1192, URL: <https://www.sciencedirect.com/science/article/pii/S1574119213000618>.
- [Cu13] Cunche, M.: I know your MAC Address: Targeted tracking of individual using Wi-Fi. In: International Symposium on Research in Grey-Hat Hacking - GreHack. Grenoble, France, Nov. 2013, URL: <https://hal.inria.fr/hal-00858324>.
- [FF18] Fritsch, L.; Fischer-Hübner, S.: Implications of Privacy and Security Research for the Upcoming Battlefield of Things. Journal of Information Warfare 17/4, pp. 72–87, 2018, ISSN: 14453312, 14453347.
- [Fr08] Fritsch, L.: Profiling and Location-Based Services (LBS). In (Hildebrandt, M.; Gutwirth, S., eds.): Profiling the European Citizen: Cross-Disciplinary Perspectives. Springer Netherlands, Dordrecht, pp. 147–168, 2008, ISBN: 978-1-4020-6914-7, URL: [https://doi.org/10.1007/978-1-4020-6914-7\\_8](https://doi.org/10.1007/978-1-4020-6914-7_8).
- [Fr09] Fritsch, L.: Business risks from naive use of RFID in tracking, tracing and logistics. In: 5th european Workshop on RFID Systems and Technologies. VDE, pp. 1–7, 2009.
- [MF20] Momen, N.; Fritsch, L.: App-generated digital identities extracted through Android permission-based data access - a survey of app privacy. In (Reinhardt, D.; Langweg, H.; Witt, B. C.; Fischer, M., eds.): SICHERHEIT 2020. Gesellschaft für Informatik e.V., Bonn, pp. 15–28, 2020.
- [Pf07] Pfitzmann, A.: Personenspezifische Bomben mit RFID-Pass, Neues Deutschland, 2007, URL: <https://www.neues-deutschland.de/artikel/108709.regierung-baut-personenspezifische-bomben.html>, visited on: 02/21/2020.
- [PH10] Pfitzmann, A.; Hansen, M.: Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology. In: Designing privacy enhancing technologies. Technische Universität Dresden, pp. 1–9, 2010.

- [TLT16] Tillekens, A.; Le-Khac, N.-A.; Thi, T. T. P.: A bespoke forensics GIS tool. In: 2016 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, pp. 987–992, 2016.
- [VG13] Valeros, V.; García, S.: How bluetooth may jeopardize your privacy. An analysis of peoplebehavioral patterns in the street. *Magdeburger Journal zur Sicherheitsforschung* 3/, 2013, ISSN: 2192-4260.
- [Wr08] Wright, D.; Gutwirth, S.; Friedewald, M.; Vildjiounaite, E.; Punie, Y.: *Safeguards in a world of ambient intelligence*. Springer Science & Business Media, 2008, ISBN: 978-1-4020-6661-0.

**Open Identity Summit 2021**

**Further Conference Contributions**





# Managing authorization grants beyond OAuth 2

Fabien Imbault<sup>1</sup>, Justin Richer<sup>2</sup> and Aaron Parecki<sup>3</sup>

**Abstract:** The Grant Negotiation and Authorization Protocol, also known as GNAP, is currently being formulated in an IETF working group. GNAP gives the opportunity to reflect on the strengths and weaknesses of OAuth 2, and highlights the new directions to improve digital access. We compare with the approach taken by OAuth 2 and show that designing authorization servers primarily as “token issuers” provides insightful consequences for security and privacy.

**Keywords:** authorization protocol, OAuth 2, GNAP

## 1 Lessons from OAuth2

### 1.1 A short history

The year was 2012, and an authorization protocol called OAuth 2 (Open Authorization 2) swept the web, allowing users to use security providers to easily log in to websites. Coupled with OpenID, OAuth 2 enables an end-user to “authenticate with” one of its providers (google, facebook, github, etc.) to a completely different website or application, therefore reducing the need to define yet another password. OAuth 2 aims to solve the delegated authorization problem. Delegation happens when a third party application, acting on behalf of a natural person, requests access to a protected resource. The naive way to solve this problem is for the natural person to give its password to the third party, but sharing passwords is a security risk and must be avoided. OAuth 2 defines flows to grant access without having to share secrets.

Solving the delegation use case had such an impact because OAuth 2 landed at a time where Application Programming Interfaces (API) really became mainstream. In 2020, 83% of the internet traffic was due to APIs (compared to the remaining 17% through HTML). Cloud based companies in particular found it convenient to better secure the access to their protected API endpoints. As Gartner points out, this trend is accelerating [Ze19]: “90% of web-enabled applications have more surface area for attack in the form of exposed APIs rather than the UI, up from 40% in 2019.” Relying on a common framework enabled easier integrations across services too, as exemplified by the

---

<sup>1</sup> fabien.imbault@gmail.com

<sup>2</sup> jricher@mit.edu

<sup>3</sup> aaron@parecki.com

widespread use of zapier amongst software as a service providers. It also reduces the risk of vendors inventing their own security mechanism. Most major services now support OAuth 2, often associated with OpenID Connect for single-sign on. OAuth 2 is heavily used to protect API first services, such as open banking. The decade experience that exists with OAuth 2 and its extensions got recently consolidated into an OAuth 2.1 draft version. If approved, this update will obsolete certain parts of OAuth 2.0 and mandate security best practices [Fe16][Pa19].

## 1.2 OAuth 2 Pillars

The “core” OAuth 2.0 spec, RFC 6749 [Ha12], isn’t a specification, it’s a “framework” you can use to build specifications from. It defines roles and a base level of functionality, but leaves a lot of implementation details unspecified or optional. The IETF OAuth Working Group has published many additional specifications to fill in the missing pieces. Implementers need to decide which grant types to support, whether or not refresh tokens are one-time use, and even whether access tokens should be bearer tokens or use some sort of signed token mechanism.

The protocol seeks to enable a separation of concerns, decoupling authentication from authorization. This is a significant difference to previous protocols, such as Kerberos, Radius or SAML. OpenID Connect (OIDC) is the de-facto identity layer on top of OAuth 2.0, with extensions emerging from the decentralized identity space.

A complete introduction to the capabilities of OAuth2 is beyond the objective of this article, the interested reader may refer to the book “OAuth2 in Action”[Ri17].

## 1.3 An example of limitation

Despite its widespread use and impressive success, OAuth 2 also has downsides. A complete discussion of the current limitations is beyond the scope of this short article, but the following example illustrates the fact that human centric authorizations cannot be implemented through OAuth 2 or its UMA2 variant [Um18]:

- a) A credentialed doctor (Dr. Bob) uses a secure wallet (capable of a non-repudiable signature) to make a request (relying party credentials, scope of resource server access, purpose of access) to patient Alice's authorization server;
- b) The AS responds with a scoped capability and holds Bob accountable for its invocation;
- c) Dr. Bob passes that capability to his employer institution or to another healthcare partner. Dr. Bob may attenuate the capability before or after it is passed to the system;
- d) Another physician in the team, Dr. Carol, signs-in to the employer system and clicks on the capability associated with Alice;
- e) The client (e.g. a mobile application) used by the healthcare team (Dr. Bob or Dr. Carol) presents the capability to the protected information and gains scoped accesses to

the resource. Organizational policies would likely require an audit trail that includes the doctors' credentials and/or the root of trust of a software statement presented by the client to ensure its authenticity.

OAuth 2 would have trouble handling such a complex but realistic and common scenario, possibly requiring coordination between several ASs and resource servers, and involving delegations and policies between multiple users (the doctors) distinct from the resource owner (the patient). By focusing on the usability of privacy and security protocols within the real-world contexts in which they have to operate, we target a human centric design [Sa05]. We therefore propose to take a fresh look at how to design a delegation protocol.

## **2 Alternative design principles with GNAP**

In this section, we explain how a new protocol currently being specified within the IETF GNAP (Grant Negotiation and Authorization Protocol) working group, goes away from some of the current OAuth 2 assumptions and limitations. The core specification document is publicly available as a draft [Ie20]. Many changes are still expected before the specification is officially published, but the general design principles have received consensus from the project charter. A formal terminology [Ie21] has been approved. Early versions of the draft are already implemented as open source projects by different stakeholders, to ensure those concepts are practically sound (as per the unofficial IETF motto: "we believe in rough consensus and running code"). Non goals have been made explicit. OAuth 2 comes with known benefits and GNAP also doesn't intend to replace OAuth 2 or its extensions. An appendix in the GNAP core specification defines how to retrofit scopes and `client_id` from existing OAuth 2 systems and enable a progressive roll-out.

### **2.1 Cryptography based security**

OAuth 2 uses shared bearer secrets, including the `client_secret` and access token, and advanced authentication and sender-constraining have been built on after the fact in inconsistent ways. In GNAP, all communication between the client instance and AS is bound to a key held by the client instance.

GNAP uses the same cryptographic mechanisms for both authenticating the client (to the AS) and binding the access token (to the resource server and the AS). It allows extensions to define new cryptographic protection mechanisms, as new methods are expected to become available over time. GNAP does not have a notion of "public clients" because key information can always be sent and used dynamically in addition to being pre-registered.

## 2.2 Interaction flexibility

OAuth 2 generally assumes the user has access to a web browser. The type of interaction available is fixed by the grant type, and the most common interactive grant types start in the browser.

GNAP allows a client instance to list different ways that it can start and finish an interaction, and these can be mixed together as needed for different use cases. GNAP interactions can use a browser, but don't have to. Methods can use inter-application messaging protocols, out-of-band data transfer, or anything else. GNAP also allows extensions to define new ways to start and finish an interaction, as new methods and platforms are expected to become available over time. GNAP is designed to allow these users to be two different people, but still works in the optimized case of them being the same party.

## 2.3 Intent registration and inline negotiation

OAuth 2 uses different “grant types” that start at different endpoints for different purposes. Many of these require discovery of several interrelated parameters. GNAP requests all start with the same type of request to the same endpoint at the AS. Next steps are negotiated between the client instance and AS based on software capabilities, policies surrounding requested access, and the overall context of the ongoing request.

GNAP defines a continuation API that allows the client instance and AS to request and send additional information from each other over multiple steps. This continuation API uses the same access token protection that other GNAP-protected APIs use.

## 2.4 Client instances

OAuth 2 requires all clients to be registered at the AS and to use a `client_id` known to the AS as part of the protocol. This `client_id` is generally assumed to be assigned by a trusted authority during a registration process, and OAuth 2 places a lot of trust on the `client_id` as a result and requires it throughout the protocol. Dynamic registration allows different classes of clients to get a `client_id` at runtime, even if they only ever use it for one request.

Instead of a `client_id` (related to a pre-registered client software), GNAP relies on client instances (identified by their key). GNAP allows the client instance to present an unknown key to the AS and use that key to protect the ongoing request. It also allows to define attestation mechanisms for the client software (for instance, the organization the client represents, a specific version, the posture of the device the client is installed on, etc.). GNAP's client instance identifier mechanism allows for pre-registered clients and dynamically registered clients to exist as an optimized case without requiring the identifier as part of the protocol at all times.

## 2.5 Expanded delegation

OAuth 2 defines the “scope” parameter for controlling access to APIs. This parameter has been co-opted to mean a number of different things in different protocols, including flags for turning special behavior on and off, including the return of data apart from the access token. The “resource” parameter and RAR extensions expand on the “scope” concept in similar but different ways [Lo20].

GNAP defines a rich structure for requesting access and supports string references as an optimization. GNAP defines methods for requesting directly-returned user information, separate from API access. This information includes identifiers for the current user and structured assertions.

## 2.6 Privacy by design

OAuth 2 has no protection against a curious AS.

GNAP intends to provide privacy preserving mechanisms based on data minimization and untraceability. Those mechanisms could either target a single AS or multiple ASs in order to reduce centralization and improve scalability.

## 3 Conclusion

This article provides a comparison of OAuth 2 and the more recent GNAP authorization protocol. The later covers simple delegation in a more consistent way but also enables advanced cases between various stakeholders involved in sensitive application domains.

In OAuth2, it is assumed that the AS is the device that’s authenticating the user, collecting consent, managing the client’s registration, and creating an access token based on whatever set of rights that are associated with all of those things. In UMA2, this is turned around by letting the resource owner present a bunch of “claims” interactively, but still at the AS. With both of these, a key aspect remains: the AS needs to gather necessary information, and issue the access token (or identifiers/assertions). Because of how GNAP works, the client software has a better opportunity to present information to the AS, either directly in the request, through external parties or by introducing the AS to another software component during the “interaction” phase. So GNAP asks, what if we think of authorization server(s) primarily as a “token issuer(s)”?

Beyond GNAP, reflecting on the current assumptions and limitations of OAuth 2 is a worthwhile exercise that would require a closer partnership between practitioners and academia. In particular, a better understanding of the security and privacy guarantees would benefit the general public and the regulatory bodies.

## Disclaimer

The authors are co-editors of the IETF GNAP specification and would like to thank the participants of the working group. Please note that this paper has been written independently and has not been endorsed by the IETF.

This work derives partially from a project (mediam) which has received funding from the European Union's Horizon 2020 research and innovation programme under the NGI\_TRUST grant agreement no 825618.

## Bibliography

- [Fe16] Fett D.; Kuesters, R.; Schmitz, G.; A Comprehensive Formal Security Analysis of OAuth 2.0, Proc. Conference on Computer and Communications Security, pp. 1204-1215, 2016, <https://doi.org/10.1145/2976749.2978385>
- [Ha12] Hardt, D.; The OAuth 2.0 Authorization Framework; <https://tools.ietf.org/html/rfc6749>
- [Ie20] IETF; Grant Negotiation and Authorization Protocol (gnap), <https://datatracker.ietf.org/wg/gnap/documents>
- [Ie21] IETF GNAP wiki, Terminology, <https://github.com/ietf-wg-gnap/gnap-core-protocol/wiki/Terminology>
- [Lo20] Lodderstedt, T.; Richer, J.; Campbell, B.; OAuth 2.0 Rich Authorization Requests, IETF, draft 3, <https://tools.ietf.org/html/draft-ietf-oauth-rar-03>
- [Pa19] Parecki A.; It's time for OAuth 2.1, <https://aaronparecki.com/2019/12/12/21/its-time-for-oauth-2-dot-1>, accessed 15/01/21
- [Ri17] Richer, J.; Sanso, A.; OAuth2 in Action. Manning, 2017
- [Sa05] Sasse, A.; Flechais, I.; Usable Security. Why Do We Need It? How Do We Get It? In: Cranor, LF and Garfinkel, S, (eds.) Security and Usability: Designing secure systems that people can use, O'Reilly, 2005
- [Um18] Kantara Initiative; User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization, <https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html>
- [Ze19] Zumerle, D.; D'Hoinne J.; O'Neill, M.; API Security: What You Need to Do to Protect Your APIs, 2019

# Why should they care? Conceptualizing the challenges of information security training

Sebastian Kurowski <sup>1</sup>, Fatma Cetin<sup>2</sup>, Rudolf Fischer<sup>3</sup>

**Abstract:** Most organizations rely on individuals without or with little security knowledge to participate in information security tasks. Intending to enable them, information security trainings are usually used. But their effectiveness is debatable. In this contribution we combine descriptive analysis with the social systems theory and current literature on organizational learning and change management to conceptualize the challenges of information security training. We find that the challenges of security training are rooted within a basic dilemma of security: its value-promise (addressing of risks) is not suitable for communication within an organization. These findings are part of an ongoing research project on trainings for IoT security.

**Keywords:** Security training, awareness, policy compliance, system theory, change management, organizational learning

## 1 Introduction

There are many tasks such as identity management, credential management, policy compliance, key management, incident management and several more, where participation of non-security users in the organization is a key to success. If credentials are not handled accordingly by their owner, they become a vulnerability. In order to enable them, information security trainings are usually used. But their effectiveness is debatable. For instance, Bulgurcu [Bu09] showed that the effectiveness of security trainings is moderated by the perceived fairness of the security measures. In our systematic approach, we are using the (social) system theory [Lu84] along with its application to risk [Lu90] and organizations [Lu11] to conceptualize the challenges of information security training (see Section 3) and match these with techniques from literature on change management. These findings are used in an ongoing research project on security training development for IoT security.

---

<sup>1</sup> Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering, Team Identity Management, Nobelstr. 12, Stuttgart, 70569, [sebastian.kurowski@iao.fraunhofer.de](mailto:sebastian.kurowski@iao.fraunhofer.de)

<sup>2</sup> University of Stuttgart, Institute of Human Factors and Technology Management IAT, Nobelstr. 12, Stuttgart, 70569, [fatma.cetin@iat.uni-stuttgart.de](mailto:fatma.cetin@iat.uni-stuttgart.de)

<sup>3</sup> University of Stuttgart, Institute of Human Factors and Technology Management IAT, Nobelstr. 12, Stuttgart, 70569, [rudolf.fischer@iat.uni-stuttgart.de](mailto:rudolf.fischer@iat.uni-stuttgart.de)  
<https://orcid.org/0000-0003-0783-131X>



## 2 Analyzing social systems in information security

The system theory by Luhmann [Lu84] is a descriptive, communication focused theory on social systems. Its focus on communication hereby allows it to provide a consistent description of a research subject [St20]. In order to describe a social system, system theory uses a subsystem hierarchy [Lu84], meaning that any system can be comprised of subsystems. Patterns and structures that contribute to the description of a social system are constituted by communication between its subsystems. Subsystems however can only communicate, if both subsystems can make the same sense out of what has been communicated. This required sense-making can be achieved by a set of e.g. shared basic elements (in the following referred to as commonalities). If, for instance, two employees, or two business units do not share some common ground for making sense out of a collaboration, it will most likely not be continued, or not be initiated. Collaboration must be hereby regarded with the aspect of time in mind. Structures and patterns in social systems can be produced and vanish again, and thus every association between systems must be continuously reproduced in order to pertain.

If we consider an organization as a system-of-systems whereas the subsystems-of-interest for us are provided by the organizations business units, then the social system of information security in organizations could be reduced down to a primary value generating business unit (user BU) and the information security focused business unit (information security BU). For collaboration between these units to take place, an association must be founded on a common ground for sense making through commonalities [Lu84]. However, there is little common ground between these business units within their goals, foundations for action, and desired outcomes. The user BU for instance acts upon working tasks, with value generating goals in mind, towards the outcomes of its value generating processes. The information security BU on the other hand acts upon the current state of the security architecture, with information security specific goals (mostly risks) in mind, and towards a future state of the organizations security architecture.

This leaves little ground for commonalities to occur naturally within the organization, which yields the question which sense these units should make out of collaborating? However, when looking at organizations one may argue that collaboration between a user BU and an information security BU sometimes take place. A commonality for such a collaboration could lie in the acceptance of information security collaboration as a necessary task to ensure the future of the organization. However, an experiment conducted in 2017 found that individuals may stop participating in information security tasks after enough working stress had been invoked on the participants [Ku18]. This shows that the willingness to participate in information security tasks may as well vanish over time, e.g. when participants start to consider information security as work impeding, and thus a value impeding activity.

A common approach to establish a common ground for sense making is usually found in risk awareness campaigns. These try to raise awareness on the risks that information

security is addressing and thus provide the ground for making sense out of information security actions. Risk however is not a naturally occurring phenomenon, but an individual anticipation due to an observed threat [Lu90]. It is thus entangled with its observer [Ba91], and therefore influenced by individual traits such as the affinity or aversion towards certain risks [KT79][Me17], the tendency to weigh known risks heavier than unknown ones [GS89][Me17], and the tendency to underestimate risks that apply to contexts further away from one's personal context [He03][Be09][No83]. With this in mind, findings that individuals with no information security background seem to perceive certain security risks differently than those with security background as found by Albrechtsen and Hovden in 2009 [AH09] seem hardly surprising. This also challenges the communication of risks, as these can hardly be justified without losing credibility either through communicated materialization scenarios that are not believed by the user BU or which seem exaggerated, or which may even be perceived as threats by the user BU [Sk98]. This concludes a basic dilemma of organizational information security. It can hardly objectively justify its actions with its risk posture.

Sometimes legal compliance is referred to as a possible solution out of this dilemma. But this only works if legal compliance is considered for the sake of it<sup>4</sup>. As soon as legal compliance is considered as evasion of sanctions, it becomes a matter of individual risk perception and again leads to described dilemma. This leaves us with the only common ground for associations of the information security BU with the user BU: The trust that this association is in the interest of the user BU. This however also involves that the view on the user BU by the information security BU changes radically from servant to customer.

### **3 Addressing social challenges of information security training**

The change management literature offers a wide range of tangible methods which provide possibilities to bring about changes in personal behavior coming from an organizational logic [Cg19][La21][VW20]. In the everyday professional life of social systems, social-emotional indicators control motivation, action, and "downstream behavioral processes" [Ur08]. Emotional experience and trust affect individual action processes as well as subjective attitudes and perspectives of individuals. Therefore, they play an essential role for the willingness to perform according to the organisational goals [LK02]. Performance for this context can be understood as the BU user's performance of safety-related tasks. Despite the existing formal organizational structures, which according to Luhmann create a basis for trust, the challenge on how to maintain trust in interpersonal communication and interaction remains. In today's debate, managing

---

<sup>4</sup> In this case legal compliance bears its own meaning, which would distinguish between either being compliant or not being compliant. Communication that bears its own meaning does not require further commonalities and is in the system theory referred to as a *success media* [Lu84]

organizational change represents a major challenge for any organization [WQ99]. The successful implementation of change comprises the Organizational (changing structures and processes), Personnel (changing behavior) and Cultural (change in values in norms) level. Amongst these, cultural change plays an essential role, as it triggers the change of values and norms, and thus fosters attitudes and behavioral changes of organizational members [He16].

Simply put, an organization learns by the totality of the organization's members learning. Individuals thus no longer comprehend problems strictly from their own point of view but relate them to the expected actions and perceptions of the organization and thus reorder their own activities in accordance with the organizational specifications [AS06]. Thus, theoretically, a commonality is established between the information security BU and the user BU. However, this contingency develops exclusively through the reproduction of basic elements that create meaning and make it possible to act according to organizational specifications. Nevertheless, it should be noted that an idealistic concept such as this requires a high degree of (intrinsic) motivation to learn on the part of employees and commitment on the part of managers who apply and support this type of learning. The principle of the learning organization includes the participation of all stakeholders through clear definitions of roles and tasks and the training of appropriate competencies. This requires a culture that reminds organizational members daily and promotes learning, especially in everyday organizational life. The following is a brief description of some of the success factors that show the most promise in implementing cultural change in an organization [La21]: **Communication tools** play a key role in terms of a credible and honest internal information policy. Communication should begin before the start of a change process and continue beyond its end. In addition, it must be extremely clear, as it is fundamentally open to interpretation and therefore susceptible to misunderstanding. Openness, empathy and constructiveness are further crucial components of communication and the central signals when resistance to change from within one's own organization must be responded to. **Participation tools** create an acceptance of those affected in the change process - provided that the offer developed for this purpose is credible, transparent integrates feedback and is meant seriously. The people affected can identify more easily with the change, which further creates positive impacts on the other individuals, since increasing participation is accompanied by an increase in motivation. For the implementation of an organizational change, additional skills, competencies and knowledge are needed to cope with the resulting new tasks. A need for **Advanced Training** naturally arises in the field of management. Managers play an essential role as promoters or multipliers, as they recognize the causes of resistance, moderate conflict discussions, increase employee motivation, conduct targeted employee discussions and establish a culture of error.

## 4 Conclusion

This paper captures the puzzle of needed, but often missing, collaboration among non-security users on critical information security issues. We conceptualized the problem using Luhmann's systems theory and were thus able to break it down to the fact that lack of collaboration between organizational units is based on an absence of meaningful elements which itself is followed by a failing credible communication and ultimately leads to (unintentional) non-compliant behavior. This is rooted within a dilemma of organizational information security: that any risk-based communication is susceptible to failure. In our view it thus makes sense to look at a broader, conceptual view on the organisation. We presented such a view with an insight into possible solution trajectories from change management and organizational learning literature. These include a focus on different communication and participation tools, and trainings. We believe that credible communication can only come from a credible organization that considers itself as a sum of its individuals, focusing on communication as a core piece for fostering participation. We aspire to deliver trainings that provide this in our future research.

## Bibliography

- [AH09] Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. *Computers & Security*. 28, 6, 476–490 (2009).
- [AS06] Argyris, C., Schön, D.A.: *Die Lernende Organisation*. Grundlagen, Methode, Praxis. Klett-Cotta (2006).
- [Ba91] Baskerville, R.: Risk analysis as a source of professional knowledge. *Computers & Security*. 10, 8, 749–764 (1991).
- [Be09] Benjamin, A.S. et al.: Signal detection with criterion noise: applications to recognition memory. *Psychological review*. 116, 1, 84 (2009).
- [Bu09] Bulgurcu, B. et al.: Effects of Individual and Organization Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviors. Presented at the (2009). <https://doi.org/10.1109/CSE.2009.484>.
- [Cg19] Cameron, E., Green, M.: *Making Sense of Change Management: A Complete Guide to the Models, Tools and Techniques of Organizational Change*. Kogan Page Publishers (2019).
- [GS89] Gilboa, I., Schmeidler, D.: Maxmin expected utility with non-unique prior. *Journal of Mathematical Economics*. 18, 2, 141–153 (1989). [https://doi.org/10.1016/0304-4068\(89\)90018-9](https://doi.org/10.1016/0304-4068(89)90018-9).
- [He03] Hermand, D. et al.: Risk target: An interactive context factor in risk perception. *Risk Analysis*. 23, 4, 821–828 (2003).

- [KT79] Kahneman, D., Tversky, A.: Prospect Theory: An Analysis of Decision under Risk. *Econometrica*. 47, 2, 263 (1979). <https://doi.org/10.2307/1914185>.
- [Ku18] Kurowski, S. et al.: On the possible impact of security technology design on policy adherent user behavior-Results from a controlled empirical experiment. *SICHERHEIT 2018*. (2018).
- [La21] Lauer, T.: Change management: Fundamentals and success factors. Springer, Berlin and [Heidelberg] (2021).
- [Le20] Lee, D.: The society of society: The grand finale of Niklas Luhmann. *Sociological Theory*. 18, 2, 320–330 (2000).
- [LK02] Lord, R.G., Kanfer, R.: Emotions and organizational behavior. (2002).
- [Lu11] Luhmann, N.: Organisation und Entscheidung. VS Verlag, Wiesbaden (2011).
- [Lu84] Luhmann, N.: Soziale systeme. Suhrkamp Frankfurt am Main (1984).
- [Lu90] Luhmann, N.: Technology, environment and social risk: a systems perspective. *Organization & Environment*. 4, 3, 223–231 (1990).
- [Lu15] Luhmann, N.: Theorie der Gesellschaft. [...] Teilbd. 2: Die Gesellschaft der Gesellschaft [...]. Suhrkamp, Frankfurt am Main (2015).
- [Me17] Mersinas, K.: Risk Perception and Attitude in Information Security Decision-making. Royal Holloway, University of London (2017).
- [No83] Nosofsky, R.M.: Information integration and the identification of stimulus noise and criterial noise in absolute judgment. *Journal of Experimental Psychology: Human Perception and Performance*. 9, 2, 299 (1983).
- [Sk98] Skowronski, J.J. et al.: Spontaneous trait transference: Communicators take on the qualities they describe in others. *Journal of personality and social psychology*. 74, 4, 837 (1998).
- [St20] Stichweh, R.: Systems theory as an alternative to action theory? The rise of 'communication' as a theoretical option. *Acta Sociologica*. 43, 1, 5–13 (2000).
- [He16] Svea von Hehn et al.: Der Einfluss der Kultur auf den Organisationserfolg. In: *Kulturwandel in Organisationen*. pp. 1–23 Springer, Berlin, Heidelberg (2016). [https://doi.org/10.1007/978-3-662-48171-4\\_](https://doi.org/10.1007/978-3-662-48171-4_).
- [Ur08] Urban, F.Y.: Emotionen und Führung: Theoretische Grundlagen, empirische Befunde und praktische Konsequenzen. Springer-Verlag (2008).
- [VW20] Vahs, D., Weiland, A.: Workbook Change Management: Methoden und Techniken. Schäffer-Poeschel (2020).
- [WQ99] Weick, K.E., Quinn, R.E.: Organizational change and development. *Annual review of psychology*. 50, 361–386 (1999). <https://doi.org/10.1146/annurev.psych.50.1.361>.

# Analyzing Requirements for Post Quantum Secure Machine Readable Travel Documents

Frank Morgner,<sup>1</sup> Jonas von der Heyden<sup>2</sup>

**Abstract:** In a post-quantum world, the security of digital signatures and key agreements mechanisms used for Machine Readable Travel Documents (MRTDs) will be threatened by Shor's algorithm. Due to the long validity period of MRTDs, upgrading travel documents with practical mechanisms which are resilient to attacks using quantum computers is an urgent issue. In this paper, we analyze potential quantum-resistant replacements that are suitable for those protocols and the resource-constrained environment of embedded security chips.

**Keywords:** MRTD; Post-quantum-cryptography

## 1 Introduction

Quantum computers will reduce the security of most of the cryptographic mechanisms in use today. For symmetric cryptography, Grover's algorithm [Gr96] speeds up searches for the secret key quadratically so that the key size needs to be doubled to keep the pre-quantum security level. The impact on asymmetric cryptography is much greater: Shor's algorithm effectively breaks schemes that are based on factorization or discrete logarithm [Sh99]. Especially for security chips used in identity documents, which typically have a validity period of 10 years, immediate action is required. Produced today, an ID document should still be securely usable in 2031. However, many experts are expecting a sufficiently powerful quantum computer around 2030. This temporal relation is known as "Mosca's Inequality"[Mo15]. Given the time required for standardization and transition to post-quantum secure systems, we need to worry about the impact of quantum computers for the cryptographic protocols used in identity documents.

To alleviate the threat of quantum computers towards cryptography, the US-American National Institute of Standards and Technology (NIST) has initiated a post-quantum cryptography (PQC) competition in 2017. By 2020 this competition has reached its third round with 7 finalists and 8 alternative candidates [Na20a]. In addition, two post-quantum secure hash-based signature schemes have been recommended in NIST SP 800-208 [Na20b] already. The German BSI, too, has started to include post-quantum secure algorithms into their technical guidelines [Bu21].

---

<sup>1</sup> Bundesdruckerei GmbH, Innovations, Kommandantenstraße 18, 10969 Berlin, Germany

<sup>2</sup> Fraunhofer AISEC, Breite Straße 12, 14199 Berlin, Germany

There are various cryptographic protocols involved in the communication between inspection systems (also called terminals) and MRTD chips (also called chips): Typically, a terminal verifies the machine readable zone of the chip via Password Authenticated Connection Establishment (PACE). This creates an end-to-end encrypted communication channel, which prevents eavesdropping and allows reading the chip's less sensitive data groups. The terminal can then use Passive Authentication to check if the Document Security Object (SOD) is unchanged and thereby verify the integrity of the data groups and of the machine readable zone. Subsequently the terminal can use either Active Authentication or Chip Authentication (version 1, CAV1) to verify the authenticity of the chip. Furthermore, Terminal Authentication (version 1, TAV1) proves the inspection system's authorization to read sensitive data such as the fingerprints [In].

Previous work on post-quantum certificates for MRTs tested how using post-quantum secure signature schemes impacted the document signing PKI [PM20]. This allows the terminal to verify the integrity of less sensitive data with Passive Authentication, but it leaves protocols involving cryptography done by the document's chip an open issue. Additionally, [KV09, GK10] devised post-quantum secure replacements for PAKE (Password authenticated key exchange), which are not suitable for replacing PACE in MRTDs due to lack of efficiency [GK10].

This paper presents intermediate results from the research project PoQuID - Post Quantum ID, which is designed as feasibility study for post-quantum secure identity documents. We analyze the cryptographic building blocks of post-quantum secure Machine Readable Travel Documents with a focus on the protocol steps that require cryptographic operations by the MRTD's chip. Our results show that some protocols can be upgraded with a post-quantum secure drop-in replacement while others need to be completely reworked due to the absence of an efficient, post-quantum secure counter part to the Diffie-Hellman key exchange.

## 2 Active Authentication and Chip Authentication

To prevent cloning attacks where data from one passport document is duplicated and used in a counterfeit passport, the terminal uses Active Authentication or Chip Authentication [In]. Both protocols verify that the chip is in possession of a secret key stored in secure memory. With Active Authentication, the terminal sends a nonce which gets signed by the chip. The terminal can then verify the signature using the chip's public key, which is secured by Passive Authentication of the Document Security Data.

For Chip Authentication, the chip has a static (elliptic curve) Diffie-Hellman key pair. Its public key is also signed by the document issuer (Passive Authentication). The terminal generates an ephemeral key pair within the same domain parameters as the chip and both compute a shared secret. The shared secret is then authenticated by both parties with a message authentication code (MAC). The advantage over Active Authentication is that the

chip does not need to sign a challenge, which avoids non-repudiation and therefore increases privacy.

Active Authentication can be easily migrated to a post-quantum secure signature scheme, although it is imperative to select this scheme for performance as the signature is generated by the chip. Since there are no Diffie-Hellman-like post-quantum algorithms considered in the NIST standardization process, the key exchange in Chip Authentication needs to be facilitated through a key encapsulation mechanism (KEM). Here, the terminal uses the Chip's public key to encapsulate a session key in a ciphertext, which is sent to the Chip and can be decapsulated by the chip with its private key. If desired, the security of the post-quantum algorithm could be strengthened by adding a conventional and well-tested cryptographic algorithm to the mix through the use of KEM combiners. This would establish hybrid security so that the protocol would be secure even if there is a flaw in the post-quantum algorithm (as long as there is no sufficiently powerful quantum computer).

### 3 Terminal Authentication

Terminal Authentication is a challenge-response protocol similar to Active Authentication. First, the terminal provides a certificate chain from the Chip's trust anchor to the terminal's certificate. Once the chip has successfully verified the signatures, it generates a challenge, which is signed by the terminal in response.

The signature scheme used in Terminal Authentication can be easily replaced with a post-quantum secure algorithm. The chip, however, needs to verify at least three signatures, one from the terminal and each individual signature from the certificates in the chain (typically with at least two certificates). Therefore the post-quantum secure signature scheme for terminal certificates and terminal signatures needs to be selected for high efficiency of verification. Also, the size of the public keys and signatures needs to be small enough to guarantee an acceptable transfer time when transmitted to the chip via NFC.

Table 1 gives an overview of the cryptographic operations performed by chip and terminal in the protocols described above.

	Chip	Terminal
Active Authentication	Signature creation	Signature validation
Terminal Authentication	Multiple signature validations	Signature creation
Chip Authentication	Key Agreement	Key Agreement, signature validation
Passive Authentication	-	Signature validation

Tab. 1: Overview of cryptographic operations performed by chip and terminal in surveyed MRTD protocols.



## 4 Post-Quantum Secure Algorithms for MRTD

When choosing the cryptographic schemes that fulfill the requirements given above, two complementary non-functional requirements need to be balanced: performance and robustness. In terms of performance, it has already been shown in [In17, A118] that the newest generation of smart card chips are capable of running asymmetric post-quantum secure cryptography. For choosing post-quantum alternatives, we assume that the chip runs on a platform similar to the ARM cortex M4 with 50 MHz CPU, AVX2 support, 48 kByte SRAM and 2 Mbyte flash memory, which is a configuration very similar to those used in recent security microcontrollers [In20]. For this theoretical analysis we ignore the overhead of creating an side-channel-free implementation.

In regards to robustness, algorithms need to be secure for the whole lifetime of the document, which is typically 10 years. Therefore we are only considering the round 3 finalists in the NIST PQC competition for use in sovereign documents. More specifically, we are considering algorithms that at least achieve NIST level 1 which represents around 128 bits of classical security. Due to the immaturity of most post-quantum algorithms, the document issuer may want to improve the robustness by integrating a classical algorithm (hybrid security) or by adding an update mechanism to the chip to achieve cryptographic agility (crypto-agility). Both of these additional approaches will not be discussed here.

### 4.1 Post-Quantum Secure Signature Schemes

While there are three signature schemes considered as finalists for standardization and two hash-based signature schemes already standardized by NIST [Na20b], only two algorithms are considered for the use in identity documents here. This is due to the fact that one finalist (Rainbow) is too inefficient for use in MRTD chips. Moreover, the hash-based schemes are an interesting option for verifying potential cryptographic algorithm updates (crypto-agility), but since they require a state management we ruled them out as the default signature algorithm in MRTD chips. As shown in Table 2, from the two remaining schemes Dilithium and Falcon, Dilithium is preferable due to faster signature creation. This is especially relevant for Active Authentication where the chip has to compute the signatures. In addition, key generation takes much longer in Falcon. As is, the surveyed protocols use static keys, so this should not matter too much, but it is still good to have the option of fast key generation during personalization of the document.

### 4.2 Post-Quantum KEMs

As shown in Table 1, terminal and chip perform a key agreement in Chip Authentication. Since there is no post-quantum Diffie-Hellman-like key exchange in the NIST competition, the Chip Authentication protocol has to be adapted to use KEMs.

	Dilithium2	Falcon512
Key generation (kCycles)	1,574	171,386
Signature creation (kCycles)	3,970	38,981
Signature size	2.42 kB	657 B
Signature verification (kCycles)	1,599	475

Tab. 2: Benchmarks for post-quantum secure signature schemes (NIST security level 1) on a Cortex-M4 processor [Fr21].

Of the four KEMs that NIST designated as finalists, Classic McEliece can be eliminated right away since its keys are too large to be efficiently transmitted between chip and terminal via NFC. The remaining three contenders are compared to each other in Table 3. For forward security it is imperative to allow for ephemeral keys, especially on the chip. As seen in the table, this requirement rules out NTRU which has very slow key generation. Kyber and SABER on the other hand are very similar across all metrics. Since Kyber and Dilithium share code, we selected Kyber as the KEM for our research project.

	Kyber512	NTRU-HRSS-701	LightSABER
KeyGen (kCycles)	463	153,104	359
Encapsulation (kCycles)	567	377	491
Decapsulation (kCycles)	525	870	464
Ciphertext size	736 B	1.14 kB	736 B

Tab. 3: Benchmarks for post-quantum secure KEMs (NIST security level 1) on a Cortex-M4 processor [Fr21].

## 5 Conclusion

In our analysis we identified PACE, Terminal Authentication and Chip Authentication as well as the Document PKI and Terminal PKI as components that need to be adapted to make MRTDs post-quantum secure. Subsequently, we identified post-quantum secure algorithms which fulfill the requirements of resource-constrained environments. As shown in section 4, of the finalists competing the NIST PQC competition Dilithium and Kyber are most suited for deployment in MRTDs as signature scheme and KEM, respectively. Another benefit of choosing two lattice-based algorithms is that they may share code (and memory) on the chip and that they may benefit from the same coprocessor capacities. Further research will need to practically evaluate the given estimates, especially considering that there will be varying performance penalties incurred from countermeasures against side-channel attacks. Another interesting question left for further research is how protocols (in this case Chip Authentication) using Diffie-Hellman key exchange can be securely adapted for use with KEMs.

## Bibliography

- [Al18] Albrecht, M.; Hanser, C.; Hoeller, A.; Poepplmann, T.; Virdia, F.; Wallner, A.: Implementing RLWE-based Schemes Using an RSA Co-Processor. In: IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019. 2018.
- [Bu21] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie 02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1. Standard, 2021.
- [Fr21] Fraunhofer AISEC: , PQDB: A comprehensive benchmark post-quantum cryptography algorithms. <https://cryptoeng.github.io/pqdb/>, 2021. Accessed: 2021-04-15.
- [GK10] Groce, Adam; Katz, Jonathan: A New Framework for Efficient Password-Based Authenticated Key Exchange. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. CCS '10, Association for Computing Machinery, New York, NY, USA, pp. 516–525, October 2010.
- [Gr96] Grover, Lov K.: A Fast Quantum Mechanical Algorithm for Database Search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. STOC '96, Association for Computing Machinery, New York, NY, USA, pp. 212–219, July 1996.
- [In] International Civil Aviation Organization (ICAO): Doc 9303: Machine Readable Travel Documents. Standard.
- [In17] Infineon Technology AG: , Ready for tomorrow: Infineon demonstrates first post-quantum cryptography on a contactless security chip. <https://www.infineon.com/cms/en/about-infineon/press/press-releases/2017/INFCCS201705-056.html>, 2017. Accessed: 2021-04-15.
- [In20] Infineon Technologies AG: , Infineon's Security Solutions Portfolio. [https://www.infineon.com/dgdl/Infineon-Security-Solutions-Portfolio-ProductSelectionGuide-v20\\_02-EN.pdf](https://www.infineon.com/dgdl/Infineon-Security-Solutions-Portfolio-ProductSelectionGuide-v20_02-EN.pdf), 2020. Accessed: 2021-04-15.
- [KV09] Katz, Jonathan; Vaikuntanathan, Vinod: Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices. In (Matsui, Mitsuru, ed.): Advances in Cryptology – ASIACRYPT 2009. Lecture Notes in Computer Science. Springer, p. 636–652, 2009.
- [Mo15] Mosca, M.: , Cybersecurity in a quantum world: will we be ready? <https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf>, 2015. Accessed: 2021-04-15.
- [Na20a] National Institute of Standards and Technology (NIST): , Post-Quantum Cryptography: Round 3 Submissions. <https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions>, 2020. Accessed: 2021-04-15.
- [Na20b] National Institute of Standards and Technology (NIST): Recommendation for Stateful Hash-Based Signature Schemes, SP 800-208. Standard, 2020.
- [PM20] Pradel, Gaetan; Mitchell, Chris J: Post-Quantum Certificates for Electronic Travel Documents. In: Proceedings of DETIPS 2020 (Interdisciplinary Workshop on Trust, Identity, Privacy, and Security in the Digital Economy), September 18 2020. Lecture Notes in Computer Science. Springer, pp. 56–73, December 2020.
- [Sh99] Shor, Peter W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Review, 41(2):303–332, Jan 1999.

# Role of Identity, Identification, and Receipts for Consent

Harshvardhan J. Pandit<sup>1</sup>, Vitor Jesus<sup>2</sup>, Shankar Ammai<sup>3</sup>, Mark Lizar<sup>4</sup>, and Salvatore D'Agostino<sup>5</sup>

**Abstract:** This article outlines issues in the current ecosystem of data sharing based on consent and the role of identity and identification. It argues how the consent mechanism is hostile to individuals in the form of: (a) inscrutable third parties who remain largely unknown; (b) denying ability to identify and manage consent; and (c) lack of technological solution. The article discusses the role and feasibility of *Consent Receipts*, and presents its role in the Privacy as Expected: Consent Gateway (PaE:CG) project for the future of accountable identity and identification mechanisms for consent.

**Keywords:** Consent, Identity, Identification, Accountability, GDPR

## 1 Introduction

Consent in the context of data protection and privacy laws is a legal basis that affords individuals control and choice over the processing of their personal data. Though laws such as the GDPR do not explicitly mention requirements regarding identity or identification of Data Subjects, it is implied for Data Controllers to establish that the Data Subject or an authorised agent on their behalf is exercising consent or rights. Where individuals already interact with services using identifiers, such as through accounts, the exercising of consent and rights does not need a separate identity and identification process. However, there is no mutual agreement on identity where individuals only interact with the service in the context of consent, such as through a cookie/consent dialogues. As a result, when the individual wishes to exercise their rights in connection with the choices made regarding consent, they have no way to indicate their identity and the service in return has no form of identification with which to validate the individual's right to access and change their consent.

Controllers, or more specifically their websites, get around this problem by using ephemeral or transient solutions such as '*cookies*' to store the information associated with given consent, and use it to enable the individual to later revisit the website and change their choices, usually through dedicated *consent management interfaces*. Apart from the fact that such interfaces and processes are under question regarding their legality [SBM20], their use is problematic given that: (a) exercising rights is conditional on existence of the cookie;

---

<sup>1</sup> ADAPT Centre, Trinity College Dublin, Ireland. pandith@tcd.ie

<sup>2</sup> School of Computing and Digital Technology, Birmingham City University, UK. vj@vitorjesus.com

<sup>3</sup> School of Computing and Digital Technology, Birmingham City University, UK. shankar.ammai@mail.bcu.ac.uk

<sup>4</sup> Open Consent, London, UK. mark@openconsent.com

<sup>5</sup> Open Consent, London, UK. sal@openconsent.com

(b) it is non-transferable to other devices or browsers; (c) the individual has no mechanism to demonstrate or challenge their consent; and (d) no coherent way individuals to manage consent through cookies given obfuscation and lack of tools/mechanisms.

On the other side of this perspective, individuals often do not understand the existence and scope of entities they often share consent with, which is compounded by the issue termed the “biggest lie on the internet”[OO20] that individuals are not aware of or do not comprehend the ‘policies’ and ‘notices’ shown online, yet agree to the presented conditions. Existing research has shown the malpractices of consent in terms of ‘dark patterns’ that manipulate and coerce consent [SBM20] the large-scale anonymity and inscrutability of third-party recipients of data [Ur20]. The California Consumer Protection Act (CCPA), passed recently in 2018, provides a mechanism for ‘opting-out’ of what it terms as ‘selling’ data to such third parties, and mandates the provision of a ‘do-not-sell’ option on websites. However, the issue remains that there is no method to identify which recipients the data has been ‘sold’ to, and to track their acceptance and enforcement of ‘do-not-sell’ right.

## 2 Consent Receipts

The Consent Receipt specification [LT17] was created by the Kantara Initiative to define an interoperable record for facilitating management of consent for both the Data Subject and the Controller<sup>6</sup> by representing metadata and context associated with given consent, and providing a unique ID for the receipt as a shared identifier for Controllers and Data Subjects to refer to consent - with the option for the receipt to be signed by the Controller.

The use of a Consent Receipt helps with the issue regarding identity and identification as it permits the Data Subject and Controller to use and refer to the same common shared record in their communication and exercising of rights. Where the Controller cryptographically signs the receipt, it also presents the possibility to use it as documentation for the Controller’s accountability by utilising the receipt as proof of consent transaction. The Consent Receipt in its current form (v1.1) has, amongst other, two significant gaps: (i) records do not concern authentication or verification of entities and information; and (ii) requires proactive participation by Controllers. Despite these shortcomings, the larger argument of using receipts as a proof and record of transactions, and its potential for establishing trust through transparency and accountability remains valid as outlined in ‘web of receipts’ [Je20].

Receipts, as an artefact, can aid in establishing the identity and proof of an interaction or a transaction regarding consent [Je20]. However, in order to perform these actions, the parties involved must agree on the methods and infrastructure used in identification and verification. There is also the issue of support and implementation by all parties involved in the receipt process - the Controller to create and issue the receipt, the web-browser or device as an agent of the Data Subject to receive and store the receipt, and the ability to inspect and

---

<sup>6</sup> Use of ISO terms in Consent Receipt is replaced here with their GDPR equivalents for consistency

verify receipts independent of either party. In its current form, the onus of receipt creation and provision is on the Controller - which diminishes its effectiveness for bad actors and prevents Data Subjects from proactively recording or challenging consent claims.

However, the concept of 'receipts' as an accountable record is gaining interest and traction. The Advanced Notice and Consent WG<sup>7</sup> (ANCR) at Kantara is currently working to update the Consent Receipt specification to address the recent legal requirements and privacy challenges. The recently published ISO/IEC 29184:2020<sup>8</sup> standard for Online Privacy Notices and Consent defines criteria and controls for consent collection and uses the Consent Receipt specification as an example of a machine-readable consent record. Additionally, the ISO/IEC 27560<sup>9</sup>, currently in drafting stage, is intended to provide a standardised implementation for consent records.

### 3 Privacy as Expected: Consent Gateway (PaE:CG) Project

PaE:CG is funded under the EU H2020 Next Generation Internet's (NGI) TRUST project funding programme which promotes development of innovative solutions for management of consent by utilising privacy enhancing technologies (PETs) such as cryptography and federated identity. The driving principle for PaE:CG is utilising receipts for an accountable mechanism while ensuring the Internet as it currently is and should remain for the most part a *pseudo-anonymous space*, while still empowering individuals with choice and control through consent. PaE:CG thus extends the existing paradigms of Consent Receipt, cryptographic identity and verification, and online identities to defining specifications and create implementations for information structures and processes across three levels: (i) service provider; (ii) end-user; and (iii) a notary or witness - a radical new concept introduced by the project to counter non-participation by some entities within the consent transaction. The project rationale and objectives can be explored in more detail via its website <https://privacy-as-expected.org/>.

#### 3.1 Consent Receipts within PaE:CG

Within the PaE:CG vision, consent receipts work as expected - they are generated for a transaction and are shared (copies) between the Controller and the Data Subject. What PaE:CG does differently is provide the ability to any entity for generation of receipt, thus permitting any participant to produce a record without relying on the goodwill or accountability of others. The receipts are to be signed, which provides guarantees regarding who produced it, at what time, and the receipt itself is meant to record the context of consent. The PaE:CG version of receipts thus enables individuals to claim records where a controller

<sup>7</sup> <https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=140804260>

<sup>8</sup> <https://www.iso.org/standard/70331.html>

<sup>9</sup> <https://www.iso.org/standard/80392.html>

does not provide any record or receipt, and conversely also enables controllers to produce records for their own transparency and accountability where individuals do not participate in the process. Ideally, both controllers and individuals would participate and sign the receipt to ensure the highest degree of accountability for all parties.

The PaE:CG specification defines protocols for use of *bearer tokens* to provide cryptographic guarantees regarding identity when receipts are generated and signed. This permits the receipt to be used for identification purposes for that specific interaction, and additional possibilities to be used further in exercising related rights such as modification or withdrawal of consent. For controllers and service providers, receipts thus provide a convenient way to build and maintain trust based on accountability, and also offer the possibility of creating self-service points that utilise receipts to manage consent and personal data without additional forms of identities. This also provides an avenue for building innovative solutions towards other new and novel forms of data sharing and controls which can be based on decentralised identifiers.

The verifiable identity protocols used in PaE:CG receipts provide a ‘proof’ and ‘record’ of consent along with pertinent information required for legal compliance and complaints. For this, the identity of Data Controllers and Third Parties need additional introspection owing to their role in the collection, use, and sharing of data. PaE:CG therefore looks towards utilising the existing identities of controllers expressed through their websites and domain names, and extends it with requirements to associate them with a legal identity. This has the additional benefit of utilising the existing mechanisms of secure identity and information based on internet and web protocols. For example, to express that consent was collected on a specific website by the specified legal identity, the information from the website’s public keys and certificates that the web-browser already verifies as part of secure connections could be potentially reused as a form of record and identity.

### **3.2 Witness to Notarise the Consent Record**

When Controllers support the use of receipts natively by implementing PaE:CG protocols, which is the ideal use-case, the interface and use of receipts is seamless for all parties. Ideally, each Third Party would also sign the receipt for complete transparency and verifiability. However, implementing such radical protocols would take time and require support, and it is expected to face barrier through non-conformance and resistance. With this in mind, the real innovation in the project concerns where Controllers or Third Parties do not support the PaE:CG protocols, and thereby do not provide receipts.

Rather than abandon the usefulness of receipts, PaE:CG allows a trusted third party to act as a ‘witness’ or ‘notary’ to the consent interaction by signing the receipt, as depicted in Fig.1. Witnesses solve the problem of transparency and auditability of organisations on the web, and allow for any party - whether it be the Data Subject, or Controller, or Third Party, to produce verifiable records as a form of claim. For Data Subjects this provides a way to

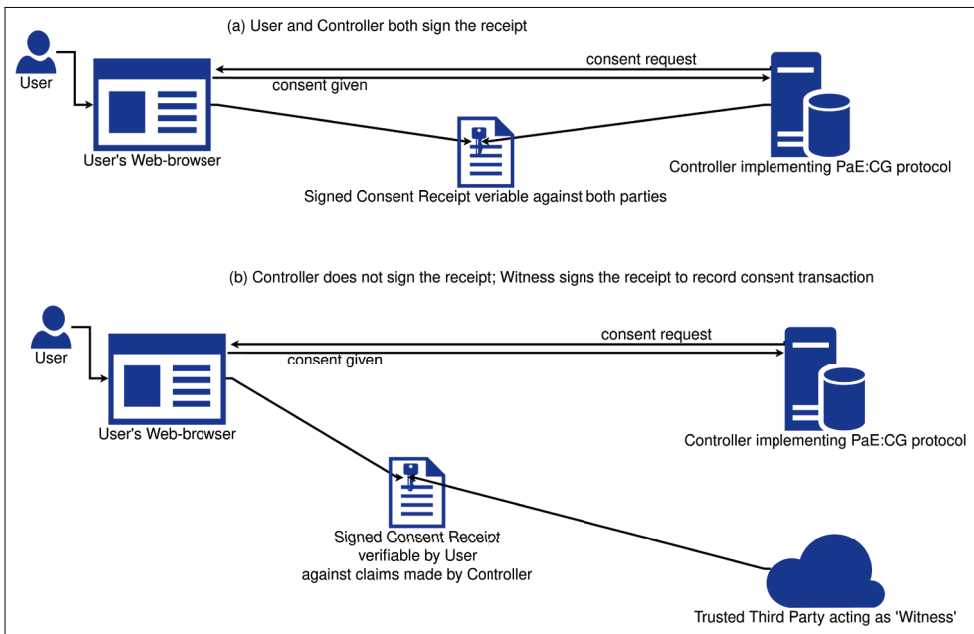


Fig. 1: Use-cases showing application of PaE:CG protocol where (a) Controller’s support signed receipts; and (b) Witness signs receipts for accountability claims

hold organisations accountable, whereas for Controllers this provides a way to document their involvement in transactions - such as scope of data sharing with a Third Party.

The difference between a Controller and a Witness is the accountability that goes along with signing of the receipt. When a controller signs the receipt, it indicates a binding claim of practices conducted by that entity. Whereas when a witness signs a receipt it indicates that the other party (or parties) have made the specified claim - which can be used as a form of documentation that can be verified to be produced at a specific time and context. As the witness is agnostic to the other entities, it can be used by either the Controller - for example to record that the individual has consented to specific purposes; or by the individual - for example to record that they consented to only some purposes. Extending the application to other avenues of accountability, the PaE:CG protocols and the use of a Witness permits individuals to also generate and demonstrate verifiable claims such as refusing consent to some party or recording information offered in a consent request.

### 3.3 Conclusion

PaE:CG thus updates the Consent Receipt specification for use with the recent legal developments while ensuring its practical accountability and implementation using protocols



based in cryptography. This will enable and encourage a new category and level of transparency on the internet through use of receipts as an artefact that identifies parties and holds them accountable. The novel concept of a Witness is promising as it provides a way for both controllers and individuals to record claims made within specific contexts that can be later demonstrated and verified. In addition to practices of accountability, the utilisation of a receipt containing signatures provides a form of identification which can be used to conduct further interactions regarding consent - such as its modification and withdrawal. The identification also provides an accountable mechanism for claims of misuse or disputes regarding the interpretation of consent. Where one of more parties - such as the Controller or Third Parties - do not participate, the possibility to utilise a witness to sign instead provides a measure of trust and verification to the claim in such cases.

Apart from providing specifications and reference implementations, PaE:CG project also provides novel avenues for further work and research into utilising existing identity and accountability mechanisms for trust, verification, and consent - especially those utilising web protocols and standards. To encourage such research, the project is contributing its work to the ongoing development of Consent standards at both ISO/IEC and Kantara and has pledged to disseminate its deliverables under open and permissive licenses.

**Funding Acknowledgements:** This work has been funded under the European Union's Horizon 2020 research and innovation programme NGI TRUST Grant#825618 for Project#3.40 Privacy-as-Expected: Consent Gateway. Harshvardhan J. Pandit is also funded by Irish Research Council Government of Ireland Postdoctoral Fellowship Grant#GOIPD/2020/790; and ADAPT SFI Centre for Digital Media Technology funded by Science Foundation Ireland through SFI Research Centres Programme and co-funded under European Regional Development Fund (ERDF) through Grant#13/RC/2106\_P2.

## Bibliography

- [Je20] Jesus, Vitor: Towards an Accountable Web of Personal Information: The Web-of-Receipts. *IEEE Access*, 8:25383–25394, 2020.
- [LT17] Lizar, Mark; Turner, David: Consent Receipt Specification v1.1.0. Technical report, Kantara Initiative, 2017.
- [OO20] Obar, Jonathan A.; Oeldorf-Hirsch, Anne: The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society*, 23(1):128–147, January 2020.
- [SBM20] Santos, Cristiana; Bielova, Nataliia; Matte, Célestin: Are Cookie Banners Indeed Compliant with the Law? Deciphering EU Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners. *Technology and Regulation*, pp. 91–135, December 2020.
- [Ur20] Urban, Tobias; Tang, Dennis; Degeling, Martin; Holz, Thorsten; Pohlmann, Norbert: Measuring the Impact of the GDPR on Data Sharing in Ad Networks. In: *ASIA CCS*. ACM, Taipei, Taiwan, p. 15, June 2020.

# Permission and Privacy Challenges in Alternate-Tenant Smart Spaces

Vitor Jesus <sup>1,4</sup>, Catarina Silva<sup>2</sup>, João Paulo Barraca <sup>2</sup>, Gilad Rosner<sup>3</sup>, Antonio Nehme<sup>4</sup>, Muhammad Waqas<sup>1</sup>, Rui L. Aguiar<sup>2</sup>

**Abstract:** We explore a ‘Smart-BnB scenario’ whereby someone (an Owner) advertises a smart property on a web platform. Renters use the platform for short periods, and may fully enjoy the property, including its smart features such as sensors. This scenario should further ensure the Renter’s privacy, so we use consent receipts and selective sharing. This paper describes a demonstrator of how smart environments can operate in a privacy respecting manner.

**Keywords:** IoT, Access Control, Permissions, Smart Homes, consent receipts

## 1 Introduction

With the commoditization of smart technology and communications, shared smart spaces are becoming increasingly common. What was previously “dumb” and “single-feature” devices, such as a simple lightbulb, are now progressively internet-enabled devices that, while delivering basic functionality (such as light) bring with it convenient added-value features. For example, a smart light bulb can have different modes of operation, be controlled remotely with a mobile application, and operations can be scheduled based on the time of the day. A simple lightbulb raises little risk but a lock on a front door or an indoor camera is a different case.

Project CASSIOPEIA (Contextually-Appropriate Selective Sharing IoT Open-standard PErmissioning Architectures) looks at such scenarios. The setting is a smart home containing a range of devices that are increasingly common for sensing and automation purposes: entertainment systems, environmental sensors, security cameras, etc. Such ‘Smart-BnB’ scenario, as we call it, we look at dynamic sharing of access to devices inside a smart-space. A Renter books a property for a period in time and an Owner sets access permissions. Such *selective delegation of access* should be simple and effective.

---

<sup>1</sup> PrivDash Ltd, UK – [vitor@privdash.com](mailto:vitor@privdash.com) (<https://orcid.org/0000-0002-5884-0446>), [waqas@privdash.com](mailto:waqas@privdash.com)

<sup>2</sup> Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, Aveiro, Portugal: [c.alexandracorreia@ua.pt](mailto:c.alexandracorreia@ua.pt) (<https://orcid.org/0000-0002-7969-8813>), [jbarraca@ua.pt](mailto:jbarraca@ua.pt) (<https://orcid.org/0000-0002-5029-6191>), [ruiilaa@ua.pt](mailto:ruiilaa@ua.pt) (<https://orcid.org/0000-0003-0107-6253>)

<sup>3</sup> Internet of Things Privacy Forum, Alton, United Kingdom, [gilad@iotprivacyforum.org](mailto:gilad@iotprivacyforum.org), <https://orcid.org/0000-0001-8254-8763>

<sup>4</sup> Birmingham City University, School of Computing and Digital Technology, Birmingham, UK – [Antonio.Nehme@bcu.ac.uk](mailto:Antonio.Nehme@bcu.ac.uk)

Furthermore, devices are expected to collect personal information raising Privacy and Data Protection problems.

This paper shares the challenges and lessons learned by our project during design. In Sect. 2 we describe at the project use-cases. In Sect. 3 we elaborate on key research consideration. Sect. 4, presents our technical approach and Sect. 5 concludes our paper.

## 2 Related Work

The sheer growth in the complexity and volume of global data flows and data processing creates problems with lack of transparency. Users do not, in general, know how their personal data is handled [Ro18] raising Privacy problems, a problem particularly challenging if information crosses boundaries such as between users, systems or countries. In this sense, systems must be designed with base rules centred in privacy while being user-centric. Access control policies must be implemented so the control of personal data relies on the data subject. In several regulations, Consent is the corner stone and under strict conditions – it must be specific, freely given, etc. – so a clear choice is enabled. To this end, Consent receipts is a new consent that promotes choice, ethics and compliance [Je20].

The Internet-of-Things (IoT) poses particular challenges as dataflows are potentially quicker and more personalised collection, including importing domains that were once “offline” or intimate – such as Smart homes [Ji18] . Consent management is a further problem – e.g., lack of screens – which requires a user-centric approach (such as project ADvoCATE [Ra18] or [Mo19]).

## 3 Challenges and Open Questions in SmartBnB scenarios

We briefly highlight some of the challenges a SmartBnB brings.

*Integration of Devices and Identities* – There is no unique agreed interoperability standard, e.g., Zigbee Home Automation, or protocols over WIFI. ONVIF may be an exception, for security cameras, but often low-end devices tend to use proprietary solutions. MQTT provides integration, but mainly for professional solutions. Large Cloud providers are a soft answer offering full stacks. Overall, we observe a highly fragmented landscape. Domoticz, Home Assistant, or Homekit are an alternative path for integration by creating software hubs supporting multiple protocols.

*User Identity* – Identity in IoT is vague and most solutions are centred around a single user. This further implicates Privacy agreements, often tied to IoT vendor cloud infrastructure – e.g., a family camera it blatantly non-compliant when choosing age.

*Delegation of access* – Beyond identity, most devices do not support multi-tenancy,

delegation of access or selective sharing. Parental controls is a common example.

*Consent Receipts* – A Consent Receipt [Je20] records the output of a transaction similar to a conventional shopping receipt. If designed with strong auditability properties, it empowers individuals, make organisations compliant and ethical and allows authorities and watchdogs to effortlessly monitor the market and resolve disputes. There is already a standard [Li17] but perhaps needs improvements for the general case beyond regulations.

*Regulatory questions* – Arguably, the most notable regulation currently is EU/GDPR for which CASSIOPEIA identified interesting questions. Two are the following. First, if our system were run by a company, it would be a Data Controller. Nevertheless, an Owner would also have some control over personal data – a notion of Joint Controller that is not completely clear in GDPR. Second is what happens to consent obtained by the Owner but temporarily delegated to a Renter.

## 4 The CASSIOPEIA Project

CASSIOPEIA investigates how we can create usable and transparent architectures enabling device owners to selectively delegate access to IoT and what happens to personal data collected during different periods. We focus on a smart home that is rented for periods to Renters. Devices collect data with varying levels of privacy and operational impact.

### 4.1 Use-cases

Our overall use-case is described in Figure 1. Before the Renter checks-in, devices are configured by the Owner to give temporary permissions to the Renter. During check-in, the Renter gives consent to collections of their personal data while in the home according to and after reviewing the Privacy Policies of each device.

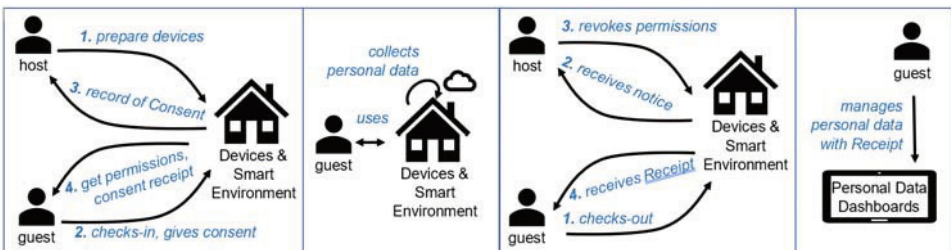


Figure 1: interaction between the host and the renter

During the stay in the Owner’s smart home, smart devices collect personal data. The

Owner should not have access to the devices, and even less the data they collect or generate. Exceptions may exist for devices with no impact to the Renter privacy that are important for security purposes (e.g., burglary), or when safety takes precedence (e.g. Smoke alarms). At the end of the stay, and a check-out procedure is actioned, permissions and consent are revoked.

In the final stage, the Renter uses the Consent Receipt to manage any of their residual data collected by the devices. After a retention period, personal data is deleted, and the Renter is notified.

## 4.2 Demonstrator Technical Approach

The project has the secondary objective of creating a publicly available, proof-of-concept demonstrator of the Smart-BnB problem, with real smart devices (e.g., actuators and sensors) to a Smart Home environment. We use “Home Assistant” (<https://www.home-assistant.io/>) with a lightweight messaging protocol for small sensors.

## 4.3 Demonstrator Technical Approach

Integrations of new smart devices are via Home Assistant; devices include security cameras, SIP doorbells, ONVIF cameras, Zigbee HA and WIFI sensors, smart TVs, etc.

Figure 2 shows the demonstrator architecture. These components offer both the views of an Owner and a Renter. Roles are not supported by Home Assistant so we had to expand the functionality. The *consent manager* is the module where consent receipts are managed and stored. Account management is a dedicated module that enables permissions to be delegated according to roles. Overall, the system architecture enhances user choice, autonomy, participation, and trust. We intend to develop a system capable of *selective sharing* and feature delegation, granular consents, transparency, and non-repudiation.

The permissioning lifecycle is as follows. On the Renter giving consent (and obtaining a Consent Receipt), the Owner delegates permissions that are effective from the check-in date and persist until checkout.

It is essential to guarantee the privacy of the Renter’s personal data. During the stay of the Renter, Owners have limited access to devices. On leaving, Renters are able to request erasure of their data, to which the relevant Data Controllers must respond by law. When a Renter leaves the house, the remaining data will be removed. Finally, Renters’ access is revoked which concludes the lifecycle. This architecture further prevents current Renters from accessing data of past Renters.

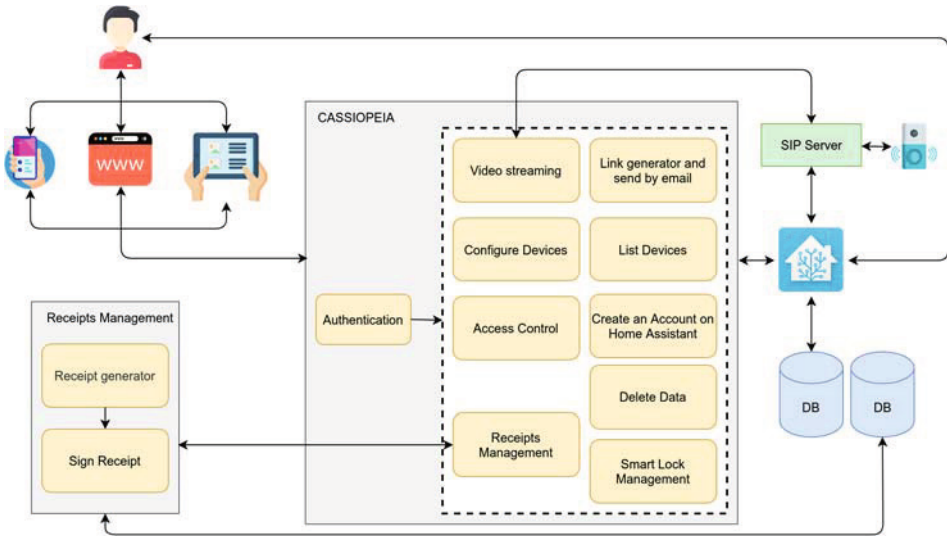


Figure 2: Overarching view of the components of CASSIOPEIA

This component to generate the receipts will be developed as an external service to CASSIOPEIA but will be customised according to the project requirements. The main features of this service will be the generation of the receipt and its control, intermediation of requests between users and data controllers, and the generation of notifications to data controllers.

The structure of the receipt is based on specification by Kantara Initiative but extensively modified to meet our requirements. Initially, a consent receipt is signed and stored on a receipt database. After the authentication on the platform, the user can access his own receipts and personal data associated with them. Personal data is stored in a protected database. Using the platform, the user can manage their receipts and revoke the associated consent while requesting, if wished, deletion of the associated data which, in the absence of a legal reason, must be honoured by the data controller.

## 5 Conclusions and Outlook

In this work, we presented the initial architecture to develop a proof-of-concept demonstrator of the Smart-BnB problem. The use of an open source platform known as Home Assistant, works as a system to collect personal data and the remaining developed systems presented in the architecture serve to guarantee the privacy (between Renter and Owner), receipts generator to manage the receipts and a database to Home Assistant store the personal data and the other database to store the receipts. As future work, we intend to make the prototype publicly available, evaluate its performance and publish the obtained

results.

## 6 Acknowledgement

This work is partially funded by NGI Trust, with number 3.85, Project CASSIOPEIA.

## 7 Bibliography

- [Je20] Jesus, Vitor. "Towards an Accountable Web of Personal Information: the Web-of-Receipts." *IEEE Access* 8 (2020): 25383-25394.
- [Ji18] Jiang, Hongbo, et al. "Smart home based on WiFi sensing: A survey." *IEEE Access* 6 (2018): 13317-13325.
- [Li17] Mark Lizar and David Turner (eds), "Consent Receipt Specification v1.1.0.", Technical report, Kantara Initiative, 2017.
- [Mo19] V. Morel, M. Cunche and D. Le Métayer, "A Generic Information and Consent Framework for the IoT," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 366-373, doi: 10.1109/TrustCom/BigDataSE.2019.00056.
- [Ra18] Rantos, Konstantinos, et al. "ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology." *International Conference on Security for Information Technology and Communications*. Springer, Cham, 2018.
- [Ro18] Rosner, Gilad, and Erin Kenneally. "Clearly opaque: privacy risks of the Internet of Things." Rosner, Gilad and Kenneally, Erin, *Clearly Opaque: Privacy Risks of the Internet of Things* (May 1, 2018). IoT Privacy Forum. 2018.

# “When need becomes necessity” - The Single Digital Gateway Regulation and the Once-Only Principle from a European Point of View

Carsten Schmidt<sup>1</sup>, Robert Krimmer<sup>2</sup> and Thomas J. Lampoltshammer<sup>3</sup>

## Abstract:

The Single Digital Gateway Regulation (SDGR) and the underlying Once-Only Principle (OOP) outlining that businesses and citizens in contact with public administrations have to provide data only once. Until now many MS and associated countries have started to implement the OOP at national level, but the cross-border implementation is still work in progress. The SDGR as one of the cornerstones of the Digital Single Market for the EU will bust this development. The authors of this paper present the development related to the SDGR and OOP in Europe. They will also show the interconnections and interdependencies between the OOP and electronic identities (eID). The paper gives an overview based on the findings of the EU-funded “The Once-Only Principle Project (TOOP)” and mobile Cross-Border Government Services for Europe (mGov4EU).

## Keywords:

Once-Only Principle, Single Digital Gateway, SDGR, DSM, mGov4EU, TOOP, eID, eIDAS;

## 1 Introduction

Digitalization is key and the topic of our age. Politics, business, and society have recognised digitalization as one of the central tasks for Europe. This includes the transformation of all related services. Especially the COVID-19 pandemic is seen as an additional and major driver for digital transformation of our society. The transformation includes both the transition of currently paper-based services in "e-services", as well as the related business processes. The latter usually presents the greater challenge. The legal framework for this is the SDGR. It will have a decisive influence on the information exchange of the several hundred administrative services covered by it. The SDGR is intended to pave the way for comprehensive information, online administrative procedures, and services. A key point here is also the "once-only principle" (OOP). The OOP requires a technical system for cross-border automated exchange of evidence and application (Art. 14 SDGR). The implementation of the SDGR entails great demands and challenges, as well as opportunities.

This paper sheds light on distinct examples within the current landscape of activities, in

---

<sup>1</sup> Tallinn University of Technology (TalTech), Ragnar Nurkse Department of Innovation and Governance, Akadeemia tee 3, 12618 Tallinn, Estonia, carsten.schmidt@taltech.ee, <https://orcid.org/0000-0001-8435-4313>

<sup>2</sup> University of Tartu, ERA-Chair, Johan Skytte Institute for Political Studies Center for IT Impact Studies, Lossi 36, 51003 Tartu, Estonia, robert.krimmer@ut.ee, <https://orcid.org/0000-0002-0873-539X>

<sup>3</sup> Danube University Krems, Department for E-Governance and Administration, Dr.-Karl-Dorrek-Straße 30, 3500 Krems, Österreich, thomas.lampoltshammer@donau-uni.ac.at, <https://orcid.org/0000-0002-1122-6908>



particular towards SDGR and OOP, with a special focus on eID and its role in establishing a European, cross-border public service infrastructure, i.e., the Digital Single Market (DSM). The remainder of this paper is structured as follows: in Section 2, we provide a background overview of SDGR, OOP, as well as two associated project initiatives for their realisation. In Section 3, we discuss challenges concerning eIDAS/eIDAS II, technical interoperability, as well as the impact of mobile approaches to the domain of eID. In Section 4, we close the paper with our conclusions and final remarks.

## 2 Background

### 2.1 SDGR

The origin of the proposal for a single digital gateway (SDG) is based on the urgent need for a more coherent, streamlined approach in Europe. This was flagged by several business organisations, the European Parliament, 17 Member States (MS) and via the platform of the regulatory fitness and performance programme (REFIT) of the EC. Besides that, by public consultation on EU citizenship, 80 % of the citizens stated out that the repetition of provision of personal data on the one side and the unavailability of them on the other side is the biggest hurdle in cross-border cases [EC17].

For a presentation to the European Parliament, the EC has investigated the gaps in digitisation of 13 key procedures (see Fig. 1) [EP17]. These key procedures are related to different areas like, e.g., working or studying abroad and setting up a business in another MS or associated country [EC17]. The purpose of the SDG is to offer EU citizens and businesses easy and non-discriminatory online access to information about EU and national rules, national procedures for compliance with these rules and EU and national assistance services, in order to help them in exercising their rights of the DSM.

### 2.2 TOOP

“The Once-Only Principle project” (TOOP)<sup>4</sup> is the first large-scale pilot (LSP) project under the Horizon 2020 Framework Programme of the EU. The TOOP project was launched on 1 Jan 2017 as an initiative of more than 50 organisations from 20 EU MS and associated countries. The main objective of TOOP is to explore and demonstrate the once-only principle across borders, to support the SDGR transition, focusing on data from businesses via three distinct pilots [LHP19], updating business register data in a cross-border context; cross-border e-services, in particular tenders; online ship and crew certificates, to enable better exchange of business-related data or documents with and between public administrations and reduce administrative burden for both businesses and public administrations. It identified various barriers (such as data protection and data-sharing requirements, implementation costs, public sector silo issues, and especially legal barriers and/or gaps) that could hinder the implementation [K17].

TOOP is using a federated IT architecture on a cross-border, pan-European scale. The

---

<sup>4</sup> <https://toop.eu/>

architecture is not built from scratch but re-uses and enhances already available building blocks in order to seamlessly preserve interoperability and to comply with regulations and existing technical standards (i.e., ISA<sup>2</sup>) [T20], [KS19]. If possible, the technical building blocks provided by the Connecting Europe Facility (CEF) (e.g., e-Delivery) are reused, amendments and additional technical solutions developed by TOOP complying with international standards set by standardisation organisations like, e.g., ETSI<sup>5</sup> or OASIS<sup>6</sup>.

### **2.3 mGov4EU**

The mobile Cross-Border Government Services for Europe (mGov4EU) began on 1 Jan 2021. Starting from the foundation of SDGR, mGov4EU provides new ways of cross-border service provision correlated and interlinked with eIDAS Regulation on cross-border identification and authentication. mGov4EU leverages for the first time both together, SDGR and eIDAS for mobile-device usage.

The project builds upon the existing eIDAS-Layer and combines it with user-centric mobile-based authentication, including a Single Sign-On (SSO) approach. At the same time, a privacy-preserving identity and consent management is established for the provision of cross-border application scenarios concerning E-Government processes and services. In addition, mGov4EU embraces the SDG-Layer, striving for a collaborative engagement with provisioning platforms concerning the delivery and re-use of digital services throughout Europe, while holding up the key elements of trust and accessibility. The therefore developed technical infrastructure will be piloted in three domains, i.e., electronic voting, smart mobility, and mobile signature.

## **3 Discussion**

The before-mentioned development concerning SDGR, the DSM, as well as the two example initiatives (TOOP, mGov4EU) have clearly demonstrated that interoperability is key for a beneficial data exchange across borders. Interoperability has to be seen from different points of view. Within this section, we focus mainly on organisational, legal, and technical interoperability based on the outcomes of the ISA<sup>2</sup> Program of the EC. In addition, we also provide an outlook towards a key challenge, namely, the paradigm shifts of mobile-first approaches within the eID context.

### **3.1 eIDAS / eIDAS II – Organisational and Legal Issues**

First, we are looking to the eIDAS regulation. The setup of the regulation was a big step forward on the way to create a common legal basis for the EU. But since the entry into force of the eIDAS in 2018, the implementation of digital identity is recognised as not harmonized across the MS. This is mainly caused by different interpretations of the regulation. Even Trust Services Providers, who are eIDAS compliant, have the procedures and requirements defined in different ways. The result is that the eIDAS

---

<sup>5</sup> European Telecommunications Standards Institute (ETSI)

<sup>6</sup> Organization for the Advancement of Structured Information Standards (OASIS)

certificates are not compatible across different MS. In order to change this fragmented state, there are mainly two options; a change of mindset and / or a change of technical implementation to accept all eIDAS qualified tools (e.g., certificates, signatures etc.)

Furthermore, as cross-border transactions and the digital economy continue to grow, and economic crimes and fraud become more sophisticated, the importance of accurately identifying and verifying counterparties - including business partners - is becoming more evident. Policies and procedures to prevent money-laundering and terrorist financing, as dictated by EU so-called Anti Money-Laundering (AML) Directives entails credit and financial institutions and other “obliged entities” to determine the true identity of a customer and the type of activity that is “normal and expected” (Know Your Customer).

**3.2 Technical Interoperability Issues**

The databases used by the different administrations in the MS are mostly designed for specific cases or services. The underlying structure of the register quite often are set up before generic rules to exchange eIDs like in the eIDAS regulation were established. The data schemes are strongly related to the provided services. This causes a gap of attributes that allows an automated exchange of and mapping of identities (identity matching issue).

Identification in Europe happens via eIDs notified under eIDAS. In this case, there is a record matching issue depending on MS infrastructure. While using notified eIDs under the eIDAS Regulation for the most part will allow data providers to match an identity with a record (evidence requested) using the attributes of the natural person provided by the eIDAS minimum data set, in some cases additional attributes are needed to ensure a match. This is based on a lack of interoperability and the credentials defined in the eID schemes of the MS (record matching issue).

The lack of a match with the regulated electronic identity circuits falls under the national sovereignty, and the consequent lack of a sound legal basis. The EC, the MS and associated countries have picked up this via the SDGR Coordination Group.

**3.3 eID and Mobile Usage**

Research has shown that user acceptance can lead to a better technological development, as well as value creation within the domain of e-government services, especially considering mobile government (m-government) [HCK13]. In this context, the combination of mobile aspects and approaches, e.g., as suggested by the mGov4EU project, can boost the acceptance and thus the usage of critical components such as eID. Tesap et al., conducted a literature review concerning factors for public acceptance of eID [TPD19]. The identified 11 core categories and their associated impact (positive, negative, bilateral, or neutral). For the sake of discussion in this paper, we focus on the categories which have been found to have the most positive influence on the acceptance of eID and combine them with mobile aspects in table 1.

---

Category	Description	Mobile Aspect
----------	-------------	---------------

---

Ease of use	Convenience/usability /comfort when using eID technology	Provision of eID functionality without the necessity of an additional artefact, e.g., an eID card
Functionality	Availability of services to be used with eID	Full eID integration with mobile e-government apps
Awareness	Understanding/knowing how to use of the provided eID solution	Know-how and experience concerning mobile phone handling is transferred to eID solutions
Trust	Institution-based trust/characteristics trust concerning the provision of eID solutions	Trust in other widely used mobile applications (e.g., banking apps) can be leveraged for eID solutions
Control and Empowerment	Control over eIdentity/Identity and empowerment of citizens	Mobile eID solutions can provide this control and empowerment anytime and everywhere

Tab. 1: Positive influential factors for eID acceptance, complemented with mobile aspects

When studying the above side-by-side comparison, it becomes obvious that eID solutions profit the most from spill-over effects of positive experience of citizens in their daily use of mobile phones. The better the eID solutions are integrated in day-to-day business and activities around the life-situations of the citizens, the higher are the changes that these provided solutions are accepted; and this is the key to a true cross-border, pan European public service provision.

## 4 Conclusions

To solve the issues related to the described problems of identity matching mostly on the data provider side and record matching mainly on the data consumer side a further alignment of the schemes and attributes in use are necessary. It is important to find solutions that covers the needs on national and international level at the same time. Therefore, a European initiative is the most valuable approach. The recommendation is to pick up the outcomes of the ongoing discussions around the implementation of the SDGR in the Members States, associated countries and the European level and feed them into the update of the eIDAS regulation. The preparation of the amendment of the eIDAS regulation is a great opportunity from a legal and technical point of view. Ideally this should be aligned with the initiative of the EC to implement a secure European electronic identity. The combination of all these activities would allow a new level of harmonisation in the field of e-Identity in Europe that can initiate a bust in using the eID on a daily basis as this can be recognised already in some of the Members States, as described before.

As solution could be the introduction of state-of-the-art mobile technologies that are supported by the implementation of sound mobile government solutions and a transition of regular (paper based) governmental services into smart government services.

## 5 Acknowledgement

This work received funding in the context of the EU H2020 projects eCEPS and mGov4EU under grant agreements 959072 & 857622.

## Bibliography

- [K17] Krimmer, R. et al.: Exploring and Demonstrating the Once-Only Principle. In (Hinnant, C. C.; Ojo, A. Eds.): Proceedings of the 18th Annual International DGO. ACM, New York, NY, USA, 06072017; pp. 546–551.
- [T20] Tepandi, J. et al.: Towards a Cross-Border Reference Architecture for the Once-Only Principle in Europe: An Enterprise Modelling Approach. In (Gordijn, J.; Guédria, W.; Proper, H. A. Eds.): 12th ifip working conference, poem 2019. SPRINGER NATURE, 2020; pp. 103 – 117.
- [KS19] Krimmer, R.; Schmidt, C.: Chancen und Anforderungen des Single Digital Gateways. In Innovative Verwaltung, 2019, 41; pp. 10–14.
- [LHP19] Lampoltshammer, T. J., John, K., Helger, P., & Piswanger, C. M. (2019). Connectathons-A Sustainable Path Towards Development in European Large-Scale Pilots. EGOV-CeDEM-ePart 2019, 207.
- [HCK13] Hung, S. Y., Chang, C. M., & Kuo, S. R. (2013). User acceptance of mobile e-government services: An empirical study. GIQ, 30(1), 33-44.
- [TPD19] Tsap, V.; Pappel, I.; Draheim, D.: Factors Affecting e-ID Public Acceptance: A Literature Review. In (Kő, A. et al. Eds.): Electronic Government and the Information Systems Perspective. Springer, Cham, 2019; pp. 176–188.
- [EC16] EC: EU eGovernment Action Plan 2016–2020 - Accelerating the Digital Transformation of Government. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2016, no. 179, pp. 1–11, 2016.
- [EP17] European Parliament: Commissioner Bieńkowska and MEPs debate the merits of the single digital gateway, 2017.
- [EC17] European Commission: The Single Digital Gateway. A proposal for easy, online navigation of the Single Market for EU citizens and businesses. <https://www.europarl.europa.eu/cmsdata/129820/PPT%20single%20digital%20gateway.pdf>, accessed 1 Mar 2021.

## *GI-Edition Lecture Notes in Informatics*

- P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.
- P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.
- P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Language to Information Systems, NLDB'2001.
- P-4 H. Wörn, J. Mühlhng, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensor-gestützte Chirurgie; Workshop des SFB 414.
- P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.
- P-6 Hans-Jürgen Appelpath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.
- P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.
- P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.
- P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.
- P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.
- P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.
- P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.
- P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni\_ (Hrsg.): The Changing Universities – The Role of Technology.
- P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.
- P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.
- P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.
- P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.
- P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.
- P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund.
- P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund (Ergänzungs-band).
- P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.
- P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.
- P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit
- P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen
- P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003
- P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web
- P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin
- P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Erfahrungen und Visionen
- P-29 Antje Dusterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems
- P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications
- P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures, Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 24. July 2003 in Darmstadt, Germany

- P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003
- P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft
- P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenber, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)
- P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenber, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)
- P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenber (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik
- P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik
- P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003
- P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003
- P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004
- P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing
- P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste
- P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistence, Scalability, Transactions – Database Mechanisms for Mobile Applications
- P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning, E-Services
- P-45 Bernhard Rumpe, Wolfgang Hesse (Hrsg.): Modellierung 2004
- P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment
- P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society
- P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications
- P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven
- P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm
- P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm
- P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik
- P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004
- P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration
- P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Ad-hoc-Netze Medienintegration
- P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government
- P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen
- P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality
- P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Rannenber, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments
- P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für informatische Bildung
- P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen
- P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit
- P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and its Applications

- P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005
- P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolfrid Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web
- P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik
- P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)
- P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)
- P-69 Robert Hirschfeld, Ryszard Kowalczyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005
- P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)
- P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005
- P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment
- P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): "Heute schon das Morgen sehen"
- P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology
- P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture
- P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz
- P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006
- P-78 K.-O. Wenkel, P. Wagner, M. Morgens-tern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel
- P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006
- P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce
- P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS'06
- P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006
- P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics
- P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications
- P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems
- P-86 Robert Krimmer (Ed.): Electronic Voting 2006
- P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik
- P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006
- P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur
- P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006
- P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006
- P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1
- P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2
- P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen
- P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies
- P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006



- P-98 Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices
- P-99 Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik
- P-100 Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik
- P-101 Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten
- P-102 Otto Spaniol (Eds.): Mobile Services and Personalized Environments
- P-103 Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)
- P-104 Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.) MMS 2007: Mobilität und mobile Informationssysteme
- P-105 Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.) Software Engineering 2007
- P-106 Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.) Software Engineering 2007 – Beiträge zu den Workshops
- P-107 Heinrich C. Mayr, Dimitris Karagiannis (eds.) Information Systems Technology and its Applications
- P-108 Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.) BIOSIG 2007: Biometrics and Electronic Signatures
- P-109 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 1
- P-110 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 2
- P-111 Christian Eibl, Johannes Magenheimer, Sigrid Schubert, Martin Wessner (Hrsg.) DeLFI 2007: 5. e-Learning Fachtagung Informatik
- P-112 Sigrid Schubert (Hrsg.) Didaktik der Informatik in Theorie und Praxis
- P-113 Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.) The Social Semantic Web 2007 Proceedings of the 1<sup>st</sup> Conference on Social Semantic Web (CSSW)
- P-114 Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.) IMF2007 IT-incident management & IT-forensics Proceedings of the 3<sup>rd</sup> International Conference on IT-Incident Management & IT-Forensics
- P-115 Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walthert (Eds.) German conference on bioinformatics GCB 2007
- P-116 Witold Abramowicz, Leszek Maciszek (Eds.) Business Process and Services Computing 1<sup>st</sup> International Working Conference on Business Process and Services Computing BPSC 2007
- P-117 Ryszard Kowalczyk (Ed.) Grid service engineering and management The 4<sup>th</sup> International Conference on Grid Service Engineering and Management GSEM 2007
- P-118 Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.) European Conference on ehealth 2007
- P-119 Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.) Enterprise Modelling and Information Systems Architectures Concepts and Applications
- P-120 Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa, Leandro Soares Indrusiak (Eds.) Coordination of Collaborative Engineering - State of the Art and Future Challenges
- P-121 Korbinian Herrmann, Bernd Bruegge (Hrsg.) Software Engineering 2008 Fachtagung des GI-Fachbereichs Softwaretechnik
- P-122 Walid Maalej, Bernd Bruegge (Hrsg.) Software Engineering 2008 - Workshopband Fachtagung des GI-Fachbereichs Softwaretechnik

- P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)  
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit  
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008)
- P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)  
9<sup>th</sup> Workshop on Parallel Systems and Algorithms (PASA)  
Workshop of the GI/ITG Special Interest Groups PARS and PARVA
- P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)  
Unternehmens-IT: Führungsinstrument oder Verwaltungsbürde  
Referate der 28. GIL Jahrestagung
- P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)  
10<sup>th</sup> Workshop Software Reengineering (WSR 2008)
- P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)  
Modellierung 2008
- P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)  
Sicherheit 2008  
Sicherheit, Schutz und Zuverlässigkeit  
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)  
2.-4. April 2008  
Saarbrücken, Germany
- P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)  
Sigsand-Europe 2008  
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems
- P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)  
1. DFN-Forum Kommunikationstechnologien Beiträge der Fachtagung
- P-131 Robert Krimmer, Rüdiger Grimm (Eds.)  
3<sup>rd</sup> International Conference on Electronic Voting 2008  
Co-organized by Council of Europe, Gesellschaft für Informatik und E-Voting, CC
- P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)  
DeLFI 2008:  
Die 6. e-Learning Fachtagung Informatik
- P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)  
INFORMATIK 2008  
Beherrschbare Systeme – dank Informatik Band 1
- P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)  
INFORMATIK 2008  
Beherrschbare Systeme – dank Informatik Band 2
- P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)  
Didaktik der Informatik – Aktuelle Forschungsergebnisse
- P-136 Andreas Beyer, Michael Schroeder (Eds.)  
German Conference on Bioinformatics GCB 2008
- P-137 Arslan Brömme, Christoph Busch, Detlef Hühlein (Eds.)  
BIOSIG 2008: Biometrics and Electronic Signatures
- P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)  
Synergien durch Integration und Informationslogistik  
Proceedings zur DW2008
- P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)  
Industrialisierung des Software-Managements  
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschaftsinformatik
- P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)  
IMF 2008 - IT Incident Management & IT Forensics
- P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)  
Modellierung betrieblicher Informationssysteme (MobIS 2008)  
Modellierung zwischen SOA und Compliance Management
- P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)  
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung
- P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)  
Software Engineering 2009  
Fachtagung des GI-Fachbereichs Softwaretechnik

- P-144 Johann-Christoph Freytag, Thomas Ruf, Wolfgang Lehner, Gottfried Vossen (Hrsg.)  
Datenbanksysteme in Business, Technologie und Web (BTW)
- P-145 Knut Hinkelmann, Holger Wache (Eds.)  
WM2009: 5th Conference on Professional Knowledge Management
- P-146 Markus Bick, Martin Breunig, Hagen Höpfner (Hrsg.)  
Mobile und Ubiquitäre Informationssysteme – Entwicklung, Implementierung und Anwendung  
4. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2009)
- P-147 Witold Abramowicz, Leszek Maciaszek, Ryszard Kowalczyk, Andreas Speck (Eds.)  
Business Process, Services Computing and Intelligent Service Management  
BPSC 2009 · ISM 2009 · YRW-MBP 2009
- P-148 Christian Erfurth, Gerald Eichler, Volkmar Schau (Eds.)  
9<sup>th</sup> International Conference on Innovative Internet Community Systems  
I<sup>2</sup>CS 2009
- P-149 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)  
2. DFN-Forum  
Kommunikationstechnologien  
Beiträge der Fachtagung
- P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)  
Software Engineering  
2009 - Workshopband
- P-151 Armin Heinzl, Peter Dadam, Stefan Kirm, Peter Lockemann (Eds.)  
PRIMIUM  
Process Innovation for Enterprise Software
- P-152 Jan Mendling, Stefanie Rinderle-Ma, Werner Esswein (Eds.)  
Enterprise Modelling and Information Systems Architectures  
Proceedings of the 3<sup>rd</sup> Int'l Workshop EMISA 2009
- P-153 Andreas Schwill, Nicolas Apostolopoulos (Hrsg.)  
Lernen im Digitalen Zeitalter  
DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik
- P-154 Stefan Fischer, Erik Maehle, Rüdiger Reischuk (Hrsg.)  
INFORMATIK 2009  
Im Focus das Leben
- P-155 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)  
BIOSIG 2009:  
Biometrics and Electronic Signatures  
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures
- P-156 Bernhard Koerber (Hrsg.)  
Zukunft braucht Herkunft  
25 Jahre »INFOS – Informatik und Schule«
- P-157 Ivo Grosse, Steffen Neumann, Stefan Posch, Falk Schreiber, Peter Stadler (Eds.)  
German Conference on Bioinformatics 2009
- P-158 W. Claudepein, L. Theuvsen, A. Kämpf, M. Morgenstern (Hrsg.)  
Precision Agriculture  
Reloaded – Informationsgestützte Landwirtschaft
- P-159 Gregor Engels, Markus Luckey, Wilhelm Schäfer (Hrsg.)  
Software Engineering 2010
- P-160 Gregor Engels, Markus Luckey, Alexander Pretschner, Ralf Reussner (Hrsg.)  
Software Engineering 2010 –  
Workshopband  
(inkl. Doktorandensymposium)
- P-161 Gregor Engels, Dimitris Karagiannis, Heinrich C. Mayr (Hrsg.)  
Modellierung 2010
- P-162 Maria A. Wimmer, Uwe Brinkhoff, Siegfried Kaiser, Dagmar Lück-Schneider, Erich Schweighofer, Andreas Wiebe (Hrsg.)  
Vernetzte IT für einen effektiven Staat  
Gemeinsame Fachtagung  
Verwaltungsinformatik (FTVI) und  
Fachtagung Rechtsinformatik (FTRI) 2010
- P-163 Markus Bick, Stefan Eulgem, Elgar Fleisch, J. Felix Hampe, Birgitta König-Ries, Franz Lehner, Key Pousttchi, Kai Rannenberg (Hrsg.)  
Mobile und Ubiquitäre Informationssysteme  
Technologien, Anwendungen und Dienste zur Unterstützung von mobiler  
Kollaboration
- P-164 Arslan Brömme, Christoph Busch (Eds.)  
BIOSIG 2010: Biometrics and Electronic Signatures  
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

- P-165 Gerald Eichler, Peter Kropf, Ulrike Lechner, Phayung Meesad, Herwig Unger (Eds.)  
10<sup>th</sup> International Conference on Innovative Internet Community Systems (I<sup>2</sup>CS) – Jubilee Edition 2010 –
- P-166 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)  
3. DFN-Forum Kommunikationstechnologien Beiträge der Fachtagung
- P-167 Robert Krimmer, Rüdiger Grimm (Eds.)  
4<sup>th</sup> International Conference on Electronic Voting 2010  
co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC
- P-168 Ira Diethelm, Christina Dörge, Claudia Hildebrandt, Carsten Schulte (Hrsg.)  
Didaktik der Informatik  
Möglichkeiten empirischer Forschungsmethoden und Perspektiven der Fachdidaktik
- P-169 Michael Kerres, Nadine Ojstersek Ulrik Schroeder, Ulrich Hoppe (Hrsg.)  
DeLFI 2010 - 8. Tagung der Fachgruppe E-Learning der Gesellschaft für Informatik e.V.
- P-170 Felix C. Freiling (Hrsg.)  
Sicherheit 2010  
Sicherheit, Schutz und Zuverlässigkeit
- P-171 Werner Esswein, Klaus Turowski, Martin Juhrisch (Hrsg.)  
Modellierung betrieblicher Informationssysteme (MobIS 2010)  
Modellgestütztes Management
- P-172 Stefan Klink, Agnes Koschmider Marco Mevius, Andreas Oberweis (Hrsg.)  
EMISA 2010  
Einflussfaktoren auf die Entwicklung flexibler, integrierter Informationssysteme  
Beiträge des Workshops der GI-Fachgruppe EMISA (Entwicklungsmethoden für Informationssysteme und deren Anwendung)
- P-173 Dietmar Schomburg, Andreas Grote (Eds.)  
German Conference on Bioinformatics 2010
- P-174 Arslan Brömme, Torsten Eymann, Detlef Hühnlein, Heiko Roßnagel, Paul Schmücker (Hrsg.)  
perspeGktive 2010  
Workshop „Innovative und sichere Informationstechnologie für das Gesundheitswesen von morgen“
- P-175 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)  
INFORMATIK 2010  
Service Science – Neue Perspektiven für die Informatik  
Band 1
- P-176 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)  
INFORMATIK 2010  
Service Science – Neue Perspektiven für die Informatik  
Band 2
- P-177 Witold Abramowicz, Rainer Alt, Klaus-Peter Fähnrich, Bogdan Franczyk, Leszek A. Maciaszek (Eds.)  
INFORMATIK 2010  
Business Process and Service Science – Proceedings of ISSS and BPSC
- P-178 Wolfram Pietsch, Benedikt Krams (Hrsg.)  
Vom Projekt zum Produkt  
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschafts-informatik (WI-MAW), Aachen, 2010
- P-179 Stefan Gruner, Bernhard Rumpe (Eds.)  
FM+AM'2010  
Second International Workshop on Formal Methods and Agile Methods
- P-180 Theo Härder, Wolfgang Lehner, Bernhard Mitschang, Harald Schöning, Holger Schwarz (Hrsg.)  
Datenbanksysteme für Business, Technologie und Web (BTW) 14. Fachtagung des GI-Fachbereichs „Datenbanken und Informationssysteme“ (DBIS)
- P-181 Michael Clasen, Otto Schätzel, Brigitte Theuvsen (Hrsg.)  
Qualität und Effizienz durch informationsgestützte Landwirtschaft, Fokus: Moderne Weinwirtschaft
- P-182 Ronald Maier (Hrsg.)  
6<sup>th</sup> Conference on Professional Knowledge Management  
From Knowledge to Action
- P-183 Ralf Reussner, Matthias Grund, Andreas Oberweis, Walter Tichy (Hrsg.)  
Software Engineering 2011  
Fachtagung des GI-Fachbereichs Softwaretechnik
- P-184 Ralf Reussner, Alexander Pretschner, Stefan Jähnichen (Hrsg.)  
Software Engineering 2011  
Workshopband  
(inkl. Doktorandensymposium)

- P-185 Hagen Höpfner, Günther Specht, Thomas Ritz, Christian Bunse (Hrsg.)  
MMS 2011: Mobile und ubiquitäre Informationssysteme Proceedings zur 6. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2011)
- P-186 Gerald Eichler, Axel Küpper, Volkmar Schau, Hacène Fouchal, Herwig Unger (Eds.)  
11<sup>th</sup> International Conference on Innovative Internet Community Systems (I<sup>2</sup>CS)
- P-187 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)  
4. DFN-Forum Kommunikationstechnologien, Beiträge der Fachtagung 20. Juni bis 21. Juni 2011 Bonn
- P-188 Holger Rohland, Andrea Kienle, Steffen Friedrich (Hrsg.)  
DeLFI 2011 – Die 9. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. 5.–8. September 2011, Dresden
- P-189 Thomas, Marco (Hrsg.)  
Informatik in Bildung und Beruf INFOS 2011  
14. GI-Fachtagung Informatik und Schule
- P-190 Markus Nüttgens, Oliver Thomas, Barbara Weber (Eds.)  
Enterprise Modelling and Information Systems Architectures (EMISA 2011)
- P-191 Arslan Brömme, Christoph Busch (Eds.)  
BIOSIG 2011  
International Conference of the Biometrics Special Interest Group
- P-192 Hans-Ulrich Heiß, Peter Pepper, Holger Schlingloff, Jörg Schneider (Hrsg.)  
INFORMATIK 2011  
Informatik schafft Communities
- P-193 Wolfgang Lehner, Gunther Piller (Hrsg.)  
IMDM 2011
- P-194 M. Clasen, G. Fröhlich, H. Bernhardt, K. Hildebrand, B. Theuvsen (Hrsg.)  
Informationstechnologie für eine nachhaltige Landwirtschaft Fokus Forstwirtschaft
- P-195 Neeraj Suri, Michael Waidner (Hrsg.)  
Sicherheit 2012  
Sicherheit, Schutz und Zuverlässigkeit Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
- P-196 Arslan Brömme, Christoph Busch (Eds.)  
BIOSIG 2012  
Proceedings of the 11<sup>th</sup> International Conference of the Biometrics Special Interest Group
- P-197 Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser, Erich Schweighofer, Maria A. Wimmer (Hrsg.)  
Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012
- P-198 Stefan Jähnichen, Axel Küpper, Sahin Albayrak (Hrsg.)  
Software Engineering 2012  
Fachtagung des GI-Fachbereichs Softwaretechnik
- P-199 Stefan Jähnichen, Bernhard Rumpe, Holger Schlingloff (Hrsg.)  
Software Engineering 2012  
Workshopband
- P-200 Gero Mühl, Jan Richling, Andreas Herkersdorf (Hrsg.)  
ARCS 2012 Workshops
- P-201 Elmar J. Sinz Andy Schürr (Hrsg.)  
Modellierung 2012
- P-202 Andrea Back, Markus Bick, Martin Breunig, Key Pousttchi, Frédéric Thiesse (Hrsg.)  
MMS 2012: Mobile und Ubiquitäre Informationssysteme
- P-203 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)  
5. DFN-Forum Kommunikationstechnologien  
Beiträge der Fachtagung
- P-204 Gerald Eichler, Leendert W. M. Wienhofen, Anders Kofod-Petersen, Herwig Unger (Eds.)  
12<sup>th</sup> International Conference on Innovative Internet Community Systems (I<sup>2</sup>CS 2012)
- P-205 Manuel J. Kripp, Melanie Volkamer, Rüdiger Grimm (Eds.)  
5<sup>th</sup> International Conference on Electronic Voting 2012 (EVOTE2012)  
Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC
- P-206 Stefanie Rinderle-Ma, Mathias Weske (Hrsg.)  
EMISA 2012  
Der Mensch im Zentrum der Modellierung
- P-207 Jörg Desel, Jörg M. Haake, Christian Spannagel (Hrsg.)  
DeLFI 2012: Die 10. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V.  
24.–26. September 2012

- P-208 Ursula Goltz, Marcus Magnor, Hans-Jürgen Appelrath, Herbert Matthies, Wolf-Tilo Balke, Lars Wolf (Hrsg.)  
INFORMATIK 2012
- P-209 Hans Brandt-Pook, André Fleer, Thorsten Spitta, Malte Wattenberg (Hrsg.)  
Nachhaltiges Software Management
- P-210 Erhard Plödereder, Peter Dencker, Herbert Klenk, Hubert B. Keller, Silke Spitzer (Hrsg.)  
Automotive – Safety & Security 2012  
Sicherheit und Zuverlässigkeit für automobile Informationstechnik
- P-211 M. Clasen, K. C. Kersebaum, A. Meyer-Aurich, B. Theuvsen (Hrsg.)  
Massendatenmanagement in der Agrar- und Ernährungswirtschaft  
Erhebung - Verarbeitung - Nutzung  
Referate der 33. GIL-Jahrestagung 20. – 21. Februar 2013, Potsdam
- P-212 Arslan Brömme, Christoph Busch (Eds.)  
BIOSIG 2013  
Proceedings of the 12th International Conference of the Biometrics Special Interest Group  
04.–06. September 2013  
Darmstadt, Germany
- P-213 Stefan Kowalewski, Bernhard Rumpe (Hrsg.)  
Software Engineering 2013  
Fachtagung des GI-Fachbereichs Softwaretechnik
- P-214 Volker Markl, Gunter Saake, Kai-Uwe Sattler, Gregor Hackenbroich, Bernhard Mitschang, Theo Härder, Veit Köppen (Hrsg.)  
Datenbanksysteme für Business, Technologie und Web (BTW) 2013  
13. – 15. März 2013, Magdeburg
- P-215 Stefan Wagner, Horst Lichter (Hrsg.)  
Software Engineering 2013  
Workshopband  
(inkl. Doktorandensymposium)  
26. Februar – 1. März 2013, Aachen
- P-216 Gunter Saake, Andreas Henrich, Wolfgang Lehner, Thomas Neumann, Veit Köppen (Hrsg.)  
Datenbanksysteme für Business, Technologie und Web (BTW) 2013 – Workshopband  
11. – 12. März 2013, Magdeburg
- P-217 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)  
6. DFN-Forum Kommunikationstechnologien  
Beiträge der Fachtagung  
03.–04. Juni 2013, Erlangen
- P-218 Andreas Breiter, Christoph Rensing (Hrsg.)  
DeLFI 2013: Die 11 e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. (GI)  
8. – 11. September 2013, Bremen
- P-219 Norbert Breier, Peer Stechert, Thomas Wilke (Hrsg.)  
Informatik erweitert Horizonte  
INFOS 2013  
15. GI-Fachtagung Informatik und Schule  
26. – 28. September 2013
- P-220 Matthias Horbach (Hrsg.)  
INFORMATIK 2013  
Informatik angepasst an Mensch, Organisation und Umwelt  
16. – 20. September 2013, Koblenz
- P-221 Maria A. Wimmer, Marijn Janssen, Ann Macintosh, Hans Jochen Scholl, Efthimos Tambouris (Eds.)  
Electronic Government and Electronic Participation  
Joint Proceedings of Ongoing Research of IFIP EGOV and IFIP ePart 2013  
16. – 19. September 2013, Koblenz
- P-222 Reinhard Jung, Manfred Reichert (Eds.)  
Enterprise Modelling and Information Systems Architectures (EMISA 2013)  
St. Gallen, Switzerland  
September 5. – 6. 2013
- P-223 Detlef Hühnlein, Heiko Roßnagel (Hrsg.)  
Open Identity Summit 2013  
10. – 11. September 2013  
Kloster Banz, Germany
- P-224 Eckhart Hanser, Martin Mikusz, Masud Fazal-Baqaie (Hrsg.)  
Vorgehensmodelle 2013  
Vorgehensmodelle – Anspruch und Wirklichkeit  
20. Tagung der Fachgruppe Vorgehensmodelle im Fachgebiet Wirtschaftsinformatik (WI-VM) der Gesellschaft für Informatik e.V.  
Lörrach, 2013
- P-225 Hans-Georg Fill, Dimitris Karagiannis, Ulrich Reimer (Hrsg.)  
Modellierung 2014  
19. – 21. März 2014, Wien
- P-226 M. Clasen, M. Hamer, S. Lehnert, B. Petersen, B. Theuvsen (Hrsg.)  
IT-Standards in der Agrar- und Ernährungswirtschaft Fokus: Risiko- und Krisenmanagement  
Referate der 34. GIL-Jahrestagung  
24. – 25. Februar 2014, Bonn

- P-227 Wilhelm Hasselbring,  
Nils Christian Ehmke (Hrsg.)  
Software Engineering 2014  
Fachtagung des GI-Fachbereichs  
Softwaretechnik  
25. – 28. Februar 2014  
Kiel, Deutschland
- P-228 Stefan Katzenbeisser, Volkmar Lotz,  
Edgar Weippl (Hrsg.)  
Sicherheit 2014  
Sicherheit, Schutz und Zuverlässigkeit  
Beiträge der 7. Jahrestagung des  
Fachbereichs Sicherheit der  
Gesellschaft für Informatik e.V. (GI)  
19. – 21. März 2014, Wien
- P-229 Dagmar Lück-Schneider, Thomas  
Gordon, Siegfried Kaiser, Jörn von  
Lucke, Erich Schweighofer, Maria  
A. Wimmer, Martin G. Löhle (Hrsg.)  
Gemeinsam Electronic Government  
ziel(gruppen)gerecht gestalten und  
organisieren  
Gemeinsame Fachtagung  
Verwaltungsinformatik (FTVI) und  
Fachtagung Rechtsinformatik (FTRI)  
2014, 20.-21. März 2014 in Berlin
- P-230 Arslan Brömme, Christoph Busch (Eds.)  
BIOSIG 2014  
Proceedings of the 13<sup>th</sup> International  
Conference of the Biometrics Special  
Interest Group  
10. – 12. September 2014 in  
Darmstadt, Germany
- P-231 Paul Müller, Bernhard Neumair,  
Helmut Reiser, Gabi Dreo Rodosek  
(Hrsg.)  
7. DFN-Forum  
Kommunikationstechnologien  
16. – 17. Juni 2014  
Fulda
- P-232 E. Plödereder, L. Grunske, E. Schneider,  
D. Ull (Hrsg.)  
INFORMATIK 2014  
Big Data – Komplexität meistern  
22. – 26. September 2014  
Stuttgart
- P-233 Stephan Trahasch, Rolf Plötzner, Gerhard  
Schneider, Claudia Gayer, Daniel Sassiati,  
Nicole Wöhrle (Hrsg.)  
DeLFI 2014 – Die 12. e-Learning  
Fachtagung Informatik  
der Gesellschaft für Informatik e.V.  
15. – 17. September 2014  
Freiburg
- P-234 Fernand Feltz, Bela Mutschler, Benoît  
Ottjacques (Eds.)  
Enterprise Modelling and Information  
Systems Architectures  
(EMISA 2014)  
Luxembourg, September 25-26, 2014
- P-235 Robert Giegerich,  
Ralf Hofestädt,  
Tim W. Nattkemper (Eds.)  
German Conference on  
Bioinformatics 2014  
September 28 – October 1  
Bielefeld, Germany
- P-236 Martin Engstler, Eckhart Hanser,  
Martin Mikusz, Georg Herzwurm (Hrsg.)  
Projektmanagement und  
Vorgehensmodelle 2014  
Soziale Aspekte und Standardisierung  
Gemeinsame Tagung der Fachgruppen  
Projektmanagement (WI-PM) und  
Vorgehensmodelle (WI-VM) im  
Fachgebiet Wirtschaftsinformatik der  
Gesellschaft für Informatik e.V., Stuttgart  
2014
- P-237 Detlef Hühnlein, Heiko Roßnagel (Hrsg.)  
Open Identity Summit 2014  
4.–6. November 2014  
Stuttgart, Germany
- P-238 Arno Ruckelshausen, Hans-Peter  
Schwarz, Brigitte Theuvsen (Hrsg.)  
Informatik in der Land-, Forst- und  
Ernährungswirtschaft  
Referate der 35. GIL-Jahrestagung  
23. – 24. Februar 2015, Geisenheim
- P-239 Uwe Aßmann, Birgit Demuth, Thorsten  
Spitta, Georg Püschel, Ronny Kaiser  
(Hrsg.)  
Software Engineering & Management  
2015  
17.-20. März 2015, Dresden
- P-240 Herbert Klenk, Hubert B. Keller, Erhard  
Plödereder, Peter Dencker (Hrsg.)  
Automotive – Safety & Security 2015  
Sicherheit und Zuverlässigkeit für  
automobile Informationstechnik  
21.–22. April 2015, Stuttgart
- P-241 Thomas Seidl, Norbert Ritter,  
Harald Schöning, Kai-Uwe Sattler,  
Theo Härder, Steffen Friedrich,  
Wolfram Wingerath (Hrsg.)  
Datenbanksysteme für Business,  
Technologie und Web (BTW 2015)  
04. – 06. März 2015, Hamburg

- P-242 Norbert Ritter, Andreas Henrich, Wolfgang Lehner, Andreas Thor, Steffen Friedrich, Wolfram Wingerath (Hrsg.)  
Datenbanksysteme für Business, Technologie und Web (BTW 2015) – Workshopband  
02. – 03. März 2015, Hamburg
- P-243 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)  
8. DFN-Forum  
Kommunikationstechnologien  
06.–09. Juni 2015, Lübeck
- P-244 Alfred Zimmermann, Alexander Rossmann (Eds.)  
Digital Enterprise Computing (DEC 2015)  
Böblingen, Germany June 25-26, 2015
- P-245 Arslan Brömme, Christoph Busch, Christian Rathgeb, Andreas Uhl (Eds.)  
BIOSIG 2015  
Proceedings of the 14th International Conference of the Biometrics Special Interest Group  
09.–11. September 2015  
Darmstadt, Germany
- P-246 Douglas W. Cunningham, Petra Hofstedt, Klaus Meer, Ingo Schmitt (Hrsg.)  
INFORMATIK 2015  
28.9.-2.10. 2015, Cottbus
- P-247 Hans Pongratz, Reinhard Keil (Hrsg.)  
DeLFI 2015 – Die 13. E-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. (GI)  
1.–4. September 2015  
München
- P-248 Jens Kolb, Henrik Leopold, Jan Mendling (Eds.)  
Enterprise Modelling and Information Systems Architectures  
Proceedings of the 6th Int. Workshop on Enterprise Modelling and Information Systems Architectures, Innsbruck, Austria  
September 3-4, 2015
- P-249 Jens Gallenbacher (Hrsg.)  
Informatik  
allgemeinbildend begreifen  
INFOS 2015 16. GI-Fachtagung  
Informatik und Schule  
20.–23. September 2015
- P-250 Martin Engstler, Masud Fazal-Baqaie, Eckhart Hanser, Martin Mikusz, Alexander Volland (Hrsg.)  
Projektmanagement und Vorgehensmodelle 2015  
Hybride Projektstrukturen erfolgreich umsetzen  
Gemeinsame Tagung der Fachgruppen Projektmanagement (WI-PM) und Vorgehensmodelle (WI-VM) im Fachgebiet Wirtschaftsinformatik der Gesellschaft für Informatik e.V., Elmshorn 2015
- P-251 Detlef Hühnlein, Heiko Roßnagel, Raik Kuhlisch, Jan Ziesing (Eds.)  
Open Identity Summit 2015  
10.–11. November 2015  
Berlin, Germany
- P-252 Jens Knoop, Uwe Zdun (Hrsg.)  
Software Engineering 2016  
Fachtagung des GI-Fachbereichs Softwaretechnik  
23.–26. Februar 2016, Wien
- P-253 A. Ruckelshausen, A. Meyer-Aurich, T. Rath, G. Recke, B. Theuvsen (Hrsg.)  
Informatik in der Land-, Forst- und Ernährungswirtschaft  
Fokus: Intelligente Systeme – Stand der Technik und neue Möglichkeiten  
Referate der 36. GIL-Jahrestagung  
22.-23. Februar 2016, Osnabrück
- P-254 Andreas Oberweis, Ralf Reussner (Hrsg.)  
Modellierung 2016  
2.–4. März 2016, Karlsruhe
- P-255 Stefanie Betz, Ulrich Reimer (Hrsg.)  
Modellierung 2016 Workshopband  
2.–4. März 2016, Karlsruhe
- P-256 Michael Meier, Delphine Reinhardt, Steffen Wendzel (Hrsg.)  
Sicherheit 2016  
Sicherheit, Schutz und Zuverlässigkeit  
Beiträge der 8. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)  
5.–7. April 2016, Bonn
- P-257 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)  
9. DFN-Forum  
Kommunikationstechnologien  
31. Mai – 01. Juni 2016, Rostock



- P-258 Dieter Hertweck, Christian Decker (Eds.)  
Digital Enterprise Computing (DEC 2016)  
14.–15. Juni 2016, Böblingen
- P-259 Heinrich C. Mayr, Martin Pinzger (Hrsg.)  
INFORMATIK 2016  
26.–30. September 2016, Klagenfurt
- P-260 Arslan Brömme, Christoph Busch,  
Christian Rathgeb, Andreas Uhl (Eds.)  
BIOSIG 2016  
Proceedings of the 15th International  
Conference of the Biometrics Special  
Interest Group  
21.–23. September 2016, Darmstadt
- P-261 Detlef Rätz, Michael Breidung, Dagmar  
Lück-Schneider, Siegfried Kaiser, Erich  
Schweighofer (Hrsg.)  
Digitale Transformation: Methoden,  
Kompetenzen und Technologien für die  
Verwaltung  
Gemeinsame Fachtagung  
Verwaltungsinformatik (FTVI) und  
Fachtagung Rechtsinformatik (FTRI) 2016  
22.–23. September 2016, Dresden
- P-262 Ulrike Lucke, Andreas Schwill,  
Raphael Zender (Hrsg.)  
DeLFI 2016 – Die 14. E-Learning  
Fachtagung Informatik  
der Gesellschaft für Informatik e.V. (GI)  
11.–14. September 2016, Potsdam
- P-263 Martin Engstler, Masud Fazal-Baqaie,  
Eckhart Hanser, Oliver Linssen, Martin  
Mikusz, Alexander Volland (Hrsg.)  
Projektmanagement und  
Vorgehensmodelle 2016  
Arbeiten in hybriden Projekten: Das  
Sowohl-als-auch von Stabilität und  
Dynamik  
Gemeinsame Tagung der Fachgruppen  
Projektmanagement (WI-PM) und  
Vorgehensmodelle (WI-VM) im  
Fachgebiet Wirtschaftsinformatik  
der Gesellschaft für Informatik e.V.,  
Paderborn 2016
- P-264 Detlef Hühnlein, Heiko Roßnagel,  
Christian H. Schunck, Maurizio Talamo  
(Eds.)  
Open Identity Summit 2016  
der Gesellschaft für Informatik e.V. (GI)  
13.–14. October 2016, Rome, Italy
- P-265 Bernhard Mitschang, Daniela  
Nicklas, Frank Leymann, Harald  
Schöning, Melanie Herschel, Jens  
Teubner, Theo Härder, Oliver Kopp,  
Matthias Wieland (Hrsg.)  
Datenbanksysteme für Business,  
Technologie und Web (BTW 2017)  
6.–10. März 2017, Stuttgart
- P-266 Bernhard Mitschang, Norbert Ritter,  
Holger Schwarz, Meike Klettke, Andreas  
Thor, Oliver Kopp, Matthias Wieland  
(Hrsg.)  
Datenbanksysteme für Business,  
Technologie und Web (BTW 2017)  
Workshopband  
6.–7. März 2017, Stuttgart
- P-267 Jan Jürjens, Kurt Schneider (Hrsg.)  
Software Engineering 2017  
21.–24. Februar 2017, Hannover
- P-268 A. Ruckelshausen, A. Meyer-Aurich,  
W. Lentz, B. Theuvsen (Hrsg.)  
Informatik in der Land-, Forst- und  
Ernährungswirtschaft  
Fokus: Digitale Transformation –  
Wege in eine zukunftsfähige  
Landwirtschaft  
Referate der 37. GIL-Jahrestagung  
06.–07. März 2017, Dresden
- P-269 Peter Dencker, Herbert Klenk, Hubert  
Keller, Erhard Plödereder (Hrsg.)  
Automotive – Safety & Security 2017  
30.–31. Mai 2017, Stuttgart
- P-270 Arslan Brömme, Christoph Busch,  
Antitzta Dantcheva, Christian Rathgeb,  
Andreas Uhl (Eds.)  
BIOSIG 2017  
20.–22. September 2017, Darmstadt
- P-271 Paul Müller, Bernhard Neumair, Helmut  
Reiser, Gabi Dreo Rodosek (Hrsg.)  
10. DFN-Forum Kommunikationstechnologien  
30. – 31. Mai 2017, Berlin
- P-272 Alexander Rossmann, Alfred  
Zimmermann (eds.)  
Digital Enterprise Computing  
(DEC 2017)  
11.–12. Juli 2017, Böblingen

- P-273 Christoph Igel, Carsten Ullrich, Martin Wessner (Hrsg.)  
BILDUNGSRÄUME  
DeLFI 2017  
Die 15. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. (GI)  
5. bis 8. September 2017, Chemnitz
- P-274 Ira Diethelm (Hrsg.)  
Informatische Bildung zum Verstehen und Gestalten der digitalen Welt  
13.–15. September 2017, Oldenburg
- P-275 Maximilian Eibl, Martin Gaedke (Hrsg.)  
INFORMATIK 2017  
25.–29. September 2017, Chemnitz
- P276 Alexander Volland, Martin Engstler, Masud Fazal-Baqaie, Eckhart Hanser, Oliver Linssen, Martin Mikusz (Hrsg.)  
Projektmanagement und Vorgehensmodelle 2017  
Die Spannung zwischen dem Prozess und den Menschen im Projekt  
Gemeinsame Tagung der Fachgruppen Projektmanagement und Vorgehensmodelle im Fachgebiet Wirtschaftsinformatik der Gesellschaft für Informatik e.V. in Kooperation mit der Fachgruppe IT-Projektmanagement der GPM e.V., Darmstadt 2017
- P-277 Lothar Fritsch, Heiko Roßnagel, Detlef Hühnlein (Hrsg.)  
Open Identity Summit 2017  
5.–6. October 2017, Karlstad, Sweden
- P-278 Arno Ruckelshausen, Andreas Meyer-Aurich, Karsten Borchard, Constanze Hofacker, Jens-Peter Loy, Rolf Schwerdtfeger, Hans-Hennig Sundermeier, Helga Floto, Brigitte Theuvsen (Hrsg.)  
Informatik in der Land-, Forst- und Ernährungswirtschaft  
Referate der 38. GIL-Jahrestagung  
26.–27. Februar 2018, Kiel
- P-279 Matthias Tichy, Eric Bodden, Marco Kuhmann, Stefan Wagner, Jan-Philipp Steghöfer (Hrsg.)  
Software Engineering und Software Management 2018  
5.–9. März 2018, Ulm
- P-280 Ina Schaefer, Dimitris Karagiannis, Andreas Vogelsang, Daniel Méndez, Christoph Seidl (Hrsg.)  
Modellierung 2018  
21.–23. Februar 2018, Braunschweig
- P-281 Hanno Langweg, Michael Meier, Bernhard C. Witt, Delphine Reinhardt (Hrsg.)  
Sicherheit 2018  
Sicherheit, Schutz und Zuverlässigkeit  
25.–27. April 2018, Konstanz
- P-282 Arslan Brömme, Christoph Busch, Antitza Dantcheva, Christian Rathgeb, Andreas Uhl (Eds.)  
BIOSIG 2018  
Proceedings of the 17th International Conference of the Biometrics Special Interest Group  
26.–28. September 2018  
Darmstadt, Germany
- P-283 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)  
11. DFN-Forum Kommunikationstechnologien  
27.–28. Juni 2018, Günzburg
- P-284 Detlef Krömker, Ulrik Schroeder (Hrsg.)  
DeLFI 2018 – Die 16. E-Learning Fachtagung Informatik  
10.–12. September 2018, Frankfurt a. M.
- P-285 Christian Czarniecki, Carsten Brockmann, Eldar Sultanow, Agnes Koschmider, Annika Selzer (Hrsg.)  
Workshops der INFORMATIK 2018 - Architekturen, Prozesse, Sicherheit und Nachhaltigkeit  
26.–27. September 2018, Berlin
- P-286 Martin Mikusz, Alexander Volland, Martin Engstler, Masud Fazal-Baqaie, Eckhart Hanser, Oliver Linssen (Hrsg.)  
Projektmanagement und Vorgehensmodelle 2018  
Der Einfluss der Digitalisierung auf Projektmanagementmethoden und Entwicklungsprozesse  
Düsseldorf 2018

- P-287 A. Meyer-Aurich, M. Gandorfer, N. Barta, A. Gronauer, J. Kantelhardt, H. Floto (Hrsg.)  
Informatik in der Land-, Forst- und Ernährungswirtschaft  
Fokus: Digitalisierung für landwirtschaftliche Betriebe in kleinstrukturierten Regionen – ein Widerspruch in sich?  
Referate der 39. GIL-Jahrestagung  
18.–19. Februar 2019, Wien
- P-288 Arno Pasternak (Hrsg.)  
Informatik für alle  
18. GI-Fachtagung  
Informatik und Schule  
16.-18. September 2019 in Dortmund
- P-289 Torsten Grust, Felix Naumann, Alexander Böhm, Wolfgang Lehner, Jens Teubner, Meike Klettke, Theo Härder, Erhard Rahm, Andreas Heuer, Holger Meyer (Hrsg.)  
Datenbanksysteme für Business, Technologie und Web (BTW 2019)  
4.–8. März 2019 in Rostock
- P-290 Holger Meyer, Norbert Ritter, Andreas Thor, Daniela Nicklas, Andreas Heuer, Meike Klettke (Hrsg.)  
Datenbanksysteme für Business, Technologie und Web (BTW 2019)  
Workshopband  
4.–8. März 2019 in Rostock
- P-291 Michael Räckers, Sebastian Halsbenning, Detlef Rätz, David Richter, Erich Schweighofer (Hrsg.)  
Digitalisierung von Staat und Verwaltung  
Gemeinsame Fachtagung  
Verwaltungsinformatik (FTVI) und  
Fachtagung Rechtsinformatik (FTRI) 2019  
6.–7. März 2019 in Münster
- P-292 Steffen Becker, Ivan Bogicevic, Georg Herzwurm, Stefan Wagner (Hrsg.)  
Software Engineering and Software Management 2019  
18.–22. Februar 2019 in Stuttgart
- P-293 Heiko Roßnagel, Sven Wagner, Detlef Hühnlein (Hrsg.)  
Open Identity Summit 2019  
28.–29. März 2019  
Garmisch-Partenkirchen
- P-294 Klaus David, Kurt Geihs, Martin Lange, Gerd Stumme (Hrsg.)  
INFORMATIK 2019  
50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft  
23.–26. September 2019 in Kassel
- P-295 Claude Draude, Martin Lange, Bernhard Sick (Hrsg.)  
INFORMATIK 2019  
50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft  
Workshop-Beiträge  
23.–26. September 2019 in Kassel
- P-296 Arslan Brömmel, Christoph Busch, Antitza Dantcheva, Christian Rathgeb, Andreas Uhl (Eds.)  
BIOSIG 2019  
Proceedings of the 18th International Conference of the Biometrics Special Interest Group  
18.–20. September 2019  
Darmstadt, Germany
- P-297 Niels Pinkwart, Johannes Konert (Hrsg.)  
DELFI 2019 –Die 17. Fachtagung  
Bildungstechnologien  
16.–19. September 2019 in Berlin
- P-298 Oliver Linssen, Martin Mikusz, Alexander Volland, Enes Yigitbas, Martin Engstler, Masud Fazal-Baqaie, Marco Kuhmann (Hrsg.)  
Projektmanagement und Vorgehensmodelle 2019 –Neue Vorgehensmodelle in Projekten – Führung, Kulturen und Infrastrukturen im Wandel  
1 Gemeinsame Tagung der Fachgruppen  
Projektmanagement (WI-PM), Vorgehensmodelle (WI-VM) und Software Produktmanagement (WI-ProdM) im Fachgebiet Wirtschaftsinformatik der Gesellschaft für Informatik e.V.  
in Kooperation mit der Fachgruppe IT-Projektmanagement der GPM e.V.,  
Lörrach 2019

- P-299 M. Gandorfer, A. Meyer-Aurich, H. Bernhardt, F. X. Maidl, G. Fröhlich, H. Floto (Hrsg.)  
Informatik in der Land-, Forst- und Ernährungswirtschaft  
Fokus: Digitalisierung für Mensch, Umwelt und Tier  
Referate der 40. GIL-Jahrestagung  
17.–18. Februar 2020,  
Campus Weihenstephan
- P-300 Michael Felderer, Wilhelm Hasselbring, Rick Rabiser, Reiner Jung (Hrsg.)  
Software Engineering 2020  
24.–28. Februar 2020  
Innsbruck, Austria
- P-301 Delphine Reinhardt, Hanno Langweg, Bernhard C. Witt, Mathias Fischer (Hrsg.)  
Sicherheit 2020  
Sicherheit, Schutz und Zuverlässigkeit  
17.–20. März 2020, Göttingen
- P-302 Dominik Bork, Dimitris Karagiannis, Heinrich C. Mayr (Hrsg.)  
Modellierung 2020  
19.–21. Februar 2020, Wien
- P-303 Peter Heisig, Ronald Orth, Jakob Michael Schönborn, Stefan Thalmann (Hrsg.)  
Wissensmanagement in digitalen Arbeitswelten: Aktuelle Ansätze und Perspektiven  
18.–20.03.2019, Potsdam
- P-304 Heinrich C. Mayr, Stefanie Rinderle-Ma, Stefan Strecker (Hrsg.)  
40 Years EMISA  
Digital Ecosystems of the Future: Methodology, Techniques and Applications  
May 15.–17. 2019  
Tutzing am Starnberger See
- P-305 Heiko Roßnagel, Christian H. Schunck, Sebastian Mödersheim, Detlef Hühnlein (Hrsg.)  
Open Identity Summit 2020  
26.–27. May 2020, Copenhagen
- P-306 Arslan Brömme, Christoph Busch, Antitza Dantcheva, Kiran Raja, Christian Rathgeb, Andreas Uhl (Eds.)  
BIOSIG 2020  
Proceedings of the 19th International Conference of the Biometrics Special Interest Group  
16.–18. September 2020  
International Digital Conference
- P-308 Raphael Zender, Dirk Ifenthaler, Thiemo Leonhardt, Clara Schumacher (Hrsg.)  
DELFI 2020 –  
Die 18. Fachtagung Bildungstechnologien der Gesellschaft für Informatik e.V.  
14.–18. September 2020  
Online
- P-310 Anne Koziolk, Ina Schaefer, Christoph Seidl (Hrsg.)  
Software Engineering 2021  
22.–26. Februar 2021,  
Braunschweig/Virtuell
- P-311 Kai-Uwe Sattler, Melanie Herschel, Wolfgang Lehner (Hrsg.)  
Datenbanksysteme für Business, Technologie und Web (BTW 2021)  
Tagungsband  
13.–17. September 2021,  
Dresden
- P-312 Heiko Roßnagel, Christian H. Schunck, Sebastian Mödersheim (Hrsg.)  
Open Identity Summit 2021  
01.–02. Juni 2021, Copenhagen

The titles can be purchased at:  
**Köllen Druck + Verlag GmbH**  
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn  
Fax: +49 (0)228/9898222  
E-Mail: druckverlag@koellen.de



Gesellschaft für Informatik e.V. (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into

- seminars
- proceedings
- dissertations
- thematics

current topics are dealt with from the vantage point of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure high quality contributions.

The volumes are published in German or English.

Information: <http://www.gi.de/service/publikationen/lni/>

ISSN 1617-5468

ISBN 978-3-88579-706-7

Open standards and interfaces as well as open source technologies play a central role in the current identity management landscape as well as in emerging future scenarios in the area of electronic identification and trust services for electronic transactions according to the eIDAS regulation (2014/910/EU), innovative payment services according to the second payment services directive (PSD2) (2015/2366/EU), trustworthy and privacy enhancing solutions according to the general data protection regulation (2016/679/EU) and other innovative applications in the area of e-health, e-government, cloud computing and the internet of things for example.