Internet of Things

IoT Governance, Privacy and Security Issues

EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS

January, 2015

> "Just as energy is the basis of life itself, and ideas the source of innovation, so is innovation the vital spark of all human change, improvement and progress."
>
> Ted Levitt

European Commission
Information Society and Media

IERC Coordinators:

Ovidiu Vermesan, Coordinator IERC Cluster, Ovidiu.VERMESAN@sintef.no

Peter Friess, Coordinator IERC Cluster, European Commission, Peter.FRIESS@ec.europa.eu

Authors

Gianmarco Baldini, (DG JRC-EC)

Trevor Peirce (Avanta Global),

Maarten Botterman (GNKS Consult)

Maria Chiara Talacchini, (DG JRC-EC)

Angela Pereira (DG JRC – EC)

Marcus Handte (University of Duisburg-Essen),

Domenico Rotondi (TXT Group),

Henrich C. Pöhls (Passau University),

Ovidiu Vermesan (SINTEF),

Atta Baddii (University of Reading),

Bertrand Copigneaux (Inno Ag),

Schreckling, Daniel (Passau University),

Luca Vigano (University of Verona),

Gary Steri (DG JRC – EC)

Salvatore Piccione (TXT Group),

Panagiotis Vlacheas (UPRC)

Vera Stavroulaki (UPRC)

Dimitris Kelaidonis (UPRC)

Ricardo Neisse (DG JRC-EC)

Elias Tragos (ICS - FORTH),

Philippe Smadja (GEMALTO)

Christine Hennebert (CEA LETI)

Martin Serrano (National University of Ireland Galway)

Stefano Severi (Jacobs University)

Giuseppe Abreu (Jacobs University)

Peter T. Kirstein (University College London)

Socrates Varakliotis (University College London)

Antonio Skarmeta (University of Murcia)

Contributing SDOs, Projects and Initiatives

iCore, GAMBAS, BUTLER, CEN/CENELEC, ETSI, ISO, PROBE-IT, SPaCIoS, IoT@Work, COMPOSE, RERUM, OpenIoT, IoT6, Value-Ageing

Acknowledgements

The IERC would like to thank the European Commission services for their support in the planning and preparation of this document. The recommendations and opinions expressed in this document do not necessarily represent those of the European Commission. The views expressed herein do not commit the European Commission in any way.

Table of content

Revision History

Revision	Date	Author(s)	Description
0.1	25/09/2013	Gianmarco Baldini, Trevor Peirce, Maria Chiara Tallachini	First draft with ToC and Ethics section
0.2	23/10/2013	All authors	New version with new template and new contributions after the meeting on the 10th of October 2013.
0.3	11/11/2013	All authors	New Version after the meeting on the 4th of November 2013. Contributions from BUTLER, COMPOSE and IOT@Work
0.4	14/11/2013	JRC authors	General revision
0.5	25/11/2013	JRC authors	Added new content in Framework against the challenges section
0.6	05/12/2013	All	Collection of new contributions/changes in different parts of the document.
0.7	09/12/2o13	JRC authors, Trevor Peirce	New contributions, formatting changes, including OpenIoT project contributions.
0.8	11/12/2013	All	Correction, new section on reference architecture and smart city scenario
0.9	12/12/2013	All	New contributions, updates after PhConf of 12/12/2013.
0.10	16/12/2013	All	Last round of contributions.
0.11	4/3/2014	RERUM	Update from RERUM project
0.12	14/03/2014	All	Another round of updates before IERC meeting on 21/03/2014, Update on OpenIoT CAS-OAuth2.0 implemented module
0.13	19/03/2014	All	Final round of updates before IERC meeting on 21/03/2014.
0.14	11/04/2014	All	Updated after the meeting in Athens
0.15	17/04/2014	Alberto Martínez, Arantxa Rentería (Tecnalia; BUTLER)	Generally: References to Value Ageing Project. Ethical recommendations for ICT development, including companion and assistive robotics. Specifically: • Updated Ethics chapter and ethics-related IoT governance: ethics and assistive robotics, hints for IoT and ethics in the IoT governance. • Map of FP7 projects contributing to

			AC05 cluster: Value Ageing project referenced. • New "Non-Technological Approach for IoT Risk Management" chapter associated to "Technological enablers and Design Solutions".
0.16	30/06/2014	Peter T. Kirstein (University College London) Socrates Varakliotis (University College London) Antonio Skarmeta (University of Murcia)	Contribution from IoT6
0.17	8/07/2014	JRC authors	New section for IoT Week report, New section of links with other ACs in the IERC, New section for standardization.
0.18	14/11/2014	Serbanati, Domenico Rotondi, Ovidiu Vermesan, Gianmarco Baldini	Some corrections. Update of Abbreviations/Glossary. Addition of references to ENISA Report, Mauritius conference on privacy.

Executive Summary

This position paper is an output of the Activity Chain 05 in the Internet of Things Cluster (IERC). The IERC has created a number of activity chains to support close cooperation between the projects addressing IoT topics and to form an arena for exchange of ideas and open dialog on important research challenges. The activity chains are defined as work streams that group together partners or specific participants from partners around well-defined technical activities that will result into at least one output or delivery that will be used in addressing the IERC objectives. IERC Activity Chain 05 is the cross-project activity, which has the objective to investigate how research can foster a trustworthy IoT at European level, identify solutions to protect the security and privacy of the citizens. These objectives can be quite challenging at the regulatory, ethical, market and technical levels.

Next to Trusted IoT, privacy, data protection and security, which is at the core of policy issues already addressed today by the IERC, there are also other policy issues of concern that will need to be addressed if IoT is to be accepted by society, and wanted to make a difference where it can. These issues in particular include global governance (how are we going to make this all happen, in the full understanding that the way forward will need to involve multiple stakeholders around the globe), ethics (what would we expect those “global IoT solutions” to respect, and how will the way IoT is implemented potentially affect the understanding of ethical impact), and radio frequency spectrum. What can we do to make sure those issues are addressed, and how can we assure citizens and policy makers are well informed, thus to be able to take conscious decisions when moving forward.

In this context, this position paper identifies relevant IoT challenges and describes solutions defined by the cluster projects, which can be used to address these challenges. FP7 projects have spent considerable effort in the definition of technical solutions and frameworks for the IoT domain. In some case, these solutions may overlap or they may leave gaps, which might become a basis for proposals for future IERC research activities and research programs like H2020. These research opportunities are identified and described in this position paper. Future activities of AC05 must address the integration of the identified solutions in this position paper with the results from the other Activity Chains in the IERC.

Introduction

The Internet of Things (IoT) is a concept being increasingly supported by various stakeholders and market forces. The idea is to connect various devices or objects ("things") through wireless and wired connections and unique addressing schemes[1] and create a pervasive environment where a person can interact at any time with the digital world and physical world. It also encompasses virtual objects and, virtual machines having digital attributes and evolving personalities. IoT opens new exciting opportunities but also new questions on the interaction between the citizen and businesses operating in the digital world. Some of these questions include the capture, processing and ownership of citizen's data and the possible need to create new legislative or technical frameworks to exercise more control over such a large and complex environment while at the same time avoiding posing unnecessary constraints to IoT market development. Other questions refer to access and effects. These questions are related to various aspects: the governance, security and privacy aspects, which cannot be separated (in the opinion of the authors of this paper) from ethical aspects.

The discussion on these aspects is not new and there is already a considerable amount of work done in previous consultations, technical reports, research activities both in Europe and around the world. This paper also surveys and considers the previous work with the acknowledgement that there may be conflicting and non conclusive results in some cases.

This position paper is the result of the Activity Chain 05 collaboration within the European Internet of Things Cluster (IERC). The IERC has created a number of activity chains to support close cooperation between the projects addressing IoT topics forming an arena for exchange of ideas and open dialog on important research challenges. The activity chains are defined as work streams that group together project partners or specific participants around well-defined technical activities that will result in at least one output or deliverable that will be used in addressing the IERC objectives. IERC Activity Chain 05 is a cross-project activity focused on making a valued contribution to IoT privacy, security and governance among the EC funded research projects in the area of Internet of Things. These three aspects are closely interlinked and they should not be discussed in a separate or isolated way. In addition, we link these aspects to Ethics. Activity Chain 05 does not define government policies but focuses upon research (which could eventually be used to support policies or standardization activities).

Various FP7 projects are funded in the area of IoT, which investigate elements of the topics governance, security and privacy. The objective of AC05 and of this position paper is to assemble a summary of this work, identify relevant

[1] Where unique address refers to a way of identifying a device with reasonable confidence at any specific point in time during the devices planned lifetime. Uniqueness is a concept for modelling purposes which can be and often is flawed in systems incorporating devices which include unplanned, seldom and fleeting device connections. The uniqueness concept dimension is a fundamental element of governance, security and privacy.

issues and challenges that must be taken into account in the next years by Horizon 2020. An additional objective is to identify and promote synergies across the projects, which can be used to define an overall framework (from the cluster projects) which can address these challenges. In detail, the objectives of this position paper are:

a) to identify the key challenges and needs for governance, security, privacy and related ethical aspects in IoT;
b) to survey the existing research in IoT for governance, security, privacy and related ethical aspects in IoT;
c) to provide a map of the activities of the FP7 projects participating to AC05;
d) to identify the technical solutions from FP7 projects, which could address the key challenges and needs from (a);
e) to define a framework derived from the solutions identified in (d);
f) to identify gaps of the framework defined in (e), which require future research;
g) to define potential actions to foster the impact of AC05 and IERC.

The deliverables of the other ACs are also considered in examining the challenges and opportunities that the current evolution of findings deliver to AC5. For example AC2 Naming and addressing schemes. Means of search and discovery, AC4 - Service openness and inter-operability issues/semantic interoperability, AC8 - Cognitive Technologies for IoT all contribute to the IoT landscape which AC5 seeks to address. Meanwhile AC5 through its actions, also pin-point considerations which influence the discussions and conclusions of these other ACs in deriving improved mutual understanding and fostering a cohesive overall picture of IoT. The other ACs, such as AC6 - Standardisation and pre-regulatory research are also closely connected with AC5 as are the other ACs but generally speaking the priority of these exchanges with these additional ACs tend to be relevant later in the process.

While, there have been frequent exchanges and discussions with other ACs in the IERC during the drafting of this position paper, we believe that this position paper is just a basis for more detailed discussions with other ACs in future phases of the IERC activity once all the AC deliverables are completed.
The overall approach in the paper is presented in *Figure 1*. From a wider analysis of the interaction between users and IoT, the main challenges and needs are identified and the contributions of the various projects to address specific issues are analyzed. The contributions from the various projects can be used to define the framework. This exercise may leave gaps, which are identified and they might become a basis for a proposal for future research activities. Finally, the paper describes the potential approaches to increase the impact of the defined framework and solutions through regulation, best practices and standardization activities (e.g., in European Standardization Organizations or ESO).

In addition, this position paper will also address aspects of safety in IoT, when critical services (e.g., health of citizens, workplace safety) are implemented by automatic systems (i.e., Cyber Physical Systems) which do not require human intervention.

This position paper will not specifically address aspects of resilience in existing critical information infrastructures even if based on IoT technologies because we believe that this analysis is part of CIIP (Critical Information Infrastructure Protection). The paper will just identify challenges in this area.
In a similar way, this position paper will not address Cybersecurity topics on the current Internet infrastructures.

The position paper has the following structure. Section

Overview of IoT Governance, Privacy and Security Issues provides a summary of the related work on Governance, Security and Privacy and the key challenges to overcome. Section *Ethics and Internet of Things* provides a wide overview of the relationship between Ethics and Information and Communication Technologies (ICT), which is refined in the relationship between Ethics and IoT for the specific aspects of Governance, Security and Privacy. Section *Map of FP7 projects in the cluster* provides a mapping of the FP7 projects deliverables and results against Governance, Security and Privacy. Section *Technological enablers and design solutions* provides a number of technical solutions, which can be designed and applied to create an "ethical" IoT and to resolve the identified challenges. The technical solutions come primarily from activities in the IERC projects. Section *Way ahead and impact* explores how the technical solutions can produce an "impact" in various areas and what could be relevant research topics in the future.

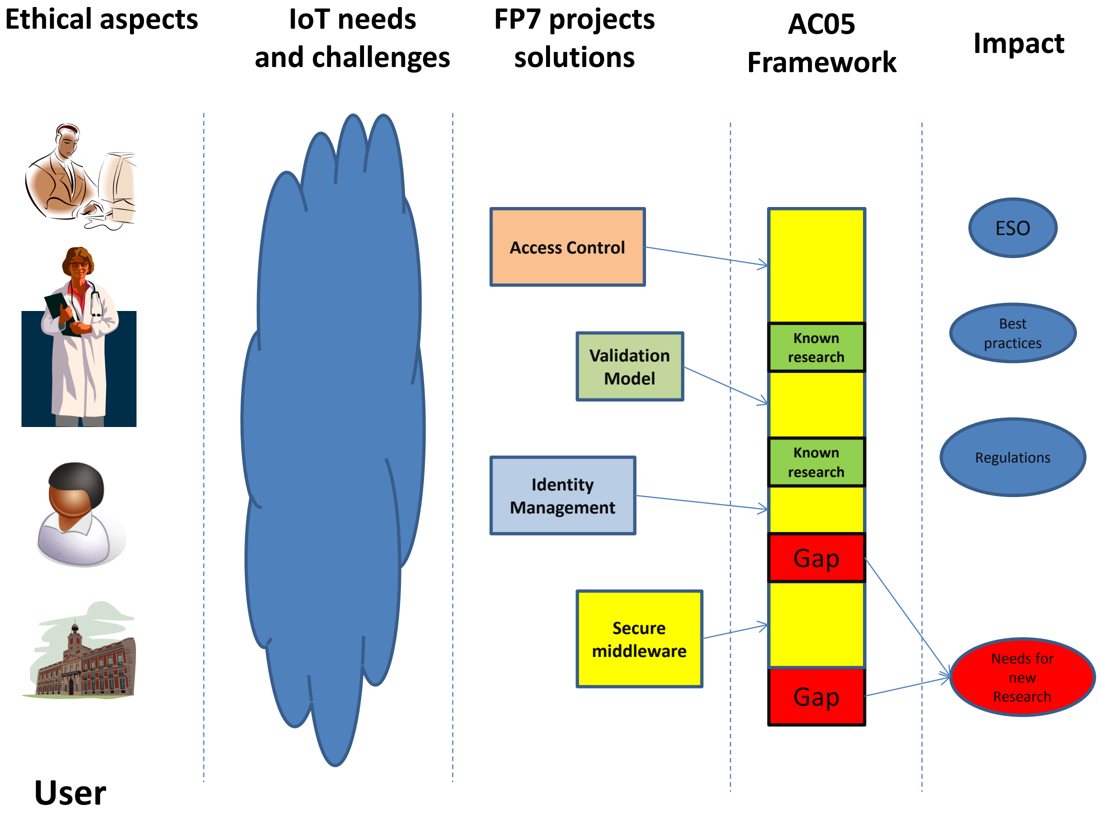


Figure 1 Overall AC05 approach

Overview of IoT Governance, Privacy and Security Issues

Related work

Governance, security and privacy are probably the most challenging issues in the Internet of Things and they have been extensively discussed in many papers. In this section we will try to summarize the capital points of these three aspects of the IoT according to the main contributions proposed in literature. The concepts of IoT Governance, Security and Privacy are also not fully defined and various definitions have been proposed by different government industry and research organizations.

Within the EU, 'Governance' refers to the rules, processes and behaviour that affect the way in which powers are exercised, particularly as regards openness, participation, accountability, effectiveness and coherence. These five "principles of good governance" reinforce those of subsidiarity and proportionality. The concept of Governance have been already applied to the Internet for specific aspects and there are already organizations like IETF, ICANN, RIRs, ISOC, IEEE, IGF, W3C, which are each responsible and dealing with a specific area.

While these organizations work on *Internet* governance, a logical step is to extend these concepts to *IoT* governance. The difficulty is that the high number and heterogeneity of technologies and devices in the IoT require even more specific Governance solutions and approaches that are more complex.

Size and heterogeneity in fact, are the two main components that affect the governance of IoT: in [1], governance is considered as a double-edged sword, because it can offer stability and support for decisions but it can also become excessive and result in an over-controlled environment. The conclusions of [2], underline the difficulty to find a common definition of IoT governance together with the different positions of many stakeholders: it seems to be premature to start a policy development and there is no agreement on finding special rules for IoT governance issues which are separated from other general rules. Nevertheless, since there are no legal frameworks for IoT governance [3], even if the differences between the IoT and the Internet have been overestimated at the beginning, an analysis of the major IoT governance issues (legitimacy, transparency, accountability, anti-competitive behaviour) seems to be worthwhile to conduct. Apart from policy or ethical aspects that influence governance itself the activities conducted in this cluster provide technical solutions that can be implemented now.

Heterogeneity requires security to overcome the impossibility of implementing efficient protocols and algorithms on all the devices involved across the many IoT application areas. Without guarantees in security, stakeholders are unlikely to adopt IoT solutions on a large scale [4] [5]. For this reason, the development of enforcement techniques to support scalability and heterogeneity, to anonymize users' data and to allow context aware data protection are key factors.
In the IoT context, it is difficult to separate the concepts of Governance, Security and Privacy, because addressing privacy and security aspects to

achieve trust in IoT would probably need governance mechanisms as well. As pointed out before, at the higher level of the interaction of IoT with users, ethical aspects cannot be disjointed from the governance, security and privacy aspects as well. In this position paper, we adopt the definitions of security and privacy already presented in [6] where privacy, data protection and information security are complementary requirements for IoT services. In particular information security has the objective to preserve the confidentiality, integrity and availability (CIA) of information.

In Europe, regarding privacy aspects, some initial work has already been performed in reference to Regulation 611/2013, Article 4 (3) in respect of creating an indicative list of appropriate technological protection measures. One major source of this preliminary work has been the reports on recommended cryptographic measures to secure persona data released by ENISA (i.e., [7], [8]).

At international level, in October 2014, at the International Conference of Data Protection and Privacy Commissioners in Mauritius, representatives of the private sector and academia joined together to discuss the changes or risks that the internet of things and big data may bring to daily life. The observations and conclusions of the discussions regarding IoT are available in Declaration on the Internet of Things[2] and a Resolution on Big Data[3]. The document is not, of course, binding. But, the fact that the Declaration and Resolution drew the consensus of a large gathering of international data protection regulators renders them relevant indicators of direction of data privacy policies and trends.

The Mauritius Declaration on the Internet of Things and the Resolution on Big Data set out principles and recommendations designed to reduce the risks associated with the collection and use of data for players in the connected devices and big data ecosystems. The Declaration and Resolution both begin by acknowledging that connected devices and big data have the capacity to make our lives easier, including by providing benefits such as predicting the spread of epidemics and combatting pollution. But, the documents also acknowledge that the internet of things and big data raise "important concerns with regard to the privacy of the individuals and civil rights, protections against discriminatory outcomes and infringements of the right to equal treatment.".

The concerns discussed at the Mauritius Conference echo those of the USA White House's May 2014 Big Data Report [9], which similarly focused on the potential use of big data to discriminate against certain groups. Among other things, the Report cautioned that increased personalization allows for "discrimination in pricing, services, and opportunities," that "serving up different kinds of information to different groups, ha[s] the potential to cause real harm to individuals," and that categorization "effectively prevent[s] [people] from encountering information that challenges their biases or assumptions," thereby cementing and potentially exacerbating existing ideological or cultural segregation.

[2] http://www.privacyconference2014.org/media/16421/Mauritius-Declaration.pdf

[3] http://www.privacyconference2014.org/media/16427/Resolution-Big-Data.pdf

In addition, according to [10], the proliferation of wireless devices with ubiquitous presence is expected to worsen the issue of privacy due to the current design of the link-layer and lower layer protocols, which usually expose information like implicit names and identifiers that can reveal users identity. As a consequence, these layers should be redesigned in order to minimize the collection of such data, conceal important information from the un-trusted parties and, to reveal proper information to the authorized or trusted parties. The management of heterogeneous devices, applications and protocols can be also addressed using the principles of service-oriented computing [11], like loose coupling and heterogeneity, achieving a significant flexibility in different levels of the IoT architecture.

Another important issue, pointed out in [1], is the implementation of IoT in a distributed way: the authors provide a detailed analysis of each aspect that show, in general, the higher level of complexity introduced by the distributed approach in the deployment of governance, security and privacy solutions. However, they also show some benefits achieved using the distributed approach, especially in terms of scalability and flexibility of governance and privacy. Also traditional access controls methods based on Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) frameworks show their scalability problems in distributed environments [12] like the ones present in IoT; the adoption of access control systems based on capability can allow users to manage their access to the resources and even delegate their own rights.

Regarding scalability, another significant challenge is to provide reliable solutions, which are scalable for the billions of objects (‘things’) linked to many different local, regional or global networks. Additionally, lots of them are nomadic or mobile objects and finding the location of and verifying the correct identity of a specific item will be a major problem for the IoT infrastructure [1][4].

This is just a sample of the IoT challenges for Governance, Security and Privacy identified in literature. The next section describes the challenges identified by the partners of the AC05 cluster projects.

Identification of challenges for Governance Security and Privacy in IoT

The objective of this section is to identify the main challenges for the Governance, Security and Privacy in IoT identified by the AC05 cluster projects and during discussions in IERC. Ethical aspects are also considered. A more extensive discussion on ethical aspects in IoT is presented in section *Ethics and Internet of Things* and some challenges are derived from the analysis in that section.

Context based security and privacy

This section describes the challenge of designing a security and privacy framework, which is able to address changes in the context (e.g., emergency crisis) or context which do not support the collection and processing of data from sensors. For example, in a surveillance scenario, bad quality images may induce false results of the "smart" functions implemented in IoT framework and hamper the overall decision process in the algorithms used to ensure the security and trust of the system (e.g., level of reputation).

The security and privacy framework has to provide features to dynamically adapt access rules and information granularity to the context (e.g., embedding *Conditions* in access rules or access capability tokens evaluated at access time, see [12]). IoT envisages an enhanced relevance of the context awareness [13] higher needs to support the orchestration and integration of different services, as, for example, envisaged by the DiY (Do it Yourself) sociocultural practice [14] and scalability, manageability and usability [15].

An additional problem is that the automatics of security and privacy technologies defined for a specific context may behave in an incorrect way in a different (or unplanned) context with the consequence of generating vulnerabilities.

Cyber-Physical systems and IoT

In recent years, the development and deployment of systems and technologies that present a tight coupling between computing devices and the physical environment has grown considerably. Some examples are sensors for monitoring the health of the persons or to increase safety or ergonomics in workplaces, smart grids for energy distribution and intelligent transport systems, which have been also addressed in the iCore project in the use cases described in this deliverable. In many cases, these systems provide services that impact the safety of the citizens. In many case, these systems or services are not reliable[4] (e.g., susceptible to a security attack) the safety of the persons can be put at risk. One example in the Smart Transportation scenario is related to Intelligent Transport Systems where a security attack on the automatic car system for driving can produce car accidents and consequent casualties or harm to citizens. In another scenario an automatic system to provide medicine to a patient can become compromised and deliver the wrong medicine to a patient. In all these systems, the physical environment provides information necessary for achieving many of the important functionalities of the ICT systems through sensors. In turn, systems that use the information from the physical environment can affect the physical environment and the persons living in this environment through actuators. These systems are also called cyber–physical systems (CPSs).

Another aspect to be addressed in the evolution of IoT regarding critical services is related to the pervasiveness of digital devices [16] [17], which have increasingly processing power and re-configurability and therefore they are vulnerable to similar malware of traditional computers. The main issue is that these devices are more and more embedded in our everyday life but they may

[4] Reliability: Comprised of multiple risk factors of which security attack is only one. Others include: Failure modes incorporating for example device or system design oversights Diminished access, speed, interoperability etc. due to indirect external factors.

not have the computing capacity to implement sophisticated security protection solutions like Trusted Computing, or Cryptography. As pointed out in [16] and [17], this context presents challenges of scalability (billions of devices to protect), harmonization and homogeneity (different protocols and technologies).

Identification in a distributed environment

Identification is closely tied to IoT governance, security and privacy. Different forms of identification are key components of multiple layers of IoT, from those embedded in the end device through to those enabling message routing and discovery. Each form of identification (numbering, addressing and naming) has a set of influencing factors which create divergence and it is important to appreciate that these differences are often necessary and sometimes advantageous. As IoT exploits established elements and applications there is a legacy environment which cannot be ignored and which must be addressed in some part or its totality. There are various ways to achieve this but each has ultimately an impact upon IoT's scope of appeal.
Distributed environments are challenging, even those which are closed, bounded by similar functional and interoperable technologies and supported by a clear governance structure. IoT faces a greater test due to: a) the breadth of legacy applications, b) the variety of technologies and their associated characteristics, c) the multitude of established governance structures, d) a wide variety of edge and near-edge domain functionalities and e) opaque stakeholder value propositions.

Much consideration is provided to edge device identification as a means to foster future IoT interoperability. There are a number of established identification hierarchies which provide interoperability and most of these ignore embedded identifiers (often referred to as 'numbering'), with a preference for user assigned identifiers i.e. 'naming'. The importance of addressing as an identifier should not be overlooked nor, confused with numbering and naming. There are also potential future opportunities considering the increasing performance of algorithms which are able to derive value from unstructured data.

The number of devices (real and virtual) potentially involved within IoT is somewhat misleading. WWRF's estimation is for 7 trillion of devices serving 7 billion of people until 2017 [18].

These estimates may be related to active devices but it may ignore those that are dormant, retired and all those identifier provisions for future devices. There are many 'hard' and 'soft' factors which determine the required characteristics of an identifier structure, including governance, security and privacy. What is clear today is that the majority of arguments presented reference legacy which encompasses a broad diversity of objectives with only some overlap. There are few propositions which focus upon the future of IoT. Many of the existing naming, numbering and addressing schemes have been created to address specific objectives at one point in time and therefore there is no one universal answer to identification which can provide for all of IoT's requirements without limiting IoT's scope or diminishing IoT's applicability.

The success of IoT, the ultimate goal requires a clear reference supported by a number of established governance bodies and key stakeholders in the absence of a central coordinating authority. Until these criteria are defined sufficiently discussions over identification schemes and governance models are likely to be drawn-out, subjective, risky and potentially inconclusive.

Device authentication

Most systems which bind IoT sensors and actuators rely on some proxy concept, i.e. sensors communicate to some more powerful entity (e.g, from the processing and storage point of view) which then authenticates the sensors on their behalf. However, the *last mile* effectively remains unprotected which is a barrier to guaranteeing important security properties such as non-repudiation. ‘Lightweight’ solutions are still an open issue for many devices. The long history of research in sensor networks domain has not produced secure and low-cost solutions feasible for most devices. Thus, new types of security primitives or mechanisms which do not only focus on the higher layers in communication protocols would be worthwhile to investigate.

Data Correlation and Information Retrieval

The Internet of Things generates data in various contexts. Combining this data may support new types of security mechanisms which allow for the enforcement of more complex security policies. However, the ability to access this large variety of data also allows the generatation of more complex and detailed user profiles. Currently, it is unclear whether the security mechanisms based on this data variety outweigh their privacy risks or whether there are security mechanisms which mitigate the disadvantages.

Anonymization of users’ data in a distributed and mobile environment

There are two main challenges for anonymization in IoT. One is related to the difficulty to anonymize the data during data collection processes (e.g., from sensors) because this would require additional technology (with increased device cost). Another is the risk of (re-)identification of the individual from the aggregation of anonymized data (see [19]).

This challenge is also related to the current debate on storing users data on remote platforms in the Internet where the provider of the platforms (e.g., Cloud provider) is mostly considered trusted. There are existing solutions which could be applied to this domain, such as multi-party computation or homomorphic functions [20] but their feasibility is unclear.

Anonymization of protocol metadata in a distributed and mobile environment

Considering aforementioned user data as the input to communication protocols, the data produced by the communication protocol and thus observable by communicating parties and outsiders must be minimized as well. This is usually termed “unobservability of communication”. Of course as long as anonymization of user data itself is not offering protection from ‘prying eyes’, this element is not critical. However hoping that encryption and anonymization of user data will be guaranteed, the communication meta-data becomes the next issue. Solving this would mean things like replacing long-term hardware identifiers with software generated ones, like the T-IMSI in UMTS was introduced to minimize tracking (see [21]).

Scalability for the billions of devices in IoT

The IoT has to master not only a wider heterogeneity of connected systems, communication technologies and resource constraints, but has also to face challenges related to the potential unbounded number of interacting entities and substantial differences in the interaction patterns [22][23].

Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) systems, as well as PKIs, are not yet able to fully address these challenges providing scalable, manageable, effective, and efficient access control mechanisms.

Additionally, RBAC, ABAC and ACL systems make hard to enforce the least privilege principle [24] [25].

IoT therefore would benefit from additional solutions, such as capabilities-based access control mechanisms, able to address the above challenges (see [12]).

Secure Setup and Configuration

Solving the challenge of scalability is closely related, but not equal, to having a secure setup and configuration method for the IoT. Self-X IoT properties present a potential attack surface to the Hardware Objects and the applications depending on them. Therefore securing the IoT requires a security architecture with the appropriate mechanisms. These typically require cryptographic credentials that can be symmetric and/or asymmetric, depending on the scenario and the requirements. The bootstrapping process to install them efficiently presents a significant challenge, especially for the large number of devices in an IoT deployment.

Physical availability of devices

The Internet of Things paradigm auspicates the availability of small-sized connected sensor/actuator devices to be embedded pervasively in the environment. By definition, these devices will thus be physically available to malicious users who could use them in different ways in order to compromise the integrity or reliability of an IoT system. The number of devices itself and their reduced capabilities make it very difficult to detect tampering and to check that they are actually operating properly.

This challenge is related to the difficulty of knowing with certainty if the device operates in the right context (for example it was not moved or the environmental conditions were not altered locally), if it was subject to firmware replacement, impersonated and so on.

Critical infrastructures and IoT

In this section, we describe the security and privacy aspects related to the use of IoT in Critical infrastructures (energy, telecom, utilities) and how the evolution of IoT may impact the deployment and management of critical infrastructures.

This challenge is related to the relationship between IoT and Critical Infrastructure (CI). IoT devices and technologies may be increasingly used in critical infrastructure like Telecom, Utilities, Energy and so on. An example of the deployment of IoT concepts to the industrial world (and therefore critical infrastructures) is the Machine to Machine (M2M) standardization activity. The challenge is to assess the new risks related to the deployment of IoT technologies and devices in the critical infrastructures and the *transfer* of IoT vulnerabilities for security and privacy to critical infrastructures. In the case, of CI, the IoT vulnerabilities may be more critical because they can impact the safety (e.g., industrial accidents) or the provision of essential services to the community (e.g., electrical power to hospitals). In some cases, the deployment of new technologies and devices in the home of the citizen or in the proximity may lead to new security or privacy issues (e.g., smart-meters). On the other side of coin, some of the IoT vulnerabilities may not be directly applicable to Critical Infrastructures or they may be mostly due to deployment issues. This means that protection and mitigation techniques for security and privacy are well known but lack of funding, non-conformance to best practices or human errors in deployment may not see the enforcement of these solutions. Even if some solutions to protect sensor nodes and pervasive devices in critical environments have been proposed [26] and could be extended and adapted to IoT needs, this latter aspect will not be addressed in this position paper.

Conflicting market interest

One of the appealing features of IoT from a business point of view is the possibility to collect and correlate data from different sources to increase the market competitiveness of the market producers. The idea is to correlate different sets of data to increase the efficiency of the product advertisements to the customer and to better satisfy his/her needs. This correlation and aggregation of the data can create a tension with the approaches or techniques, which have the objective to protect the data of a person (e.g., privacy). As described in [1] and [27], this tension could also be the reason for the low deployment of privacy enabling technologies, which is one of the main challenges this paper tries to address.

Considering IoT in an evolving Internet

While IoT cannot expect today to influence the Internet's evolution it is surely affected itself by the evolution of the Internet. There are two principal aspects of evolution to be considered: how the Internet is used and, elements of the configuration of the technical platform. Undoubtedly, media attention upon surveillance means that data security and privacy is playing a role in shaping both use and the configuration of the Internet. Initiatives to embed 'Dark' Internet style security (e.g. Tor) and privacy protection as a default through standardization will create challenges for 'Big Data', law enforcement (e.g. LI), surveillance, etc. If such an Internet environment becomes the defacto 'trusted' Internet would it be socially acceptable for IoT to remain outside?

Can such an evolution indeed benefit IoT security and privacy? What are the implications for IoT governance?

Delegation of human autonomy in IoT

IoT opens towards futures of seamless hybridized interactions between human beings, their extended ICT-mediated capabilities, and smart and dynamic objects displaying emerging unplanned behaviours. Agents and actors join towards unintended, unforeseen and unexpected outcomes. In this context, “artefacts” like wearable sensors, connected medical devices and other implantable devices are incorporated by users, becoming extensions of the human body or mind enhancing the interface between humans and the environment; in this type of relations the artefacts may not be strongly perceived by users. Voluntarily or not, the user may need to rely on models and technology to achieve the chores that technology is meant to help her/him with. Hence, the strong mediation inherent to IoT developments, will lead eventually to shifting or delegation of human autonomy and agency to the objects of the IoT with potential risk to the privacy or even security of the users. If noticed, artefacts will act on the user’s behalf; if not noticed artefacts will act on their developers’ worldviews, intentionality and interests. This strong mediation poses challenges to human agency. This challenge is similar to *Cyber-Physical systems and IoT* which is more focused on safety aspects.

Human IoT Trust relationship

Linked to the previous challenge *Delegation of human autonomy in IoT,* there is also the concept of evaluation of the level of trust a human has in IoT systems, services or devices. In information and communication technology (ICT) trust has been considered as a crucial component of digital interactions, and has been dissected in a variety of potential meanings and dimensions and, through the merging of trust in humans and trust in machines. Trust and confidence have different shades of meanings. However, Trust can also be defined as the level of confidence, which an entity can ensure to another entity or entities for specific services and in given context [28]. Even if trust has been often used with reference to human beings, trust can also be associated to a machine or digital system (e.g., web site), which points out at the importance of analyzing and measuring the level of trust in a digital society.

Here we have to make a distinction between trust and trustworthiness and how these two terms are adopted in the IoT domain. Usually, trust is the belief of a user that the system is functioning normally and will deliver what it has promised and what the user requires. Contrary to trust (that is mostly subjective to each user’s belief), trustworthiness is mostly objective and can be considered as a metric of how much a system deserves the trust of its users. Trustworthiness can be defined according to some criteria, i.e. by evidence of current and past behaviour, by the system availability, if it provides accurate and reliable information, if it avoids information leaks, etc. Furthermore, in cases of M2M communications in an IoT domain, the devices that are exchanging information with each other have to know which devices are trustworthy so that sensitive information is only sent to those devices. Thus, trust can be considered not only as a metric of how much a user trusts a system, but also how much a device trusts another device and how much a device trusts the user that has requested sensitive data from that device. As a result, trust in the IoT domain is included in three layers: (i) from users to devices, (ii) between devices and (iii) from devices to users.

In ICT, knowledge production has entered the debate as a possible path to trust as a vehicle for valued and respected relationships. Collaboration in knowledge processes has been at the core of the most traditional scientific community ethics, namely the so-called “ethos” of science. Today, knowledge co-production can contribute to trusted ICT digital interactions [29], [30]. European citizens’ values and fundamental rights provide a specific framework that needs to be explored, together with its opportunities and challenges.

Risks of isolation and confinement

On the one hand, ICT technologies can play a great role to minimize the risk of isolation not only by facilitating social contact but also increasing citizen’s access to work. Mobility and security solutions support people’s participation in community, and leisure and social activities. Telehealth and other communication and online services enable a lifestyle where one does not need to leave their home to satisfy their needs, hence reducing the opportunity for human contact and potentially contributing to a voluntary confinement. In the closer future, the use of companion robots in isolated and sparsely populated areas can also help to alleviate some of the social isolation effects.

To ensure that these benefits are realized it is necessary to consider potential risks and negative impacts arising from the application of these technologies, because an inadequate use of them may lead to further social isolation and confinement when not meeting certain requirements.

It is not a real fact already proven but an envisioned concern that should not be skipped out. Some people may be already isolated, and embracing ICT technology may not be so much harmful; even the contrary. But the risk of social isolation exists for all of us, at least at a certain extent. The level of human contact needs to be addressed not only at the design stage of technology and services associated with it, but even more importantly so, in its implementation.

The role of human contact cannot be underestimated both in terms of emotional impact on the person and ‘physical’ link to the community, to the world, strongly needed in elders. Tele health and tele care technologies are the main affected. The Social Care Institute for Excellence (European Commission, 2006) recommends that tele care must not be seen as an alternative to direct social care or informal support, but rather a way to meet low-level needs. One danger relates to people becoming over-dependent on health monitoring devices at home giving them a feeling of safety, which may lead to a reluctance to go out and leave the safety of their home behind. Besides, a growing culture of fear to leave one’s home due to perceived dangers in society may be further encouraged.

In order to make positive impact on people’s lives the technology and its application need to be *trusted, accepted, wanted, accessible and usable.* IoT must be prepared to avoid,

- the citizen failing to use the services (there are many potential causes for it, technology-related but also user-related)
- the citizen substituting completely face-to-face services (or moving significantly to virtual environments and unreal worlds),

- the citizen misunderstanding technology, especially its usefulness and impact on the main user, and
- the citizen mistrusting in the technology-based systems and services.

Gaining trust, acceptance, willingness and good understanding of accessibility and usability of such technology is very important for all the ICT users involved. Ultimately, ICT needs to be seen as a tool that connects people, provides alternatives or supports existing relations and not a technology that replaces personal relations. Therefore, any policy promoting the use of ICT for ageing should be underlined by this principle

Ethics and Internet of Things

Ethics and science & technology

Ethical inquiry, broadly understood, has always dealt with identifying the right guidance for human actions towards other and themselves [31]; therefore ethics has been concerned with the criteria to find out what is right and wrong, good and bad. In general, while pre-modern moral (and legal) philosophies have mostly found and founded these criteria in an objective natural order of things to which human beings (or even non-human beings and all entities) had to conform [32] the main (and still widely applied) modern philosophical systems have rooted ethical judgment in the human abilities related to rational reasoning and self-reflection. Some major modern philosophical systems (such as, though in different ways, the Kantian and the Benthamite) have directly justified the connection amongst rational, moral, and civic life by constructing humans as rational subjects, as moral subjects, and as members of a(n explicitly or implicitly assumed) "social contract", namely as entitled to interests and/or rights in a social life. Concepts flowing from these approaches such as human autonomy and dignity, or respect for human well-being are essential elements of contemporary democratic societies, and lie at the core of some fundamental human rights.

Common to these traditions is the assumption that human beings can access the knowledge necessary to augment their ability to make their judgments about good and bad course of actions in an autonomous way (namely free from all authorities, mundane or divine).

Even though several philosophical traditions have argued for other foundations of morality e.g. based on religious or ontological discourses, or on the non-rational but emotional character of morality, the term ethics (and ethics as an academic discipline), as different from morality, has been mostly characterized as the "rational inquiry" about values and reasons underlying human actions. This is especially true when the ethical discourse concerns science and technology as knowledge-based endeavours and their social developments.

In fact, the emergence of ethics as a public (and a publicly relevant) discourse and as a form of normativity at the interface between the private and the social dimension started at the end of World War II, when the failures of the scientific community's ethos in respecting individuals in research became tragically evident. Ethics has played an important role in dealing with concerns in the governance of emerging techno-scientific fields, where human rights and other values may be at stake.

This is why, in the early 1990's, ethics has also been given, in Europe and the US (and then in an increasing numbers of countries, as well as in national and international organizations), an institutional dimension through the establishment of ethics bodies (local and national committees and commissions). Starting with life sciences – followed by nano-sciences and technologies, synthetic biology, and other emerging technologies – ethics has increasingly become a normative "soft tool" with the tasks of analysing, improving, and promoting respect for rights and values (also encompassing the animal welfare and environmental values), as well as of contributing to integrate values in the legislative process. Moreover, ethics is also well established in the areas of European research and experimentation, and represents a necessary part of all research projects, with principles often directly stated by the law. Even though, with the entry into force of the TFEU at the end of 2009, European values and fundamental rights have become formally established, not only ethics has maintained its broader proactive meaning and role, but, despite its formal framing as non-binding policy advice, it has undoubtedly gained wider spaces – due to the largely undetermined outcomes of new technologies – and has also acquired the status of "indicator of normativity" making it similar to "soft law" in the governance of new emerging technologies.

Ethics & ICT

The ethical reflection about computers and computerized societies –later extended to all ICT— was started roughly in the same period of the ethics of biomedicine and the life sciences. Norbert Wiener, who is considered as a pioneer in computer ethical thinking, already in 1950 began to identify and analyse the impacts of information and communication technology upon human values like life, health, happiness, security, knowledge and creativity [33]. The literature that followed has been wide and diversified [34] [35] [36], with the emergence of the field of computer ethics and its unique nature in posing unprecedented problems [37]; reflections on global information ethics, and the issues at the interfaces between humans and machines, on artificial intelligence, robotics, the Internet, and all ICT.

However, despite these lively and prolonged debates, a major difference between ICT ethics and bio- or life sciences ethics was that no real need for an institutionalized approach to ethics has emerged in ICT until recently. The ICT domain has been regulated, at least in Europe, mostly through legal instruments. For a long time ICT normative issues have been primarily identified with privacy and data protection (and, with less emphasis with intellectual property rights); and legislation has widely taken care of these concerns by building a comprehensive legal framework –composed of both hard and soft laws (e.g. non-binding Opinions from Art.29 WP and EDPS).
Only more recently several relevant normative issues other than privacy have become apparent, and specific roles for ethics, especially in rapidly developing sectors (such as IoT), have been envisaged.

Another field requiring dedicated reflection is ICT research ethics – and IoT research ethics – that, for the time being, has been primarily, and definitely insufficiently, framed by borrowing principles from traditional biomedical ethics, and only by bearing in mind issues of interference between ICT and the human or animal body.

Ethics and Assistive Robotics

A specific chapter related to assistive robotics appears to be necessary due to the high intrusiveness level introduced by these ‘smart devices’ coming up to the IoT world and strongly affecting the privacy and intimacy of the citizens, namely for elderly people, as main target group for companion and assistive robotics in the near future. Domestic robots enter in our private spaces and their presence is more than a mere physical one. Usually they offer certain degree of autonomy and interaction with users, even some kind of intelligence and/or behaviour. It moves spontaneously and the user interface includes advanced techniques such as voice, image, and gestures, are offered to the user. This kind of robots is provided with natural verbal and non-verbal interaction, an embodiment, social *situatedness* (meaning that gestures and mimicking are correlated to the content of the human-robot dialogue) and even emotions. All these features make assistive robots be treated as living entities, and people interacting with them tends to treat them not as a technological device, but adopting them as companions.

VALUE AGEING[5] project (“Incorporating European Fundamental Values into ICT for Ageing: A vital political, ethical, technological, and industrial challenge”) is an ongoing European project aiming to investigate and better address social, ethical and value implications of ICT for ageing to advance the shared values and strategic vision of the EU towards the role of ICT for ageing societies, and with an special focus on assistive robotics. This project, focused on ethical recommendations, considers all aspects related to ICT field, including robotics, and its considerations can be surely extendable to the rest of population, further than elders or ageing constrains.

This project proposes in one of its public deliverables titled “Report on non-technological issues of assistive robot for elderly[6]” the starting points to define the minimum ethical consideration that an assistive robot should comply with. These starting points could reasonably be extended to any other ICT field in mind as described in *Table 1*.

[5] http://www.valueageing.eu/

[6] http://www.valueageing.eu/wp-content/uploads/2012/10/D2.4_Report_on_non_technological_issues_of_assistive_robots_for_elderly.pdf

Table 1 Ethical Principles

Respect for autonomy (right to liberty)	Dignity Informed consent
Non maleficence (avoiding harm)	Safety Social solidarity, inclusion and exclusion Isolation and substitution of human contact Discrimination and social sorting
Beneficence	Universal service Accessibility Value sensitive design Sustainability
Justice	Equality and fairness
Privacy and data protection	Collection limitation and retention Data quality Purpose specification Use limitation Confidentiality, security and protection of data Transparency Individual participation and access to data Anonymity Privacy of personal communications, monitoring and location tracking Privacy of the person Privacy of personal behavior

A good review of those ethical principles can be found in the "*Report on good practices, ethical guidance and designing a dialogue roadmap*" of the SENIOR Project[7]. All ethical principles applied to e-inclusion and ICT can also be applied to or exchanged with assistive robotics. This document also states that "*moral rights and duties of assistive robots may arise if the robot is perceived not as a simple functional machine, but as being provided with human-like features and behavioural patterns, in such a way that it can develop social interactions with humans. When speaking about human-robot relationships, an important concept is trust, as it is present in such kind of interactions (a person trusting someone or something means the possibility of not getting what he/she was expecting from the other, and therefore is betrayed). The precise behaviour (more or less complex) of autonomous robots is not completely known when the system is in the design phase. Their actions are generated when the robots are working, under circumstances that could be, or not, predicted at design time. As a consequence, their behaviour might be unexpected and out of control, thus affecting to the trust the owner had on it.*" The conclusion is that current assistive robots are far from being considered intelligent beings or have any moral conduct programmed. They are not able to take decisions on complex problems. But, in the future, the developments related to artificial intelligence (learning, reasoning, etc.) will bring us many open questions.

[7] SENIOR project. *Report on good practices, ethical guidance and designing a dialogue roadmap*. 2009. (Online: http://www.ifa-fiv.org/wp-content/uploads/2012/12/059_Report-on-good-practices-ethical-guidance-15-Nov-09.pdf)

Talking in terms of ethical approval and due to the mobility of robots, their capacities of navigation, self-location, obstacle avoidance, and potentially, decision-making by their own, some important recommendations are provided within VALUE AGEING reports:

- It must be capable of communicating the intention of doing something to the user, and this latter one must be able to cancel robot's intention.
- It must respect the personal space of the person (keeping a certain distance) to avoid the user feeling that the robot invades their intimacy and privacy. This behavior of the robot should be adjustably automatically by detecting the user's behavior and verbal and non-verbal emotions.
- It must include, of course, the guarantee of confidentiality and privacy of the data acquisition and communication.
- An option to switch off the robot completely must be provided.
- It should integrate a feature that allows the user ask the robot to hide away (for example, go to another room, disconnect cameras, etc.).

All these functions are relevant for the user in order to keep the dignity, privacy and intimacy without affecting safety issues (for example when the user has visitors in his/her home).

From ICT to IoT ethics

In the past decades, several emerging fields in applied ethics have been described as involving a radical paradigm shift in the approach to morality. This has been the case for bioethics [32], environmental ethics [38], and also ICT ethics [37] and [35]. Without entering in a theoretical discussion about these proposed foundations, it has to be recognized, however, that ICT display some special features, not necessarily involving a specific foundation for ethics, but certainly requiring some major revisions.

It has been widely recognized that, as "enabling technologies" which apply to, and interact with, all other technological fields, not only do ICT introduce, or deepen certain ethical concerns and reframe numerous techno-scientific fields, but directly affect and have the potential to reshape several human abilities and capacities in ways that are only partially foreseeable, not to mention controllable.

This potential for an "anthropological change," namely a conspicuous reshaping of some established assumptions and requirements about human knowledge, skills, behaviours, and expectations, already detectable in what has been defined "the networked self" [39], namely how the wide exposure of individuals to the Internet and social networks is reframing the way users cognitively, psychologically, and existentially reflect, respond to, and creatively interpret their connected lives. This is already a challenge for (primarily Western) cultures dominated, in the past three centuries, by individualistic and atomistic approaches to society and human relationships. As the phenomena of open knowledge, crowdsourced knowledge, and also crowdsourced funding are showing, individuals are progressing towards, and are equipped for, more connected and collaborative behaviour than existing ethical and legal concepts allow them to do [40] and [41].

IoT is magnifying the existing challenges to individual knowledge and human control of technological processes and the consequences of technology-mediated actions. In IoT the traditional modern construction of the subject – the subject of knowledge and the moral subject—, still pervading most current ethical and legal concepts [42], has to confront the complexities of the duty to know in context where knowledge can be limited, as well as the hybridized interactions between subjects and objects, agents and actors (object behaving subject-like).

The traditional assumptions embedded in rights and obligations – as well as in the way regulatory processes are framed and organized— about human knowledge, awareness, control, and capability to deal with uncertainties require major adjustments to cope with the complexities of new technologies. Already in 1979, in reflecting on the technological power acquired by humankind, the philosopher Hans Jonas [43] highlighted, in connection with the notion of responsibility, the new moral "duty to know" (before acting). He showed how the most prominent modern philosophies (such as the Kantian and Bentham's systems) did not require from participants to the social contract to be knowledgeable or expert; while this increased need for knowledge has become an essential element for contemporary life.

As to IoT, its paradox is that, while users are asked to know more, they also need to be aware that their knowledge is structurally limited. The radical uncertainty implied by the complexity of some emerging technology and, definitely by IoT has been described by the French epistemologist Jean-Pierre Dupuy as follows. "The key notion here is that of informational incompressibility, which is a form of essential unpredictability. In keeping with von Neumann's intuitions on complexity, a complex process is defined today as one for which the simplest model is the process itself. The only way to determine the future of the system is to run it: there are no shortcuts. This is a radical uncertainty" [44].

The task of creating an epistemic statute for the lack of knowledge may proceed hand in hand with a behaviour of active scientific wisdom, self-reflexivity, awareness of the value-laden dimensions of science, the intentions of making choices more legitimate and shared. In a similar way, responsibility should be rethought and reframed in order to connect individual and collective responsibility in terms of shared decisions and commitments [45]. Moreover, even though the concept is not discussed in relation to IoT, the current understanding of precaution goes beyond the idea of an emergency principle about science, while the concept of responsibility is expanding beyond liability and accountability. Precaution is democratically understood and endorsed as a form of responsible action, while responsibility is now depicted in worldwide policies on emerging technologies as the normative tool that brings precaution to individuals, making them self-reflexive about their actions. This tendency to reframe precaution also as an individual (and not only as an institutional) principle together with responsibility has several reasons, connected to the changes brought about by new technologies (such as nanotechnology and synthetic biology) and to how these are reshaping both the scientific community and society.

Some ethical hints for IoT

Several documents reflecting on the specificity of IoT ethics have highlighted and agreed on the following elements [46], [47] and [48].

- A separation between privacy and other ethical issues, primarily based on the fact that privacy is widely regulated (at least in part) by law, as opposed to other ethical issues arising from IoT.
- The focus on the need for more knowledge for citizens/users, framed as an ethical issue about education. Attention is also paid to metaphors used in the construction on knowledge about IoT, mostly reflecting and favouring a mechanistic, under control (and therefore reassuring), vision.
- Identity, autonomy (and informed consent), trust, and agency as specific concerns – often treated as separately identified issues.
- Other relevant issues concern the social digital divide, both as a problem of individual rights and of distributive justice.
- Human agency.
- Fear of increasing social isolation.

It may be useful to point out here that some further elements can be outlined and may be usefully discussed. For instance, freedom is not adequately expressed, and is mostly reduced to autonomy. However, freedom means more. Freedom is creativity, the capability of inventing and shaping reality and human acts in less constrained ways than those pervasively allowed by technological and digital architectures – and how this is going to affect human skills. It is the liberty to experience a more direct relation to reality processes in the making of things – while the increased distance from reality induced by virtualization can trigger unlearning. Responsibility is another item not sufficiently analysed in relation to users – whilst it is problematized, together with accountability, in relations to industry and institutions, especially as to its legal meanings and implications. IoT adds new challenges to the existing issues of individual moral responsibility in creating multiple identities and in shaping virtual behaviour [47].

Moreover, the broad concept of human agency [49] seems to have the potential to usefully connect the issues of identity, autonomy, and privacy (at least as to its ethical side). Widely defined, human agency refers to the human capacity to act as a subject rather than as a deterministic mechanism. It deals knowledge and awareness, freedom, control on thoughts and acts; and their human limits.

We refer to what is commonly described as "digital divide", describing other diffuse divides that the unauthorised and unquestioned automations, seamless transfers and unnoticed ubiquity featured by IoT may create due to overwhelming consent demands and lack of usability in the human-IoT interaction. The divide in this case is not exclusively related to lack of skill, but also to what we could call "consent fatigue", this posing additional challenges to individuals with reduced autonomy such as children and the elderly. With IoT, where the kinds of promised interconnectivity involve billions of entities (including people) and transactions for which mechanisms of authentication and consent need to be put in practice, consent may become an inapplicable concept. Those who are knowledgeable and skilled enough and empowered to control the working of the technology will master it, will be able to protect themselves against abuse, and to choose amidst the technological offer or opt-out if they deem it necessary. Hence, the rising divides in these cases have, paradoxically, implications for knowledge production, skills development and empowerment. Those who cannot keep the pace with the pervasiveness will progressively become deskilled, disempowered and unknowledgeable.

The viability of ICT solutions for an '*ageing well'* scenario which gathers a huge market depends on their appeal, usability, reliability, accessibility and affordability. To make ICT appealing to older people, the devices and services need to be tuned to their needs and abilities and the benefits of such solutions clearly articulated. The ICT products and services should provide users with an intuitive experience, aesthetically pleasing design, high reliability, and feelings of confidence and being in control. The issue of reliability is particularly important for telemedicine technologies, where the trust in reliability of the IoT devices and systems and the confidence on how the personal information is handled and communicated is essential for their adoption. Accessibility, especially in the relation to skills and access to hardware and software amongst the disadvantaged groups, and affordability are essential underlying factors[8].

This implies the necessity to raise awareness and to educate citizens/users in their relationships with IoT –a recommendation highlighted and shared by most documents on the Internet of Things [46] and [47]. Attention and awareness should be paid to the potential for passive acceptance of mechanical acting, and towards not reducing all normative issues to technical fixes. In other words, there is a need to prevent human agents from behaving just as "actants", namely as causal forces instead of intentional, responsible subjects.
The daily substitution of human-mediated relations with ICT-mediated forms of life to, as well as the transfer of most life aspects and decisions to ICT devices, can give rise to a situation where these automatic, invisible mechanisms hinder and impair the specific skills for moral experience, perception, and learning. Similarly to how the predominant and pervasive use of hand-typing is leading to a loss of handwriting ability, scholarly research is increasingly revealing that the deprivation of real life experiences and the prolonged exposure to virtual life are gradually de-sensitizing people to moral aspects of human relations (doing harm, non-respect, insensitivity to vulnerability) and making them unable to connect and integrate their virtual and non-virtual lives.

Even more, social isolation is one of the main concerns, especially for older people, producing not only negative emotional effects, but in some cases also leading to depression and accelerated physical decline. ICT technologies reduce the risk of isolation by facilitating communication with relatives and friends as well as assisting in meeting new people through social networks, work and learning opportunities. If used inappropriately, they have a potential to deepen social isolation and lead to exclusion. The loss of confidence in one's cognitive abilities - decreasing in competency as a result of overreliance on technology, and reduced willingness to engage with the outside world

[8] http://www.valueageing.eu/wp-content/uploads/2013/12/07AGE03_D3.6.1_FINAL-Executive-Summary.pdf

combined with an often exaggerated perception of dangers outside the home can lead to the development of a fear of going out.

The adoption of ICT technologies may decrease the need to go out leading to reduced opportunities for social interaction. This concern is strongly associated with telemedicine and telecare technologies. By satisfying most medical needs through home based solutions, older people's opportunity for interaction with the outside world may be further diminished. When introducing an assistive robot in the lives of an elderly (in their homes or when they are in nursing homes) similar but enlarged ethical issues arise. Whilst for young people that trend to social isolation might be an own decision, for elderly people that is just a fear, and even a threat, of losing human contact, of increasing social isolation in which many of them already live, of depersonalization in their personal assistance. The elderly can see an ICT and assistive robotics as a positive complement to their daily support, but not as a substitute of the human care, the human touch they need to keep on engaged to life.

In the IoT domain, the challenges to human acting become even more extreme. As explained in the previous section *Delegation of human autonomy in IoT*, "artefacts" can be introduced by devices and functionalities of an IoT smart environments in which the interface between humans and environment is progressively enhanced and the perception of the artefacts themselves is in some way reduced. Hermeneutic relations on the other hand refer to relations where the artefacts provide a representation of reality requiring interpretation, decisions being taken based on such interpretation (e.g. a thermometer, wearable sensor). With IoT both types of relationships are emphasised and hybridised; users are likely to stop "noticing" the artefacts (sensors, RFID tags, cameras, etc.) that communicate among themselves in autonomous ways, and at the same time through the algorithms and models driving their activity these artefacts encapsulate representations of reality and worldviews. This latter condition, amounts to a deeper form of not "noticing" technology; it is not only about the artefact but also, more importantly, about the invisibility of the interaction itself (data transfers, decision and action). Voluntarily or not, the user will need to rely on models and technology to achieve the chores that technology is meant to help her/him with. Hence, the strong mediation inherent to IoT developments, will lead eventually to shifting or delegation of human autonomy and agency to the objects of the IoT with potential risk to the privacy or even security of the users. If noticed, artefacts will act on the user's behalf; if not noticed artefacts will act on their developers' worldviews, intentionality and interests. This strong mediation poses challenges to human agency.

Spaces for ethics in the governance of IoT

In this respect, not only ethics as a soft law instrument should have room in the framework of IoT governance, but IoT governance seems to require an ethical commitment towards human agency. This should become an active commitment in IoT governance: the commitment towards a full concept of humanness and towards a "duty to preserve human acting."

This commitment towards human agency translates, in IoT governance, into focusing on the most fruitful integration between the technical and human dimensions. IoT governance should encompass a mixture of technological and normative approaches, by integrating and complementing human(ness) skills, specific ICT education and learning (digital human behaviour), and technological fixes.

Broadly speaking, techno-legal approaches are defined as "ethics-by-design," "rights-by design," "ambient law" [50]. By-design normativity consists of mechanisms "embedded within the entire life cycle of the technology, from the very early design stage, right through to their ultimate deployment, use and ultimate disposal" [51].

The idea is to integrate normativity into information and communication systems and solutions, which may encompass making procedural a variety of values that can be relevant to users/citizens. As, for instance, Schindler et al. [47] have highlighted, "ethical products" – from environmentally friendly to cruelty-free products – have shown how ethical values can be translated as a matter of preference in the marketplace, where different products compete to gain citizens' trust.

From this perspective, together with ethics by design, also "ethics in design" deserves attention in the governance of IoT. If "by-design" approaches explicitly aim to create built-in algorithms for law enforcement, "ethics in design" raises awareness about the processes through which values and norms become embedded in technological architectures. While ethics-by-design looks at how to technically transform values and rights into algorithms, ethics-in-design looks at the normativity of architectures to make value choices apparent and transparent. This approach may include, for instance, having "benevolence" embedded in technology and also opens the space for looking at the ethical education of "designers" in order to have them framing products and procedures according to a vision of what is "worth" [17].

Merging technical solutions (such as by-design measures, certifications and self-certifications, institutional and corporate digital memories) with trust-generating human behaviours (direct repeated experiences, consistent institutional and/or corporate behaviour, prolonged relationships and reliability, available information and reputation, etc…) can lead to "more robustly" trusted and effective digital relationships – together with more education and the development of new psychological skills specific to the digital world. An integration of human and technological dimensions in the governance of IoT is not only more legitimate (ethically and democratically), but it may also prove more effective. This is especially needed in IoT, where the traditional forms of "informed consent" are often not applicable, and other trust and trusted procedures have to be imagined [47].

This situation calls for a variety of normative and educational measures to be adopted. Engineers and ICT application designers should work together with ethicists and lawyers in order to build collective trans-disciplinary knowledge of the relationships between technology and normativity. Moreover, both normativity "by-design" and in-design" require establishing new forms of protection. Normativity consciously and unconsciously inscribed in, and embodied by, artefacts should be made explicit and transparent before and during the design phase, when normative decisions are taken and transformed into programs and functions [52] [53]. The spaces for ethics on IoT deserve spaces of debate that include citizenry and not only the promoters, developers, vendors of this vision. What is needed is much more than education; is engagement. The persons using these technologies should be entitled to have a saying in what values and by what social norms they want to live in the future and what legacy they wish to leave for others that will come.

Through time ethics has become a policy flexible tool capable of representing and serving different normative roles, and complementing legally binding instruments: a form of soft law [47], namely to those "rules of conduct which, in principle, have no legally-binding force but which nevertheless may have practical effects" [54]. And soft normativity has gained greater relevance as innovation is largely happening far from regulatory control, while the normative process for emerging technologies is taking place, both in the US and the EU, as a recursive "learning process" which, as such, needs structural flexibility [45].

The ethics challenges described in this section are described in section *Identification of challenges for Governance Security and Privacy in IoT.*

Map of FP7 projects in the cluster

Introduction

The objective of this section is to:

- provide a mapping of the deliverables of the FP7 projects to Ethics, Governance, Security and Privacy;
- identify and map the project results/technical solutions from FP7 projects in AC05, which can address Ethics, Governance, Security and Privacy and support the design and deployment of frameworks;
- describe the AC05 projects and their involvement in Governance, Security and Privacy aspects.

Map of deliverables from FP7 projects to Governance, Security, Privacy and Ethics.

Table 2 identifies the deliverables from the FP7 projects, which compose AC05 cluster.

Table 2 Map of FP7 project deliverables to AC05

Projects	Governance	Security	Privacy	Ethics
iCore	D2.4	D2.2, D2.3	D2.2, D2.3	D1.3
BUTLER	D4.1,D6.6	D1.2, D2.1,D3.1, D3.2, D2.4, D4.3, D5.1	D1.2, D2.1, D4.1, D5,2, D6.6	D4.1,D6.6
GAMBAS		D3.1.x, D3.2.x	D3.1.x, D3.2.x, D3.3	

IoT@Work	D2.1 (addressing)	D3.1, D3.2, D3.3	D3.1,D3.2, D3.3	
SPaCIoS		D2.1.1., D2.1.2,D2.3.1	D2.1.1., D2.1.2,D2.3.1	
RERUM		D2.x,D3.x, D4.1	D2.x, D3.x	D3.4 (Trust), D4.2 (Trust)
COMPOSE		D5.1.1, D5.2.1, D5.4.1, D5.3.1, D5.3.2, D5.4.2, D7.1.1	D5.2.1, D5.4.1, D5.4.2, D7.1.1	D7.1.1, D9.1.1, D10.3.1.1
OpenIoT		D2.2, D2.3 D4.2.1, D4.3.1, D5.2.1	D2.2, D2.3 D4.2.1, D4.3.1, D5.2.1	D4.3.2
Value Ageing	D2.4, D3.6.1			D2.4, D3.6.1
IOT6		D2.2	D2.2	

Map of the results/technical solutions from FP7 projects

Table 3 identifies the technical solutions from the FP7 projects, which compose AC05 cluster. A detailed description of the proposed solutions is provided in section Technological enablers and design solutions.

Table 3 Map of technical solutions proposed by each FP7 project

Projects	**Governance**	**Security**	**Privacy**	**Ethics**
iCore	Usage Control Toolkit	Usage Control Toolkit	Usage Control Toolkit	Best Practices-Guidelines
BUTLER		Authentication Solutions	Privacy Solutions	Survey on ethical use of IoT
GAMBAS		Policy-based access control,	Anonymised data	

		Secure distributed query processing	discovery	
IoT@Work		Capability Based Access Control		
SPaCIoS		Modelling, Validation and testing		
RERUM		Secure Self-Configuration Secure Object-2-Object Communication. Compressed Sensing (CS) Platform for Run-time Reconfigurability of Security (PRRS) Cognitive Radio (CR) inspired M2M communications (for availability of wireless communications)	Privacy Enhancing Technologies (PET) for adequate protection of citizen's privacy in Smart City applications.	Developing a model for the trustworthiness of information exchanged in the IoT based on security and reputation management mechanisms. Developing trusted routing overlays.
COMPOSE		Usage Control, Sticky policies, Static Analysis, Object Code and Source Code Instrumentation, Declassificati	Usage Control, Sticky Policies, Static Analysis, Declassification, Data Provenance, Security	

		on, Security Contracts, Data Provenance	Contracts	
OpenIoT		Access Control Server Module, Usage control for mobile applications	Implemented Role-Based Assignation Algorithm	Best practice Guidelines for mobile end users
Value Ageing	Value metrics. Creating a database of best practices.			Ethical recommendations.
IoT6		Support to security by using proxy to interface devices.	Mapping of device properties to IPv6 network addresses through identifiers, which are stored in protected areas.	

Projects contributing to AC05 cluster

iCore

The iCore cognitive framework is based on the principle that any real world object and any digital object that is available, accessible, observable or controllable can have a virtual representation in the “Internet of Things”, which is called Virtual Object (VO). The virtual objects (VOs) are primarily targeted to the abstraction of technological heterogeneity and include semantic description of functionality that enables situation-aware selection and use of objects. Composite virtual objects (CVOs) use the services of virtual objects. A CVO is a cognitive mash-up of semantically interoperable VOs that renders services in accordance with the user/stakeholder perspectives and the application requirements.

A complete description of the iCore framework is out of the scope of this position paper. Here, we will focus on the definition of the Usage Control Toolkit, which is an important element of the overall iCore framework to address aspects of Governance, Security and Privacy. The Usage Control Toolkit provides an open source collection of metamodels for specification of a computer system structure, behavior, information, context, and organizational roles. Such metamodels provide the foundation for security engineering tooling add-ons and metamodel extensions to address requirements of governance, security and privacy.

BUTLER

The goal of the BUTLER project is the creation of an experimental technical platform to support the development of the Internet of Things. The main specificity of the BUTLER approach is its targeted “horizontality”: The vision behind BUTLER is that of a ubiquitous Internet of Things, affecting several domains of our lives (health, energy, transports, cities, homes, shopping and business) all at once. The BUTLER platform must therefore be able to support different “Smart” domains, by providing them with communication, location and context awareness capabilities, while guaranteeing their security and the privacy of the end users. The issue of security and privacy is therefore central in the BUTLER project and has to fulfill several requirements. The main ones are reported below:

- well known issues of data security, both at data storage level and data communication levels exist in IoT applications. The diversity and multiplicity of the “things” connected by the internet of things, and of the data exchanged further amplify and complicate these requirements;
- the applications enabled by the Internet of Things may pose additional privacy issues in the use that is made of the data. From the collection of data by the applications (which should be conditioned by an “informed consent” agreement from the user), to the profiling, exchange and sharing of these data necessary to enable true “context awareness”.

Data technical protection mechanisms include two major aspects. One is the protection of the data at data storage, the other one the protection of the data at communication level. The protection of data at communication level is one of the major areas of research. Many communication protocols implement high level of end-to-end security including authentication, integrity and confidentiality. At communication level, the major issue is the deployment process of the security keys and the cost of the required hardware and software environment to run the security algorithms in efficient and secure way.
However, Privacy and Security do not only refer to security of the exchange of data over the network, but shall also include: a) Protection of the accuracy of the data exchanged, b) Protection of the server information, c) Protection of the usage of the data by explicit, dynamic authorization mechanisms, d) Selected disclosure of Data and e) The implementation of “Transparency of data usage” policies.

The BUTLER project also addresses the Security and Privacy challenges from the point of view of their implication on business models. To specify the horizontal IoT platform envisioned in BUTLER, the project started from the gathering and analysis of the requirements from up to 70 use cases. The analysis of these use case not only produced requirements for the specification of the platform but also valuable information on the potential socio-economic impact of the deployment of a horizontal IoT and on the impact on the associated business models.

If treated accordingly, the ethics and privacy issues transforms from a threat to an opportunity. Better understanding of the service by the user increase

acceptance and create trust in the service. This trust becomes a competitive advantage for the service provider that can become a cornerstone of his business model. In turn the economic interest of the service providers for ethics and privacy issues, derived from this competitive advantage, becomes a guarantee for the user that his privacy will be respected.
The involvement of end users in proof of concepts and field trials is another specificity of the BUTLER project. The end user involvement is key to validate not only the technical qualities of the BUTLER platform (technology feasibility, integration and scaling) but also to assess the perception of end user and their acceptance of the scenario envisioned for the future “horizontal” IoT.

However the involvement of end user in the scope of the project requires handling their data and privacy concerns carefully. The following issues must be considered in the organization of end user involvement: a) technical security mechanisms must be set up to ensure the security and privacy of the participants. This involves secured data communication and storage, and in the scope of the BUTLER project these are addressed by the enabling security technologies developed and integrated in the BUTLER platform; b) the participants must be well informed of the scope and goal of the experiment. In the case of BUTLER, this involves specific efforts to explain the scope and goal of the project to a larger public; c) The consent of the participants must be gathered based on the information communicated to them. The consent acknowledgment form must remind the participants of their possibility to refuse or withdraw without any negative impact for them; d) finally both a feedback collection and a specific complaint process have been designed to offer the possibility to the participants to raise any issue identified.

BUTLER provides an Authorization Server as a security service path distinct from the application path. The Authorization Server and the managed resources share bootstrap security credentials enabling generation of session keys. The Authorization Server authenticates user and application for providing the application with access token and session keys for accessing a specific resource.

The protocol is based on OAuth2.0, already used by Facebook and Google, and identified as a mature technology used for Identity Management (see Identity management section).

The Identity Management is a new security and privacy service provided by the Authorization server that also enables the pseudo-naming.

BUTLER provides a lightweight bootstrapping mechanism between the sensor nodes and the gateway at Wireless Sensor Network (WSN) level based on the use of asymmetric cryptography with the elliptic curves. This can address the challenge of Device authentication. This lightweight bootstrapping handshake is designed for large scale deployment of sensor devices, which can also address challenge Secure Setup and Configuration.

The joint use of the Authorization Server at application level and of the bootstrapping mechanism at WSN level enables to address end-to-end and hop-by-hop security problem between a sensor node belonging to the IoT domain and an end-user application connected on Internet. The gateway located at the border between the Internet world and the WSN domain ensures the communication standard interoperability. For the hop-by-hop security mechanism, the gateway authenticates to the Authorization Server in the Internet world and the sensor node bootstraps to the gateway in the WSN domain. The security credentials generated by the Authorization Server could be pushed by the gateway to the sensor node. This mechanism may be useful for mobility scenario. For the end-to-end security mechanism, the sensor node authenticates to the Authorization Server to retrieve the security credentials.

BUTLER provides also a threat analysis model that could be used to evaluate the threat on dedicated use cases and scenarios.

Finally BUTLER strongly supports information-theoretic security at the physical layer to increase the privacy of wireless communications due to its achievable characteristics: unbreakability, provability, and quantifiability. Information-theoretic security is stronger than traditional computational security because no assumptions on the computational power of the eavesdropper are needed and perfect secrecy can be theoretically achieved [55]. On these bases, BUTLER proposes in particular a concrete implementation of secret key generation for short-range communication systems, introducing the concept of geometric secrecy.

GAMBAS

The GAMBAS project develops an adaptive middleware to enable the privacy-preserving and automated utilization of behaviour-driven services that adapt autonomously to the context of users. In contrast to today's mobile information access, which is primarily realized by on-demand searches via mobile browsers or via mobile apps, the middleware envisioned by GAMBAS enables proactive access to the right information at the right point in time. As a result, the context-aware automation enabled by the GAMBAS middleware will create a seamless and less distractive experience for its users while reducing the complexity of application development.

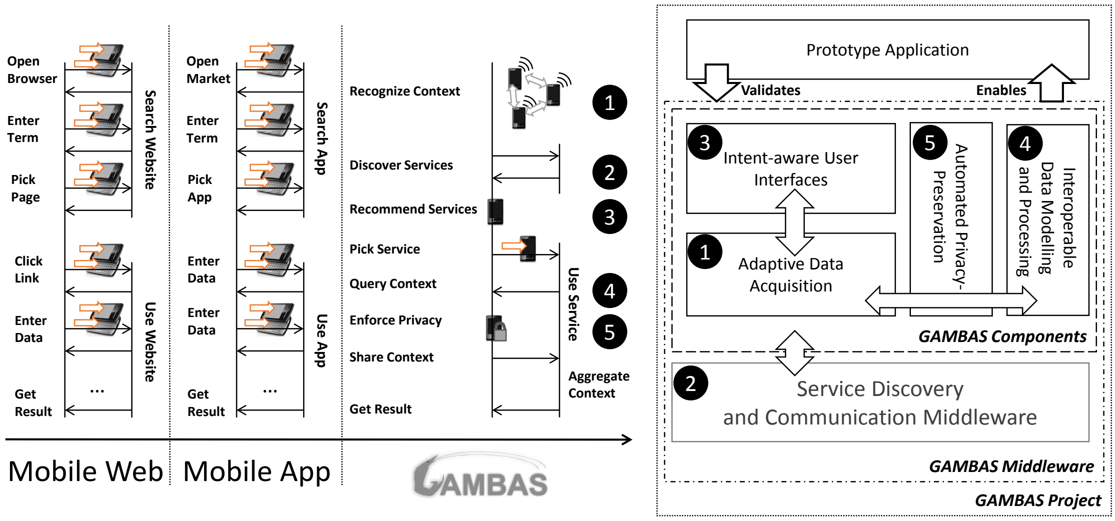


Figure 2 GAMBAS Middleware

As indicated in Figure 2, the core innovations realized by GAMBAS are the development of models and infrastructures to support the interoperable representation and scalable processing of context, the development of a generic, yet resource-efficient framework to enable the multimodal recognition of the user’s context, protocols and mechanisms to enforce the user’s privacy as well as user interface concepts to optimize the interaction with behaviour-driven services.

From a security and privacy perspective, the developments in GAMBAS are centred on a secure distributed architecture in which data acquisition, data storage and data processing are tightly controlled by the user. Thereby, security and privacy is based on the following elements:

- Personal acquisition and local storage: The primary means of data acquisition in GAMBAS are personal Internet-connected objects that are owned by a particular user such as a user’s mobile phone, tablet, laptop, etc. The data acquired through the built-in sensors of these devices is stored locally such that the user remains in full control. Thereby, it is noteworthy that the middleware provides mechanisms to disable particular subsets of sensors in order to prevent the accumulation of data that a user may not want to collect and store at all.
- Anonymized data discovery: In order to enable the sharing of data among the devices of a single user or a group of users, the data storages on the local device can be connected to form a distributed data processing system. To enable this, the GAMBAS middleware introduces a data discovery system that makes use of pseudonyms to avoid revealing the user’s identity. The pseudonyms can be synchronized in automated fashion with a user defined group of legitimate persons such that it is possible to dynamically change them.
- Policy-based access control: To limit the access to the user’s data, the networked data storages perform access control based on a policy that can be defined by a user. In order to reduce the configuration effort, the GAMBAS middleware encompasses a policy generator tool that can be used to derive the initial settings based on the user’s sharing behaviour that he exhibits when using social services.

Secure distributed query processing: On top of the resulting set of connected and access-controlled local data storages, the GAMBAS middleware enables distributed query processing in a secure manner. Towards this end, the query processing engine makes use of authentication mechanisms and encryption protocols that are bootstrapped by means of novel key exchange mechanisms that leverage the existing web-infrastructure that is already used by the users.

SPaCIoS

The vision of the Internet of Services (IoS) entails a major paradigm shift in the way ICT systems and applications are designed, implemented, deployed and consumed: they are no longer the result of programming components in the traditional meaning but are built by composing services that are distributed over the network and aggregated and consumed at run-time in a demand-driven, flexible way. In the IoS, services are business functionalities that are designed and implemented by producers, deployed by providers, aggregated by intermediaries and used by consumers. However, the new opportunities opened by the IoS will only materialize if concepts, techniques and tools are provided to ensure security.

State-of-the-art security validation technologies, when used in isolation, do not provide automated support to the discovery of important vulnerabilities and associated exploits that are already plaguing complex web-based security-sensitive applications, and thus severely affect the development of the IoS. Moreover, security validation should be applied not only at production time but also when services are deployed and consumed.

Tackling these challenges is the main objective of the SPaCIoS project, which has been laying the technological foundations for a new generation of analyzers for automated security validation at service provision and consumption time, thereby significantly improving the security of the IoS. This is being achieved by developing and combining state-of-the-art technologies for penetration testing, security testing, automatic learning, model checking, and related automated reasoning techniques.

More specifically, in SPaCIoS we have been developing both techniques for property-driven security testing, a variant of testing that applies techniques that make security properties (e.g., confidentiality and authentication) testable, and techniques for vulnerability-driven testing, where tests or test strategies are derived from vulnerabilities (e.g., XSS) that are likely to invalidate the security goals. Automated support to these testing activities is being achieved by generating test cases with model checking and related automated reasoning techniques, applied to a (possibly inferred) model of the System Under Validation (SUV), the security goals, and a model of the attacker. The possibility of applying model checking for this purpose has been investigated in the predecessor project AVANTSSAR, which developed the AVANTSSAR Platform, which comprises SATMC and the other model checkers CL-AtSe and OFMC, and successfully applied it the verification of Internet protocols, most notably leading to the discovery of a vulnerability in the specification and then in the actual implementation of the SAML-based Single Sign-On for Google Apps.

These techniques are all being implemented and integrated into the SPaCIoS Tool, whose architecture is depicted in Figure 10 In its main workflow, the tool takes as input a formal description of the SUV, the expected security goals, and a description of the capabilities of the attacker, and automatically generates and executes a sequence of test cases on the SUV through a number of proxies (e.g., http-proxies). Other workflows of the tool are possible.
We have been applying the tool as a proof of concept on a set of security testing problem cases drawn from industrial and open-source IoS application scenarios, thereby paving the way to transferring project results successfully to industrial practice (e.g., to the business units of SAP and Siemens, who are project partners) and to standardization bodies and open-source communities.

RERUM

The main objective of RERUM is to develop, evaluate, and trial an architectural framework for dependable, reliable, and secure networks of heterogeneous smart objects supporting innovative Smart City applications. The framework will be based on the concept of “security and privacy by design”, addressing the most critical factors for the success of Smart City applications.

The rapid growth of cities aggravates many challenges associated with living in urban environments. The IoT paradigm has been suggested as a solution. The key challenge for IoT towards Smart City applications to ensure its reliability. For RERUM reliability incorporates many intertwined areas including issues of security, privacy, availability, robustness and flexibility towards changing environmental conditions. Without guarantees that Smart City IoT objects are:

- sensing the environment effectively, efficiently, timely, and trustworthily,
- exchanging the information securely,
- safeguarding the privacy of human input and object sensed information,

users are reluctant to adopt this new technology that will be a part of their everyday lives, which results in a decrease of the market value of Smart City applications for the service providers.

The ultimate goal of RERUM is to allow IoT to become the fundamental enabler towards a *truly smart* City, having the citizen at the centre of attention. The work will be driven by the requirements of the target Smart City applications and by an assessment of the threats and open security issues in existing IoT frameworks for Smart Cities.

RERUM aims to develop a framework which will allow IoT applications to consider security and privacy mechanisms early in their design phase, ensuring a configurable balance between reliability (requiring secure, trustworthy and precise data) and privacy (requiring data minimization for private information, like location). The RERUM framework will comprise architecture, built upon novel network protocols and interfaces as well as the design of smart objects hardware.

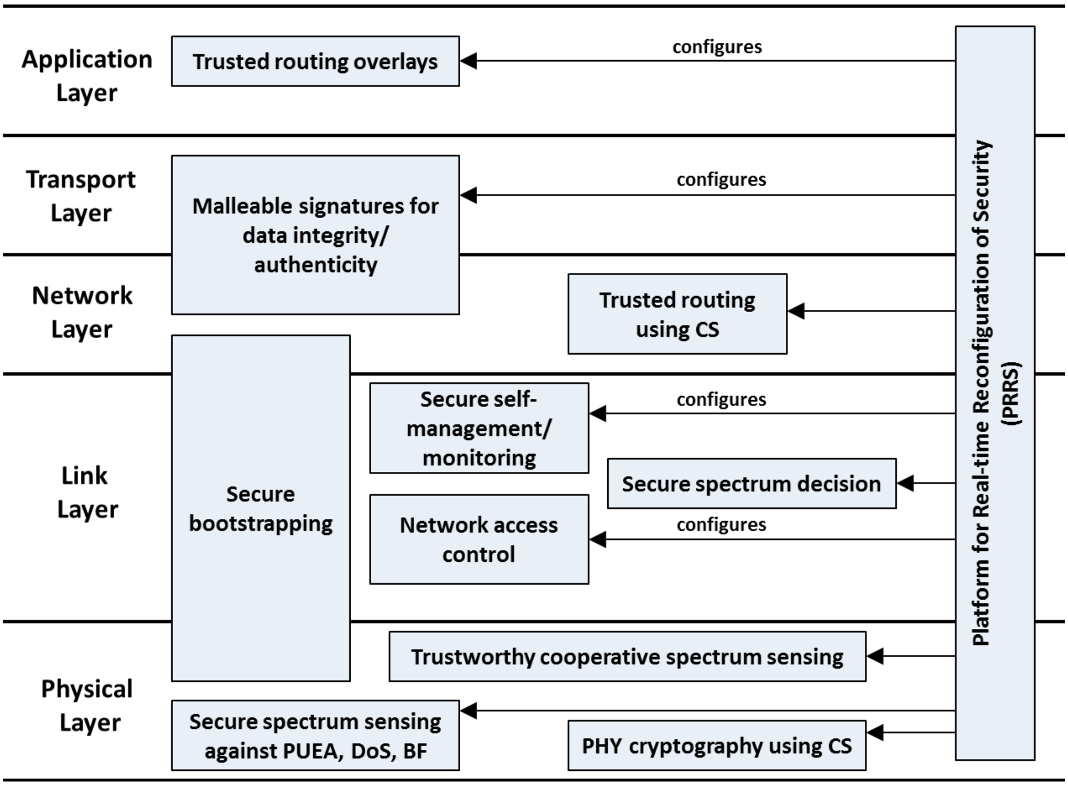

Application Layer
Trusted routing overlays
configures
Transport Layer
Malleable signatures for data integrity/ authenticity
configures
Network Layer
Trusted routing using CS
Secure self-management/ monitoring
configures
Link Layer
Secure bootstrapping
Secure spectrum decision
Network access control
configures
Physical Layer
Trustworthy cooperative spectrum sensing
Secure spectrum sensing against PUEA, DoS, BF
PHY cryptography using CS
Platform for Real-time Reconfiguration of Security (PRRS)

Figure 3 Foreseen Technologies of RERUM affect all layers of the ISO/OSI stack, but RERUM's focus lies on lower layers

Figure 3 shows RERUM's technologies and illustrates the project's understanding of the privacy- and security-by- design paradigm. RERUM's architecture will be configurable, suiting a wide range of applications, not limited to the domain of Smart Cities. Following the "privacy-by-design" approach RERUM will question current technology focussed design decisions in the light of privacy. RERUM's goal is to allow application designers to increase the privacy of the users, via data minimization, with the smallest possible impact on functionality, the so called "privacy-by-design positive sum" [56].

The work will follow an iterative approach starting from an initial definition of the architecture and the respective mechanisms that will be refined as the work progresses in order to mitigate any identified issues. The project's key scientific areas of focus are:

- security, privacy and trust in IoT-based smart objects;
- information security and privacy in smart city applications;
- reliable interconnectivity of smart objects based on Cognitive Radio;
- energy efficient operation of smart objects;
- performance and scalability analysis of IoT;
- Smart City applications.

RERUM considers four smart city applications to drive the requirements for system development and these will be developed and tested in the trials: Smart transportation, environmental monitoring, home energy management and indoor comfort quality monitoring.

IoT@Work

The IoT@Work project focused on harnessing IoT technologies in industrial and automation environments in order to realize the so-called Plug-and-Work (i.e. seamlessly addition and configuration) of production units.

The IoT@Work project adopted a Capability Based Access Control mechanism[9] for managing access control (including rights delegation) to some of the project's services and, specifically, to its Event Notification Service (ENS) middleware [57].

Capabilities are communicable and unforgeable tokens of authority. By virtue of the possession of a capability token, a process/subject can access a resource/service exercising the rights that the capability token grants. A capability based access control and rights delegation approach has the following advantages:

- the Principle of Least Authority (PoLA) is the default
- supports a more fine-grained access control
- less security issues (no Confused Deputy problem)

[9] The software is available as open source (Apache License 2.0) at http://code.google.com/p/txt-iot-technologies/

- externalizes and distributes the management of the authorization process
- no issues related to the complexity and dynamics of identity management

The IoT@Work capability based approach supports: access right delegation, capability tokens revocation, fine-grained access rights. Token elements are based on the SAML/XACML standards (with some extensions). The following figure provides an overview of the capability based access control mechanism developed in the IoT@Work project.

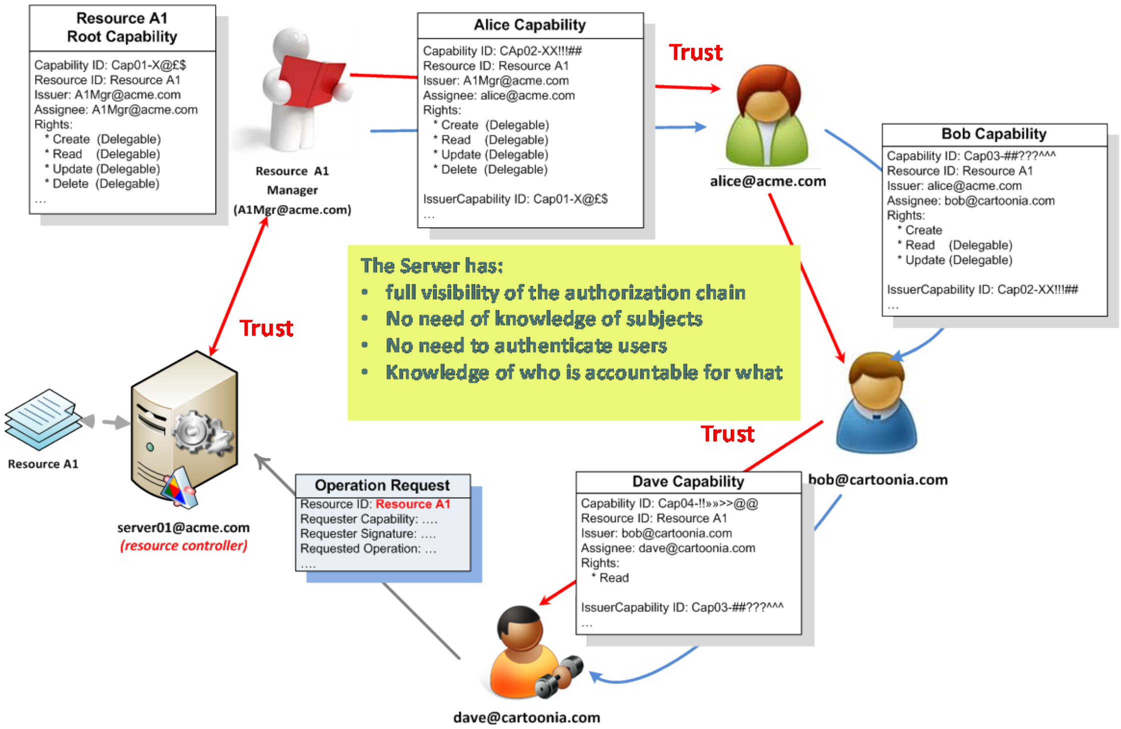


Figure 4 CapBAC authorization

As evident from the figure, each subject has its own capability token that states what rights (e.g., operations) that subject can exercise on a given resource (identified via an URL).

The *Resource Manager* (e.g., a system administrator) creates a first capability token (*Root Capability* in the picture) that assigns rights (as well as if it can delegate these rights) to itself as the owner of the capability (i.e., who can exercise the rights stated in the capability) on resource(s) (the resource is identified via URLs). The capability token contains other information (e.g., the validity period of the capability, the issuer, etc.) and is digitally signed by the issuer (for a *Root Capability* is the *Resource Manager*). The server that is in charge of managing access to the specified resource has to trust the *Resource Manager* and, therefore, its *Root Capability*.

The *Resource Manager* can generate new capability tokens for other users (e.g., for *Alice* in the figure above) using its *Root Capability*, granting them one or more of its rights. It can also flag some or all of the granted rights as delegable so they can create further capability tokens on their own (e.g., *Alice* issues a new capability for *Bob* granting him a subset of her rights). The new capability token has to be digitally signed by the issuer (e.g., by the *Resource*

Manager for the *Alice* token, by *Alice* for the *Bob's* one, etc.) and includes the capability token of the issuer. Each subject in the delegation chain can freely create (and takes responsibility) as many capabilities as required if it has the right to delegate some of its rights.

A subject (e.g., *Dave* in the picture) that needs to access a resource must provide with the access request its own capability token (e.g., *Dave Capability* in the picture) and prove it is the owner of the presented capability token (e.g., digitally signing the access request). The Resource Manager must perform the following checks to decide whether to accept or deny an access request:

- the presented capability and its authorization chain are correct (e.g., the *Dave's Capability* is well formed and its digital signature is correct, then that the *Bob's Capability* is correct and the links between the *Dave's* and *Bob's* capabilities are correct, up to the *Root Capability*)
- the access request is within the scope of the presented capability
- the access request is signed by the requester.

The capability tokens are XML documents based on the *Security Assertion Markup Language* (SAML) and *eXtensible Access Control Markup Language* (XACML) standards (with some extensions).

The IoT@Work access control mechanism envisages the possibility to revoke a capability token before its expiration date to address issues related to changes of subject's roles or in an organization, compromised certificates, etc.
The revocation mechanism assures that only properly authorized subjects can revoke issued capability tokens (see [12] for more details). The mechanism, as described in [12], can even support encrypted and anonymous capability tokens to improve confidentiality and privacy.

COMPOSE

Main goal of the Collaborative Open Market to Place Objects at your Service is to simplify the development of Applications for the Internet of Things. For this purpose, COMPOSE takes a similar approach as iCore and abstract from physical *things* and models them as virtual entities, so called service objects. They are simple units which can generate data for further processing and can be composed into units performing more complex data processing tasks. Service objects also represent actuators which can receive control data.

Service objects interact with services. The latter are entities with more complex program logic provided by developers. Comparable to service objects, services can also be composed, manually or automatically by a composition engine. Services run in the COMPOSE platform which is implemented by a cloud. Further, the project offers an integrated SDK and an IDE to support the development of new service objects or services and also of applications. Applications are offered to users of the COMPOSE platform through a marketplace. They interact with services and/or service objects and are executed on different platforms, e.g. web-servers or smartphones.

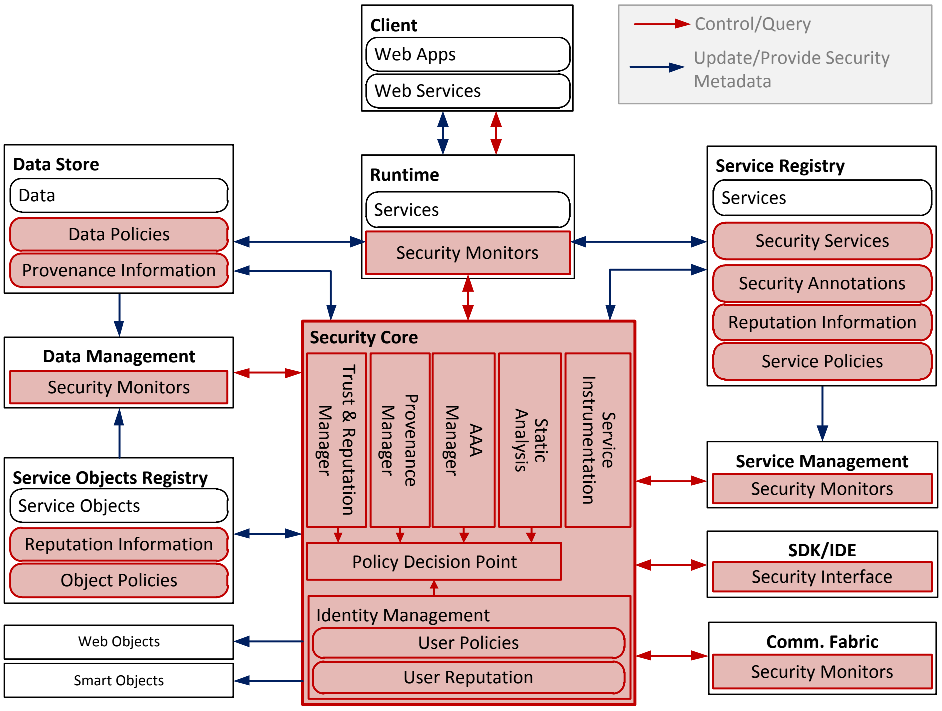


Figure 5 COMPOSE Security architecture

The security framework in COMPOSE (see *Figure 5*) takes a different approach which accounts for the high flexibility required for new IoT applications and the diverse user needs for security and privacy.

Instead of only defining coarse-grained security policies for service objects or services, our security framework will be controlled by fine-granular data security policies. Static analysis will allow us to generate information flow details for service objects and services. This allows us to identify potentially non-compliant flows. Using a set of security primitives and security services which are provided by the platform, we instrument source code in order to generate services which are compliant with as many security policies as possible and with as little user interference as possible. Contracts which describe pre-conditions, effects, and flows within a service or API will support this task. To also cover security policies and program logic which describe undecidable properties, we use selective runtime monitoring.

Further, the project also involves user feedback, and the monitoring of functional as well as non-functionality to accumulate reputation about service objects, services, developers, and other principals in COMPOSE. These mechanisms support developers and users during the decision process which applications should be deployed in their scenario.

Finally, COMPOSE also uses data provenance, to record the origin of data and the operations performed on them, by which entity, and at which point in time. While the collection of such data is obviously privacy critical, it can help to enforce more complex security policies, e.g. Chinese wall policies, prevent attempts to link data and perform in depth information retrieval, or it can be used to identify misbehaving services. So, with appropriate privacy preserving techniques and the assumption that the cloud provider is trusted, the user can benefit from the collection of data provenance information.

OpenIoT

OpenIoT is an open source middleware for getting information from Internet connected devices, sensor networks, or simply sensors connected to the Internet and allows you for deploying and executing new intelligent services without worrying what exact “things” are used for provisioning the services. The open source OpenIoT project is offered as implemented reference framework enabling a new range of large-scale intelligent and dynamically defined Internet of Things applications, by following cloud computing delivery models. The provided open source middleware framework enable on the fly deployment of services and dynamic provisioning of particular use cases based on cloud/utility-based infrastructure. OpenIoT can easily deploy particular use IoT cases related to smart cities, intelligent manufacturing and smart agrifood through responding to appropriate end-user requests enabling the dynamic, self-organizing and self-managing of cloud environments using IoT sensor data. The OpenIoT middleware framework therefore serves as a blueprint for non-trivial IoT applications, according to a utility cloud-based support model.
OpenIoT addresses the following key research issues:

- **Autonomic**: OpenIoT establishes a dynamic formulation of utility-based services for Internet-connected objects (devices, sensors, objects), following on the fly defined end-users’ requests.
- **Cloud/Utility Based**: OpenIoT applications are provided as a service (e.g., Sensing-as-a-Service) over dynamically created and configured societies of “things” and according to a utility cloud computing model “pay-as-you-go” model.
- **Open Source and Royalty free**: OpenIoT is offered as an open royalty free implementation. To this end, OpenIoT is implemented and where applicable extending existing popular open source middleware platforms (e.g. the Global Sensor Networks (GSN) platform.
- **Dynamic**: OpenIoT establishes a dynamic orchestration of internet-connected objects and related resources in cloud environments. This dynamic orchestration enables response to dynamically defined end-users’ service requests.
- **Optimal and Self-Managing**: OpenIoT platform continues working to optimise associated energy efficiency and bandwidth resources constraints mainly for cloud environments.
- **Scalable**: The OpenIoT framework supports IoT applications involving trillions of things, which are geographically /administratively dispersed (as part of inter-domain environments).
- **Secure, trustworthy and privacy friendly**: OpenIoT is endowed with inherent security, trustworthiness and privacy friendliness. The project investigates the economics of privacy and security with a view researched utility metrics of the cloud infrastructure.
- **Mobility**: OpenIoT will enable continuous detection of mobile data produced by the “things”, which can be used to support continuous service feedback. . The goal is to offer a generic method mobile sensor data for both centralized and distributed environments.
- **Quality of Service negotiation and adaptation.** OpenIoT will offer advanced and interactive services, with focus on complex QoS constraints and the problems related to QoE in heterogeneous all-IP environments and converged 3GPP networks.

OpenIoT Architecture is comprised by seven main components as depicted in *Figure 6*. The Sensor Middleware, the Cloud Data Storage, the Scheduler in conjunction with Discovery Services functionality, the Service Delivery and Utility Manager, the Request Definition, the Request Presentation and the Configuration and Monitoring, all of them secure-enabled by the Trust-Module (TM).

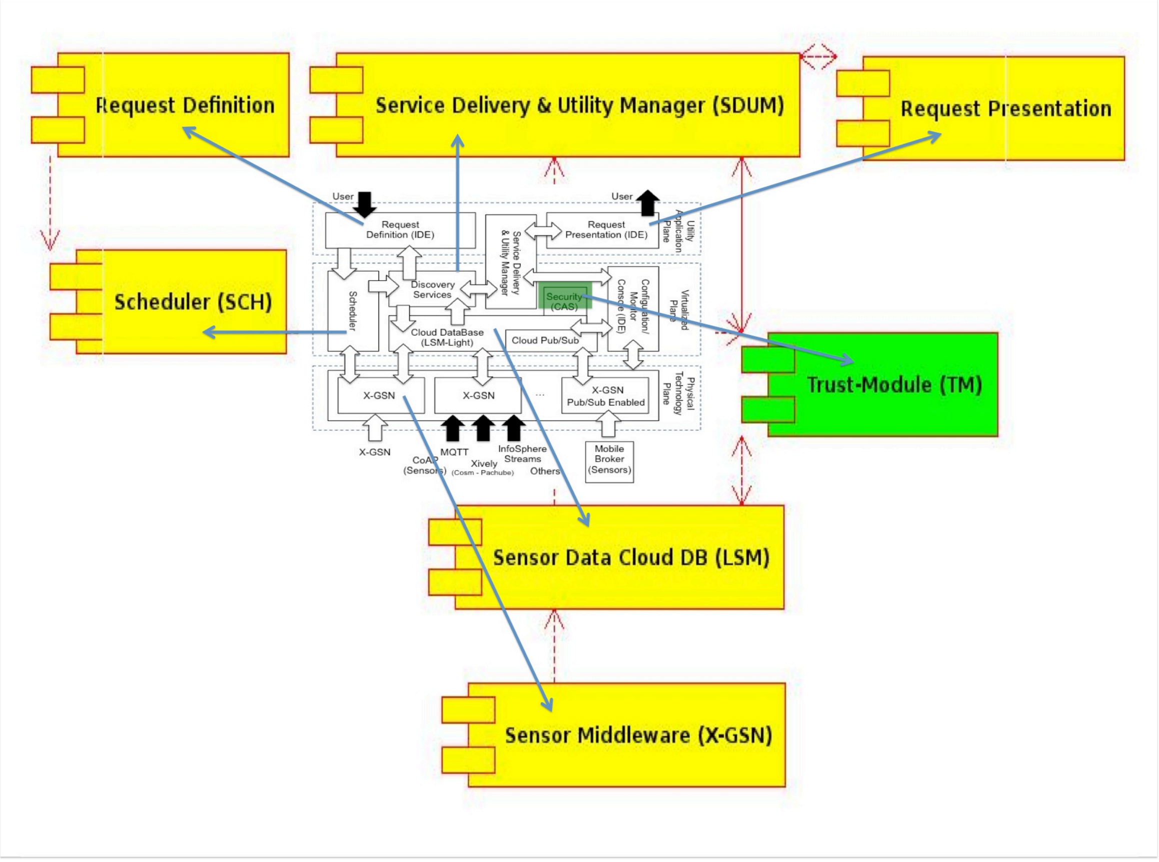


Figure 6 OpenIoT Security Access Control via Trust-Module (TM).

Privacy and Security is the baseline service formulation mechanisms of OpenIoT support role-based authentication and authorization, towards ensuring authorized access to sensors and services. The Trust-Module (TM) contains all the metadata descriptions for secure Authentication using OpenIoT 2.0 principles for the role-based algorithms. TM is defined as part of the Control Access Server (CAS) using OAuth2.0 [58] among main Core Components Functional Blocks. In addition to these mechanisms, the OpenIoT middleware uses utility-driven privacy and security mechanisms as part of Privacy and Security activity of the project.

A prominent gap in the IoT research arena is the lack of open source implementations of integrated IoT middleware functionalities, which could boost the wide adoption of IoT applications beyond early realizations and open-source projects such as Global Sensor Networks (GSN)[10]. Likewise it is evident the lack of a trusted, structured, configurable and integrated middleware solution for the cloud-based delivery of IoT services and OpenIoT aims at researching and providing the privacy and security module (following OpenID [59]) for this as an approach. OpenIoT rely on open source

[10] Global Sensor Network project, http://sourceforge.net/apps/trac/gsn

implementation for an IoT stack for cloud-based delivery. To this end, OpenIoT will continue on researching about possible exploitable open source background technology/projects that can be integrated in the OpenIoT middleware.

Value-Ageing

Value Ageing project builds upon the key principles of the SENIOR project[11]. Value Ageing is not a technological project but a multi-disciplinary industry-academia partnership and pathways action incorporating European fundamental values into ICT for ageing. So it's focused on how to manage ethics issues when technology, especially ICT, is involved in the solution provision. Good technology is not just about making something better; it is about doing something different and consequently making people think differently. Everybody should understand both the way in which existing values are driving technology innovations, and how technology in its turn is changing people's standards. Social scientists and ethicists should learn from technologists, and in their turn technologists should learn from scholars working on human values.

Consequently, this Value Ageing project deepens into a vital, political, ethical, technological, and industrial challenge, aiming to foster cooperation between non-commercial and commercial entities on a joint research project about the incorporation of Fundamental Values of the EU in ICT for Ageing. It offers a vital instrument to incorporate fundamental EU principles in industrial strategies and technological awareness in policy setting.

Basically, it focuses on "incorporating ethics in technology". Technology is not merely a means to an end; technical standards define major portions of social environments, human activities, life patterns, and so on. Values and policies are "frozen" in technology solutions. Embedding ethics and social considerations in technology implies understanding how technology is impacting society, what values are communicated to users by a technology or technological application, how technology choices are made at various decision making levels, and how different values can be built in technology by selecting different technological solutions and design options.

By means of (1) carrying out a comprehensive fact finding exercise; (2) developing specific metrics, and creating a database of best practices; and finally (3) identifying, evaluating, displaying and distinguishing alternative policies; one important final result, by the end of 2014, is already being a full set of facts and recommendations at all levels to integrate ethics into ICT:

- ICT developments impacting on dignity and non-discrimination of older citizens,
- ICT developments impacting on freedom and autonomy of older citizens,
- ICT developments impacting older people's living conditions and environment

[11] Value-Ageing project: http://www.valueageing.eu/senior-project/

- Corporate Social Responsibility (CSR), and Ethical Codes in ICT for ageing,
- Scenario exercise (supporting policy makers and technology developers for the interaction between end-users and ICT technologies)
- Best Practices identification, analysis and collection, and Governance issues and policy options.

IoT6

IoT6's main concerns are with how IPv6 can contribute to IoT. Aspects of governance, security and privacy are addressed in [60]. The main focus is on studying applications in smart buildings – mainly using legacy equipment. Thus one activity has been developing mechanisms where the properties of the legacy systems can be translated into IPv6 addresses. Gateways, with the least significant 64 bits of the IPv6 address being used in the mapping. Because the least significant bits are used, this mapping has no impact on the Internet routing to the gateway. A system called Glowbal was developed to deal with this mapping algorithmically for different technologies. This allowed the automation of the addressing of the legacy technologies using only IPv6 address features [61]. Another feature of our approach has been to store the properties of the gateways in a resource discovery system called Digcovery [62]. This has interfaces to different database systems which are used in different domains like cloud computing, mobile telephony and RFID - facilitating their being used together. Sophisticated Use Cases have been developed in this environment, but the earlier work did not include much on security. This was partly because the legacy systems themselves had little or no provision for secured operation, because they worked mainly in the local environment. There was some work on the strain that certain encryption algorithms would put on constrained devices. Also in D3.1 [63] some aspects of authorization related to Digcovery functionalities were considered. Finally, in D2.3 [64] also included some implementation and evaluation of IPsec and a lightIPsec version for Contiki in order to provide support for secure and mobile communications.

Recent work has continued, of course, along the original directions, but a parallel stream has developed [65]. It was realised that the IP addresses were often stored in DNS stores. These had the great advantage of being globally accessible, and the DNS system has been shown to be able to scale to very large numbers of devices. Moreover, recent work on DNSSEC has shown how the addresses could be authenticated. At the same time, the DNS has no confidentiality on its addresses; anybody can access it. There has been a concern that as a result, mechanisms like the use of IPv6 address features to express properties of end devices, might reveal too much about these devices to unauthorised users. In addition, the use of address features to express properties of different technologies, might compromise the jurisdiction of address space management, which is currently the province of IANA, the Internet Registries and the IETF. As a result these proposals might encounter strong opposition.

Partly for the above reasons, and partly in order to address security and scaling in a more homogeneous and holistic manner, recent work in IoT6 has also pursued another track. Instead of concentrating on IPv6 addresses, it has considered systems based on identifiers. Partly because of the limited resources at our disposal, and partly because of the excellent fit with the security and scaling problems, we have been considering the use of the CNRI HANDLE system [66] in this environment. We do not consider that system a complete fit, but it does meet most of our needs. We expect both to demonstrate this excellent fit and to propose how comparatively small modifications to this class of systems could be the basis of a methodology with a large applicability, providing security and scaling, and able to deal with heterogeneous devices at the same time. Not only will it be able to provide real security, but also it can be an important tool in achieving a large-scale, widely applicable, infrastructure.

The HANDLE system was developed for a different class of applications; the persistent, secure, naming and storage of multimedia documents. Unlike many of the experimental systems being developed in this cluster, it has a proven track record of deployment, and its properties have been verified experimentally. There is substantial experience of its functionality.

The basic concept of HANDLE is of a set of Handles with an arbitrary set of Names. The Names are structured in a hierarchical fashion, with a global registration of Name-Space down to a certain level, and User-managed Name-Space below it. They denote the Names by the term *Handles*. By *User* is meant any entity that has contracted to manage a unique part of the Name-Space. In this respect, the HANDLE Name-Space is very similar in concept to the DNS system. There are then two vital differences. First there is the syntax of Handles, second there is the security infrastructure built around it. These result, of course, in many other differences. The syntax of Handle attributes is an arbitrary length set of *Type/Value* pairs. Some of these *Types* will be registered in a global directory to aid wide interoperability and a common parlance; others will be registered only in more local registries managed by the owner of the Handle space. The second is that access and management of Handles and their attributes is restricted by authorisation credentials. Each User HANDLE space has an administrator nominated by the User entity; we will call him/her the Local HANDLE Administrator (LHA). He/she is given a private security credential by the Global HANDLE Administrator (GHA). Only the GHA can manage the Handles in the Global HANDLE space; the LHA has complete management rights on the Local HANDLE space. This right includes delegation of management of subsidiary HANDLE space as with the DNS. The DNS has a metadata that defines the domain administrators that are authorised to manage DNS records. HANDLE goes further, in addition to the authorisation only of the LHA to manage Local Handles, it also has a metadata to restrict the access to Handle records only to authorised users. The LHA can define these access rights in a fine-grained manner.

There are three subsystems of the HANDLE system architecture: the HANDLE Identity Resolver (HIR), the HANDLE Store (HS) and the HANDLE Registry (HR). Limited versions of the HR and HS are bundled with the HIR, and only that component is used in IoT6. There are public domain implementations for the Local systems, and plug-ins for use of some of the facilities through a web browser.

The Handle syntax can be used to define all the properties of devices. Since one Handle Type is another Handle, these descriptions can be very generic – and even refer to entries in other domains like the EPC structure [67]. One can also specify security attributes to devices represented by the Handle in the attributes. While, of course, such attributes can be stored only in an encrypted form for added security, in any case access to the attributes is limited only to users so authorised by the LHA when the Handle was set up.

Using such techniques, we show how it is possible to set up complex authorisation facilities, while keeping the load on the end-devices minimal. All operations on end-devices require authorisation, all data from end devices are authenticated. However by performing most of the more complex authorisation and authentication activities in servers running applications where the resources are less constrained, the load on the end-devices can be minimised.

Both the Global and the Local servers can be replicated and split up if the number of entries so requires for performance reasons. While management of Local Handles remains a local matter, the access to them is always possible through the Global system. The system is now completely accessible via the IPv6 infrastructure; both servers and user processes are IPv6 enabled.

One *type* of attribute can be an IPv6 address; this provides the link between the Identifier space and the network space. IPv6 features include multicast; this allows a direct link to be established between Handles and group operations, by using multicast addresses for the group operations. If the end-systems are IPv6 enabled, the normal network level multicast can be used; it they are a legacy technology, some intermediate process may have to be employed. The use of Identifiers with access only to authorised users, and network addresses as attributes, allows technology features to be used safely in the Identifier space without compromising systems knowledge in the address space. The use of IPv6 allows secure inter-process communication to be provided by use of DTLS, and easy integration with 6LoWPAN wireless networks for remote IP-enabled devices.

Because to the way the total system has been implemented, it is very scalable, and can introduce real security into IoT systems – while keeping the load on end-devices minimal. We will be demonstrating complete exemplars of the system as validations proofs-of-concept.

Technological enablers and design solutions

The objective of this section is to identify technical solutions, best practices and approaches, which could be used to address the challenges described in section *Identification of challenges for Governance Security and Privacy in IoT*. This section is divided in two parts. The first part identifies the solutions and approaches provided by the FP7 projects, which compose the clusters. The second part identifies the solutions and approaches, which are available in the research domain and the market. These solutions can be used to support the definition of the framework described in section *Architectural framework*.

Some solutions proposed by different projects can be quite similar. For example, policy management frameworks are provided by various projects in the cluster. In the section, which describes the architecture framework, these similarities are identified in connection to the challenges.

Solutions from Clusters projects

Usage Control Toolkit

The usage control policies implemented in the iCore project, consist of authorizations and obligations specified as Event-Condition-Action (ECA) enforcement rules. These rules use as a reference a set of inter-related design models representing different aspects of the IoT system, and are used as input for the runtime components in the framework. This solution to enable monitoring of ECA rules and execution of security enforcement behaviour [68][69] is named the Model-based Security Toolkit, or just SecKit.

The SecKit consists of a collection of metamodels for specification of a computer system structure, information, behaviour, context, identities, organizational roles, and security rules. These metamodels provide the foundation for security engineering tooling add-ons and metamodel extensions to address requirements of governance, security and privacy. The SecKit adopts a generic design language to represent the architecture of a distributed system across application domains and levels of abstraction including refinement relations support inspired in the Interaction System Design Language (ISDL) [70].

The following figure gives a high-level overview of the design models supported by the SecKit, which are system (structure, information, behaviour), context, identity, role, and security rules. These models provide the foundation for the design and runtime tooling, and extensions/add-ons focusing on specific security aspects of a computer system.

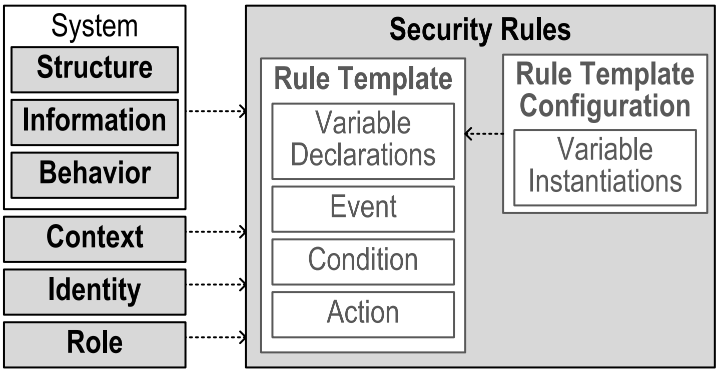


Figure 7 Design Models

The first step using the SecKit is the specification of the System behaviour, structure, and information model. Figure 8 shows an example of this model where a Smart Home entity interacts with a Medical Center through an interaction point. The details about this interaction and the information exchanged are depicted in the behavior model, which in this example is the *Access heart rate* interaction, which exchanges the *bpm* (beats per minute) information. The entities in our system model are a one-to-one mapping to the iCore concepts of VOs and CVOs.

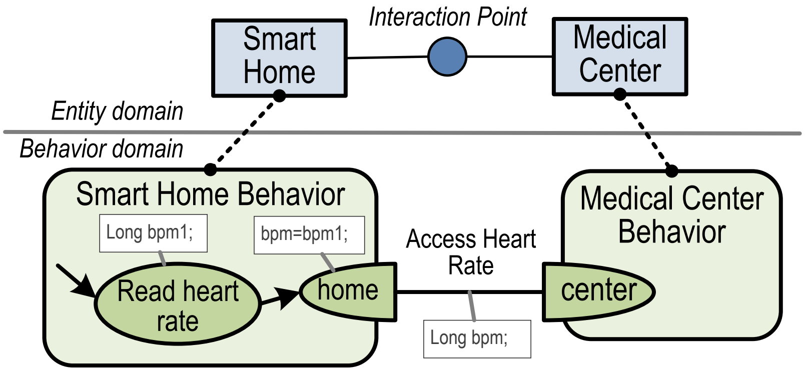


Figure 8 Entity and Behavior Model representing IoT System

In addition to the specification of the system models the SecKit also includes metamodels for specification of Context, Identity, and Role models. The identity model specifies the identity types and attributes that are allowed in this identity types. The role model specifies the organization role hierarchy, with the possible of inheritance of membership. For example, *Doctor* and *Nurse* could be specified as sub-roles of the *Health Professional* role.

The context model specified types of Context Information and Context Situations. Context Information is a simple type of information about an entity that is acquired at a particular moment in time, and Context Situations are a complex type that models a specific condition that begins and finishes at specific moments in time. For example, the *GPS location* is an example of a context Information type, while *Fever* and *In One Kilometer Range* are examples of situations where a *patient* has a temperature above 37 degrees Celsius and a *target* entity has a set of nearby entities not further than one kilometer away. *Patient* and *target* are the roles of the different entities in that specific situation.

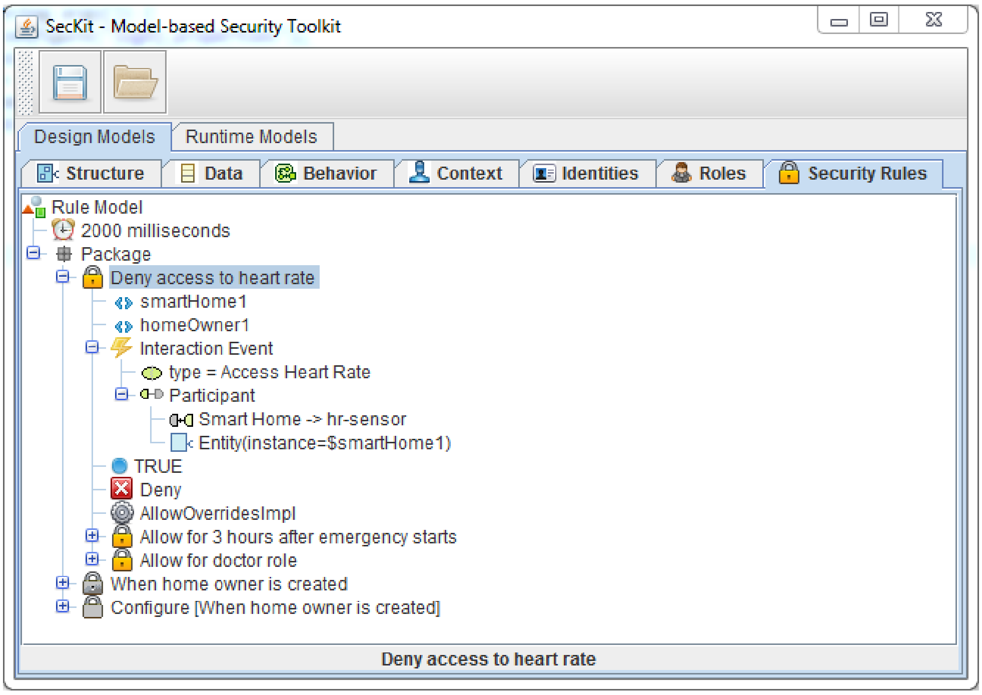
The specification of authorization and obligation policies is done in the SecKit using an Enforcement Rule model containing *Rule Templates* that must be explicitly instantiated using *Rule Template Configurations*. A rule template follows an ECA semantics defined over discrete traces of sets of events, when the trigger event (E) is observed and the condition (C) evaluates to true the action (A) is executed. Templates are parameterized with variables that are instantiated by the template configuration. The Rules specified using the SecKit make reference to the design models of the system (structure, behaviour and information), roles, context, and identities.

Events in our framework represent the actions and interactions between VOs, CVOs, and Services in the iCore framework. We model the start of an activity, ongoing activities, and the completion of an activity with the event modalities: *start*, *ongoing*, and *completed*. To support enforcement of usage control policies including authorization decisions we model *tentative* and *actual* events. A tentative event is generated when an activity is ready to be started by the iCore framework but has not yet started, giving the opportunity for the execution of enforcement actions.

A tentative event may trigger the execution of an enforcement behaviour to allow or deny the execution of the activity. If the activity is allowed it is also possible to specify an optional modification or delay of the activity execution, for example, anonymizing activity data before the activity takes place. The execution part of an enforcement template may trigger the execution of additional activities, for example, notifications or logging of information.

The condition part of a rule template consists of event pattern matching, propositional, temporal, and cardinality operators. The expressiveness is bigger than existing languages for access control like XACML and allows for great flexibility and re-use of modular policy specifications.

Figure 9 shows a screenshot of the SecKit Graphical User Interface (GUI) implementation for specification of design models. More specifically, this figure shows the tab with the Security Rules design model. The security rule template highlighted "*Deny Access to Heart Rate*" specifies that when the interaction type "*Access Heart Rate*" is about to be executed (tentative) it should be denied if the entity instance participating in this interaction is the one assigned to the variable *$smartHome1*. The condition part of this rule is simply *TRUE*. This screenshot illustrate some of the important features of the SecKit support, including support for variables, nested rules, and instantiation of templates.



```
Rule Model
  2000 milliseconds
  Package
    Deny access to heart rate
      smartHome1
      homeOwner1
      Interaction Event
        type = Access Heart Rate
        Participant
          Smart Home -> hr-sensor
          Entity(instance=$smartHome1)
      TRUE
      Deny
      AllowOverridesImpl
      Allow for 3 hours after emergency starts
      Allow for doctor role
    When home owner is created
    Configure [When home owner is created]
```

Deny access to heart rate

Figure 9 Specification of Security Rules using SecKit

The highlighted rule in Figure 9 is the default case for the interaction "*Access Heart Rate*", which simply prevents it from happening. In case one of the nested rules evaluates to "Allow" this decision overrides the default case, which is the semantics of the "*Allow Overrides*" combining algorithm. The two nested rules in this example allow the interaction to happen in case of emergency (context condition), or in case a doctor tries to perform the interaction (organizational role). Additional details about the SecKit are described in the following publications [68] [69].

Using the SecKit enforcement rules, policies can be specified for authorizations and obligations inside an outside of an administrative domain. For example, the owner of a smart home can specify the instantiation of an enforcement rule that should be evaluated by an iCore-enabled smart city infrastructure outside the home or (s)he can specify rules to manage authorizations and obligations of the devices inside of the smart home. The delegation of policies and mutual establishment of domain identities can be done using a trust negotiation approach.

Sticky Flow Policies

Stick flow policies combine sticky policies for data with their flow policies, i.e. a data item in a system using this technology is annotated with a security policy which describes how a data item can be used and which conditions have to be satisfied before an item can flow to another entity.

The security architecture proposed in COMPOSE strongly relies on sticky flow policies. In this section we will briefly outline the potential which arises from the use of such policies.

Similar to ECA rules as used in iCore, flow policies consist of a conditional and an *action* part. Conditions are simple Boolean propositions and actions are described by read and write activities on a specific target respectively. A set of such rules annotated to a data item forms a policy. These policies are able to model RBAC [24] and we are currently extending their expressiveness to the usage control model.

While COMPOSE still defines regular access policies on its principals, flow policies trigger and instantiate various enforcement mechanisms. So called platform monitors are integrated in the central logical entities of the system architecture. They enforce compliant flows of data between service objects, services, and users. However, they also monitor during runtime whether developer defined program logic induces insecure flows. For this purpose, we deploy mechanisms which are similar to simple taint tracking approaches. Due to the fine granularity of flow policies, we can also achieve a higher flexibility of applications while maintaining the least privilege principle to improve the security of data stored in the platform.

To maintain scalability and efficiency of data processing, flow policies are also used to statically analyse services. Similar to validation framework proposed by SPaCIoS, an abstract model of the application is generated and we investigate whether the execution traces of an application are compliant with the flow policies defined over the data potentially processed by the service. The simplicity of the flow policies supports the efficiency of this approach.

The result of this analysis is used by an instrumentation component in COMPOSE which modifies the original object code. We inline appropriate monitors, i.e. reference monitors, logging monitors, or monitor hooks. While reference monitors take the classical task of enforcing policies, logging monitors can generate critical logging information, which can also be used for the precise monitoring of the behaviour of a service, e.g. for data provenance or trust and reputation systems. Finally, monitor hooks can be used to selectively delegate or synchronize the enforcement task to a platform monitor instance.

Thus, sticky flow policies combined with a set of sophisticated enforcement mechanisms allow a user or provider to control the use and flow of data generated by his things while retaining the flexibility of application developers.

Secure Middleware based on policy management

As many future IoT applications will require the automated sharing of context information that is gathered autonomously by means of sensors, privacy preservation must an integral concept. Privacy in the GAMBAS project concentrates on the following three points:

1. the privacy preserving design and implementation of mechanisms and protocols for context information sharing;
2. the development of extraction tools that gather and generalize privacy policies from a set of web services automatically;
3. the integration of these mechanisms, protocols and tools into an adaptive data acquisition framework developed in GAMBAS.

Context-sharing enabled objects must be able to answer the question which information should be shared with whom. This question can be automatically answered, if the object has a fine-grained privacy policy that contains both the trusted objects and the context characteristics allowed for sharing. Additionally, an object needs mechanisms that enforce this policy. The contents of a policy are typically user and thus, object dependent. Many users have different opinions about what kind of context should be regarded as private and not every object supports all types of context. As a consequence, we can expect that some policies might be more restrictive than others. To make things worse, the current situation of the user might have an influence on his current context sharing policy, so it must be updated regularly. This dynamic nature and the dependency on the user do not allow the creation of one static policy that is valid for every object, user and situation. Instead, a user dependent policy is necessary that can be updated according to the changes.

The manual creation of this kind of privacy policy is already a tough task for the user. For manual creation, a user must think of all different context characteristics that could appear and define a fine-grained access control scheme. Additionally, groups of users must be defined and be given different access rights to the characteristics. If new users appear, they must be inserted in the present scheme without creating inconsistencies. A similar process will occur, if a new context characteristic is discovered. Thus, using a manual approach for policy creation, the user would be busy creating a policy and the achievable benefit from sharing may be less than the loss of time that was needed for creating the policy.

To avoid the overhead of manual policy creation while supporting the privacy-preserving sharing of context information, the middleware proposed in GAMBAS encompasses tools to automate the generation of the privacy policy. Using social networking sites, where users already define their privacy preferences with regard to several types of context information (including current location and private contents), it is possible to obtain user groups and access rules for context information. This is closely related to approaches such as the privacy wizard described in [71] which try to extract policy information from a social networking site. However, these approaches do not apply the policies to further sharing of context information. Thus, the developments in GAMBAS can be considered an extension to support the automatic generation of context sharing policies since they only consider the aggregated context of social networking sites and not the fine-grained context of physical sensors.

Besides from policy generation, the mechanisms that are necessary to enforce the policy must also be fully automated. Thereby, the mechanisms must enforce the policy while preserving the privacy. For example, if it is necessary to detect whether an object belongs to a specific user group, doing so should not reveal the existence of the group nor the associated access rights. To do this, GAMBAS encompasses protocols which enforce the policy, i.e. are gathering the needed information from other objects, looking up the access rights specified in the policy and finally share this information in a way that it cannot be gathered by unauthorized objects. As a consequence, the GAMBAS middleware entails a complete privacy-preservation framework that enables the automatic generation of a user-specific policy as well as the enforcement of the policy at runtime.

Capabilities based policy management

On the security management side, it is worthwhile to highlight as the IoT@Work access control mechanism (and capability based mechanisms) makes possible to split the security assurance issue among the involved actors (e.g., smart objects, services, etc.) therefore reducing the need of complex middleware. Indeed, each capability token can be tailored to a specific resource (e.g., the token can report operations that are specific to that resource) without affecting tokens for other resources (while in an RBAC/ABAC systems where roles, operations, etc. must be defined in a consistent way to have a manageable set of elements and rules). Additionally, the IoT@Work mechanism decouples the access control from the Identity Management aspects, therefore heavily reducing the management effort and the complexity of trusted, federated IAM (Identity and Access Management) middleware.

Contracts

To efficiently analyse services and their compositions and in order to describe the security relevant actions of security services, COMPOSE also proposes the concept of security contracts.

Contracts describe a promise of a service towards the platform to behave in a certain way. COMPOSE contracts promise to change the security state of data and system entities in a pre-defined way, define preconditions which need to be satisfied before execution, and describe the flow of data during execution. If not annotated to system services, which are initially provided by COMPOSE, such contracts are automatically generated and over approximate the service behaviour. Thus, they can be used during development, static analysis, and automatic service compositions to efficiently interact with a user. However, even if the results may seem sound, they may not be precise and induce false positives. Thus, they can give a first hint on the processing of information and speed up demanding analysis techniques but need to be complemented with appropriately precise refinement methods to reduce user interference.

In contrast, the contracts for declassifiers, security services, and security primitives defined by system developers can be used to patch noncompliant flows in service compositions. For this purpose we identify the conditions not satisfied in noncompliant traces. By using services which satisfy these contracts, we can automatically assemble or at least support the generation of services compliant with the security requirements of the data they process.

Models for verification and testing

The techniques and technologies developed in the scope of SPaCIoS cover most of the activities related to the modelling, verification and testing of web services. Reasonably, these steps are expected the take place during the service development process. Hence, the tools implemented within SPaCIoS should integrate with state-of-the-art service development environments (SDEs). Among the existing SDEs, we opted for an integration with Eclipse. Implementing the SPaCIoS Tool as an extension of the Eclipse platform offers several advantages. As a matter of fact, Eclipse is a widely used SDE commonly adopted by both industry and academia. Eclipse has a rich support for creating and importing platform extensions, namely plugins: developers may customize their platform by installing plugins satisfying their specific needs. Thus, developers using Eclipse can easily include the SPaCIoS technology in their working environment.

The SPaCIoS Tool consists of a collection of sub-tools, each of which depends from the tool front-end, being an Eclipse interface extension, and contributes by publishing its own functionalities. Also, a tool can directly contribute to the Eclipse workspace if it needs to. Since all the controls are mapped into the Eclipse workbench, the developers interact with the standard Eclipse interface they are experienced with.

As shown in Figure 10, the SPaCIoS Tool combines state-of-the-art technologies for penetration testing, security testing, automatic learning, model checking, and related automated reasoning techniques. In its main workflow, the SPaCIoS Tool takes as input a formal description of the SUV, the expected security goals, and a description of the capabilities of the attacker, and automatically generates and executes a sequence of test cases on the SUV through a number of proxies (e.g., http-proxies). We now briefly describe the different components of the tool and how they are used in the main workflow of the tool usage.

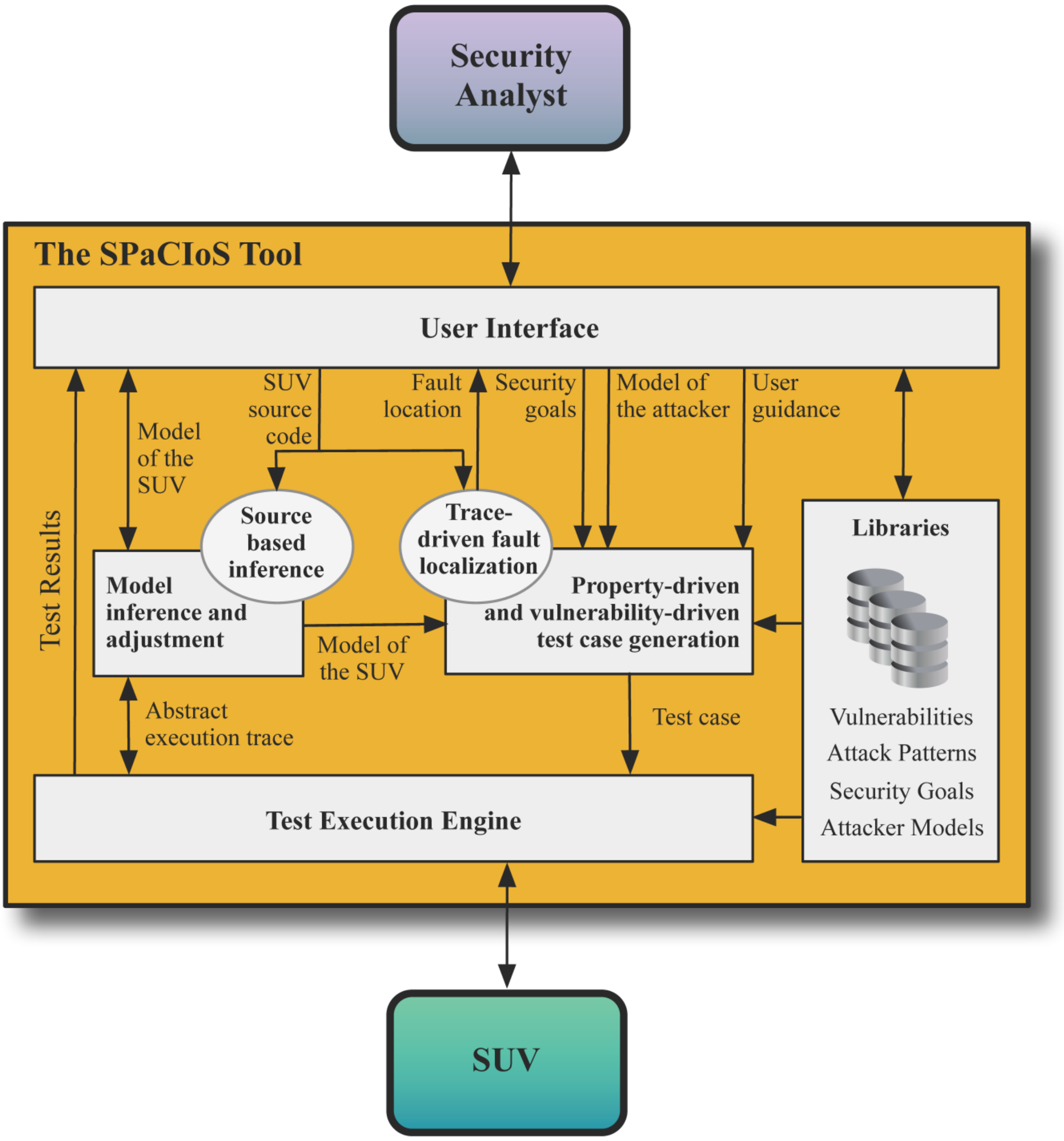


Figure 10 SPaCIoS tool for modeling and evaluation

The Property-driven and vulnerability-driven test case generation component is in charge of the generation of the test cases starting from a formal model of the SUV and its environment, along with a description of the expected security property (or, dually, of a security vulnerability). It also exploits a trace-driven fault localization based on the source code of the SUV, when available. The test cases generated are such that their execution should lead to the discovery of violation(s) of the security property (or should confirm the existence of the security vulnerability, respectively).

There are four different categories of elements in the Libraries component: vulnerabilities, attack patterns (a set of rules for describing an attack), security goals and attacker models. All these sets are used as input for the property-driven and vulnerability-driven test case generation component. Moreover, attack patterns are also used to guide the analyst in the iterative penetration testing phase and in the refinement of abstract traces involving respectively the Eclipse user interface and the test execution engine.

The Model inference and adjustment component has the twofold task of building a formal model of the SUV (possibly via source-based inference) and of the environment, and to adjust the available one. The construction of the model is necessary whenever no model is initially available. This is performed offline, i.e., before starting the test case generation and testing the SUV. Model adjustment is instead an online activity that is triggered when the execution of a test reveals a discrepancy between the model and the SUV and/or the environment.

The test cases are finally executed by the Test Execution Engine (TEE) by handling the exchange of messages with the SUV.

Authentication/Authorization

The Authorization Server in BUTLER is the single point for security management. All actors shall delegate authorization management and user management to the Authorization Server.

The Authorization Server enables separation of the setup of the trust and the security of the data transfer between resource consumer (application) and resource provider. The trust enabler is not involved in data transfer; this separation allows implementation of privacy requirements. Here it is up to the Resource Consumer to support privacy requirements following current regulation concerning data storage and data usage. The security protocol allows end-to-end security between resource consumer (application) and resource provider (server, gateway and object). The application accesses resources on behalf of a user.

The authorization server provides authentication and authorization WEB services and WEB portal both for server administrators and final users. Final users can manage their resources, give access permissions to others users (acquaintance) to access their resources, manage access tokens generated for specific application and resource.

RERUM will design and implement mechanisms for secure object-to-object and object-to-internet communication, to ensure that no intruders or unauthorized users/objects gain access to the system. RERUM will research hop-by-hop, end- to-end and PKI-based authentication considering the limited resources of smart objects. The project will use related work as a reference point, as found in [72] for intermediate hop- to-hop authentication, [73], [74] for end-to-end authentication and [75] for an adoption of the public-key cryptography based schemes for data concealment in wireless sensor networks.

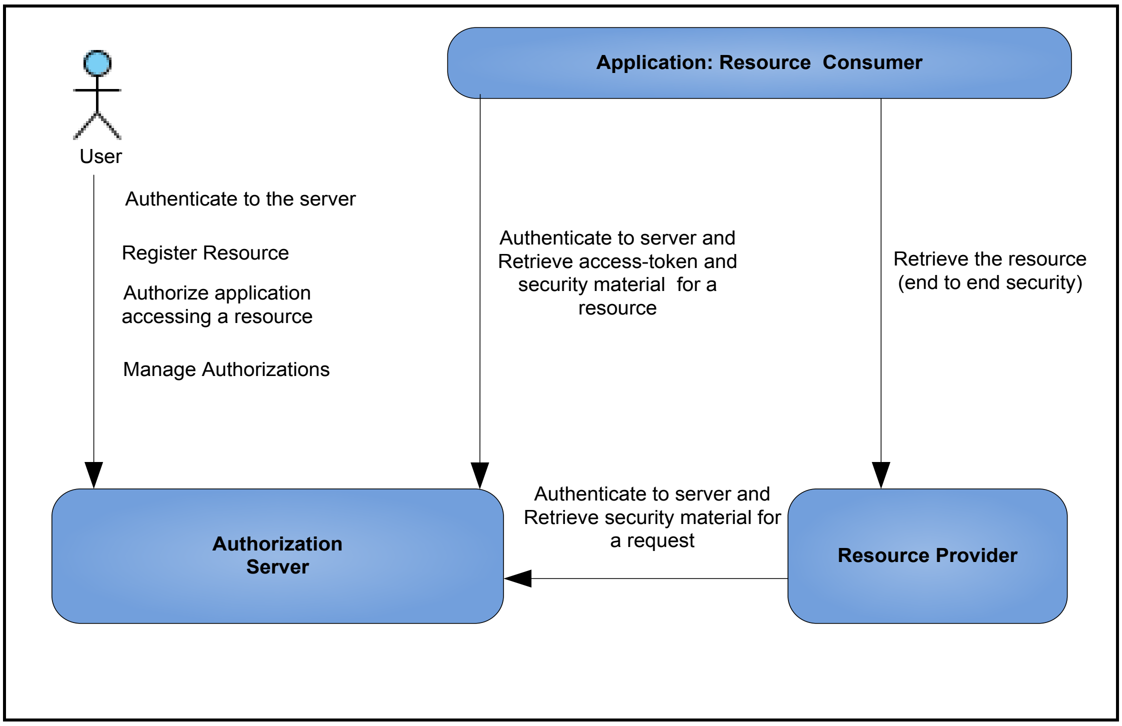

Application: Resource Consumer
User
Authenticate to the server
Register Resource
Authorize application accessing a resource
Manage Authorizations
Authenticate to server and Retrieve access-token and security material for a resource
Retrieve the resource (end to end security)
Authenticate to server and Retrieve security material for a request
Authorization Server
Resource Provider

Figure 11 Authorization solution

The use case presented in Figure 11 can be summarized as follows:

1. A User authenticates towards the Authorization Server
2. The User registers resource metadata to the Authorization Server.
3. Later, an application accesses the Authorization Server to retrieve an access-token for a specific resource always on behalf of an authenticated user – if the user is not already authenticated to the Authorization Server, it shall authenticate. Once authenticated, the user shall grant the application to retrieve the access-token.
4. Using the access token, the application can securely access the resource by giving the resource access-token.

This authorization solution is derived from BUTLER security services, which include:

- Secure Transport of messages between any device and Authorization Server.
- Retrieval of the Access Token.
- User authentication to Authorization Server.
- Client application authentication to Authorization Server.
- Resource Registration
- Resource Authentication to Authorization Server.
- Object Key Management.
- End to End security between (application) Resource Consumer and Resource Provider.

Authorisation and Service Composition using HANDLE

IoT6 has extended the ideas of the previous section to to allow the authorisation to be extended to multiple management domains. By using the HANDLE system (63). The previous section emphasised that the authorisation service in Butler is restricted to single management domains. With the HANDLE System, there is indeed one over-riding HANDLE domain. However, However the structure of the system is that once a contact has been registered with the Global Handle Service, that entity CAN have the authority to set up, register and manage all identifier space suffixes. It is a current Governance issue that CNRI will permit two forms of subscription – a very low rate if one is authorised only to register other identifier in the one domain, or a rate one thousand times higher to be authorised to manage completely the suffix identifier space. That policy will presumably change when the Global Handle Namespace is managed by the DONA Foundation – a not-for-profit foundation registered in Geneva. Switzerland. For the purposes of this report, we should note that the HANDLE technology is quite capable of being extended to multiple management domains – including its authorisation services. Indeed in many of its user communities, including the Chinese, this now occurs. Indeed the Chinese are adopting cryptographic suites that are not shared outside China. From a technical viewpoint, the assumption should be made that this type of technology is in no way restricted. From a sustainability viewpoint it must be realised that multiple management domains have cost implications, and that these must be considered in the financial basis.

In itself, the IoT6 solution does not address differently the security policy, authorisation and context sharing of the preceding – except it may actually extend them. There are facilities for authorising and managomg separately individual components of a given identifier; we are not clear whether this is envisaged in the Butler approach. There are also built-in facilties for context sharing – both in management domain and globally. The HANDLE Types can be registered both globally and in a restricted domain. Attributes of an Identifier can be the Handles (i.e. Identifiers) in other management domaions. Thus even the authorisation of Handles in one domain are constrained to its management space, the access to some of its components can be fixed in another space. To give an example, an attribute of a specific IoT subsystem may be a component that is registered in the Eletronic Products Code (EPC) system. In that case the access to the characteristics of the EPC component are constrained by the EPC access policies.

The HANDLE mechanisms are particularly useful in the set-up and operatoins differenences mentioned in the precedinng sections. The fine-grained authorisation mechanisms are immediately appricable to the detailed assignment of roles in the different phases. Several other aspects of the IOT6 approach using HANDLE are relevant:

- The fine-grained authorisation model is well-suited to secure storage and retrieval of security and authorisation tokens.
- The built-in mechanisms for recording each transaction is invaluable in compiling audit trails.
- Since the identifiers can have as attributes IP addresses provides a mechanisms for allowing algorithmic construction of identifiers in a protected space while the network addresses can be in unprotected space - without revealing properties of the system to unauhorised bodies.
- Because the same component can have multiple identifiers, this approach gives a mechanism for specifying group operations – by having the different identifiers belonging to different groups. This may

be further reflected in using different multicast groups at the Ipv6 network level.

- Because attributes can refer to processes, one can compose more complex applications by having an attribute of one identifier point to the identifier of a subsequent process - with the parent providing the relevant authorisation.

Cryptography in IoT

This section describes various innovative cryptographic systems, which have been proposed by the AC05 projects.

- Malleable Signature Schemes (MSS) is proposed in RERUM project. MSS just like classical digital signatures, strive to protect signed data from undetected malicious modifications. The concept of malleable signatures allows an additional, designated party, frequently called the sanitizer, to be authorised by the signer to modify a previously signed message in an authorised way. For all actions not authorised and for all parties not specified as sanitizers, any modification would result in a signature verification failure. Thus, MSS can allow only certain Privacy Gateways to act as trusted sanitizers to make privacy preserving changes to integrity-protected information. This will decrease the integrity compared to an unmodified original value. However, in the MSS approach, this balance can be configured to suit the applications needs regarding the level of integrity protection and the level of privacy.
- Compressed Sensing (CS) proposed by RERUM will also allow achieving a very high level of encryption combined with energy efficiency, two basic requirements of IoT applications. This will help address security as well as privacy issues in the IoT [76].
- Cryptographic integrity and authenticity
  To ensure that no intruders or unauthorized users/objects will gain access to the system RERUM will research hop-by-hop, end-to-end and PKI-based authentication considering the limited resources of smart objects. BUTLER has addressed cryptography and authorization for constrained smart objects by introducing an efficient and secure mutual authentication and key establishment protocol that is based on Elliptic Curve Cryptography (ECC) [77]. This approach allows the secure communication with low computational resource on smart objects. More specifically, it introduces an “offline key assignment” procedure used to authenticate each node by generating a public/private key pair for encryption and decryption of the messages. Authentication is achieved with a generation of a private key based on a prime number stored on the node.

In the past year, BUTLER has led several experiments in many contexts to acquire data sets measurements from physical sensors embedded in the nodes and from radio characteristics. BUTLER has analyzed the entropy containing in each source with the new min-entropy estimators recommended by the NIST in their last document dated august 2012. The novelty of this analysis is brought by a statistical analysis performing on the data source samples instead on the output of the random number generator.

BUTLER has discerned several relevant sensors to harvest entropy in nominal mode. But, when the nodes are idle, the sensors are not stimulated and the entropy is reduced. Observing the fact that all nodes are able to receive a radio signal, BUTLER focuses on the analysis of the radio statistics: RSSI (Received Signal Strength Indicator), the LQI (Link Quality Indicator) and the erroneous packets received by the nodes as the errors due to the channel degradation are singular for a given peer-to-peer link. In conclusion, the LQI and the erroneous packets are relevant entropy sources.

So, BUTLER started to design a lightweight true random number generator that can be embedded on very small nodes running with Contiki. Several health tests have been developed to scan in live the "health" of the entropy source in the embedded device. A true number generator cannot rely on only one source. As a consequence, several sources have been considered, each with their health test. In the next year, BUTLER will define the post-processing and finalize the TRNG design.

The study realized to design a tiny true embedded random number generator enables the nodes to generate their own cryptographic features. However, the node is not able to manage X.509 certificates. We introduce a new handshake mechanism based on the hypothesis of a reduced diffusion of the public key of the referent gateway.

In addition, in the BUTLER project, the joint use of the Authorization Server at application level and of the bootstrapping mechanism at WSN level enables to address end-to-end and hop-by-hop security problem between a sensor node belonging to the IoT domain and an end-user application connected on Internet. The gateway located at the border between the Internet world and the WSN domain ensures the communication standard interoperability. For the hop-by-hop security mechanism, the gateway authenticates to the Authorization Server in the Internet world and the sensor node bootstraps to the gateway in the WSN domain. The security credentials generated by the Authorization Server could be pushed by the gateway until the sensor node. This mechanism may be useful for mobility scenario. For the end-to-end security mechanism, the sensor node authenticates to the Authorization Server to retrieve the security credentials.

Last (developed in time) but not least, BUTLER proposes a new dynamic, information-theoretic, secret key generation (SKG) schemes for short range communication (SRC) [78]. The goal is to enable communicating pairs to locally produce secret keys to seed their embedded cryptography systems without using classic, aforementioned, computational cryptography. Current key exchange schemes, under the framework of information-theoretic secrecy, exploit the entropy of the communication channel to extract the secret bits. However, for the scenario under consideration, characterized by very short and LOS links between devices, the previous assumption is not anymore valid. Therefore the new proposed SKG scheme exploits the AWGN conditions faced by SRC systems to build geometric secrecy regions within which eavesdroppers cannot acquire phases exchanged between the legitimate pair.

Management functions

RERUM will also develop distributed self-management and self-monitoring mechanisms for detecting faults in the network and monitoring smart object status. Key statistics to be monitored are energy, status (on or off), link state, lost packet count etc. That way, any object or link failures will be automatically detected and efficient self-healing algorithms will be applied to resolve these issues. For monitoring and management of the security events RERUM proposes to adopt the ideas behind the Platform for Run-time Reconfigurability of Security (PRRS), a component in the Future Internet core architecture. The PRRS allows an end-user application or service to direct a request to the PRRS framework describing its particular security requirements, which will then be built from available services offered and finally deployed. PRRS will also monitor violations during runtime by instantiating a runtime monitor in the instantiated security solution.

Secure Setup and Configuration

RERUM's envisioned framework for Smart City IoT requires a security architecture with appropriate mechanisms for the bootstrapping process. Cities must be enabled to install the IoT especially for larger number of devices.
Existing operational credential bootstrapping and key management protocols require the existence of some initial credentials as a starting point. Also key pre-distribution protocols, e.g. applied in wireless sensor networks, assume the configuration of some initial credential information before operation. RERUM will take approaches to initially bootstrap credentials on the IoT objects, and how to use them to update operational keys, and analyze their applicability on the desired Smart City applications. To avoid any incidents during network bootstrapping, RERUM will take into account existing bootstrapping protocols (such as EAP, PANA, 802.1x, CoAP, and 6LoWPAN) and will define mechanisms to optimize the process, enhance the security to minimize attacks for the desired Smart City applications.

In this respect, RERUM will re-design basic self-X properties of smart objects to embed security and privacy mechanisms. Auto-configuration mechanisms will also be developed with built-in security and context-awareness, enabling the secure exchange of security settings through the network.

The utilization of Cognitive Radio technology can also be considered as part of a secure auto-configuration mechanism for mitigating jamming or interference in cases of wireless interconnectivity of smart objects [79]. RERUM aims at work on lightweight spectrum management techniques that will allow each smart object to identify the unused frequencies and transmit on them. Jamming or interference can be detected automatically and can be avoided utilizing fast and efficient spectrum mobility techniques.

Audit and monitoring solutions

For monitoring and management of the security events RERUM proposes the Platform for Run-time Reconfigurability of Security (PRRS), a component in the Future Internet core architecture. The PRRS allows an end-user application or service to direct a request to the PRRS framework describing its particular security requirements, which will then be built from available services offered and finally deployed. PRRS will also monitor violations during runtime by instantiating a runtime monitor in the instantiated security solution.

Using Pseudonymization

The same ability of third parties to know that two entities are exchanging data can be a violation of privacy. Both users and services might need to operate in given scenarios without releasing identification, addressing or other sensitive information the other endpoint. This can be in conflict with the some requirements related to authentication, authorization and non-repudiation.

By using a trusted Pseudonymization infrastructural service (see IoT6 project), which provides temporary fictional identities (pseudonyms) with coherent credentials and authorization policies, an IoT system can satisfy both privacy and non-repudiation requirements.

Trust and Reputation Systems

The concept of trust (as described before in this paper) is not clearly defined in literature and various definitions are available as pointed out in [80]. One definition can be that Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends. Reputation is also linked to Trust and reputation and can be defined as a measure of trust where each entity maintains reputation information on other entities, thus creating a “web”, which is called a web of trust. The work by Golbeck and Hendler [80] [81] uses ontologies to express trust and reputation information, which then allows a quantification of trust for use in algorithms to make a trust decision about any two entities. The quantification of this trust and associated algorithms are called trust metrics. Various technologies and approaches have been proposed in literature to provide trust in ICT systems. In many cases, other solutions proposed in other sections of this paper can be re-used to create a trust and reputation system. What is important in IoT is to provide the capability to measure the level of trust an entity (device, service or user connected to the IoT) can provide to another.

COMPOSE manages reputation of virtual objects represented by service objects, services, applications, and users. Through the monitoring of various reputation dimensions such as popularity, user feedback, service compliance to its promised behavior, its quality of service, or its security properties (such as defined by policies or contracts) appropriate reputation values are accumulated. This accumulated reputation is used in a trust metric to compute trust values for the respective COMPOSE entities. Access control modules and enforcement monitors in the respective security architecture use these trust values to grant resource access or prevent the execution of particular processing steps. As a consequence, trust values can also be used to define security policies. Finally, trust values for COMPOSE entities are used during the development process. During the assembly of new services or applications, developers may also prefer to use components with higher trust values.

In the context of IoT and the machine-to-machine networking the notion of trust is of major relevance. RERUM considers Trust playing a key role in IoT acceptance and focuses on increasing the trustworthiness of the system for giving incentives to both Users and Service providers for adopting and investing on the IoT technologies. Trust in RERUM's setting can be quantified as the expectation that an object will act as originally planned, or within a set of protocol parameters. To address the notion of Trust RERUM will introduce the concept in the core of the system through all its layers, with a specific focus on smart objects. The key concept is that only fully trusted smart objects will be allowed to exchange sensitive user data and that only data generated by trusted smart objects will be taken into account in the system/application decisions. In order to measure smart object trustworthiness, a weight model capturing the data context may be used. Weight will not only be determined by the input provided by users, but also by the time it was last updated and by the effect that the context really has in the related service. Additionally, a reputation management mechanism will be developed in RERUM, fusing the data gathered by all smart objects and evaluating the results to identify malicious or misbehaving objects.

Solutions not defined in the Cluster projects

The objective of this section is to provide a brief overview of the potential technologies and approaches not adopted in the IERC 2013 cluster projects, but which can be used and deployed in IoT to support Governance, Security and Privacy and an Ethical use of IoT by users. This survey is not exhaustive because research activities in these topics are extremely wide. For example, a search of the term security and privacy in IEEE Explore (only one of the leading publishers in research) returns 12857 hits. In addition, some solutions presented here have been used in previous FP7 projects (and they will be probably used in future Horizon 2020 projects). For example, IDEMIX in Primelife and ABC4Trust. In addition, we note that various projects in the cluster have defined or used Identification solutions, but they do not have a sufficient level of maturity.

Identity management

Identity Management refers to Identity of user or objects. In the digital world, user must have one or more identities. Generally speaking, an identity is managed by an Identity Provider. The main role of the Identity Provider is to provide verifiable identity attributes to Service Provider. The associated liability is managed though a contract between Service Providers and Identity Providers. Examples of mature Identity Management technologies are the following:

- FaceBook-Connect API [82] enables FaceBook members to log to external websites. The implementation relies on OAuth 2.0 [58] both for accessing resources and user identification: users attributes are seen as standard resources by the open graph. This brings some security concerns. The FaceBook's OAuth 2.0 implementation is not totally standard particularly in the way applications refresh their tokens.

- Google Identity Management. Google uses standard OAuth-2.0 [58] for accessing the protected resources and relies on OpenID [59] for user identification.
- Kantara/Liberty Framework. Kantara Alliance - the new name of the Liberty Alliance - Framework [83] is based on SAML 2.0. The framework is more than an Identity Federation Management because it is also supports Attribute Provider generally implemented by Identity Provider. For user attribute management, the framework is based on Identity Web Service Framework ID-WSF 2.0.
- Microsoft Cardspace [84]. Cardspace is based on the concept of information card – the infocard. In Infocard, the Service Provider is the Relying Party (RP); the Identity Provider is called the STS for "Security Token Service". Strictly speaking Microsoft Cardspace refers to the client implementation of the solution. Microsoft Cardspace is a "Claim Based Identity" system where the user can select from a user interface - the Identity Selector – the Identity Provider he wants to use. Each Identity Provider shall register at Identity Selector a card - also called infocard related to the Identity Provider. This infocard declares the URL of the Identity Provider and the claims supported by the Identity Provider. On Service Provider request, the Identity Selector displays infocard that are compliant with Service Provider requirements. User selects one infocard, then he authenticates to the related Identity Provider. The IDP computes the identity and returns it to the Service Provider through Identity Selector. Microsoft Cardspace uses SAML 1.1 token – it does not rely on SAML Protocol to exchange data. More specifically, it does not rely on "SAML Web Brower SSO Profile" but on "Identity Selector Interoperability Profile".

MERA [85], [86] (modular Enhanced Role Authentication) privacy enabler protocol consists of allowing the access to an e-service/resource that requires user profile in the following conditions:

- without disclosing user's private identification data to the Service Provider,
- while proving implicitly to the Service Provider that the user fulfills the access criteria,
- and preventing Identity Provider from acquiring knowledge about the very nature of the service requested by the card bearer from the Service Provider.

MERA fulfills the requirement of an anonymous credential system, since an identity provider (called the issuer or Identity Provider) issues a credential to a user. The credential contains the user's information (attributes). The user (called the prover) can use the credential to prove to a third party (called verifier) that she has a credential containing the required attributes or properties of the attribute without revealing further information. The proof is cryptographically secure and can be verified.
The modular enhanced role authentication is an authentication and secure channel protocol between a smart card and a client (of the smart card). The mERA has two modules (protocols):

- MERA1-3 establishes a weak secure channel, with authentication of the client.

- MERA1-7 includes client authentication, secrecy, and establishing a strong secure channel, with forward secrecy. Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) is used to setup the confidentiality of the exchange.

Identity Management has been placed in this section “Solutions not defined in the Cluster projects) because the current cluster projects were not specifically focused on Identity Management solutions. On the other side, previous FP7 projects have provided significant contributions to these areas. In particular, we would like to mention the Stork I and II project[12], whose objective was to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID and the PRIMELIFE project[13], whose objective was to address the core privacy and trust issues pertaining to use of Internet by individuals (IDEMIX in was used in PRIMELIFE as described in [87]).

Other identification technologies like biometrics, sign-on, are already available in the market for many years and they are not described here because there are many different implementations and the main concepts are well known.

Autonomic Computing

Autonomic Computing is the concept of implementing self-management functions in distributed systems to adapt to changing internal or external conditions without or minimal human intervention. Autonomic Computing was first started in 2001. Autonomic computing concepts could be used to support a resilient cyber physical systems and improve its overall security as described in [88] and other references but there is still a lack of research on how to adapt and tailor existing research on autonomic computing to the specific characteristics of CPS, such as high dynamicity and distribution, real-time nature, resource constraints, and lossy environments.

Anonymizing the Traffic in the Networks

Anonymizing networks aim to provide their users anonymity while issuing communications on the Internet. Many reasons may lead users to mask themselves to avoid their identification ranging from the freedom of speech in repressive countries, to the realization of illegal activities. Several anonymity systems exist; some just provide anonymous communications (Tor [89], I2P [90]) and others provide in addition anonymous storage functionalities (Freenet [91], GNUnet [92]). Systems including distributed data store are also called anonymous publishing networks by opposition to anonymizing networks.

In this section, we will first present the algorithms used to achieve anonymity in communications without describing a specific system. We will then briefly present the architecture of Tor and I2P. The most famous anonymizing

[12] Stork I and II projects, https://www.eid-stork.eu/

[13] Primelife project, http://primelife.ercim.eu/

network: Tor is designed to provide anonymity of communications issued by users toward Internet through the Tor network while I2P is designed to provide anonymity of communications that are within the network limits. Therefore, their architecture is different: in particular, Tor has a lot of exit nodes toward Internet while I2P only has a few but has in opposite every node participating to inner-routing. For additional material on the specific sub-case of anonymous publishing networks, readers may refer to the previous references.

To hide the originator of the message, most of the current anonymizing networks are based on onion routing [89] and layered encryption. Anonymizing networks can be categorized in 2 types: high-latency and low-latency networks.

In high-latency networks, time is not a constraint when delivering packets. Such systems rely on the concept of mix [93] which is a process that basically accepts messages, groups these messages into a batch and forwards them later on in a random order, when a threshold is triggered (based on the time, number of received messages, etc.). As they introduce much latency while creating buffer of messages, high-latency anonymizing systems provide better anonymity but are not suited for time-sensitive information. They can for example be used for email delivery while Internet browsing needs low-latency systems. Content between the sender and the receiver is always encrypted in an end-to-end way. This is to ensure the privacy of the communication as well as their anonymity, because the content itself can leak information about the two communicating parties. Additionally, to avoid possible correlations from eavesdroppers who compare the payload of the packets captured before and after the relay, the communication going in and out the relay must be encrypted with different keys: the sender encrypts the message already encrypted for the receiver with the public key of the relay before sending it.
Different low-latency anonymizing systems exist which are based on different routing approaches. The simplest way to achieve anonymity is to use single proxy as a relay that will hide the identity of the sender. However this architecture has obvious limitations, the proxy being a single point of trust and a single point of failure. To reduce the trust given to the proxy, several proxies can be used in cascades, either following a fixed predefined route or a free route dynamically computed. This architecture is called onion-routing and extends the mix strategy. The number of nodes serving as relays between the sender and the receiver is the path length. The path length is usually defined to include three nodes in most anonymizing systems. In fact, as relays only know the next step, using three relays ensure that two nodes cannot directly build a cooperation to break the anonymity of the communication as the first relay and the third do not directly know each other, and the second relay do neither know the source nor the receiver of the message. The two following anonymizing networks, Tor and I2P are both low-latency systems.

The **Tor network**[14] is based on onion-routing and use both relays and layered encryption (based on TLSv3) to build anonymity. The message sent by the source this wrapped in as much encryption layer as intermediate nodes will be used to forward the message, so that each relay only has the minimum

[14] Tor network, http://www.torproject.org/

information needed to forward the message to the next step, reducing the risk of linking information. Tor's architecture uses three main entities: directory servers, clients or onion proxies and relays or onion routers. The specific path used for a communication is called a circuit and is computed a priori by onion proxies which know the different relays from the directory servers. Relays can be used for different purposes: simple forwarding relay, guard nodes to enter the network, exit nodes communicating with external Internet nodes, etc. Additional constraints can be applied on the path selection to improve performances or anonymity, for example: routers from the same operator or country are not chosen for the same path. Tor is actually widely used with 400.000 users per day and uses 3.000 different routers and 1.000 exit nodes.

The **I2P network**[15] is also a low-latency message-oriented anonymous network. I2P main goal is to provide anonymity between I2P nodes rather than between a client node and the external Internet. Since the anonymity of the outgoing traffic is not the goal of the network, the number of exit nodes is reduced compared to Tor. I2P has a fully distributed architecture and each node connected to I2P becomes a possible router. A specific algorithm selects, for each path, the peers to be used as relays so that onion routing and layered encryption can be used to provide anonymity. The path through a selected list of nodes is called a tunnel and is a key concept in I2P. Each tunnel is unidirectional so that full duplex communications between two parties will involve 4 tunnels, each being composed of an entry point, several routers and an endpoint. Tunnels are built to balance performances and anonymity, the performance of each peer being known thanks to permanent profiling. Moreover, tunnels are reset every 10 minutes to avoid monitoring attacks.

The distributed design of I2P improves the network scalability and resilience to shut-down attempts, by opposition to Tor which leverages a central server directory. I2P supports different applications like anonymous web-browsing, chatting, file-sharing, etc. Most of the applications interact between each other within the I2P network. Applications communicating on top of I2P no longer use IP addresses but directly the location independent identifier (virtual address) provided by I2P and called destination. The link between the destination address of a node and its router counterpart (that uses the IP address) is secret which provides the anonymity.

Privacy Enhancing Technologies (Anonymous Credentials)

U-Prove [94] is a privacy-enhancing technology that enables the issuance and presentation of cryptographically protected claims. A U-Prove token (or U-Prove credential) is a set of cryptographically protected claims or attributes that are related to a user. As an example, a U-Prove credential can be used for authenticated anonymity and pseudonymity in electronic communication and transaction systems.

U-prove is a user-centric technology aiming at improving the privacy of the user by using tokens based on "blind signature" [95] instead of standard PKI

[15] I2P network, http://www.i2p2.de

signature. A blind signature is a cryptographic signature such that the signer does not view the message content, i.e. the signer signs a blinded message. Later, the cryptography mechanism permits the requester to recover the un-blinded signature. When the un-blinded message and un-blinded signature are disclosed, anyone can check the validity of the signature like for a standard PKI signature. A U-prove token is a partially blind signature - it enables the user to selectively disclose some certified attributes by using cryptographic proofs-of-knowledge. A U-Prove credential consists of a private key, a public key, a set of attributes, and a signature by the credential issuer. The signature is jointly computed by the token issuer and the user such that the issuer sees the attributes but not the public key.

Identity Mixer (Idemix) [96] is a privacy-enhancing technology developed at IBM Research that enables the issuance and presentation of cryptographically protected claims. An Idemix credential is a set of cryptographically protected claims or attributes that are related to a user. As an example, an Idemix credential can be used for authenticated anonymity and pseudonymity in electronic communication and transaction systems.
Idemix is an open-source library implemented in Java; the latest specification of the Identity Mixer cryptographic library is version 2.3.1. The Idemix has been used in European projects PRIME and Primelife[16]. IBM has proposed Idemix in the European project (ABC4Trust). The technology Idemix is a user-centric technology aiming at improving the privacy of the user by using tokens based on "group signature" instead of standard signature. A group signature scheme [97] is a cryptographic signature for allowing a member of a group to anonymously sign a message on behalf of the group. It enables a verifier to check that a signature on a message has been done by a member of a group, but not which particular member of the group has signed. In a classical group signature scheme, there is a group manager who is in charge of adding and removing group members. Optionally, the group manager or another entity called revocation manager has the ability to reveal the identity of the original signer in the event of disputes, i.e. the ability to revoke the signature anonymity. Idemix is based on a large body of cryptography research in group signatures (see [98]).

Trust Negotiation

Trust negotiation has been originally designed for open distributed computing environments [99], where the goal is to allow unknown parties to gain access to services and resources. Trust negotiation is based on the iterative requests and disclosures for credentials among the parties to achieve an adequate level of trust, which permits the access to the resources.

As indicated in [100], the practical deployment of trust negotiation techniques can be different, depending on the context and factors like the diversity of the computing devices, the link used to transmit the credentials and the computing power of the devices. As described in [6], trust negotiation in mobile ad-hoc networks requires intensive public key cryptographic calculation, extensive checking and exchange of credentials, which can be

[16] Primelife project, http://www.primelife.eu

excessively onerous on mobile devices and wireless links. For this reason, an essential criterion for the choice of the trust negotiation technique is the optimization of computing and communication resources.

Physical Unclonable Functions

Physical Unclonable Functions (PUF) is the concept of using intrinsic physical characteristics of the devices for identification. In [101], the authors apply this concept to RFID technology to improve the robustness of the authentication of PUF. As described in [101] PUF exploits the physical characteristics of the silicon and the IC manufacturing process variations to uniquely characterize each and every silicon chip. Since it is practically impossible to model, copy, or control the IC manufacturing process variations, PUFs not only make these chips unique, but also effectively unclonable.

More formally, PUF is a function that maps a set of challenges to a set of responses based on an intractably complex physical system; a challenge is an input to the function, and a response is the output. The input can be implemented in different ways. For example, it can be an RF emission. The function can only be evaluated with the physical system, and is unique for each physical instance. Hence, the PUF function provides a static mapping between challenges and responses, which is a "random" assignment.

Architectural framework

This section describes how the previous solutions can be integrated in the architectural framework and in an example of an operational scenario (Smart City/Smart Home). To visualize how the solutions identified in *Technological enablers and design solutions* can become the building blocks of a more complex framework for Governance, Security and Privacy and how they can be deployed in IoT, we used two approaches. The first is to map the identified solutions in a more general architectural framework like the one provided by IoT-A, the second approach is to show the use of the solutions in an operational scenario like the Smart City scenario defined in the iCore project.

Reference architecture

In this section, we map the identified solutions to the reference architecture described in IoT-A deliverable D1.5 [102]. IoT-A was a FP7 project focused on the definition of an architectural reference model, which can be used by the European research projects and the IERC in the IoT domain.

A new representation of the IoT-A functional architecture with the solutions identified in this position paper is presented in *Figure 12*. In the figure, the various solutions presented in section *Technological enablers and design solutions* are mapped to main functional blocks of the IoT architecture.

The solutions are represented as icons ("balls") with a coloured border for the solutions presented by the FP7 projects (section *Solutions from Clusters projects*), while "grey" balls represents solutions from the section *Solutions not defined in the Cluster projects*).

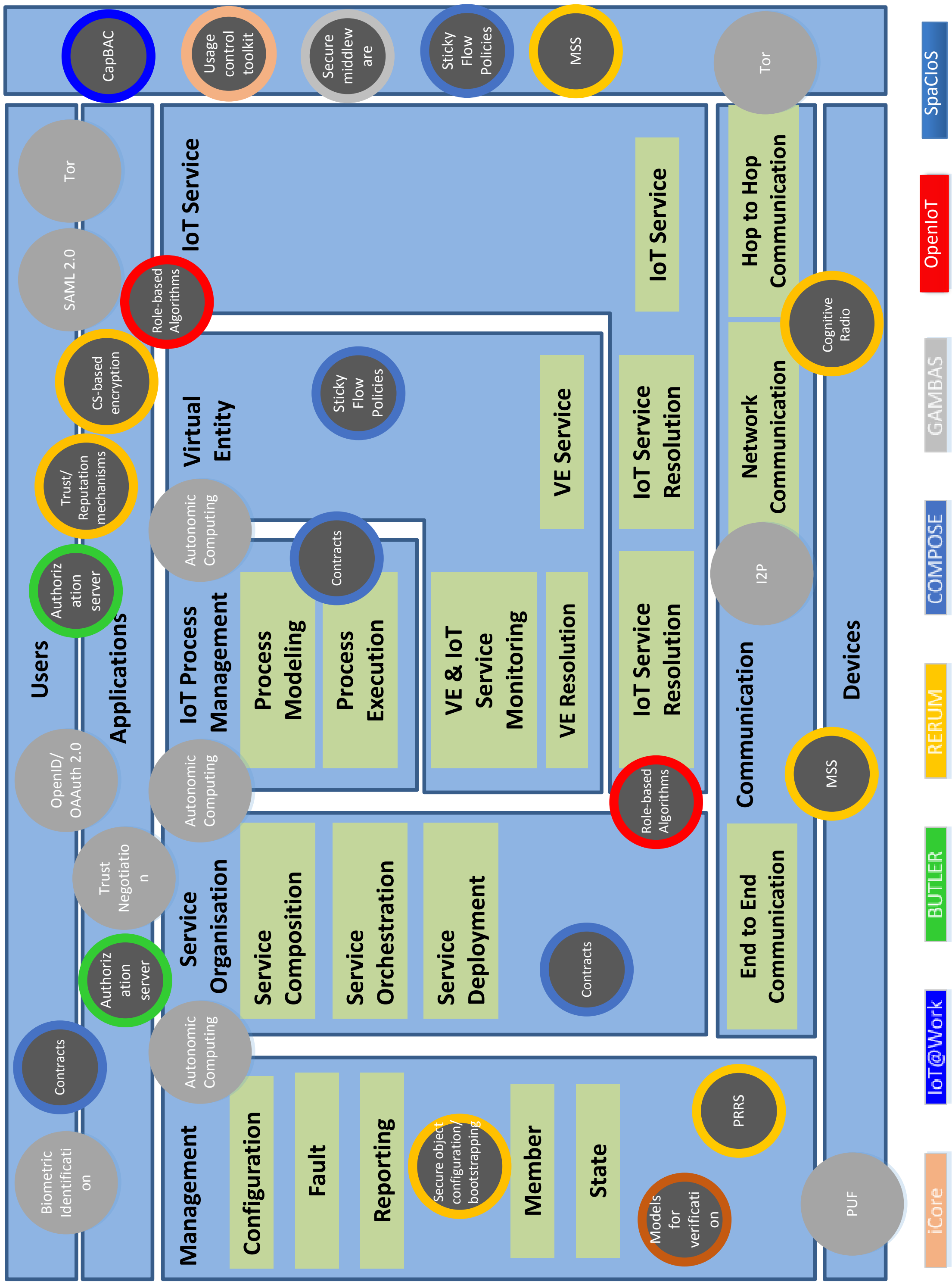


Figure 12 Potential solutions and IoT-A reference architecture

The mapping between the icon identifiers and the solutions from section *Technological enablers and design solutions* is provided in *Table 4*:

Table 4 Mapping between icons and solutions

Name of the icon	**Name of the solution**	**Related project**
Usage Control Toolkit	Usage Control Toolkit	iCore
Sticky Flow Policies	Sticky Flow Policies	COMPOSE
Secure Middleware	Secure Middleware based on policy management	GAMBAS
CapBAC	Capabilities based policy management	IOT@work
Contracts	Contracts	COMPOSE
Models for Verification	Models for verification and testing	SPaCIoS
Authorization Server	Authentication/Authorization	BUTLER
MSS	Cryptography for Use in IoT	RERUM/BUTLER
CS-based encryption	Encryption using Compressed Sensing	RERUM
PRRS	Management functions	RERUM
Secure object configuration and management	Secure object configuration and management (and bootstrapping)	RERUM
Audit	Audit and monitoring solutions	RERUM
Trust/Reputation Mechanisms	Trust and Reputation Systems	COMPOSE/ RERUM
Cognitive Radio	Cognitive Radio can mitigate attacks on wireless data communications, i.e. security attacks like jamming	RERUM
OpenID/OAuth 2.0, Biometric Identification	Control Access Server (CAS), Identity Management and Role-based Security Access Control	OpenIoT
Autonomic Computing	Autonomic Computing	OpenIoT
Tor, I2P,	Anonymizing the Traffic in the Networks	N/A
U-Prove, Idemix	Privacy Enhancing Technologies (Anonymous Credentials)	N/A
Trust Negotiation	Trust Negotiation	N/A
PUF	Physical Unclonable Functions	N/A

Most solutions can be embedded and support a specific function in the IoT-A reference architecture, other solutions can be used in different functions. For example, the Usage Control Toolkit can be used transversally in different functions of the reference architecture and for this reason, it has been positioned in the figure on the right side. Instead, the PRRS can be used to support the Management function, while the Authentication/Authorization from BUTLER can be used to support user/application layers and the interaction with the other functions.

The evolution of the reference architecture is addressed in AC01 of IERC, while specific functions are managed in specific ACs. The mapping presented in this section is dependent on the work done in the other ACs, which will probably modify and refine the reference architecture. As a consequence, the brief overview presented in this section must be revisited once the work of the other ACs is completed.

An additional task, which could be performed on the reference architecture and the smart city scenario, is the drafting of a threat analysis in a similar way to what has been done in IoT-A deliverable D1.5 [102] in section 5.2.9. Other projects (e.g., BUTLER) has also worked on the identification of security and privacy threats. A complete threat analysis has not been done here in this phase, because the activities of the other ACs are not complete yet and a common operational scenario (e.g., Smart City) has not been defined yet in the IERC. Still, we believe that this would be a useful exercise in a later phase of IERC.

In fact, BUTLER has completed the threat analysis for some use cases in IoT and this threat analysis can be integrated in this document.

Smart City/Home scenario

In this paper, we will re-use the Smart City/Home Scenario from the iCore project (deliverable D6.1).

The scenario is composed by the following main entities: Smart Home, Ambulance/Hospital/Government (traffic management) and Police department.

Today a smart home should easy up the life of the consumer with technical devices that provide a variety of functions like remote activating/deactivating power sockets, automatic heating systems or alarm systems. The issue from end-user point (owner of a smart home) is to combine different sensors and actuators without the complicated installation of various networks or even the technical know how about those systems at all. The setup phase usually is not applicable without technical knowledge and background information. For this reason smart home scenarios rarely find their way into elderly home care stations. Old people want to live on their own, but it is dangerous to be without any care taking or without medical care a whole day. Every minute saved in the rescue process after a heart attack or a fall is essential for survival or at least much less painful and much less costly treatment. To gain medical attendance or at least assisted living it is important to apply an easy-to-use and easy-to-install care system that can fulfil different, specific user requirements due to an easy-to-manage personalization process.

Therefore, from an end-users perspective, an IoT system should be able to provide the following services/applications to the elderly or impaired people:

- Provide security to the user in terms of real-time alarm (fall detection, pulse alarm, etc.) in a convenient manner (e.g. without limiting daily routine through cables, heavy weighted sensors or devices).
- Enable access through well-designed and easy to use User Interfaces (UIs) that allow the configuration (setup/change) of the preferred individual and specific conditions on various parameters (e.g. the environmental temperature, the humidity or the light intensity).
- Provide panic-mode button, enabling the users to alert attendance in case of emergency based on their own judgement.
- Receive recommendations for the user coming from the IoT system according to rules approved by a nurse/doctor or by a care taking assistant or by a family member/friend.
- Enable emergency assistance from a nurse, a day care assistant or a family member/friend according to dedicated individual rules specified in IoT (e.g. in service templates) with the possibility to choose and authenticate the assistant (prevention against false assistants, frauds, crimes).
- Reminders that will help the patients to follow certain activities, such as performing ergo sports or taking medicine in the right time and order.
- Provide additional services that will enhance the independent life and will facilitate the elderly or the patient (e.g. a system for the remote control (open/close) of door(s), a service that will automatically send the orders of medicines or a service that will take over to monitor the people outside of the home by caring for their safety – e.g. to control traffic lights so as to help people to cross the road near the Smart home).

In a medical care station or in a hospital the doctors or nurses like to monitor environmental conditions and/or the health status of patients. Wireless sensor networks can be used to collect the data and to communicate all values to a central place like the medical care taking office or a hospital staff room. In emergency cases, the staff can react on critical or alarm notifications immediately without the distress call from a patient.

This use case is interesting from an IoT perspective, as there is a complex ownership of sensitive private data and real world objects that are associated to patients and their vital functions. Nevertheless next to the sensitive data the self-configuration of the IoT system can be used to easily share information about the patients with nurses, doctors and instructed personnel remotely.

The ICT infrastructure required can be deployed only locally in medical care stations and with the permission of the patients. The IoT ecosystem can be applied inside the medical care centre, taking into account sensitive data that will be secure and protected by appropriate mechanisms, allowing in parallel, the remote monitoring of patients as well.

From a nurse/doctor or medical staff perspective, the IoT application should be able to provide:

- Real-time monitoring of health status of patients (e.g. vital conditions such as pulse, body temperature, fall detection, etc.) and automatic alerts, warnings or actuation of alarms in case of emergency or crossing certain threshold defined individually, e.g.: the patient faints.
- Real-time monitoring of environmental conditions in the smart home (temperature, humidity, luminosity, etc.) and configuration of specific thresholds, for the sensed data, that will trigger automatically specific compensation functionalities (e.g. if temperature is lower than x degrees then turn on the heating system).
- Early-warning in case of estimation for system failure to ensure the reliable fulltime monitoring of patients by activating different systems.
- (Self) Rehabilitation assessment using wearable sensor devices remotely monitored by doctors or physiotherapists.
- Secure ownership of sensitive data with shared access rights depending on the security level (doctors, nurses, trainee, etc.).
- Easy-to-setup, control the monitoring system for the patient.
- Automatically combine certain information streams on an individual base for the patients (e.g. accelerometer and pulse measure sensor to enhance knowledge of conditions).

For a day care assistant or a family member an IoT application can provide beneficial functionalities to easy up the activities related to assisting elderly people in the daily life. Usual day care assistants provide a service for elderly people in their everyday life like ingesting pills, purchasing and delivering demanded materials and food, assistance in indoor work or checking vital functions. Many services can be provided as outpatient care either from companies specialized in ambulatory care or from family members supported by the federal Ministry of Health.

This use case is interesting from an IoT perspective, as it will handle different scalability factors depending on the user. For ambulant day care companies it is necessary to share and store sensible data of the patients with dedicated ownerships beginning from the assistance of the patients up to the supervision of the department. It is required to share patient's information between employees through all working shifts to provide full-time support without losing any information. As a family member the IoT system shall provide a remote interface to inform about vital functions or in case of emergency or any other threshold crossing individually defined. Therefore from a day care assistant and family member point of view the IoT should be able to provide the following services/applications:

- Record protocols of assistance remotely to share between involved employees/stakeholders.
- Monitor and store health status (e.g. vital functions like pulse and body temperature that are measured during a visit).
- Provide alarm system in case of individual threshold crossing or emergency (e.g. fall detection, requested help, etc.).
- Secure ownership of sensitive data with shared access rights depending on the security level (family member, day care assistant, trainee, …) and possibility to share this data with hospital or doctor in case they are required (e.g. normal visit or even emergency) – structured and integrated patient's consent management with context awareness and automatic switching in emergency situations.

- Share real time task scheduler between involved employees/stakeholders (optimize and ensure job completion including quality control).
- Provide additional services that will enhance the quality of the independent life and will facilitate the patient (e.g. any smart home system, such as for the remote control (open/close) of door(s) or a service that will automatically pre-announcements of the orders of medicines).

From pharmacy perspective, the pre-order of medicine can be optimized with knowledge about the private stock and the availability. To achieve an optimized inventory a pharmacy could communicate to doctors and patients in order to get previous knowledge of needed medicine before a patient will arrive at the pharmacy. A pharmacy then will be able to inform the patient directly about the availability of the needed medicine. Next to the easier communication the patient can receive the medicine via post mail at home without the need to go to a pharmacy. The patient can also be guided to the pharmacy, where the dedicated medicine is available/in stock without waiting times. The IoT system should be able to provide following services/applications:

- Monitor sensitive data about stock of medicine.
- Provide secure interface to inform about changes in therapy/medicine between doctor, patient and pharmacy.
- Automated pre-order system to optimize availability of medicine in the pharmacy, as well as to advice several equivalent medicine in case of lack of the preferred (subject to be approved by a doctor or pharmacy expert).

As a system operator, ownership, privacy and security of the information is of crucial interest. Privacy and security is more about to concern in health applications. From system operator point of view iCore will provide following services:

- Ownership management capability.
- Security, privacy and access rights management of the information.
- Scalability of health data and information management system.
- Self-X capability and intelligence in the systems to enable autonomic decisions or specific proposals to be approved (e.g. depending on the emergency level).
- Flexibility in terms of scalability (e.g. number of users that can be managed at a site, etc).

The potential implementation of the smart city/smart home scenario is shown in *Figure 13* where the emulated smart city includes a smart home that is equipped with actuators and sensors hosted by Wireless Sensor Network (WSN). The medical center uses sensor measurements from networks deployed in the smart home in order to monitor both patient's vital parameters and environmental conditions (lights, temperature, etc.). In a similar way, the Mobile Centre, Police Department and Government collect data coming from sensors installed in the city and monitor crucial activities: links for data exchange among these entities are preferably wireless.

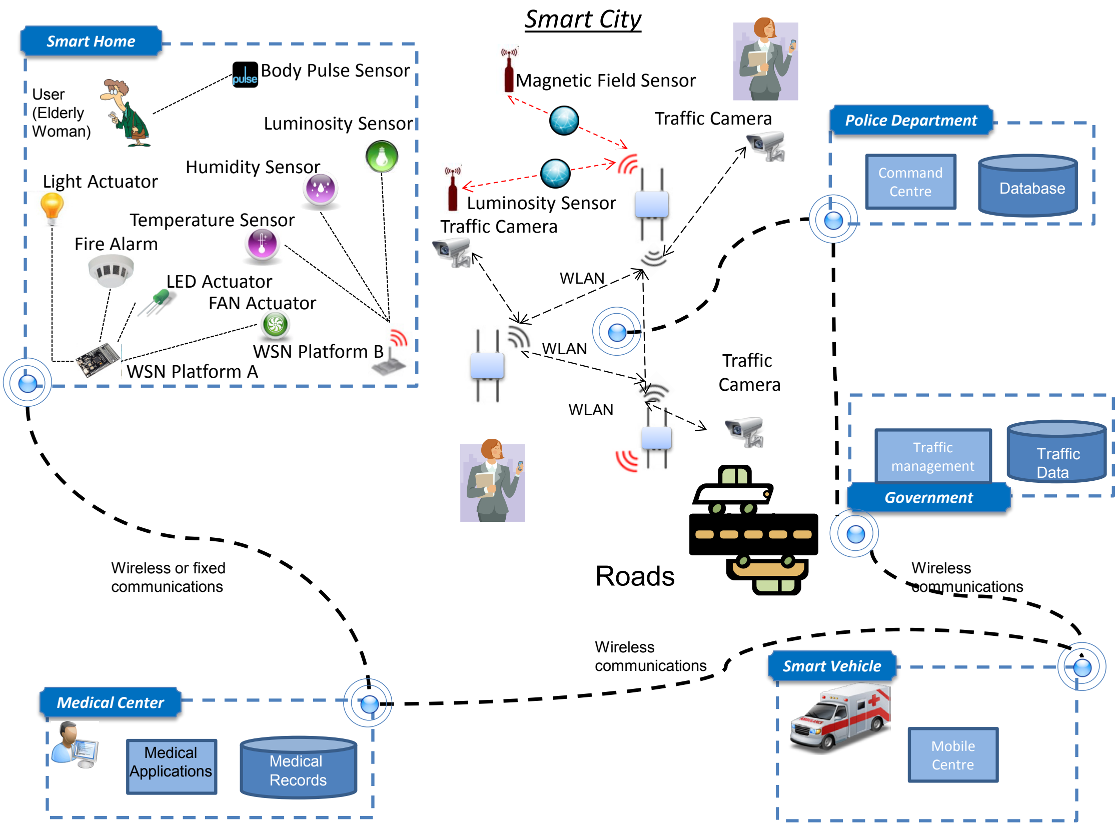


Figure 13 Smart City/Smart home Scenario

The solutions proposed in the framework can be inserted in this kind of scenario to support specific and critical parts of the architecture from the technical point of view. The *Usage Control Toolkit* intervenes in all that situations in which a secure identification of the context, the role and the identity of the actors involved in the smart scenario is needed. For example, if vital parameters of the patient overtake a given threshold an automatic alarm is sent to the Medical Centre and then to the Smart Vehicle that has to come into action: staff in the vehicle, according to their roles and the defined policies, are allowed to consult sensitive patient's information relevant for that context.

At the same time, *Sticky Flow Policies* can be employed to annotate security policies of the data flowing from an entity to another: the example given above is a typical situation in which information on how to exchange and use data flowing through the network in the scenario are essential. Moreover, since data flowing in the network are particularly sensitive and channels usually wireless, the *Malleable Signature Schemes (MSS)*, together with the other cryptography solutions proposed in the framework, can guarantee integrity and authenticity of the data while the *Authorization Server* and the *Bootstrapping protocols* authenticate and authorize of both users and devices, assuring only authorized access to the resources.

The *Secure Middleware* will help to easier detect the context and then automatic switching and authorizations: fast, correct and also privacy aware context detection are crucial issues in (medical) emergency situations. In the same way, depending on the context, the *CapBAC* mechanism will ensure the correct application of rights granted to different actors also relying on information coming from *Trust and Reputation Systems* about their reputation.

The overall behaviour of the solutions deployed in the smart environment should constantly be monitored and evaluated, in order to verify proper working, errors, gaps and possible improvements. To this end, audit and monitoring solutions like *Platform for Run-time Reconfigurability of Security (PRRS)* and the *Models for Verification* can collect all the information to evaluate and monitor the system but also to certificate quality of services and establish service level agreements for all the sites involved in the scenario.

Framework against the challenges

Here we describe how the framework is able to address the challenges identified in section *Identification of challenges for Governance Security and Privacy in IoT*.

IoT challenges schema

The whole structure of this paper is basically centred on the identification of main IoT challenges and subsequent presentation and analysis of the possible solutions. This approach can be summarized and depicted as shown in *Figure 14*: the schema is essentially a graph in three different levels, two of which, the first and the second ones, identify the challenges and the third one the solutions proposed in the framework. The matching between the solutions proposed in *Solutions from Clusters projects* and the Icons is the same already provided in *Table 4*.

Challenges are identified at two different levels, considering the subdivision into the three main topics of governance, security and privacy (macro challenges level) which are explained in more details at the second level (detailed challenges level); it can be seen that one challenge in the second level can originate from more than one macro challenge.

The specific solutions level contains the components of the framework that address the challenges above. Each solution is identified by the colour of the corresponding project that contributed to its integration in the framework. One or more solutions can be grouped on the basis of their common characteristics or tasks they absolve. For example, the Authentication and Authorization Server proposed in the BUTLER project, the Usage control toolkit of iCore, the CapBAC of IoT@Work and the Secure middleware of GAMBAS are all related to Access Control and then grouped; the last one, Secure middleware, also absolve to tasks related to data protection and for this reason is placed partly inside the box.

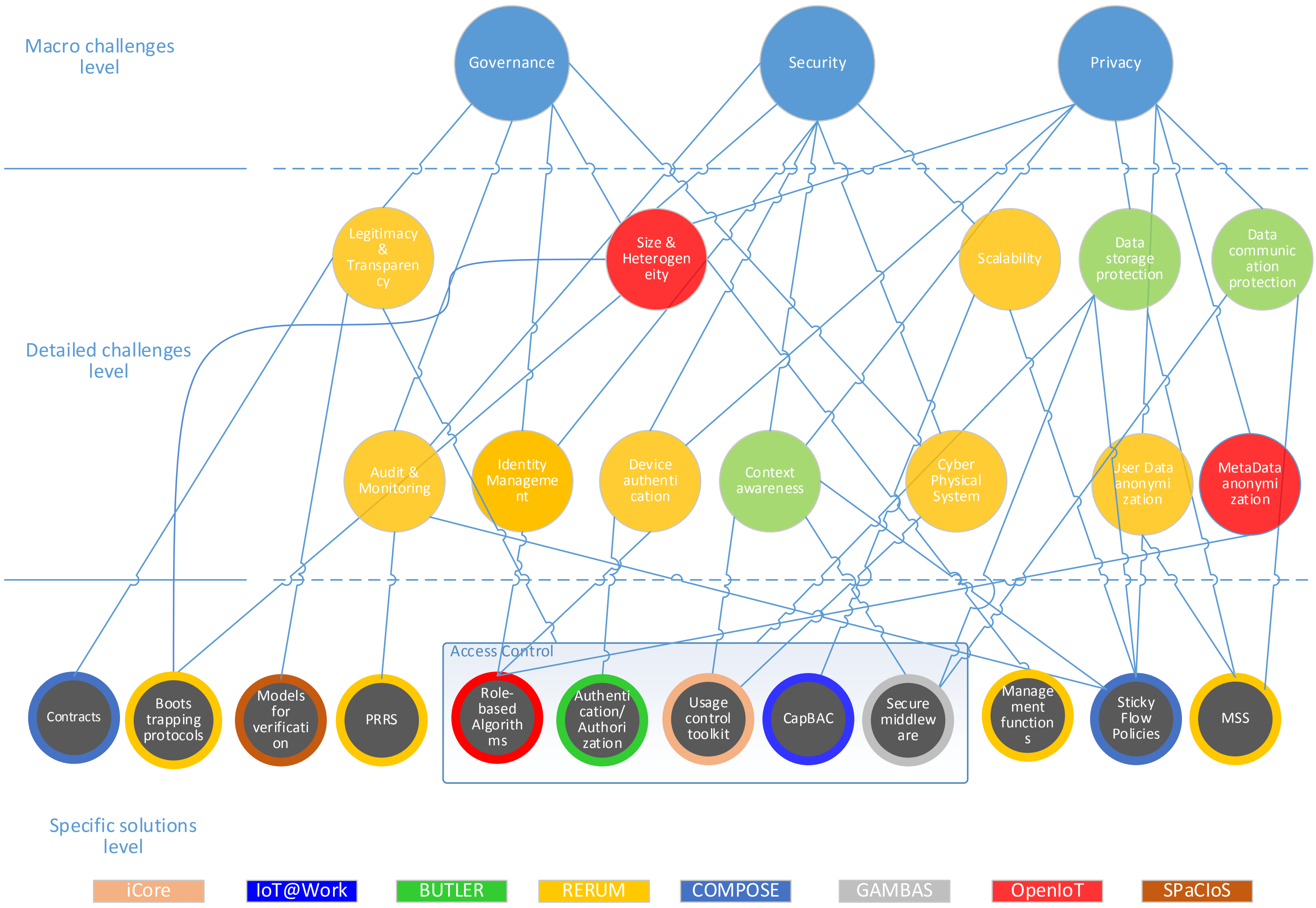


Figure 14 The IoT challenges schema

Challenges in level two are in three different colours: green, orange and red. Green means that the challenge has been satisfactorily addressed by one or more solutions proposed in level three, orange that the solutions can be improved or increased and red that solutions for the challenge are not sufficient. In this way, it is possible to see which areas of IoT need to be investigated again and also where it is necessary to search for already existing technologies that can be adapted to address a specific challenge. For example, the figure shows that the challenges of Size & Heterogeneity and MetaData Anonymization are not well addressed: this means that more efforts should be made to investigate in these areas specifically for the IoT. Indeed, as explained in the overview of the challenges, these problems are not new at all and have already been investigated for classical networks and Internet.

Starting from this assumption and from the gaps identified by the graph proposed in *Figure 14*, the first part of the effort should be focused on finding and trying to adapt products and solutions that already solve similar problems in different contexts. For example, the challenge of the data anonymization, could be addressed using the same approach that Tor (The onion routing) employs to protect TCP communications.

In this way we obtain a new graph (*Figure 15*) in which, in the lowest level, appear existing technologies that can possibly fill the gaps or be a valid starting point to reach this end. The candidate existing technologies are classified according to their level of maturity: consolidated technologies (more than 10 years), medium level of maturity (between 3 and 10 years) and emerging technologies (less than 3). This gives a first indication of the effort needed to improve a technology in terms of research and studies and also contributes to the determination of the new colour of the challenge addressed. Adding possible solutions help us to see if and how a red or orange challenge in the second level is improved by a technology proposed in the third level. For the particular example of Tor we can see an improvement from a red to an orange level for the MetaData anonymization challenge: even if Tor protects the transport of the data, it does not solve all the anonymity problems and the protection of personal information. For the same gap, we also indicated I2P as a complementary solution, but since both technologies should be integrated and especially tuned on IoT systems we do not reach a green.

For the Identity Management challenge, orange in *Figure 14*, according to the Identity management subsection, in *Figure 15* it is possible to list several technologies and techniques employed to solve particular problems or applied in particular contexts. In this way we can see an improvement to green even if, as just explained for Data anonymization challenge, an effort to adapt, integrate and create reference standards and schemas especially for IoT applications is needed. This means also that a big part of the effort should firstly address the Governance macro challenge, which plays a fundamental role in the coordination and standardization of possible technical solutions. For the same reason the Size&Heterogeneity challenge has difficulties to reach the orange state even tough good technical solutions have been proposed in the framework.

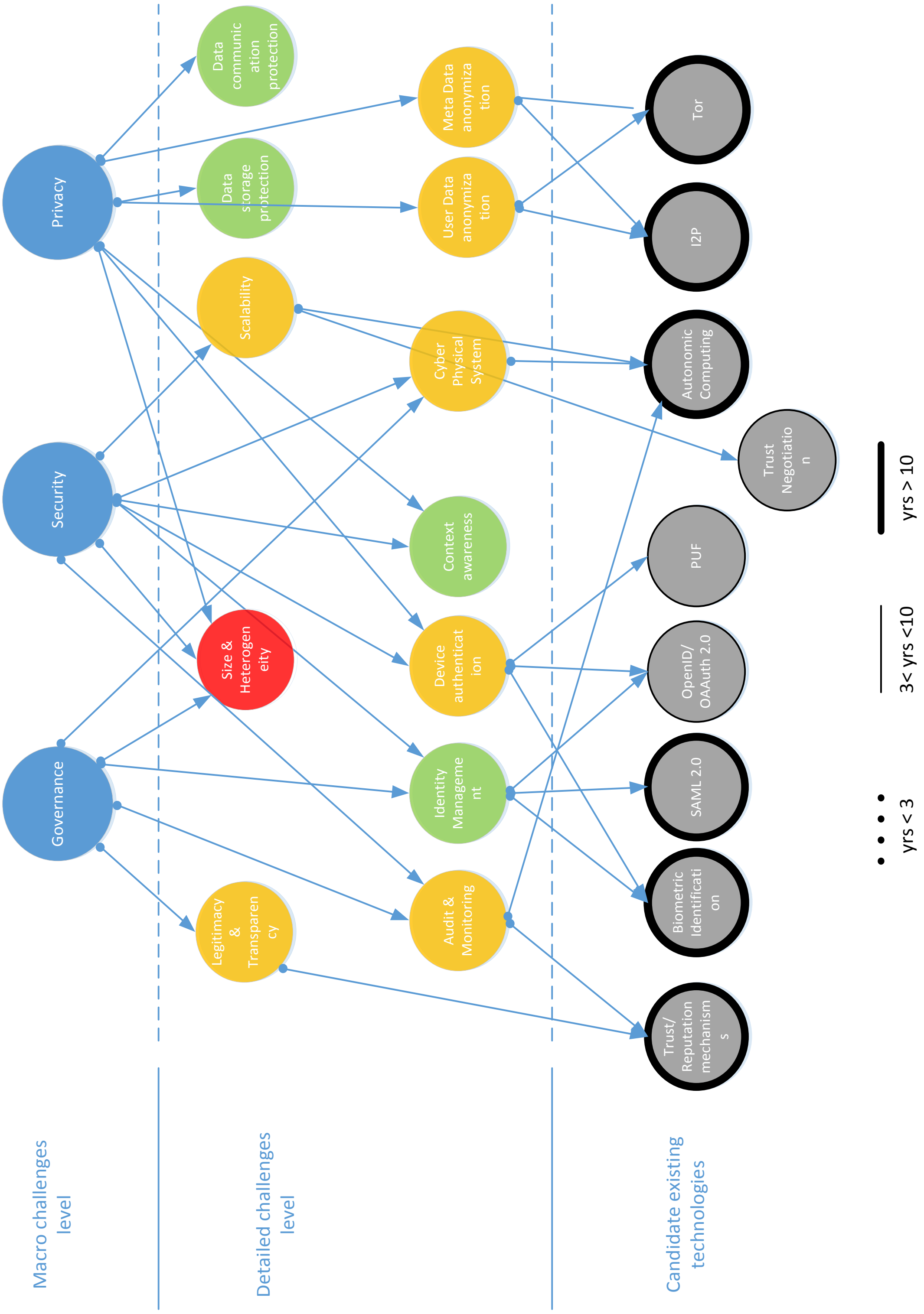


Figure 15 Addressing residual IoT challenges with existing technologies

Way ahead and impact

Introduction

This position paper has been created in the context of the European Research Cluster on the Internet of Things and it is mostly focused on the research domain; therefore, this paper will not propose specific policy recommendations. Regarding specific policy recommendations, we refer to the Communications and technical reports available on the DG CONNECT Trust and Security page [103] and excellent report by Rand [1].

In this paper, we just present the following considerations regarding the policy context:

1. Even if we are successful in identifying potential options for the future research work for Governance, Ethical, Security and Privacy aspects in IoT, we must also highlight that without policy or standardization support, any research solution risks being non-effective and the research work wasted.
2. IoT is going to be pervasive in many different domains with different operational and technical requirements and various contexts. The deployment of technical solutions to ensure anonymization or access control can be quite different in each specific context. Research activities should also focus on the deployment and organizational aspects.
3. It is widely acknowledged that in order to make inroads into establishing influence and effective controls over IoT's overall direction some form of global governance is needed as soon as practically possible. Without IoT governance the adoption of an IoT supporting the IERC definition will be challenging due to the breadth of legacy application solutions, technologies and stakeholder interests. Those organizations which have been promoted as IoT governance sole custodians will require some process of adaptation enabling them to inspire stakeholder confidence in fulfilling their principle requirements. There is a very real potential for IoT fragmentation if adequate time and efforts are not invested in the process of establishing IoT governance without taking great care and paying sufficient respect to major influencing sectors. To gain a unified cross platform and application domain IoT will require governance. The earlier a start can be made the more chance IoT has of being built upon broad accessibility. An IoT governance framework offers inclusion and an influential start-point towards the establishing of a fully effective and sustainable IoT governance model built upon the expectations of progressive convergence. To achieve this framework more focused governance related efforts are required to define and analyse the variety of governance stakeholders (who) and, in defining the initial key IoT governance requirements metrics (what, with measurable objectives/targets). This research would provide the basis for a governance framework proposal which can be refined through peer review in the establishing of an initial working model. This working model may set-out under the leadership of one body or equally a number of organizations, the essential aspect is that it establishes sufficient authority through due diligence.
4. There is a tension between the anonymity of users in the IoT world and the need by law enforcers to identify criminal activities. In this sense, anonymity could be a double-edged sword and this aspect should be taken in consideration in the definition of governance, security and privacy solutions.

For the identification of the potential research activities, we also refer to the excellent Red Book "Roadmap in the area of Systems Security" [104] produced by SysSec consortium and its constituency. The scope of the Red Book is wider than this position paper, which is specific for IoT, but many considerations and recommendations from [104] can be applied for IoT as well.

At a general level, the most significant issue in IoT is the fragmentation of the market and the IoT context in various vertical systems with specific governance, security and privacy solutions. User (business, government, public, etc.) requirements are the main drivers for the development of IoT systems and infrastructures by manufacturers and service providers. The rights of the citizen (e.g., privacy) must be guaranteed and the government can definitively play a role in this context. The governments have the responsibility to protect the citizen rights and this implies a political and policy stand through concrete actions. On the other side, government actions should also balance the risk of hampering business and market developments which could benefit the community and improve the technological evolution and competitiveness of the European Union.

Research Opportunities

More specifically and with reference to the gaps identified in *Framework against the challenges,* we can identify the following research opportunities:

- **Usability in Authentication** (also mentioned in [104]). There is a considerable gap between security and usability in current forms of authentication. Researchers have defined strong authentication mechanisms, but the generic user may have difficulty to use them because they are difficult to implement or apply (see digital divide challenge). On the other hand, security mechanisms (text-based passwords or 4-digit PINs), which are easier to use can provide low security guarantees. One research challenge is to invent new rich authentication mechanisms, variants or combinations of the currently existing ones that provide better security without sacrificing usability.
- **Design methodology to mitigate the digital divide**
  To address ethical needs, usability needs to be ensured by design that incorporates diverse range of needs of heterogeneous population -even when age-segmented, provides aesthetically pleasing and intuitive solutions that encourage an older user rather than promote a feeling of inadequacy. Older users should be a part of the design process in all its stages following the co-creation and co-design approaches. The product design should be focused on promotion of *Design For All* methodology rather than niche solutions. The design phase of mass produced ICT products should consider how these products could be easily and cheaply adopted as products by citizens and namely by older users. Many of the ethical and regulatory issues associated with e-health and telemedicine are well documented, particularly privacy and data protection, informed consent, equity and accessibility. Further research is needed to consider less recognized implications, such as the risk of confinement, social isolation, the potential of a person’s home becoming their health clinic, risks associated with quality of online professional practice and electronic health resources, regulation of online research with a view of protecting the privacy of contributions,

and impact of ICT technology adoption on the user relationships and potential changes to personal responsibility.

- **Policy management access control** has been proposed by various projects with different names in the IERC cluster (see *Solutions from Clusters projects*). The European research community has a sufficient level of knowledge in this area to progress on a next step to develop a complete framework, which can be standardized and made available to the community. In particular, the framework can be used to support mobile security and deployed on mobile platforms (e.g., based on android) to support security and privacy of the users even from their mobile devices. The definition of this access control will target significant challenges identified in this paper and other references: the capability to provide control to the user and his/her data and the capability to enforce regulations, best practices or soft laws through policies.
- **Certification of IoT services.** As described before, there should be a way to provide a level of confidence for trust of entities, which provide IoT services to the user. While organizations and regulators aspects can be preeminent in "certifying" an IoT Service (e.g., a web server or a device), technical solutions can be provided to support the certification process. One example is the validation and modelling tool defined in *Models for verification and testing*.
- **Trust, Reputation and Identity management frameworks,** which can provide a complete and coherent mechanism to the user. While specific solutions have already been identified in *Technological enablers and design solutions*, more work must be done in defining a coherent framework and investigate the deployment challenges (see also section 21 and 25 of [104]). Research efforts should be directed to address interoperability issues among different IoT service providers and usability for the users. The identity inheritance process between an user and its IoT devices should also be deeply investigate, to enforce the control the citizen should have on the IoT device actions when operating in his name
- **IoT information flow control, privacy and IoT data fusion.** IoT promises to be more and more pervasive in the coming future. Sensors and smart devices will collects and transmit huge amount of data. In several cases, data collected by a single IoT device will not infringe relevant portions of the citizen privacy. However aggregation of huge amount of data coming from geographically and logically sparse sensors, can jeopardise the privacy of the citizen. Frameworks allowing to perform, given a set of policies, trusts, privacy-preserving data fusion and mining, would be required to exploit the huge potentialities of the IoT data collection capability, while at the same time protecting and preserving the citizen's privacy right.
- **IoT authentication and communication's integrity.** Authentication and confidentiality are normally achieved through the use of traditional crypto-systems, generally based on PKI paradigms. However, IoT is, by definition, composed by fully distributed systems, with discontinuous connection availability and, not rarely, with energy-consumption and computational power constraints. Under this light, new, distributed and lightweight authentication and integrity frameworks should be explored to cope with the peculiarities of IoT devices.

- **Security in Cyber-physical systems.** While some solutions have already been proposed in the area of Cyber-physical systems (e.g., autonomic computing), there is still work to do in the definition of security solutions to address security threats to specific protocols (e.g. ICS). In this context, new standards are required, both from a technological and a governance perspective. The evolution of CPS must also take in consideration the increasing use of commercial COTS in the industrial infrastructures for improved cost effectiveness. Such COTS may not be designed on the basis of the same requirements defined for the rest of infrastructures and this may create new vulnerabilities as integration issues may arises.
- **IoT Software development and validation.** Software in IoT is often developed without taking into consideration security implications. As for others ICT field in the past, projects should identify means to cope, on a side, with the performance and quick-prototyping requirements of the IoT world, and on the other with the pressing need for standards for secure software development in the IoT.
- **Vertical/Horizontal access control. Access control and authorization** are important aspects of several M2M scenarios, they involve a number of M2M roles in different positions depending on use cases. A general authorization and access control framework can be extracted that involves a few invariable access control notions which are mapped to M2M roles according the scenarios; such general authorization and access control mechanism needs device identity and security credentials. However, in real world IoT applications the supporting devices are progressively less bound to one specific system operator. As a consequence use of these devices within a secure vertical or horizontal use case requires a means to securely integrate the device in the security framework by setting up device identities and security credentials. The research projects shall investigate how to rely on dynamic device runtime environment to extract and securely disclose invariant data for a reasonable duration that can be used as initial security credentials enabling the bootstrapping of the end-to-end security and the user control of such security mechanisms.

Each of these research opportunities is linked to the solutions identified in section *Technological enablers and design solutions* and to current regulatory and standardization activities. A summary of the potential impact is provided in *Table 5*.

Table 5 Summary of the research opportunities

Research Opportunity	**Potential Impact**
Governance Framework Study and Support Action.	Developing the foundation to a multi-stakeholder governance framework which supports the IoT definition developed by the IERC. Additional supporting actions to form an initial operational IoT governance model built upon the preliminary foundational study.
Policy management access control	The results from the existing IERC cluster projects could be re-used to develop a toolkit, which can be

	made available for free (downloadable) by the EU to support the privacy and security of the citizen. The toolkit could be created in combination with other existing tools (e.g., Tor). The toolkit could be easy to download from an EU web page and it should be easy to install (e.g., like an application or anti-virus). While a Horizon 2020 project could complete the framework, the deployment and maintenance of this framework could be challenging and would require the support of a private company.
Usability in Authentication	Based upon existing and anticipated IoT use cases establish the criteria and measures for determining usability as a benchmark for future research and standardization prioritization. Define best practices and guidelines to improve the usability of authentication solution once they are deployed in the market.
Design methodology to mitigate the digital divide	Research in a *Design For All* methodology for all class of users rather than niche solutions for specific classes of customers. The design phase of mass produced ICT products should consider how these products could be easily and cheaply adopted as products by citizens and namely by older users.
Certification of IoT services	The definition of tools to validate and certify an IoT service could support the certification process described in Article 39 of [105] (REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data)
Trust, Reputation and Identity management frameworks	Develop the key common criteria which ensure interoperability between IoT cross domain applications through exploitation of the governance framework (see *Governance Framework Study and Support Action*). Develop trust and reputation mechanisms, which could support the interaction between user and IoT services. In a similar way to *Certification of IoT services*, these mechanisms could assess the level of trust of IoT services and provide an indication to the user. The mechanisms could be embedded in standards, recommended as best practices for IoT development or requested by regulations.
IoT information flow control, privacy and IoT data fusion	Based upon the established IoT Architectural Reference Model (ARM) determine the control of information flow from digital device (e.g. smart phone) to Cloud and, addressing potential security threats to data governance.
IoT authentication and	As above but focused upon common shared

communication's integrity	requirements for IoT device and service authentication and related communication integrity.
Security in Cyber-physical systems	The solutions defined in this research activity could be a direct input and contribution to standardization activities in the industrial sector: for example ETSI TC M2M.
IoT Software development and validation	The results from these research activities could be embedded and drafted in Best Practices or Guidelines.
Vertical/Horizontal access control. Access control and authorization	The results of this research activity could be a direct contribution to ETSI TC M2M and similar standardization activities.

Links with Standardization activities

The following standardization activities are identified:

- ETSI Machine to Machine (M2M) and oneM2M

ETSI TC M2M has investigated security aspects in TS 102 690 and TS102 921 through the definition of interfaces and related security solutions. In particular, M2M uses XML_DSIG and XML_ENC to provide integrity, message authentication, and/or signer authentication services for data of any type. Future work will address the issue of hiding the identity of the users to validate privacy requirements. ETSI TC M2M WG4 is dealing with Security aspects.

AC5 can participate to the activities of ETSI TC M2M WG4, by proposing the solutions defined in the cluster projects. The contributions must be based on the level of maturity and applicability to the industry context. This analysis must be done in AC5 before a contribution is proposed to M2M.

One example is the policy based framework from iCore, which can enhance the Access control mechanism adopted in M2M and described in TS 102 690 Functional architecture.

From M2M, the standardization activity has continued in oneM2M, which has been launched in July 2012. oneM2M is committed to unifying the global M2M community by developing a cost-effective, widely available service layer that meets the needs of both the communications industry and vertical industry members.

oneM2M is governed by a Steering Committee (SC) made up of all Partners, and is supported by Finance, Legal and MARCOM sub-committees, as well as a Methods and Procedures group. Technical work is progressed by a Technical Plenary, organized into five working groups: Requirements (WG1), Architecture (WG2), Protocols (WG3), Security (WG4), and Management, Abstraction, & Semantics (WG5).

AC5 could contribute to WG4. At this moment, it is not clear which security solutions defined in AC5 are more suitable for OneM2M.

- OASIS Message Queuing Telemetry Transport (MQTT)

Message Queuing Telemetry Transport (MQTT) TC, explicitly designed for IoT networks and based on the already-industry-deployed MQTT v3.1 and the Eclipse Foundation open source framework; and the OASIS standard Advanced Message Queuing Protocol (AMQP), widely used in the financial industry.

The OASIS standards MQTT and AMQP are valid starting point to support a secure middleware for the flow of data in the IoT world. From this point of view, solutions for specific IoT devices and systems defined in AC5 can be integrated with MQTT for secure data flows. For example, the policy based frameworks defined in GAMBAS and iCore are already integrated with MQTT.

The OASIS eXtensible Access Control ML (XACML) can be extended with the policy based framework defined in the AC5 projects and integrated with identification based solutions.

Links with other Activity Chains in the IERC

AC1 - Architecture approaches and open platforms
AC5 contribute to AC1 in two ways:

- By providing software frameworks and libraries, which are the implementations of security and privacy solutions defined in AC5 projects. For example: the Usage Control Toolkit of iCore is going to be uploaded to AC1 web site so that it will be available to all the research community
- By contributing and enhancing the security and privacy solutions defined in the Architecture Reference Model.

AC2 - Naming and addressing schemes. Means of search and discovery
Currently (June 2014), there are no specific collaborations in this area, but the naming and addressing of objects is directly related to identification and authentication of IoT objects.

AC3 - IoT innovation and pilots
Currently (June 2014), there are collaborations at the moment.

AC4 - Service openness and interoperability issues/semantic interoperability
The concept of interoperability and certification of IoT objects is directly linked to security and privacy because the certification can become a “brand” of security and privacy solutions implemented in IoT systems to better protect the citizen and his/her personal data.

AC6 - Standardisation and pre-regulatory research
We discussed with AC6 the standardization opportunities identified in Links with Standardization activities related to ETSI M2M, oneM2M and OASIS.

AC7 - Cognitive Technologies for IoT
Currently (June 2014), there are collaborations at the moment.

AC8 - Societal Impact and Responsibility in the Context of IoT Applications
Ethical aspects are addressed in AC5 and they are an important link to AC8. One of the topics which are jointly explored between AC5 and AC8 is how to use policies to give more control to the user for his/her personal data. In addition, the consent of the user can be implemented in a more effective way on the basis of solutions provided by AC5.

Report from IoT Week, June 2014, London UK

Activity Chain 5 participated to the IoT Week in London in two sessions:

- IERC-Trusted Internet of Things (17th June)
- Semantic Interoperability; Security, Privacy, Trust & the ARM

Table 6: Participants in the IERC-Trusted Internet of Things

Name/Surname	Organization/Company	Project
Raffaele di Giovanni Bezzi	European Commission DG CONNECT	
Maarten Botterman	GNKS	Smart Action
Ricardo Neisse	European Commission DG JRC	iCore
Jorge Cuellar	Siemens	RERUM
Juan David Parra	Passau University	COMPOSE
Christine Hennebert	CEA-LETI	BUTLER

The panel had a very active discussion on the definition of the new Data Protection Regulation and how this is going to impact the evolution of IoT. It was discussed that IoT connected objects can generate an enormous amount of data, some of which actually constitute personal data.
How is the new data protection regulation going to deal with that?

The main elements of the new data protection regulation are:

- *A right to be forgotten*: When you no longer want your data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.

- *Easier access to your own data*: A right to data portability will make it easier for you to transfer your personal data between service providers.

- *Putting the user in control*: When your consent is required to process your data, you must be asked to give it explicitly. It cannot be assumed. The goal is to make the citizen responsible for his/her own data.

- *Data protection first*, not an afterthought: 'Privacy by design' and 'privacy by default' will also become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example on social networks.

We discussed in the panel how these request could be implemented through technological solutions and standardization processes. There was a general agreement that current consent process is not efficient. Users must read a very long text and approve it. An alternative way would be to create pre-defined policies which could be adopted by the user to access IoT services/applications. These policies could also be customized by the user or different policies can be pre-defined for different type of users (young generations, elderly people and so on).

Privacy by design can be quite challenging to implement because of the different technologies/interfaces which exist or will exist. On the other side, various solutions identified in the projects can overcome these challenges. The main focus on the solutions should be on the identification of the different objects present in IoT, a secure middleware for the exchange of data and policy based framework, which can be used to protect the data or implement privacy by design. The presentations provided by BUTLER, iCore, RERUM and COMPOSE were along these lines and we identified a common approach, which will be developed further in the following months.

The proposed approach is to combine the policy-based framework designed in the four projects in combination to a federated identity management scheme. The policy-based framework is able to support different context or changes of contexts, support both access/storage of data but also the flow of data originating from the IoT devices and sensors to the main central servers.

In the Semantic Interoperability; Security, Privacy, Trust & the ARM session, Gianmarco Baldini presented the current activities of AC5 and the next steps. The plan is to finalize the IERC position paper in July and start a new deliverable, which will describe the proposed framework and how it can be integrated in the ARM or linked to standardization activities. The main outcomes of the presentation and the subsequent discussion were that:

1) A link to standardization activities is needed to support the concept of IoT certified products or best practices guidelines where security and privacy requirements can be validated. This is similar to the certification of commercial products for safety reasons in healthcare, automotive sector.
2) The proposed framework and related solutions will be a direct input to the Architecture Reference Framework.

Conclusions

From the contribution to IoT research provided by IERC projects there has been a significant progress achieved in formulating answers to the many question of IoT governance, security and privacy. This work provides a number of foundational elements to the IERC's IoT definition. This document provides a snap-shot of current European research. More it provides a structure to make it clearer how and where the existing IERC research adds value and fits together. This serves to highlight the gaps where future research is needed or would be beneficial.

IoT governance is one of the key remaining challenges. Achieving the right governance framework is critical to IoT's success across all aspects from architecture, through standards to implementation. IoT embraces a breadth of established, emerging and evolving technologies across a variety of vertical domains that to achieve open interoperability and an environment for market driven application innovation IoT requires an inclusive governance framework which is as yet inexistent. The value of independent leadership, the development of multi-stakeholder supported criteria and backed by the EC would be in providing a suitable adequately resource backed initiative to establish a trusted environment for multi-stakeholder participation and support. This offers the best opportunity to minimize the persistent risk of IoT fragmentation between ISPs, MNOs, supply chain, Smart Cards/Embedded, ITS, Banking/payment, WSN, etc. each with their own preferred agenda backed by their particular sector governance body.

Trust and usability are critical success factors for much of ICT, IoT included. IoT security and privacy features addressing today's needs and those that provisions for the requirements of tomorrow need to be sympathetic to the end user while accommodating an anticipated increasing complexity of requirements from the expansion of cross domain applications. Performance, complexity, costs are all factors which influence adoption in addition to those that engender trust. While there have been important progress made and actions planned to address usability there are nevertheless remaining a number of potential gaps in the overall 'trust' framework where further research would be potentially beneficial.

Through the efforts of the IERC IoT is on the right path. However the research is still required in order to extend the path to a point where there has been sufficient consideration of the IoT vision enablers for IoT to flourish backed by sustainable commercial exploitation.

Annex 1: List of relevant organizations and fora working with IoT governance, security and privacy issues

- US Federal Trade Commission workshop on “Privacy and Security Implications of the Internet of Things” (http://www.ftc.gov/bcp/workshops/internet-of-things/)
- Kantara Initiative (http://kantarainitiative.org/) and its User Managed Access work group (http://kantarainitiative.org/confluence/display/uma/Home)
- The Internet Governance Forum. http://www.intgovforum.org/
- Internet Corporation for Assigned Names and Numbers. http://www.icann.org/
- World Privacy Forum. http://www.worldprivacyforum.org/
- Future of Privacy http://www.futureofprivacy.org/
- IoT Forum http://iot-forum.eu/

Annex 2: Terms, Abbreviations and Definitions

This position paper use terms, which have different definitions in different domains. The objective of this annex is to provide a description of the main definition with the identification of the source where the definition comes from. In some cases, more than one definition is proposed.

Acronym	**Meaning**
3GPP	3rd Generation Partnership Project
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks Specification for high-level communication protocols using radios based on the IEEE 802.15.4 standard for wireless sensor networks. Supports IPv6 address.
AAL	Ambient Assisted Living
Access Control	'Access control' is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [106]
ACID	Atomicity, Consistency, Isolation, Durability
ACL	Access Control List
Active tag	An RFID tag that uses a transmitter to return information as opposed to reflecting a signal back from the reader as a passive tags do. Most active tags are battery powered, though they may gather energy from other sources. Typical, active tags can be read from up to 100 meters.
Agile Reader	An RFID reader that reads tags operating at different frequencies or using different methods of communication between RFID tag and reader.
AIDC	Automatic identification and data capture. A broad term that covers methods of identifying objects, capturing information about them and entering it directly into computer systems without human involvement. Technologies normally considered part of auto-ID include bar codes, biometrics, RFID and voice recognition.
AIM	1) Automatic identification manufacturers. 2) Association for Automatic Identification and Mobility. Global trade association that provides products and services related to data collection, automatic identification, and information management systems.
Air Interface Protocol	Rules that govern how RFID tags and RFID readers communicate.
AMR	Automatic Meter Reading Technology

Antenna	The conductive element to send and receive tag data. Passive low- frequency tags (135 kHz) and high-frequency tags (13.56 MHz) use a coiled antenna that couples with the coiled antenna of the reader to form a magnetic field. Readers have antennas that are used to emit radio waves. The RF energy from the reader antenna is “harvested” by the tag antenna and used to power the tag microchip to reflect back its signal back to the reader.
Anti-collision	A general term used to cover methods of preventing radio waves from one device from interfering with radio waves from another. Anti-collision algorithms are also used to read more than one tag in the same reader’s field.
API	Application Programming Interface
Applicator	A label-printing device to print and apply pressure-sensitive labels to RFID tags. Pressure sensitive labels consist of a substrate and an adhesive. Used for shipping, content, graphic images or complying with standards such as UPC or GS1.
ARM	Architecture Reference Model
ASCII	American Standard Code for Information Interchange. The code is used in the transmission of data. It consists of eight data-bits used to code each alphanumeric character and other symbols.
Asset tracking	The most common RFID tag application. RFID asset tagging increases asset utilization, identifies the last known asset user, reduces lost items and automates maintenance routines.
Authentication	A security mechanism allowing the verification of the provided identity. [106]
Authorization	Granting of rights to perform some activity to some entity, human agent or process until revoked. [106]
Auto-ID center and labs	A non-profit collaboration between private enterprise and researchers for the development of a global tracking network using RFID tags carrying Electronic Product Codes (EPCs). The center closed in Sep. 2003. The center’s research continues at Auto-ID Labs in universities around the world, and is headquartered at the Massachusetts Institute of Technology.
Automatic identification	Methods to collect data and enter into computer systems without human involvement. Technologies normally considered part of auto-ID include bar codes, biometrics, RFID and voice recognition.
AWARENESS	EU FP7 coordination action Self-Awareness in Autonomic Systems
Backscatter	A method of communication between passive (or semi-

	passive) RFID tags and the readers. The tag reflects back a signal from the reader, usually modulated and at the same carrier frequency.
BACnet	Communications protocol for building automation and control networks
BAN	Body Area Network
Bar code	A patterned series of vertical bars of varying widths used by a computerized scanner for inventory, pricing, etc.
Base station	An RFID tag reader that is connected to a host system
Battery-assisted tag	These RFID tags incorporate batteries and use the battery power to run the tag circuitry and sometimes an onboard sensor. They communicate with the tag reader using the same backscatter technique as passive tags though they have a longer read range because all of the energy gathered from the reader is reflected back to it. Also known as "semi-passive RFID tags."
BDI	Belief-Desire-Intention architecture or approach
Beacon	Active or semi-active RFID tags programmed to broadcast a signal at set intervals.
Biometrics	Techniques designed to recognize and authenticate the identity of people based upon one or more intrinsic physical or behavioral traits (e.g., fingerprints and retinal patterns). Because biometric traits cannot be lost or forgotten like passwords and are impossible to copy or distribute they make very effective identifiers if they can be read accurately.
Bistatic	A bistatic RFID interrogator or reader uses a one antenna to transmit energy to the RFID tag and a different antenna to receive reflected energy back from the tag.
Bit	Binary Digit. The basic unit of information in a binary numbering system. 1's and 0's are used in a binary system.
Bluetooth	Proprietary short range open wireless technology standard
BPM	Business Process Modelling
BPMN	Business Process Model and Notation
BPWME	Business Process Workflow Management Editor
BUTLER	EU FP7 research project uBiquitous, secUre inTernet of things with Location and contExt-awaReness
CAGR	Compound annual growth rate
Card operating system	Software in a smart card that manages the basic functions of the card, such as terminal communication,

	security management and data management.
CE	Council of Europe
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CEO	Chief executive officer
CEP	Complex Event Processing
Character	Data character. A letter, digit or other member of the ASCII character set.
Character set	That character available for encoding in a particular automated identification technology.
Checksum	Code added to a data block on an RFID chip that is checked before and after data transmission from tag to reader to evaluate whether data has been corrupted or lost.
Circular-polarized antenna	A UHF reader antenna that produces radio waves in a circular pattern. As the waves move in a circular pattern, they have a better chance of being received, though circular polarized antennas have a shorter read range than linear-polarized antennas. Used in situations where the orientation of the tag to the reader cannot be controlled.
Closed-loop systems	RFID tracking systems where the tracked item never leaves the company's control and the system does not have to use open standards
CMMS	Computerized Maintenance Management system.
CoAP	Constrained Application Protocol
Commissioning	The process of writing a serial number to a tag and associating that number with the tagged product in a database.
Compatibility	RFID systems are compatible if they employ the same protocols, frequencies and voltage levels and are able to operate together within the same overall application.
Compliance label	A label that indicates conformance to industry standards for data content and format. Compliance labelling standards ensure a similar labelling approach that clearly defines the label format, usage, and the information to include on the label. There are no RFID compliance labelling standards yet but some consider bar-code labels with embedded UHF EPC tags as compliance labels.
Concentrator	A device that communicates with several RFID readers for the purpose of gathering data, which it then filters and passes on the information to a host computer.
Conducted power	The RF power supplied by an RFID system to the antenna. It is measured at the cable to antenna

	connection. In the U.S., Federal Communication Commission regulations limit maximum conducted power to 1 watt.
Contact less smart card	A credit card or other card incorporating an RFID chip to transmit information to a reader without having to be swiped.
CRC	Cyclic Redundancy Code/Check. The CRC-16 is used as error detection code for the backscattering operation of the tag. If errors are detected, the tag will retransmit the involved data to the reader.
CRUD	Create, Updated, Delete
CSS	Chirp Spread Spectrum
D1.3	Deliverable 1.3
Data carrier	A medium for storing machine-readable data, such as bar codes and RFID tags. May also refer to the carrier frequency for data transmission.
Data field	RFID chip memory assigned to a particular data type. Data fields may be protected or written over. For example, a data field might contain information about where an item should be sent, and when the destination changes the new information is written to the field. A protected data field could be used to store an Electronic Product Code, which doesn't change during the life of the product it's associated with.
Data retention	RFID tags can retain data for over 10 years depending on temperature, humidity and other factors.
Data subject's consent	The 'data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. [107]
Data transfer rate	Number of characters that can be transferred from RFID tag to reader over a specified time. Baud rate defines how quickly readers can read information on a RFID tag, and is different from read rate, which refers to how many tags can be read over a specified time.
DATEX-II	Standard for data exchange involving traffic centres
DCA	Data Collection and Analysis
Dead tag	An RFID tag that cannot be read by a reader.
De-tune	When a UHF antenna is placed close to metal or metallic material, the antenna can be detuned to better receive RFID waves of a certain length from a reader so that the RFID tag can be read, but results in poor performance. OMNI-ID tags do not need to be de-tuned.
DHT	Distributed Hash Table

Dipole	Antenna consisting of two straight electrical conductors or “poles”. The antenna is typically ½ wavelength from end to end. In an RFID transponder the antenna is connected to a microchip.
DNS	Domain Name System
DOI	Digital Object Identifier
Domain	Distinguished part of an abstract or physical space where something exists.
Domain identification number	String of characters representing the value of the identifier assigned to a domain.
DoS/DDOS	Denial of service attack Distributed denial of service attack
DoW	Description-of-Work
DSO	Decision Support Ontology
Dual dipole	An antenna that contains has two dipoles. The goal of the dual dipole design is to reduce the tag’s orientation sensitivity.
Dual interface smart card	A card containing a microchip that can be read either when in contact with a reader or read remotely using radio waves.
Dumb reader	A tag reader with limited computing power that converts radio waves from a tag into a binary number, passing it to a host computer with little or no filtering.
Duty cycle	Length of time a tag reader is set to emit energy. European Union regulations permit tag readers to be on no more than 10 percent of the time.
EC	European Commission
eCall	eCall – eSafety Support A European Commission funded project, coordinated by ERTICO-ITS Europe
ECC	Error Checking and Correction. Mathematical techniques used to identify symbol damage and reconstruct the original information, based upon the remaining data in a damaged or poorly printed code.
EDA	Event Driven Architecture
EEPROM	Electrically Erasable Programmable Read-Only Memory. A method of storing data on microchips where bytes can be individually erased and reprogrammed. More expensive than factory programmed RFID tags where the number is written into the chip silicon during manufacture, but offers more flexibility because the end user can write an ID number to the tag at the time the tag is going to be used.

EH	Energy harvesting
EHF	Extremely high frequency, (frequency range 30GHz – 300GHz)
EIB	European Installation Bus
EIRP	Effective Isotropic Radiated Power. A measurement of RFID tag reader antenna output which is used in the United States and elsewhere, usually expressed in watts.
Electronic seal	A method of sealing a digital document in a manner similar to that used for electronic signatures. Electronic seals enable computers to authenticate that document or electronic messages have not been altered, providing a level of security in digital communications.
EMF	Electromagnetic Field
EMI	ElectroMagnetic Interference. This occurs when the radio waves of one device alter the waves of another device. Cells phones and wireless computers may produce radio waves that interfere with RFID tags.
EMR	Emergency Response
Encryption	Altering data so that it cannot be read by those for whom it is not intended. In RFID systems encryption is used to protect stored information or to prevent the interception of communications between RFID tag and reader.
ENOB	Effective Number Of Bits
EPC	Electronic Product Code A serial number created by the Auto-ID Center that will complement barcodes. The EPC identifies the manufacturer, product category and individual item.
EPC-ALE	Electronic Product Code Application Level Events
EPC Discovery Service	An EPCglobal Network service that allows companies to search for every reader that has read a particular EPC tag.
EPC Gen2	EPC Generation 2. The RFID standard ratified by EPCglobal for the air-interface protocol for the second generation of EPC technologies.
EPC global	An organization which objective is world-wide adoption and standardization of EPC technology in an ethical and responsible way.
EPC Information Service	A network infrastructure that enables companies to store data associated with EPCs in secure online databases with different levels of access.

EPC-IS	Electronic Product Code Information Sharing Electronic product code information service
EPROM	Erasable Programmable Read-Only Memory. Non-volatile memory in an RFID tag that can be erased by exposure to intense ultraviolet light and then reprogrammed.
ERP	Enterprise Resource Planning. Effective Radiated Power. A measurement of the output of RFID tag reader antennas used in Europe, usually expressed in watts.
Error correcting mode	A mode of data transmission between RFID tag and tag reader so that errors or missing data is automatically corrected.
ERTICO-ITS	Multi-sector, public / private partnership for intelligent transport systems and services for Europe
ESOs	European Standards Organisations
ESP	Event Stream Processing
ETSI	European Telecommunications Standards Institute An independent, non-profit organization that defines telecommunications standards for Europe. Responsible for standardization of broadcasting and related areas, such as intelligent transportation, medical electronics and RFID
EU	European Union
Exabytes	10^{18} bytes
Excite	Tag readers “excite” a passive tag when the reader transmits RF energy to activate the tag and cause it to transmit data back to the reader.
Factory programming	Some read-only RFID tags must have their identification number written into the microchip at the time of manufacture. This is known as factory programming. That data cannot be over-written or modified.
False read	When a tag reader reports the presence of an RFID tag that does not exist. Also called a phantom transaction or false read.
Far-field communication	RFID tags farther then one full wavelength away from the tag reader are said to be “far field”, within one full wavelength away is “near field.” Far field signals decay as the square of the distance from the antenna, while the near field signals decay as the cube of distance. Passive RFID tags that use far field communications (UHF and microwave systems) have a longer range

	than tags using near field communications (low- and high-frequency systems).
FDIS	Final draft international standard, (Ref. ISO).
FI	Future Internet
FIA	Future Internet Assembly
Field programming	RDIF tags with non-volatile EEPROM memory can be programmed after they are shipped from the factory so that users can write data to the tag once it is placed.
FI PPP	Future Internet Public Private Partnership programme
FIS 2008	Future Internet Symposium 2008
Fixed reader	An RFID interrogator mounted to a permanent or non-mobile structure enabling users to read RFID tag numbers attached to movable items.
F-ONS	Federated Object Naming Service
Form factor	The transponder packaging type; thermal transfer labels, plastic cards, key fobs, etc.
Forward channel	Energy path from the tag reader to the RFID tag
FP7	Framework Programme 7
Free air	Reading an RFID tag that is not attached to anything
FTP	File Transfer Protocol
GDS	Global Data Synchronization. The process of matching a manufacturer's master files with retailer's product information. GDS is a prerequisite to deploying RFID in open supply chains to ensure that RFID serial numbers refer to the correct database product information.
GFC	Global Certification Forum
GIS software	Geographical Information System software. For recording, analyzing and managing geospatial data (data referenced to a fixed location). With GIS software users can run queries, analyze spatial information, and create maps.
GLN	Global Location Number. A numbering system developed by EAN International and the Uniform Code Council as a way to identify legal entities, trading parties and locations to support electronic commerce. GLNs can identify functional entities (e.g., a purchasing department), physical entities (e.g., a particular warehouse) and legal entities or trading partners (e.g. buyers or sellers).
Global commerce initiative	Founded by manufacturers, retailers and trade industry associations to improve international supply chains for consumer goods through collaborative development and EAN International/Uniform Code Council standards and best practices, including use of

	EPC.
GPL	General Public Licence
GreenTouch	Consortium of ICT research experts
GS1	Global Standards Organization
GSN	Global Sensor Networks
GTIN	Global Trade Item Number GS1 Global trade item number, (see also SGTIN). Standardized system of identifying products and services created by the Uniform Code Council and EAN International. Product identification numbers, such as EAN/UCC -14, are based on the GTIN.
GUID	Global Unique Identifier
Hadoop	Project developing open-source software for reliable, scalable, distributed computing
Harvesting	The way passive RFID tags gather energy from RFID reader antennas
HF	High Frequency. This is generally considered to be from 3 MHz to 30 MHz. HF RFID tags typically operate at 13.56 MHz. Typical, can be read from less than 1 meter away and transmit data faster than low frequency tags but consume more power.
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
Hub	Repeater for wireless or cable bounded data traffic
Human readable identification	The letters, digits or other characters associated with specific symbol characters that are incorporated into linear bar code or two-dimensional symbols.
Hybrid card	A smart card that has both a no-contact IC and a contact IC, so that a hybrid card acts as two separate cards.
IAB	Internet Architecture Board
IBM	International Business Machines Corporation
ICAC	International Conference on Autonomic Computing
ICANN	Internet Corporation for Assigned Name and Numbers
ICS	International classification for standards, (ref. ISO).
ICT	Information and Communication Technologies
ICO	Internet Connected Object
iCore	EU research project Empowering IoT through cognitive technologies
ID	Identification number (unique). String of characters representing the value of the identifier
Identification	Act of associating identification numbers to an object

Identification scheme	Definition and description of the structure of identifiers
Identification system	Set of formal rules for objects to be identified in a given domain
Identifier	Attribute associated with an object to unambiguously identify it in a specified domain
Identity	The identity of the object is an identifier that can be used to identify an object on the system. At system level, the identity can be mapped to a user identity if – and only if – the identifier of the object is unique.
IEC	International electro-technical commission. An international standards organization dealing with electrical, electronic and related technologies.
IEEE	Institute of Electrical and Electronics Engineers
IERC	European Research Cluster for the Internet of Things
IETF	Internet Engineering Task Force
Induction loop	A coil-wire transceiver used when doing RFID reads in the presence of metal.
Inductive coupling	The transfer of energy from one circuit to another through mutual inductance. In RFID systems using inductive coupling, the tag reader antenna and the RFID tag antenna each have a coil which together forms a magnetic field so that the tag draws energy from the field to change the electrical load on the tag antenna. The change is picked up by the tag reader and read as a unique serial number.
Inlay	Inlays can be considered “unfinished” RFID labels, as they are a chip attached to an antenna and mounted on a substrate. Usually sold to label converters who turn them into smart labels. Also known as inlets.
INSPIRE	Infrastructure for Spatial Information in the European Community
Intelligent reader	A reader that can filter data, execute commands and perform functions similar to a personal computer.
Intentional radiator	A device that produces a RF signal for the purpose of data communications. Examples are cordless phones and door openers.
Interoperability	The ability for RFID tags and readers from different vendors to communicate. Interoperability testing assesses the ability different systems to exchange information and use the data that has been exchanged.
Interposer	A device connecting an RFID microchip to an antenna to create an RFID transponder.
Interrogation zone	Area in which a tag reader can provide enough energy to power up a passive tag and receive back information. Also known as the read field or reader field. RFID tags

	located outside the interrogation zone do not receive enough energy from the reader to produce a signal.
Interrogator	See Reader.
IO	Integrated Operations
I/O port	Input/Output port. Connections on an RFID reader for external devices. An output device could be a panel that opens when a tag is read. An input device could be a photoelectric eye to turn on the reader when an object breaks the beam.
IoE	Internet of Energy
IoM	Internet of Media
IoP	Internet of Persons
IoS	Internet of Services A software based component that is delivered via different networks and Internet. The Internet of Services based on RFID applications has to address the privacy issues. IoS is not just about technology, but also about usage, community building, deployment, business models, public policy, security and privacy.
IoT	Internet of Things a) The Internet of Things is a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies. [108] b) The Internet of Things builds out from today's internet by creating a pervasive and self-organising network of connected, identifiable and addressable physical objects enabling application development in and across key vertical sectors through the use of embedded chips, sensors, actuators and low-cost miniaturisation [1] c) A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. "Things" are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information "sensed" about the environment, while reacting autonomously to the "real/physical world" events and influencing it by running processes that trigger actions and create services with or without direct human intervention.

	Interfaces in the form of services facilitate interactions with these “smart things” over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.
IoT6	EU FP7 research project Universal integration of the Internet of Things through an IPv6-based service oriented architecture enabling heterogeneous components interoperability
IoT-A	Internet of Things Architecture
IoT-est	EU ICT FP7 research project Internet of Things environment for service creation and testing
IoT Governance	There are still conflicting opinions on what IoT Governance should be (TBD) (see also [6])
IoT-GSI	Internet of Things Global Standards Initiative
IoT-i	Internet of Things Initiative
IoV	Internet of Vehicles
IP	Internet Protocol
IPSO Alliance	Organization promoting the Internet Protocol (IP) for Smart Object communications
IPv6	Internet Protocol version 6
ISA100	Specification for high-level communication protocols using radios based on the IEEE 802.15.4 standard for industrial applications.
ISM frequency bands	Industrial, scientific, and medical frequency bands.
ISO	International Standards Organization
ISO 19136	Geographic information, Geography Mark-up Language, ISO Standard
Issuing organization/issuing agency	Organization being entrusted by a registration authority to assign identification numbers in a given domain.
IST	Intelligent Transportation System
IT	Information technology.
ITS	Intelligent Transport Systems
JCA-IoT	Joint Coordination Activity on Internet of Things
JSF	Java Server Faces
KNX	Standardized, OSI-based network communications protocol for intelligent buildings
KU-tag	An RFID tag that reads objects containing metal or liquid. At just 1.5 millimetres in thickness it is one of the thinnest RFID tags designed to operate under such

	conditions.
LF	Low frequency. This is generally considered to be from 30kHz to 300kHz. Low frequency tags typically operate at 125 kHz or 134 kHz. Disadvantages of such tags are they have to be read from within 1 meter typically and data transfer rates are slow, though they are less subject to interference than UHF tags.
LGPL	Lesser General Public License
License plate	A simple RFID tag that contains a serial number associated with database information as a way to simplify the tag and reduce cost.
License tag number	The information contained with the symbol character set to uniquely identify the component. As a minimum the information shall contain the manufacturers CAGE code followed by an asterisk (ASCII separator) and trace code (lot, member or serial number).
Linear-polarized antenna	An antenna designed to focus radio energy from the reader in one orientation or polarity, thereby increasing the read distance and providing increased penetration through dense materials. In order to be read accurately, RFID tags designed to be used with a linear polarized antenna must be aligned with the reader antenna.
LLRP standard	A standard to foster RFID reader interoperability and create a foundation for technology providers to offer capabilities that meet industry-specific requirements.
LNCS	Lecture Notes in Computer Science
LOD	Linked Open Data Cloud
Lot number/batch number	String of characters representing the value of the identifier assigned to a group of specimens considered as one object to identify the specimens that are manufactured together under assumed identical conditions and in a limited time interval
Low-level reader protocol standard	A standard to promote RFID reader interoperability and improve capabilities to meet industry-specific requirements.
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Media Access Control data communication protocol sub-layer
MAPE-K	Model for autonomic systems: Monitor, Analyse, Plan, Execute in interaction with a Knowledge base
makeSense	EU FP7 research project on Easy Programming of Integrated Wireless Sensors

MB	Megabyte
mDNS	Multicast DNS
MEMS	Micro-Electro-Mechanical Systems. Systems made up of components between 1 to 100 micrometers in size (0.001 to 0.1 mm). An RFID MEMS tag with micromechanical components is designed to withstand wide temperature ranges as well as gamma radiation and may be used on medical devices.
MES	Manufacturing Execution System. A system that allows companies to control critical production activities and improve traceability, productivity and quality.
Metadata / meta information	Information (irrespective of its form) used to describe a real or abstract object.
MF	Medium frequency, (frequency range 300kHz – 3MHz).
Microwave	Microwave frequencies are generally considered to be from 300MHz to 300GHz. RFID tags that operate at 5.8 GHz (or above 415 MHz) have very high transfer rates and typically can be read up to 10 meters but are costly and use a lot of power and are expensive.
Middleware	RFID software that resides on a server between readers and enterprise applications and used to filter data or manage readers across a network.
MIPS	Material management system, (ERP system).
MIT	Massachusetts Institute of Technology
Mobile reader	An RFID interrogator that is easily transported, allowing employees to read RFID tags attached to items in a warehouse or other setting along the supply chain.
Monostatic	An RFID reader that uses the same antenna to transmit RF energy to and receive RF energy from an RFID tag.
MPP	Massively parallel processing
MRP	Manufacturing Resource Planning
Multimode	RFID transponders that can be programmed to operate and comply with multiple standards.
Multiple access schemes	Techniques to increase the amount of data that can be wirelessly transmitted within the same frequency spectrum. RFID readers may use Time Division Multiple Access (TDMA) so that they read tags at different times to avoid interference.
Multiplexer	A technique that allows a reader to have more than one antenna and reduces the number of readers needed to cover a given area while preventing the antennas from interfering with each other.
NIEHS	National Institute of Environmental Health Sciences

NFC	Near Field Communication RFID tags closer than one full wavelength away from the tag reader are said to be “near field”, while more than one full wavelength away is “far field.” Near field signals decay as the cube of the distance from the antenna, while far field signals decay as the square of distance. Passive RFID tags that use far field communications (UHF and microwave systems) have a longer range than tags using near field communications (low- and high-frequency systems).
Noise	Random or ambient electromagnetic energy found in the operating environment of RFID equipment. Other RF devices such as robots, electric motors and other machines may cause noise.
Nominal range	The read range at which at which an RFID tag can reliably be read.
NoSQL	not only SQL – a broad class of database management systems
Null spot	An area in the RFID tag reader field that does not receive radio waves. This is a common issue with UHF systems.
OASIS	Organisation for the Advancement of Structured Information Standards
Object	A physical or non-physical “thing”, i.e. anything that might exist, exists or did exist and is considered as an entity treated in a process of development, implementation, usage and disposal.
Object identification number	String of characters representing the value of the identifier assigned to an object (synonyms used; product number, item number, part number, article number, product identifying number, traceability number (serial or batch)).
OEM	Original equipment manufacturer
OGC	Open Geospatial Consortium
OMG	Object Management Group
One-time programmable tag	Also known as a field-programmable tag, it is RFID tag memory that can be programmed once and is then write-protected. After the memory is written to it is considered read only memory.
ONS	Object Naming Service A system for looking up unique Electronic Product Codes (EPCs) and information about the item associated with the code.
OpenIoT	EU FP7 research project Part of the Future Internet public private partnership

	Open source blueprint for large scale self-organizing cloud environments for IoT applications
Orientation	Position of a reader antenna in reference to a tag antenna. In UHF systems reader antennas can be linear- or circular-polarized. When using a linear polarized antenna the tag and reader must be in alignment to achieve the maximal reading distance.
Outsmart	EU project Provisioning of urban/regional smart services and business models enabled by the Future Internet
PAN	Personal Area Network
Part identification data	Markings used to relate parts to their design, manufacturing, test, and operational histories.
Passive tag	RFID tag without an internal battery or power source. The energy is gathered from the reader, these radio waves are converted by the tag antenna into current. The tag reflecting back the signal (modulated) from the reader.
Patch antenna	A square reader antenna made from metal or foil.
PDA	Personal Digital Assistant Personal Data Assistant
Personal Data	'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. [107]
PET	Privacy Enhancing Technologies
Petabytes	10^{15} byte
Phantom read	When a reader reports the presence of a tag that doesn’t exist. Also called a false read or phantom transaction.
PHY	Physical layer of the OSI model
PIPES	Public infrastructure for processing and exploring streams
PKI	Public key infrastructure
Power level	The amount of RF energy emitted from an RFID tag reader. The higher the power output the longer the read range. Many countries regulate power levels to avoid interference with other devices.
PPP	Public-private partnership
Privacy-enhancing technologies	As a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the

	functionality of the information system. [109]
Probe-IT	EU ICT-FP7 research project Pursuing roadmaps and benchmarks for the Internet of Things
Processing of personal data	'Processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. [107]
Programming a tag	The act of writing data to an RFID tag. When a serial number is first written to a tag it is called “commissioning”.
PSI	Public Sector Information
PT	Personnel Tracking System
PV	Photo Voltaic
QoI	Quality of Information
QR-Code	Quick Response Code
Quiet tag	RFID tags that are only readable with reader output at full power, or which can be read only at very close range.
RDF	Resource Description Format The Resource Description Framework is a standard model for data interchange on the Web. RDF has features that facilitate data merging even if the underlying schemas differ, and it specifically supports the evolution of schemas over time without requiring all the data consumers to be changed.
Read	The process of retrieving RFID tag data by broadcasting radio waves at the tag and converting the waves the tag returns to the tag reader into data.
Reader	A device used to communicate with RFID tags via radio waves, it has one or more antennas that emit radio waves and receive a signal back from the tag. Tag readers are also sometimes called interrogators.
Reader field	The area a tag reader can cover. Tags outside the field do not receive radio waves emitted by the tag reader and cannot be read.
Reader module	Reader electronics (digital signal processor and circuit board) can be placed in a dedicated device or an RFID label printer, for example.
Reader talks first	A passive UHF reader initially communicates with RFID tags in its read field by sending energy to the tags. The tags do not transmit until the reader requests them to

	do so. The reader finds tags with specific serial numbers by asking all tags with a serial number that starts with either 1 or 0 to respond. If more than one responds, the reader might ask for all tags with a serial number that starts with 01 to respond, and then 010. Also known as “walking” a binary tree, “tree walking”, or “singulation”.
Read-only	RFID tag memory that cannot be altered unless the microchip is reprogrammed.
Read range	The distance from which tag readers can accurately and reliably communicate with RFID tags. Active tags have longer read ranges than passive tags because they have their own power source for signal transmission. In passive tags the read range is controlled by frequency, reader output power, antenna design, and the method used to power up the tag. Low-frequency tags use inductive coupling which requires the tag to be close to the reader.
Read rate	A specification describing how many tags can be read within a given period or the number of times a single tag can be read within a given period. Alternatively, the maximum rate that data can be read from a tag expressed in bits or bytes per second.
Read-write	RFID tags that can store new data, often used on reusable containers and other storage assets. When the contents of the container are changed, new information is written to the tag.
Registration authority	Organization responsible to receive and acknowledge applications from organizations wishing to become an issuing organization in a given domain.
REST	Representational State Transfer
Reverse channel	The path energy travels from the RFID tag to the interrogator, or reader. It is also sometimes called the back channel.
RF	Radio Frequency
RFFE	Radio Frequency Front End
RFID	Radio Frequency Identification A technique for identifying unique items using radio waves. Typically a tag reader communicates with an RFID tag, which contains digital information. There are also “chipless” forms of RFID tags that use material to reflect back radio waves beamed at them.
RFID tag	See Tag.
RSD	Redundant Signed Digit
RSSI	Received signal strength indication is a measurement of the power present in the received radio signal, (IEEE 802.11 protocol).

RTLS	Real-Time Locating System. A technique for finding the position of assets using active RFID tags. Three reader antennas are positioned to receive signals from tags in their common read field. Triangulation is used to calculate the asset location.
R/W	Read/Write
SASO	IEEE international conferences on Self-Adaptive and Self-Organizing Systems
SAW	A technology for automatic identification using low power microwave radio frequency signals that are converted to ultrasonic acoustic signals by a piezoelectric crystalline material in the transponder. Variations in the reflected signal can be used to identify an object.
Scanner	An electronic device, such as an RFID tag reader, that sends and receives radio waves. When combined with a digital signal processor that turns the waves into data, the scanner is called a reader or interrogator.
SDO	Standard Developing Organization
SEAMS	International Symposium on Software Engineering for Adaptive and Self-Managing Systems
Semantic web	It is a Web of data that provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries. It is a collaborative effort led by W3C with participation from a large number of research and industrial partners.
Semi-active tag	Sometimes used for semi-passive tag, (see semi-passive tag).
Semi-passive tag	RFID tag with an internal battery. The battery is used to power the microchip's circuitry, but not used to send a signal to the reader. Some semi-passive tags sleep until they are woken up by a signal from the reader to conserve battery life. These tags are sometimes called semi-active tag or battery assisted tags. The names are used rather interchangeably to describe this type of tag.
SENSEI	EU FP7 research project Integrating the physical with the digital world of the network of the future
Serial number	String of characters representing the value of the identifier assigned to an individual specimen of objects or an object type
SGTIN	Serialized Global Identification Number GS1 Serialized Global Trade Item Number, (see also GTIN).
SHF	Super high frequency, (frequency range 3GHz –

	30GHz).
Shielding	The use of a Faraday cage, Mylar sheet or metal barrier to prevent radio frequency noise from interfering with tag readers or to prevent readers from interfering with other devices.
SIG	Special Interest Group
Signal attenuation	The drop in RF energy from an RFID tag or tag reader as a function of distance is proportional to the inverse square of the distance. Attenuation can be increased by external factors as well such as the presence of liquids or metal.
Singulation	A passive UHF reader initially communicates with RFID tags in its read field by sending energy to the tags. The tags do not transmit until the reader requests them to do so. The reader finds tags with specific serial numbers by asking all tags with a serial number that starts with either 1 or 0 to respond. If more than one responds, the reader might ask for all tags with a serial number that starts with 01 to respond, and then 010. Also known as “walking” a binary tree, “tree walking”, or “reader talks first”.
Skimming	Reading an RFID tag covertly.
SLA	Service-level agreement / Software license agreement
Slotted antenna	An antenna designed as a slot cut into an electrical conductor connected to the transponder. Slotted antennas have the same orientation sensitivity as dipole antennas.
SmartAgriFood	EU ICT FP7 research project Smart Food and Agribusiness: Future Internet for safe and healthy food from farm to fork
Smart card	Any payment card that contains an embedded microchip. A contact less smart card uses RFID technology to send and receive data.
Smart label	A bar code label that contains an RFID transponder is considered “smart” because it can store information and communicate with a reader.
Smart reader	A reader that can filter data, execute commands and perform functions similar to a personal computer.
SmartSantander	EU ICT FP7 research project Future Internet research and experimentation
SOA	Service Oriented Approach
SON	Self Organising Networks
SOS	Sensor Observation Service
SPARQL	Simple Protocol and RDF (Resource Description Framework) Query Language

SPS	Sensor Planning Service
SSN	Semantic Sensor Networks
SSW	Semantic Sensor Web
SRA	Strategic Research Agenda
SRIA	Strategic Research and Innovation Agenda
SRA2010	Strategic Research Agenda 2010
SSN	Semantic Sensor Networks
Structure	The order of data elements in a message
Substrate	The material (paper, plastic, metal, etc.) upon which a RFID tag is placed.
SWE	Sensor Web Enablement
Switch	A more advanced hub
Synchronization	Controlling the timing of tag readers that are close together so they don't interfere with one another during the read process.
Tag	A microchip attached to an antenna capable of reflecting/ transmitting data. Some tags also receive and store data. They are packaged so that it can be attached to or into an object, animal or person, programmed with a unique serial number. Some tags are also managing additional information. A RFID tag receives signals from a tag reader and sends signals back to the reader and can be active, passive or semi-passive. RFID tags are also sometimes called transponders.
Tag talks first	How tag readers in a passive UHF system identify tags in their field. When RFID tags enter the reader's field they immediately announce their presence by reflecting back a signal, which is useful in an environment where items are moving quickly.
Tamper-evident tag	An RFID tag that signals a reader when a container has been opened without authorization.
TC	Technical Committee
TDS	Tag Data Standard
T-IMSI	T-International Mobile Subscriber Identity
Traceability	Ability to trace (identify and measure) the stages that lead to a particular point in a process
Track and trace	The process of gathering information about the movement and location of items
Transceiver	A device that both transmits and receives radio waves.
Transponder	A combination of a transmitter and a receiver, (TRANSmitter /resPONDER). RFID tags are sometimes referred to as transponders because they can be activated when they receive a predetermined signal.

	RFID transponders come in many forms, including smart labels, simple tags, and smart cards. See also Tag.
TTCN-3	Testing and Test Control Notation version 3
UCC	Uniform Code Council. The non-profit organization that oversees the Universal Product Code (UPC), the North American bar code standard.
UHF	Ultra high frequency. The frequency band from 300 MHz to 3 GHz. RFID tags typically operates between 840 MHz to 960 MHz so they can send information faster and farther than high- and low frequency tags.
UII	Unique Item Identifier is the code that identifies any item in an RFID tag, (e.g. the EPC codes are a subset).
UML	Unified Modelling Language
UPC	Universal Product Code. The 12 digit data format encoded in UCC bar codes
URI	Universal Resource Identifier
URN	Universal Resource Notation
USDL	Unified Service Description Language
UWB	Ultra-wideband
VO	Virtual Object
W3C	World Wide Web Consortium The World Wide Web Consortium develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential and is a forum for information, commerce, communication, and collective understanding.
Wi-Fi	Wireless network according to IEEE 802.11.xx standard.
WirelessHart	Specification for high-level communication protocols using radios based on the IEEE 802.15.4 standard for industrial applications.
WMS	Warehouse Management System. A methodology to control the movement and storage of materials within a warehouse and process the associated transactions, including shipping, receiving, put away and picking. WMSs may use bar-code scanners, mobile computers, wireless LANs and RFID.
Work-in-process tracking	The use of RFID to track manufacturing changes reduces manual data collection and ensures that the right processes are performed at the proper time on the correct product.
WORM	Write Once, Read Many. An RFID tag that can be written to once and thereafter can only be read.
Write range	The maximum distance over which data can be written

	to an RFID tag.
Write rate	The rate at which information is written to a tag and then verified as being correct.
WS&AN	Wireless sensor and actuator networks
WSN	Wireless Sensor Network
WS-BPEL	Web Services Business Process Execution Language
X12 EDI	The American National Standards Institute electronic data interchange standard developed for inter-industry electronic exchange of business transaction data.
XML	eXtensible Markup Language
Zettabytes	10^{21} byte
ZigBee	Low-cost, low-power wireless mesh network standard based on IEEE 802.15.4 Specification for high-level communication protocols using low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). Used in RF applications requiring low data rate, long battery life and secure networking.

References

[1] Helen Rebecca Schindler, Jonathan Cave, Neil Robinson, Veronika Horvath, Petal Jean Hackett, Salil Gunashekar, Maarten Botterman, Simon Forge, Hans Graux. Europe's policy options for a dynamic and trustworthy development of the Internet of Things, RAND Europe. Prepared for European Commission, DG Communications Networks, Content and Technology (CONNECT).

[2] EU IoT Task Force. 2012. Final Report of the EU IOT Task Force on IOT Governance. Brussels, November 14, 2012

[3] Rolf H. Weber, Internet of things – Governance quo vadis?, Computer Law & Security Review, Volume 29, Issue 4, August 2013, Pages 341-347, ISSN 0267-3649

[4] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Networks 57 (10) (2013).

[5] D. Miorandi, S. Sicari, F. D. Pellegrini, I. Chlamtac, Internet of things: Vision, applications and research challenges, Ad Hoc Networks 10 (7) (2012) 1497.

[6] Conclusions of the Internet of Things public consultation. http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation. Last accessed 24 October 2013.

[7] ENISA. Recommended cryptographic measures - Securing personal data http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/recommended-cryptographic-measures-securing-personal-data. November 2013.

[8] ENISA. Algorithms, Key Sizes and Parameters Report. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report. October 2013.

[9] US White House. BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES.

http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. May 2014.

[10] Subharthi Paul, Jianli Pan, and Raj Jain. 2011. Architectures for the future networks and the next generation Internet: A survey. *Comput. Commun.* 34, 1 (January 2011), 2-42.

[11] Kiev Gama, Lionel Touseau, Didier Donsez, Combining heterogeneous service technologies for building an Internet of Things middleware, Computer Communications, Volume 35, Issue 4, 15 February 2012, Pages 405-417, ISSN 0140-3664.

[12] S. Gusmeroli, S. Piccione, D. Rotondi, A capability-based security approach to manage access control in the internet of things, Mathematical and Computer Modelling 58 (5) (2013) 1189.

[13] Mehra, P. 2012. Context-Aware Computing: Beyond Search and Location-Based Services. IEEE Internet Computing, 16, 2 (March-April, 2012), 12-16

[14] Trappeniers, L., Roelands, M., Godon, M., Criel, J., and Dobbelaere, P. 2009. Towards Abundant DiY Service Creativity Successfully Leveraging the Internet-of-Things in the City and at Home. In Proceedings of the 13th Int. Conf. on Intelligence in Next Generation Networks (Bordeaux, France, October 26 - 29, 2009). ICIN 2009.

[15] Uckelman, D., Harrison, M., and Michahelles, F. (eds.) 2011. Architecting the Internet of Things. Springer-Verlag Berlin Heidelberg.

[16] Conti Marco, Sajal K. Das, Chatschik Bisdikian, Mohan Kumar, Lionel M. Ni, Andrea Passarella, George Roussos, Gerhard Tröster, Gene Tsudik, Franco Zambonelli. 2011. Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence, Pervasive and Mobile Computing, Volume 8, Issue 1, February 2012, Pages 2-21, ISSN 1574-1192, http://dx.doi.org/10.1016/j.pmcj.2011.10.001.

[17] Cockton, Gilbert. 2006. Designing Worth is Worth Designing. NordiCHI, 14-18 Ocyober: 165-174.

[18] Lene Sørensen and Knud Erik Skouby (eds.), “User scenarios 2020 – a worldwide wireless future”, OUTLOOK - Visions and research directions for the Wireless World, Wireless World Research Forum, No4, July 2009.

[19] Ramachandran, A., Singh, L., Porter, E. and Nagle, F., ‘Exploring Re-identification Risks in Public Domains’, Proceedings of the Tenth Annual International Conference on Privacy, Security and Trust (PST), 2012, pp.35–42, 2012.

[20] Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias. 2011. Semi-homomorphic encryption and multiparty computation. In *Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology* (EUROCRYPT'11), Kenneth G. Paterson (Ed.). Springer-Verlag, Berlin, Heidelberg, 169-188.

[21] Kristian Gjøsteen, George Petrides, and Asgeir Steine. Secure and anonymous network connection in mobile communications. 2012.

[22] Issarny, V., Georgantas, N., Hachem, S., Zarras, A., Vassiliadist, P., Autili, M., Gerosa, M., and Hamida, A. 2011. Service-oriented middleware for the Future Internet: state of the art and research directions. Journal of Internet Services and Applications 79, 1 (2011), 23-45. DOI=http://dx.doi.org/10.1007/s13174-011-0021-3

[23] Christophe, B., Boussard, M., Lu, M., Pastor, A., and Toubiana, V. 2011. The web of things vision: Things as a service and interaction patterns. Bell Labs Technical Journal, 16, 1 (June 2011), 55-61. DOI= http://dx.doi.org/10.1002/bltj.20485

[24] Yee, K. P. 2003. Secure interaction design and the principle of least authority. In Proc. of the 21st Int. Conf. on Human Factors in Computing Systems – Workshop on HumanComputer Interaction and Security Systems, (Ft. Lauderdale, FL, USA, April 6, 2003). CHI 2003. ACM, New York, NY, USA

[25] Saltzer, J.H. and Schroeder, M.D. 1975. The protection of information in computer systems. In Proceedings of the IEEE, 63, 9, (Sept. 1975), 1278-1308. DOI=http://dx.doi.org/10.1109/PROC.1975.9939

[26] G. Fenu and G. Steri, “Safe, fault tolerant and capture-resilient environmental parameters survey using WSNs,” in *Security and Privacy in Mobile Information and Communication Systems (First International ICST Conference, MOBISEC 2009, Turin, Italy, June 2009, Revised Selected Papers)*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), A. U. Schmidt, and S. Lian, Eds. Springer Berlin Heidelberg, 2009, vol. 17, pp. 180–189. http://dx.doi.org/10.1007/978-3-642-04434-2_16

[27] Cave, J. et al., Does It Help or Hinder? Promotion of Innovation on the Internet and Citizens’ Right to Privacy, final report, European Parliament, 2011

[28] Ion, Mihaela; Danzi, A.; Koshutanski, H.; Telesca, L., "A peer-to-peer multidimensional trust model for digital ecosystems," Digital Ecosystems and Technologies, 2008. DEST 2008. 2nd IEEE International Conference on, vol., no., pp.461, 469, 26-29 Feb. 2008.

[29] Benkler, Y. and Nissenbaum H. 2006. Commons-based Peer Production and Virtue. The Journal of Political Philosophhy, 14, 4:394-419.

[30] Benkler, Y. 2011. The Penguin and the Leviathan. New York: Random House.

[31] Copp, David. 2007. The Oxford Handbook of Ethical Theory. Oxford University Press: Oxford-New York 2007.

[32] Proper, Michel. 2011. La philosophie du droit. PUF:Paris.s

[33] Wiener, Norbert. 1950. The Human Use of Human Beings. Houghton Mifflin:Boston MA.

[34] Bynum, Terrell Ward and Simon Rogerson. 1996. Special issue of Science and Engineering Ethics, 2, 2:131-247.

[35] Floridi Luciano and J.W. Sanders. 2002. Mapping the foundationalist debate in computer ethics. Ethics and Information Technology, 4:1-9.

[36] Van den Hoven Jeroen and John Weckert (eds). 2008. Information technology and moral philosophy. Cambridge University Press: Cambridge-New York.

[37] Moor James H. 1985. What Is Computer Ethics. Metaphilosophy, 16, 4: 266–275.

[38] Naess, Are. 1973. The shallow and the deep, long-range ecology movement. A summary. Inquiry 16:95-100.

[39] Cohen, Julie. 2012. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice, Yale University Press:New Haven NJ.

[40] Benkler, Yochai and Helen Nissenbaum. 2006. Commons-based Peer Production and Virtue. The Journal of Political Philosophy 14, 4:394-419.

[41] Benkler, Yochai. 2011. The Penguin and the Leviathan. Crown Business: New York.

[42] Jasanoff, Sheila (ed). 2011. Reframing Rights. Bio-Constitutionalism in the Genetic Age. MIT Press: Cambridge MA.

[43] Jonas, Hans. 1984. The Imperative of Responsibility. University of Chicago Press: Chicago IL (Frankfurt am Mein 1979).

[44] Dupuy, J.P. (2004) 'Complexity and Uncertainty a Prudential Approach to Nanotechnology. European Commission. A Preliminary Risk Analysis on the Basis of a Workshop Organized by the Health and Consumer Protection Directorate General of the European Commission', in Brussels 1-2 March 2004.

[45] Von Schomberg, R. (2012) 'Prospects for Technology Assessment in a Framework of Responsible Research and Innovation', in M. Dusseldorp and R. Beecroft (eds), 26 Technikfolgen abschätzen lehren: Bildungspotenziale transdisziplinärer Metho-den,Wiesbaden: Springer VS Verlag, pp. 39-61.

[46] Van den Hoven Jeroen et al. 2013. Fact sheet-Ethics Subgroup IoT - Version 4.0. Conclusions of the Internet of Things public consultation. Available at https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

[47] Schindler Helen Rebecca et al. 2013. Europe's policy options for a dynamic and trustworthy development of the Internet of Things. SMART 2012/0053, RAND Corp., European Union 2013.

[48] Value Ageing' project. Incorporating European Fundamental Values Into ICT for Ageing: A vital political, ethical, technological, and industrial challenge. Ref. online: www.valueageing.eu

[49] Arendt Hannah. 1998. The Human Condition. University Of Chicago Press: Chicago IL (1958).

[50] Hildebrandt, Mireille and Antoinette Rouvroy (eds). 2011. The Philosophy of Law Meets the Philosophy of Technology. Autonomic Computing and Transformations of Human Agency. Routledge:London.

[51] EDPS (European Data Protection Supervisor). 2010. Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (Opinion on Privacy By Design). OJ C 280, 16.10.2010.

[52] Nissenbaum, Helen. 2011. From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice-versa)? Berkeley Technology Law Journal, 26, 3:1367-1386.

[53] Pagallo, Ugo. 2012. Good Onlife Governance: On Law, Spontaneous Orders, and Design, Onlife Project, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Contribution_Pagallo.pdf

[54] Snyder, Francis. 1993. Soft law and institutional practice in the European Community. European University Institute working paper, LAW no. 93/5.

[55] G. Pasolini, D. Dardari, S. Severi and G. Abreu: "The Effect of Channel Spatial Correlation on Physical Layer Security in Multi-antenna Scenarios," Proc. IEEE Fourty-Seventh Asilomar Conference on Signals, Systems and Computers, (Asilomar 2013), November 3-6, 2013 (Invited).

[56] A. Cavoukian. (2011, January) Privacy by Design: The 7 Foundational Principles, Revised Version.

www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

[57] S. Gusmeroli, S. Piccione, D. Rotondi, "IoT@Work Automation Middleware System Design and Architecture," presented at 17 IEEE International Conference on Emerging Technology and Factory Automation (ETFA'12), September 2012.

[58] OAUTH Specification http://oauth.net/2/

[59] OpenID 2.0 http://openid.net/specs/openid-authentication-2_0.html

[60] IoT6 D2.2, "Distributed IPv6-based Security, Privacy, Authentication and QoS".

[61] A, J. Jara, M. A. Zamora, and A. Skarmeta, "Glowbal IP: an adaptive and transparent ipv6 integration in the internet of things, Mobile Information Systems", 2012.

[62] Jara, A. J., Lopez, P., Fernandez, D., Castillo, J. F., Zamora, M. A., Skarmeta, A. F. "Mobile Digcovery: Discovering and Interacting with the World through the Internet of Things", Personal and Ubiquitous Computing, 10.1007/s00779-013-0648-0, Springer-Verlag London, (2013).

[63] IoT6 D3.1, "Look-up/discovery, context-awareness, and resource/services directory".

[64] IoT6 D2.3, "Report on IPv6 based advanced features".

[65] IoT6 D5.4, "Intelligence distribution tests and evaluation report".

[66] The HANDLE System. http://www.handle.net

[67] EPC Information Services Standard, http://www.gs1.org/gsmp/kc/epcglobal/epcis

[68] Neisse, Ricardo, Alexander Pretschner and Valentina Di Giacomo. "A Trustworthy Usage Control Enforcement Framework," International Journal of Mobile Computing and Multimedia Communications (IJMCMC) 5 (2013): 3, doi:10.4018/jmcmc.2013070103.

[69] Neisse, R.; Doerr, J., "Model-based specification and refinement of usage control policies," Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on , vol., no., pp.169,176, 10-12 July 2013, doi: 10.1109/PST.2013.6596051.

[70] D. Quartel, "Action relations - basic design concepts for behaviour modelling and refinement," PhD Thesis University of Twente, 1998.

[71] Lujun Fang and Kristen LeFevre. 2010. Privacy wizards for social networking sites. In *Proceedings of the 19th international conference on World wide web* (WWW '10). ACM, New York, NY, USA.

[72] M. Bagaa et al., "SEDAN: secure and efficient protocol for data aggregationinwirelesssensornetworks,"in*Proc.ofIEEELCN*. IEEE, 2007, pp. 1053–1060.

[73] R. Riggio and S. Sicari, "Secure aggregation in hybrid mesh/sensor networks," in *Ultra Modern Telecommunications & Workshops*. IEEE, October 2009, pp. 1–6.

[74] A. Coen-Porisini and S. Sicari, “SeDAP: Secure data aggregation protocol in privacy aware wireless sensor networks,” in *Proc. of the 2nd Int. Conf. on Sensor Systems and Software*. Springer Verlag, 2010.

[75] E. Mykletun, J. Girao, and D. Westhoff, “Public key based cryp- toschemes for data concealment in wireless sensor networks,” in *Proc. of IEEE ICC’06*. IEEE, September 2006, pp. 2288–2295.

[76] A. Fragkiadakis, I. Askoxylakis, E. Tragos, "Joint compressed-sensing and matrix-completion for efficient data collection in WSNs", in Proc. of the IEEE CAMAD 2013, Berlin, Germany, September 2013.

[77] Sarmad Ullah Khan, Claudio Pastrone, Luciano Lavagno, Maurizio A. Spirito, “An Authentication and Key Establishment Scheme for the IP-Based Wireless Sensor Networks”, Procedia Computer Science, Volume 10, 2012, Pages 1039-1045.

[78] S. Severi, G. Pasolini, D. Dardari and G. Abreu: “A Secret Key Exchange Scheme For Near Field Communication,” Proc. IEEE Wireless Communications and Networking Conference, (WCNC, 2014), April 6-9, 2014.

[79] E. Tragos and V. Angelakis, “Cognitive Radio Inspired M2M Communications (Invited Paper),” in IEEE Global Wireless Summit 2013.

[80] J. Golbeck, J. Hendler. Accuracy of metrics for inferring trust and reputation. Proceedings of the 14th International Conference on Knowledge Engineering and Knowledge Management (2004).

[81] J. Golbeck, J. Hendler. Inferring reputation on the semantic web. Proceedings of the 13th International World Wide Web Conference (2004).

[82] FaceBook-Connect API - http://developers.facebook.com/docs/guides/web/

[83] Liberty Framework http://www.projectliberty.org/specs/ and Kantara http://kantarainitiative.org/

[84] Windows/Microsoft CardSpace http://msdn.microsoft.com/en-us/library/aa480189.aspx

[85] ANTS, Gemalto, Oberthur Technologies, and Safran Morpho, Technical report: Restricted Identification through Access to e-Services with privacy preserving credentials, France ANTS, December 2011.

[86] Gemalto, Oberthur Technologies, and Safran Morpho, Technical report: Privacy Protocol Semantic, criteria list and privacy-preserving credentials format, France ANTS, December 2011.

[87] Jan Camenisch, Simone Fischer-Hübner, Kai Rannenberg (Eds.): Privacy and Identity Management for Life. Springer 2011 ISBN 978-3-642-20316-9

[88] Gurgen, Levent; Gunalp, Ozan; Benazzouz, Yazid; Gallissot, Mathieu, "Self-aware cyber-physical systems and applications in smart buildings and cities," Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013 , vol., no., pp.1149,1154, 18-22 March 2013.

[89] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The second-generation onion router,” in roceedings of the 13th USENIX Security

Symposium, August 2004. [Online]. Available: citeseer.ist.psu.edu/dingledine04tor.html

[90] J.P. Timpanaro, I. Chrisment, O. Festor, Monitoring the I2P network. Research Report RR - 7844, INRIA (December 2011)

[91] Ian Clarke, Theodore W. Hong, Scott G. Miller, Oskar Sandberg, Brandon Wiley, "Protecting Freedom of Information with Freenet" in IEEE Internet Computing, 2002.

[92] K. Bennett and C. Grothoff, "gap - Practical Anonymous Networking," in Designing Privacy Enhancing Technologies. Springer-Verlag, 2003, pp. 141–160.

[93] R. Rivest, and David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24:84-88, 1981.

[94] Paquin, C., & Thompson, G. (2010). U-Prove CTP White Paper. Microsoft Corporation.

[95] Chaum, D. (1983). Blind signatures for untraceable payments. Advances in Cryptology - Proceedings of Crypto'82, (pp. 199-203).

[96] Idemix - Camenisch & Van Herreweghen, Design and Implementation of the Idemix Anonymous Credential System, 2002.

[97] Chaum, Eugene; van Heyst (1991). "Group signatures". *Advances in Cryptology — EUROCRYPT '91*. Lecture Notes in Computer Science **547**: 257–265.

[98] Jan Camenisch and Anna Lysyanskaya. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In Proc. of Advances in Cryptology - Eurocrypt, 2001.

[99] A. Lee, K. Seamons, M. Winslett and T. Yu, "Automated Trust Negotiation in Open Systems Secure Data Management in Decentralized Systems", Advances in Information Security, 2007, Volume 33, Part III, 217-258,

[100] G. Yajun, W. Yulin, "Establishing Trust Relationship in Mobile Ad-Hoc Network," Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on , vol., no., pp.1562-1564, 21-25 Sept. 2007.

[101] Devadas, S; Suh, E.; Paral, S.; Sowell, R.; Ziola, T.; Khandelwal, V., "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," RFID, 2008 IEEE International Conference on , vol., no., pp.58,64, 16-17 April 2008.

[102] Internet of Things–Architecture IoT-A. Deliverable D1.5– Final architectural reference model for the IoT.

[103] DG CONNECT Trust and Security. https://ec.europa.eu/digital-agenda/en/telecoms-and-internet/trust-security.

[104] SysSec Red Book is a Roadmap in the area of Systems Security. http://www.red-book.eu/m/documents/syssec_red_book.pdf.

[105] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final.

[106] ETSI TErms and Definitions Database Interactive (TEDDI). http://webapp.etsi.org/Teddi/.

[107] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[108] ITU, ITU Internet Reports 2005: The Internet of Things, Executive Summary, International Telecommunication Union, 2005.

[109] Van Blarkom, G. W., Borking, J. J., Olk, J. G. E., Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents, 2003.