A View on the Role of Information Security on ICT-enabled Judicial Systems

George Eleftherakis[1], Konstantinos Rousis[1],
Mauro Cislaghi[2], and Stefano Somaschini[2]

[1] South-East European Research Centre (SEERC),
17 Mitropoleos Str., 54624 Thessaloniki, Greece
{geleftherakis,konrousis}@seerc.org,
http://www.seerc.org
[2] Project Automation S.p.A.,
42 Viale Elvezia, 20052 Monza, Italy
{mauro.cislaghi,stefano.somaschini}@p-a.it,
http://www.p-a.it

Abstract. The increased Internet penetration and the demand for more transparent, efficient, effective and less bureaucratic services are only few of the reasons that led European Commission (EC) to commit to a modernisation of governments and their transition from paper-based to electronic solutions. One of the most sensitive aspects every government should consider in the context of such a modernisation is the field of Justice. Although most of the procedures are highly inefficient they are proven to work and there is a very high risk involved in tampering with these or the data they deal with. The most prominent issue is guaranteeing that any information flowing within judicial electronic systems are treated securely. This paper identifies the most common security objectives being set in ICT enabled solutions for judicial environments; as found in several on-going and finished projects co-funded by the European Union (EU). These objectives are discussed within the context of Justice and the state-of-the-art of Information Security is presented as possible solutions. Finally, a number of security initiatives and organizations which try to standardise solutions and approaches to common challenges are discussed.

1 Introduction

The vast growth of Internet penetration worldwide (from 0,4% of total population in 1995 to 24% in 2008 [1]) and especially in the developed countries (e.g. in Europe today almost 50% [1]) provides the infrastructure needed for the transition from paper based to electronic systems. The European Commission (EC) from the early stages adopted in its strategy as a priority the use of Information and Communication Technologies (ICT) as a tool for improving the quality of services for the citizen. Modernisation of governments (eGovernment) enables better services, security and democracy by reducing bureaucracy, enforcing transparency, and improving efficiency and efficacy of the established procedures. The i2010 eGovernment Action Plan [2] is a clear indication of EC's commitment to the transition of European governments to an effective eGovernment model while at the same time it presents the first extremely encouraging results.

One of the most highlighted fields in EU policy documents is the sensitive field of Justice. While this field is usually referred to with the term "eJustice", the authors of this paper support that Justice is not going to change per se but rather that ICT will provide more effective and less error prone tools to support the judicial procedures, still widely performed on paper and with manual work. These tools will enhance and promote the work already carried out by judicial actors and at the same time will provide more transparency, leading thus to better control and detection of corruption and fraud.

While there are many benefits, there are also many challenges. Among the most critical key enablers are interoperability and security [2]. Interoperability issues arise mostly during the integration of different eGovernment systems, both at national and European level, mainly due to disparities among member states' legal and technological infrastructures. Security concerns are more prominent in situations where sensitive or classified information is involved, and probably, the most representative example is Criminal Justice.

This paper presents the possible uses of ICT in the field of Justice, as shown through several completed and ongoing EU co-funded research projects. Using the results of this investigation the most common security objectives were identified and are presented. At the same time, state of the art information security techniques are presented as possible ways to meet the identified objectives. Finally, several initiatives which oversee security research and aim to establish security patterns and best practices are presented.

The following section provides an overview of EU co-funded projects which had as main aim the digitalization of procedures found in the Justice field. Section 3 discusses the security objectives found in these projects, explains them in detail with analogies drawn from Justice and provides the enabling technologies. Section 4 briefly presents some of the most important EU and US security initiatives and section 5 concludes this paper.

2 ICT in the Field of Justice

There has been a number of projects funded by the European Union (EU) focusing directly on the field of ICT-enabled justice. In their vast majority, they faced some security issues in one aspect or another. SecurE-Justice [3] is a successfully completed project which was funded under the 6th Framework Programme (FP6). The project was targeted on the investigation and debate phases of trials and its main objective was to allow testimonials, witnesses and interrogations to be performed remotely (i.e. online).

The main motivation was that by having the actors from different cities or countries participating in these phases of the trial, critical time would be gained and expenses (traveling, accommodation, etc.) would be reduced. Obviously, many security concerns arise when an interrogation or a testimonial is conducted online. First of all the identity of a witness should be concealed such as any unauthorized party intercepting the communication link cannot identify her (i.e. privacy/anonymity). Moreover, the exchanged information between legitimate participants should not be readable by third persons eavesdropping on the link (i.e. confidentiality), nor be modifiable without the legitimate principals being able to realize it (i.e. integrity). SecurE-Justice met these objectives by

using a number of state-of-the-art technologies such as biometric authentication of principals, encrypted communication channels, etc.

Another successfully completed project, funded under FP6 as well, is the E-Justice [4]. Its main aim was to apply state-of-the-art access control mechanisms in the context of legal infrastructures. An important outcome of the project was the development of the necessary technologies in order to allow biometric authentication of principals via their face and fingerprint samples. Moreover, it dealt with authorization issues of the authenticated principals in workflow-controlled systems.

A more recent project which by the time of publishing of this paper is still in progress is J-WeB [5]: a judicial cooperation environment specifically for cross-border criminal matters investigation phase between EU and countries of the enlarging Europe. This environment should allow judicial actors from different countries to share evidences, exchange information and opinions regarding trials, and the like. By default, this kind of information is highly classified and should be retrievable only by the authorized principles. J-WeB uses a combination of authentication mechanisms (two-factor authentication) in order to allow principals to access resources: a smart-card and a fingerprint scanner [6, 7]. Moreover, it is of crucial importance that actions taken by any user, such as accessing or uploading an evidence, cannot be denied (non-repudiation) in a later stage.

It is likely that security objectives will be profound in future projects relating to ICT-enabled justice and as such their study should take place within the context of this field [8]. The next section describes in detail the security objectives identified in the aforementioned projects, with direct references to them where possible.

3 Security Objectives in Judicial Systems

With the enormous acceptance of personal computers and the Internet during the last decades, and the computerization of many of the procedures that in the past were followed manually (i.e. paper-based), an inevitable information explosion occurred. Although in its majority this information relates to entertainment (articles, movies, songs etc.), there are many cases where highly classified data are involved.

Information Security had set a number of objectives regarding electronic information, some of them directly derived by the non electronic world. Qualities such as conversation privacy were not even thought few decades ago. If two persons wished to discuss privately, they could just take a walk to an open area and it was unimaginable how someone could eavesdrops them without noticing it. These days are long gone and in the Information era such self-evident qualities have to be rethought in a different context [9].

Research and industry are jointly working on a number of such objectives from confidentiality and access control to anonymity and privacy. The focus of this section is given to the objectives directly relating to the field of justice, as identified by EU-funded projects completed or still running, and are discussed within this context. Namely, access control is considered first, confidentiality and integrity follows, and non-repudiation and privacy concludes this section.

3.1 Access Control

Access Control is undoubtedly the most common security objective any judicial system has to meet. It encompasses two related but distinct objectives[3]: *authentication* and *authorization*. In person-to-person talk authentication is rarely an issue. Each participant is aware of to whom she talks just by looking at her face or by recognizing her voice. Even when a person meets another for the first time, usually someone they both know makes the introduction. This is not the case however in the digital era.

When someone is exchanging e-mails, or even communicating in real-time with someone over a network, there is no simple way of authentication. Similarly when someone reads an electronic document, she can not be easily sure of its original author. Authentication in the context of Information Security is the binding of a real-world identity to an equivalent electronic one. Its importance in the field of justice is of paramount importance. If a judge communicates to a criminal who impersonates another judge, she may reveal highly classified information or even take decisions based in false facts.

Authentication mechanisms can be conceptually divided into three categories [8]:

1. Something you know. This is the most common category where a principal is authenticated according to something she knows such as a PIN, a password, her mother's maiden name, and the like.
2. Something you have. In this category fall the mechanisms requiring from the principal to present something she carries with her in order to authenticate. A typical example is the use of a smart card.
3. Something you are. This method refers to biometrics where a principal is authenticated by providing a sample found on her body, which is unique among other people. The sample may derive from her fingerprint or iris and is checked for matching with an already stored sample of the same person.

A *two-factor authentication* is called the technique of combining two of the aforementioned categories. For instance, the J-WeB project suggested the use of both smartcards and fingerprint scanning in order to authenticate principals [7]. Obviously, the requirement of authentication mechanisms that fall in more than one category can reduce the chances of a compromise but at the same time the availability may be decreased. A typical drawback of biometrics is the annoyance of the legitimate principals upon failed matching (negative false) of the given and the stored sample.

A lot of emphasis has been put to develop authentication systems which are pervasive and unobtrusive to their users. As a result a judicial actor may not be even aware that she is authenticated while her RFID tag broadcasts her PIN to an RFID reader and the automatic door opens for her. Nonetheless, the internals behind such solutions are quite complex and they utilize a variety of technologies.

The key technology enabling authentication nowadays is the public key cryptography. The main concept is that every principal is assigned with a unique pair of keys one of which called the public, and the other called the private. The principal publicizes her

[3] The term Access Control is found sometimes in literature to refer only to authorization. In this paper is used to encompass both authentication and authorization.

public key unworryingly in order for other principals to encrypt messages destined to her. Later, she can decrypt them using her private key which as its name suggests, is known only to her.

A very interesting feature of this technology is that by having a principal encrypt a message with her own private key, anyone else can decrypt it with her public key, thus verifying who sent it. The last is sometimes useful on its own and is known by the name of *digital signature*.

Authentication on its own is rarely adequate to cope with the complex needs of today's information systems. The reason lies in the fact that principals should have permissions upon objects on a fine-grained manner rather than on a black and white fashion. These issues are addressed by authorization which typically follows the authentication phase. The main concern of authorization is not who someone really is (i.e. authentication), but what she is allowed to do in a given system.

As an example, both a judge and a judge clerk may be authenticated in a judicial electronic system, but under no circumstances they should be authorized with the same privileges. While a clerk might be able to access legislative decisions and documents in order to perform paper-work, she should not be able to access evidences for a case. Even among judicial actors who belong to the same level of hierarchy, authorization procedures are essential. While a judge should be able to access information regarding a case assigned to her, she should not be able for a case which is assigned to another judge.

The requirements of authorization usually derive directly from the hierarchy, organization, and specifics of the environment in which is deployed. It is common for companies with more than few employees to categorize them according to the roles they possess. One of the first authorization models which is still widely used is the Role-Based Access Control (RBAC) [10–12] and it is based in exactly this observation. In RBAC, each user is assigned to one or more roles and each role is associated with a set of permissions (and maybe a set of restrictions). As mentioned though persons that may possess the same roles may be needed to have permissions on different resources. Although RBAC implementations support this, it is obvious that the complexity of management increases.

Consequently, a very crucial requirement for any authorization system is to be flexible on both users and managers perspective. More recent alternatives to RBAC are the capability-based access control models, where the authorization procedure of a user depends on the credentials she presented upon her request [13]. Such models may not even require authentication a priori but rather ensure on-the-fly that the requester is the same person with the one shown in the credentials [14, 15]. This leads to new possibilities such as dynamic trust delegation: "A judicial actor in Greece, which has a set of certain permissions, issues a credential in order to allow a colleague of her from Italy, who is not an authorized user of the system, to have a subset of her permissions." Finally, there are also hybrid approaches, combining characteristics of both capability-based (e.g. KeyNote [16]) and role-based (e.g. RBAC) models, such as Aether [17].

3.2 Confidentiality and Integrity

Even if it is assumed that two principals[4] are authenticated properly and are authorized to exchange some information, anyone eavesdropping on the communication link can capture the information irrespectively of her authorization status. It follows that protection of unauthorized access to the exchanged data are of utmost importance. Due to the nature of networks, eavesdropping may not be detectable so the aim is to prevent any unauthorized adversary from getting a meaningful context out of the captured data, rather than preventing her from capturing them at all.

The objective of pertaining this quality is known to the information security field as confidentiality. The enabling technologies for meeting this objective rely on cryptographic primitives. The sending party encrypts the information before transmission and the receiving party decrypts them upon receipt. The two operations, encryption and decryption, are based on cryptographic keys, which are known only to the communication parties. Anyone intercepting this information but is not aware of the key is unable to extract any meaning.

The specifics of how the keys are used in order to encrypt and decrypt information belong to the field of cryptography and thus are outside of this paper's scope. In short, if symmetric cryptography is utilized the same key is used for both encryption and decryption. In asymmetric cryptography (aka public-key cryptography), each principal has a pair of keys: a public and a private. Any other principal who wants to send something confidentially to her, encrypts it with her public key. Afterwards, the first principal can decrypt it with her own private key which is assumed to be known only to her.

The important thing is that technologically there exist a variety of good cryptographic protocols which can ensure confidentiality, without requiring extensive knowledge of the field. Moreover, confidentiality can be embedded to systems seamlessly as in the case of J-WeB portal [5]. A requirement of this project was that judges could exchange information such as evidences, history, opinions etc. By default, this kind of information is highly classified and having the public or any party involved in a trial reading them could lead to disastrous effects. The specific algorithm used in order to ensure confidentiality in this project was a symmetric cryptosystem known as 3-DES, a stronger variant of the older Data Encryption Standard (DES).

Two important factors for selecting a good encryption algorithm are the length of the key used, in bits, and the amount of testing it had received. The US standard for encryption is currently a variation of the Rijndael algorithm, mostly known as the Advanced Encryption Standard (AES). Certainly there exist other good candidate such as Blowfish, RSA, IDEA, SEAL, PGP and its variants, and many others [18].

The state of the art in encryption is based on the use of quantum mechanics in order to perform quantum cryptography [19]. Although this technology has been implemented, it is still available only in governmental applications and in some large corporations with high security demands. The main advantage of quantum cryptography relies on its different nature of standard communication networks. While in the latter an eavesdropper may be impossible to detect, in quantum distribution channels anyone

[4] In this context a principal is not necessarily a person; it may be a handheld device, a biometric or other authentication device, a database, a server, and the like

trying to eavesdrop disturbs the system and thus is detectable [19]. Nonetheless, the high cost of equipment, the relatively short distances, and the lack of a demonstrated threat to existing protocols, limits the spread of quantum cryptography.

Yet another security objective is integrity which refers to the quality of being able to identify unauthorized alteration of information. As an example, judicial decisions regarding finalized trials should be made publicly available. In an information system this would mean that a kind of document would have to be uploaded on a public file server. In the case that anyone intercepting the transmission from the judge to the server was able to tamper the original message without this being identified by the end-users, consequences would be disastrous. Any criminal with incentive would be able to misinform the public regarding the trial's decision.

According to the EU-funded project SecurE-Justice [3], integrity is of much greater importance than confidentiality during trials which are held as public events. Thus, it is essential to have the means of understanding whether the initial document has been tampered in any way since its original creation.

The main technology used to achieve integrity is hash and Message Authentication Code (MAC) functions. There is a variety of such functions available such as MD5, SHA-1, RIPEMD-160, and others. Currently, a new hash function is under development which will be selected via open competition and will be made official in 2012 under the name Secure Hash Algorithm-3 (SHA-3). As already mentioned, another alternative widely used to achieve integrity is digitally signing a document. By signing the document using a private key any attempt made to alter this information will result to a failure while verifying the signature with the corresponding public key. Although confidentiality and integrity are typically two faces of the same coin [3], they satisfy two completely different requirements and they should not be confused.

3.3 Non Repudiation and Privacy

An important objective judicial information systems are called to meet is non-repudiation. According to this objective, it should be ensured that a party in dispute cannot refuse the validity of a statement or a contract. For the shake of example, when a judge makes publicly available a trial's decision, she should not be able at a later point to deny that she did it. Similarly, it may be important when a judicial actor gains access to an evidence not to be able to refuse it [3].

It follows that authenticity and integrity are prerequisites for non-repudiation. If for example a judge is not required to authenticate in order to access an evidence, there is no way to be sure if she did actually accessed it, and even in this case that she did, she can repudiate it. On the other hand, if integrity is not met, any judge publicizing a decision can later argue that she publicized a different document which was altered by someone else.

In addition to authenticity and integrity, digital signatures are typically used in order to ensure non-repudiation. By having the author of a message (or document) to sign it with her private key, there is no way that she could later refuse its creation. Obviously, if her private key is compromised things get much more complex as she would be able to refuse any action signed by this key. The solutions to this problem vary from certification revocation lists to the use of timestamps in each action in order to resolve

issues when someone reports a key compromise and an action with this key takes place later on. Nonetheless, most of these details depend on the security models and policies each organization adopts.

When non-repudiation has to be ensured for acquired documents and evidences, an access tracking mechanism is usually needed [3]. Although the enabling technology is again based on public key cryptography, such mechanisms allow for unobtrusive non-repudiation of document retrieval.

Although non-repudiation is of crucial importance, there are cases where actions taken from users should not be concealed to third parties. The most typical example is the identity, location, and testimony of a witness [3]. This is the *privacy* objective and most of the times encryption is the main means to achieve it. By ensuring a secure communication channel and some form of pseudonymity (i.e. instead of the witness's name a random ID should be displayed), privacy can be respected while at the same accountability is preserved(i.e. non-repudiation). The most significant research on privacy has been conducted under the scopes of e-voting systems [20] (zero-knowledge proofs, blind signatures etc.) and medical informatics [21] (randomisation, pseudonymity etc.).

Finally, it may be necessary for certain occasions where two principals communicate securely (e.g. a witness with a prosecutor) none of them to be able to prove what the other party had said. This is in essence the opposite of non-repudiation and it falls under the objective of privacy. *Deniable authentication* [22] is the most common way to satisfy such requirements by utilizing shared MAC keys between the participants who want to communicate in such a fashion. None of the participants can prove to a third party what the other had said as the message could have been as well forged by themselves [23].

4 Security Initiatives

As standards are necessary in order to achieve uniform adoptions among different industries, organizations, and their systems, similarly there is a need for security initiatives suggesting patterns and best practices in order to ensure that security is becoming an integral part of every information system. During the last decade, a number of initiatives focusing on the most crucial aspects of information security has been established. The rest of this section will focus on them, the role they serve along with their aims, as well as the proposed solutions on meeting the objectives discussed in the previous sections.

4.1 Liberty Alliance

Liberty Alliance [24] (Lib.All) was formed in 2001 and its focus is to address issues of identity management. Specifically, it provides specifications and recommendations for topics such as identity assurance, governance, and theft, strong authentication, privacy and trust, and others.

Currently, more than 150 organizations are members, with the management board be consisted of key players in the market such as America OnLine (AOL), Sony Ericsson, Hewlett-Packard, Oracle, Novel, and Sun Microsystems. A concrete objective

of liberty alliance is to establish trust among stakeholders in the Internet: end-users, vendors, corporations, and governments.

Furthermore, a number of specifications has been published concerning identity management, privacy, and interoperability such as IAF, IGF, ID-WSF, and many others. As a next step, products and devices adhering to these specifications are able to be certified directly by the initiative. In order to address more efficiently the different issues which concern the initiative, 9 special interest groups (SIGs) have been established. Each of them focuses on specific issues such as Web services harmonization, health information management, standards coordination, and others.

Quite interesting in the scope of this paper is the eGovernment group (eGov-SIG) which acts as a forum to discuss best practices by government and organizations on the national, regional, and municipal levels. The eGov-SIG aims to share solutions and technical approaches as a means of avoiding the "wheel reinvention". Lastly, it tries to drive the adoption of standards-based identity management mechanisms in governments, on a global basis.

4.2 Global Trust Center

Global Trust Center [25] (GTC) is an independent international organization with prime mission to enable trust in interactions spanning the non-digital and digital worlds. The main problem it addresses is that while in the real world, a signature can be used to perform a contract and the person signing be accountable for it, a digital signature has no legal traceability. GTC aims to map the real world identities to digital ones, with all rights, benefits, assumptions, and obligations the former have.

Although GTC was established in Sweden, it tries to involve all EU State Members and assist them on how to implement electronic identity policies in legal and infrastructural terms. The main suggested technology is a Public Key Infrastructure (PKI). Moreover, GTC has developed a life time digital identity holder. According to this, individuals would be able to map their identity to an electronic one for both professional and private use and enjoy a legal status over the Internet. Except the benefits and protections an individual will enjoy, it will also be accountable for any responsibility her signature may carry.

4.3 Methods Standards Certification Initiative

The Methods Standards Certification Initiative (MSCI) has been established by the Security Task Force and it is placed clearly within the existing European Commission policy on security with reference to security interoperability and development of new and evolution of present security standards [26]. It strives to involve both member states and organizations in the development and adoption of the standards with the aid of national and international standards organizations such as CEN/ISSS, CENELEC, ETSI, ENISA, etc.

An expected result of the MSCI would be to initiate actions which will eventually lead to awareness, participation in development, and adoption of security standards. A crucial objective for achieving this would be the increase of training and certification in security standards by European companies, products, and personnel.

4.4 Other Initiatives and Organizations

Another organization which overlooks the actions of security initiatives in the EU, as well as the development of security standards, is the European Network and Information Security Agency [27] (ENISA). Moreover, it had initiated the "Awareness Raising" (AR) community which aims to inform the public with regards to information security issues concerning individuals, professionals, and organizations.

Another initiative dedicated to information security issues is the Network and Information Security Steering Group [28] (NISSG), established by the Information and Communications Technologies Standards Board (ICTSB) and supported by CEN, ENISA, and ETSI. NISSG maintains a report which provides both an overview of existing security standards, as well as recommendations to be carried out by the European Standards Organization and other related bodies.

Finally, the International Telecommunications Union Telecommunications Standardization Sector (ITU-T), had established the Study Group 17 (SG17) in order to address security-related problems and concerns [29]. SG17 is supported by both ENISA and NISSG and its main achievement is the development of the ICT Security Standards Roadmap. Similarly to the NISSG report, this document includes all relevant standards along with their status, best practices, as well as proposals for new security standards which will meet the future needs.

5 Discussion

The most common security objectives in information systems supporting judicial activities are rather similar to the ones most critical systems have. Although this is not surprising, security research under a specific scope, such as this of Justice, cannot be considered redundant: the most common reason for security protocols failures is due to changes in the system and the environment [8] and as field experts very often point out, there is no such thing as a plug and play solution when it comes to security [30]. There are a myriad of technologies meeting most of the identified security objectives in different ways, but it is of crucial importance to understand an environment in depth in order to choose the most suitable. Another issue to consider when having so many available technologies to pick from, as mentioned earlier, is interoperability. While Service Oriented Architectures (SOAs) and in particular Web Services seem like a possible solution to interoperability problems faced in electronic judicial systems [5], security should be again an integral part of such an integration as the possible communication interfaces increase exponentially.

Another critical aspect of any system which should be secure is the awareness and training level of its users. Unfortunately, people are the weakest link of the security chain and sometimes an uninformed user is enough to bring down the whole security [9]. On the other hand, such tools aim to support Justice and its servants and not to create difficulties or, as put in i2010, citizens to be left behind [2]. Proper education and increase of security awareness is only one side of the coin, the other is unobtrusive and easy-to-use applications, well integrated with the established workflows which have been proven to be working.

Many of these challenges are addressed by security initiatives and organizations which continuously monitor the developments of the field and try to improve and standardize them. Guidelines exist for user-education and training, security policies, safe use of technology, interoperability and many other challenges already mentioned. The next step is industry adoption, generation of feedback, and further improvement.

References

1. Internet World Stats: Usage and Population Statistics. (2008) http://www.internetworldstats.com/.
2. i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All (2006) http://ec.europa.eu/information_society/activities/egovernment/docs/highlights/comm_pdf_com_2006_0173_f_en_acte.pdf.
3. SecurE-Justice project: Secure communication and collaboration framework for the judicial co-operation environment, FP6IST/507188/71241 (2004)
4. EJUSTICE project: Towards a global security and visibility framework for Justice in Europe, FP6IST/001567/74600 (2004)
5. J-WeB project: Collaboration environment for judicial European network in Western Balkans, FP6IST/045331/80529 (2007)
6. Cislaghi, M., Eleftherakis, G., Mazzili, R., Mohier, F., Intravaia, D., Pellegrini, D., Ferri, S., Giuffrida, V., Vuksanovic, V., Negroni, E.: Regional judicial cooperation using an innovative ICT platform for cross border investigations. In: International Conference for Entrepreneurship, Innovation and Regional Development ICEIRD. (2008)
7. Cislaghi, M., Eleftherakis, G., Mazzili, R., Mohier, F., Ferri, S., Giuffrida, V., Negroni, E.: Secure judicial communication exchange using soft-computing methods and biometric authentication. In: International Workshop on Computational Intelligence in Security for Information Systems CISIS'08. (2008)
8. Anderson, R.: Security Engineering: A Guide to Building Dependable Distributed Systems. 2^{nd} edn. John Wiley & Sons, Inc., New York, NY, USA (2008)
9. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons, Inc., New York, NY, USA (2004)
10. Sandhu, R.S., Coynek, E.J., Feinsteink, H.L., Youmank, C.E.: Role-based access control models. IEEE Computer **29**(2) (1996) 38–47
11. Ferraiolo, D., Kuhn, D.: Role-based access control. In: Proceedings of NIST-NSA National Computer Security Conference. (1992) 554–563
12. Ferraiolo, D., Kuhn, D., Chandramouli, R.: Role-Based Access Control. Artech House (2003)
13. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: SP '96: Proceedings of the 1996 IEEE Symposium on Security and Privacy, Washington, DC, USA, IEEE Computer Society (1996) 164
14. Blaze, M., Ioannidis, J., Keromytis, A.D.: Experience with the keynote trust management system: Applications and future directions. In: iTrust. (2003) 284–300
15. Keromytis, A.D., I., S., Greenwald, M.B., Smith, J.M.: The STRONGMAN architecture. In: Proceedings of the 2003 DARPA Information Survivability Conference and Exposition. Volume 1. (2003) 178–188
16. Blaze, M., Feigenbaum, J., Keromytis, A.: The KeyNote Trust Management System (Version 2). RFC 2704 (1999)

17. Argyroudis, P.: Authorization Management for Pervasive Computing. PhD thesis, Trinity College Dublin (2006)
18. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2^{nd} edn. John Wiley & Sons (1996)
19. Bruss, D., Erdélyi, G., Meyer, T., Riege, T., Rothe, J.: Quantum cryptography: A survey. ACM Comput. Surv. **39**(2) (2007) 6
20. Balopoulos, T., Gritzalis, S., Katsikas, S.K.: Specifying electronic voting protocols in typed msr. In: WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, New York, NY, USA, ACM (2005) 35–39
21. Baumer, D., Earp, J.B., Payton, F.C.: Privacy of medical records: It implications of hipaa. SIGCAS Comput. Soc. **30**(4) (2000) 40–47
22. Dwork, C., Naor, M., Sahai, A.: Concurrent zero-knowledge. In: STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing, New York, NY, USA, ACM (1998) 409–418
23. Borisov, N., Goldberg, I., Brewer, E.: Off-the-record communication, or, why not to use pgp. In: WPES '04: Proceedings of the 2004 ACM workshop on Privacy in the electronic society, New York, NY, USA, ACM (2004) 77–84
24. Liberty Alliance. (Lib.All) `http://www.projectliberty.org/`.
25. Global Trust Center. (GTC) `http://www.globaltrustcenter.org/`.
26. Methods Standards Certification Initiative. (MSCI) `http://www.securitytaskforce.org/index.php?option=com_content&task=view&id=11&Itemid=95`.
27. European Network and Information Security Agency. (ENISA) `http://www.enisa.europa.eu/`.
28. Network and Information Security Steering Group. (NISSG) `http://www.ictsb.org/Working_Groups/NISSG/Index.htm`.
29. International Telecommunication Union Standardization Sector Study Group 17. (ITU-T SG17) `http://www.itu.int/ITU-T/studygroups/com17/index.asp`.
30. Ferguson, N., Schneier, B.: Practical Cryptography. John Wiley & Sons, Inc., New York, NY, USA (2003)