OPEN SECURITY ISSUES IN GERMAN HEALTHCARE TELEMATICS

Ali Sunyaev
Department of Informatics, Technische Universität München, Munich, Germany

Jan Marco Leimeister
Department of Economics, Universität Kassel, Germany

Helmut Krcmar
Department of Informatics, Technische Universität München, Munich, Germany

Keywords: Security analysis, Healthcare telematics, Electronic health card, Information systems security, Healthcare IS security.

Abstract: Developments in German healthcare telematics aim at connecting existing information systems of various service providers and health insurers via a common network. Such a linking of different systems and infrastructure elements creates a complex situation that has to deal with high priority requirements for data security, data safety, and data integrity as it concerns sensitive data such as personal medical information or administrative operational data. This paper provides a security analysis of the German healthcare telematics infrastructure under development and derives security measures to overcome the identified vulnerabilities. This analysis of open issues in the security concept of German healthcare telematics might be helpful for both future research and practice in healthcare information systems security.

1 INTRODUCTION

The nation-wide healthcare telematics infrastructure under development in Germany is based on the introduction of the new *electronic Health Card (eHC)*, which will replace the health insurance card currently in use (Sunyaev et al., 2009a). Based on smart card technology, eHC will provide additional functionalities through healthcare data management, e.g. electronic transfer of prescriptions and diagnostic data. Therefore, experts predict several improvements in data management for the healthcare sector, including cost savings (Guah and Fink, 2008), streamlined communications between involved parties, and for patients more control over the handling of their medical data (Schabetsberger et al., 2006).

Since eHC and the corresponding healthcare telematics infrastructure manage highly confidential medical information, including data on patients' health conditions, course of disease and hereditary diseases (Lorence and Churchill, 2005), requirements regarding privacy, safety, security and availability of such data throughout the system are extremely sensitive. Disclosure of patient medical data could have severe social consequences, e.g. denial of employment or insurance because of certain illnesses (Mandl and Kohane, 2008). As possible vulnerabilities and leakage of confidential data is a recurring problem in the modern information system landscape, an in-depth security analysis of this healthcare telematics system is indispensable.

In this paper, we first introduce the German healthcare telematics infrastructure. Chapter 3 explains details of the analysis, including the examined specification documentations and components, the identification of threads and required security requirements. The security analysis we conducted was implemented according to the ISO 27001 security standard. In chapter 4, the results we achieved are presented and explained in

Sunyaev A., Leimeister J. and Krcmar H. (2010).
OPEN SECURITY ISSUES IN GERMAN HEALTHCARE TELEMATICS.
In *Proceedings of the Third International Conference on Health Informatics*, pages 187-194
DOI: 10.5220/0002694801870194

detail. The final chapter concludes the security analysis and offers a look at further development in this area.

2 HEALTHCARE TELEMATICS INFRASTRUCTURE

While the current healthcare system in Germany is based around a health insurance card which only stores insurance data, the planned German healthcare system is based on the eHC smart card which will contain an on-card microprocessor for enhanced services, such as ciphering or the digital signing of data (Schweiger et al., 2007). The eHC possesses two different types of functions. These include mandatory functions, such as administrative data and the electronic prescriptions. These functions allow the physicians to check the administrative data of the patient and to write prescriptions on the eHC. On the other hand there are the voluntary medical functions such as the emergency data record and, eventually, an electronic patient record. The emergency data includes medical information (e.g. blood group and allergies). Fluoroscopic images, laboratory findings, operation reports and other examination data can be stored in the electronic patient record. The eHCs will be mandatory for every German citizen. Furthermore, each healthcare provider will receive a *Health Professional Card (HPC)* and the essential computer equipment (e.g. the *connector* that interconnects *primary systems*, *card terminals* and *communication infrastructure*).

Most of the sensitive medical data will not be stored on the card itself, but will instead be archived in central databases connected to hospitals, medical practices and pharmacies through a network of secure components, the *Healthcare Telematics Infrastructure (HTI)*. Using secure VPN connections over the Internet, the data can be retrieved at any time if the request is authenticated using the eHC and the HPC belonging to healthcare providers (physician, pharmacist and all other categories of healthcare personnel).

Both cards have a clearly defined structure and set of functions. Sensitive medical information will be protected by a PIN and is only available with the HPC of a doctor. Thus, it should not be possible to add additional functions or to create additional certificates (Huber et al., 2008). This makes it very difficult to use the cards for further purposes.

2.1 Functions of the HTI and its Expansion

After its initial launch, the function of the eHC and HTI will subsequently be expanded in several stages. While the usage of the eHC itself and its base function is mandatory, an insured person may choose whether or not to use most of provided enhancements.

During the first stage after its introduction, the eHC will serve as storage for personal and insurance-related data (e.g. name and address of the patient, date of birth, insurance number, etc.). The backside of the smart card will feature a form that enables the card to serve as a *European Health Insurance Card (EHIC) (Marschollek and Demirbilek, 2006)*. This first stage of the nation-wide introduction of the eHC is mandatory for all insured persons in Germany.

In the second stage, the eHC will also be used to store prescription data, replacing the current system of paper-based prescription forms. Prescriptions may also be stored centrally in the HTI; the card will then serve as an access key. This second stage of eHC introduction in Germany will also be mandatory.

Functions to be introduced in stages three and four will be optional. Planned enhancements include storage of emergency medical data on the eHC, an electronic patient record and a record of medication history, in order to prevent dangerous pharmacological interactions. The data will either be stored on the eHC, or in a central HTI database, or both.

2.2 HTI Architecture

The HTI can be divided into a central and a peripheral part, using secure connections over the Internet for communication. Figure 1 shows a schematic representation of the German HTI[1].

The central part of the HTI offers online services through VPN connections, which can be accessed by *Medical Service Providers* (MSPs), such as physicians or hospitals, as well as by patients. The central HTI servers will be located and maintained in several computing centers under the direct supervision of gematik, German national healthcare's IT body.

[1] For a more detailed explanation of the HTI please refer to the public development documentation provided by gematik mbH at their corporation website (http://www.gematik.de)

The peripheral part of the HTI is located at the workplace of medical service providers. It is connected to the local LAN and consists of a connector, card readers and the required smart cards (eHC, HPC). The connector has interfaces to provide local connectivity within the LAN, as well as establishing and managing VPN connections with VPN concentrators at the central HTI.

The software used by the medical service provider, a so-called *primary system,* is not part of the peripheral HTI but can access card readers and cards through the connector. These primary systems are used by MSPs to manage and store patient medical and administrative data and also to perform accounting and other healthcare-related tasks. As these software products are created and maintained by third party companies, their security aspects are not subject to governmental control and are not covered in the HTI specification documents provided by gematik. However, these systems were also examined during the security analysis, because they are connected to the HTI and handle the same sensitive medical data.

3 SECURITY ANALYSIS OF THE HTI

3.1 Examined Components and Specification Documents

The analysis focuses on the peripheral HTI parts, which are more exposed and thus more vulnerable to possible attack scenarios than central HTI components. The components examined in the analysis are *Smart Cards, Connectors, Primary System,* and *Card Reader*s as well as the interaction processes between these components.

All available specification documents were examined during this analysis. Therefore, the information on which the results are based is accessible to any interested person or possible attacker using publicly available documents about the HTI. gematik has released the majority of its specification documents publicly so any internal or confidential documents should likely be insignificant for an analysis. Furthermore, several deficiencies were discovered within the specification documents, which refer to missing parts of documentation that still have to be fulfilled by gematik.

The following German legal documents were used: (SGB, 2007) (Social Security Code), (BDSG, 2003) (Federal Data Protection Law), (SigV, 2001), (SigG, 2001) (Electronic Signature Act) and (StGB, 2005) (Professional Discretion).

The following specification documents have been examined for the analysis: (gematik, 2007b), (gematik, 2006a), (gematik, 2006b), (gematik, 2006c), (IBM et al., 2004), (gematik, 2007a), (gematik, 2008j), (gematik, 2008k), (gematik, 2008b), (gematik, 2008c), (gematik, 2008d), (gematik, 2008e), (gematik, 2008f), (gematik, 2008g), (gematik, 2008h), (gematik, 2008a), and (gematik, 2008i).

Documents not included here contained no security-relevant aspects. All recent documents are included in the gematik release 2.3.4, the most current specification release available at present (May 2009).

3.2 Identification of Security Requirements

Security requirements for the HTI are explained in detail within a privacy concept (gematik, 2008j) and a security concept (gematik, 2008k). Legal documents regarding the eHC and basic IT security resources were also searched for requirements during this security analysis.

4 RESULTS OF THE SECURITY ANALYSIS

4.1 Cross-component Analysis of the German HTI

The cross-component analysis was intended to analyze processes; the mentioned components are involved in. Furthermore, the cross-component analysis included a critical review of the development documents from a security-based point of view.

Combination of Medical and Administrative Data. (IBM et al., 2004, p. 30) states that security must not depend on the reliability of a single person. However, in (IBM et al., 2004, p. 20) it is explained that the key for combining separate administrative and medical data is to be held by the ”Federal Commissioner for Data Protection and Freedom of Information” a position held by a single person. This deficiency is still present, as (gematik, 2008k, p. 180) states that data may be combined by selected persons while the data privacy delegate of the insurance company is involved. This suggests that a single person is still in control of this particular key.

Unauthorized Transfer of Medical Data. In (SGB, 2007, SGBV, 294a) it is stated that by law, depending on the medical issue, full medical data has to be given to the insurance company without the patient's consent. This exception conflicts with a basic requirement found in (gematik, 2006a, p. 63) stating that no one is allowed to access medical data without the permission of the insured person. Furthermore (SGB, 2007, 2007, SGBV, 291a, para. 3) states that insurers must inform the affected patient about the transfer of data. This possible vulnerability remains as long as (SGB, 2007, SGBV, 294a) is not changed, for example by involving the HTI in data transfer. Using the eHC, it would be possible to securely transfer the data to the insurance provider, while involving the insured in the process using the eHC to grant permission.

Missing Backup Method for Electronic Prescriptions. According to (IBM et al., 2004, p. 19), an alternate backup process must be created for every electronic HTI process. (gematik, 2006b, p. 28) however states that there will be no backup process for the filling of prescriptions by pharmacies. Although this statement was purged from (gematik, 2008e), there is still no trace in (gematik, 2008b) and (gematik, 2008c) of a backup process. This means that a patient with a prescription stored on an eHC would have to either revisit their doctor to get a paper prescription, go to another pharmacy with a working HTI connection or wait until the HTI is working again. This is obviously an inconvenient and potentially dangerous situation, depending on the person's health.

Possibility to Issue the Same Prescription Twice. If the above-mentioned backup process is implemented using paper-based prescriptions, a patient would possess a prescription in both digital and paper form, allowing them to fill both in different pharmacies (by filling the paper-prescription at a pharmacy with HTI problems and the electronic one in a pharmacy where the HTI is working). The possibility of prescriptions being filled twice would violate requirements concerning accountability and non-repudiation. This is, however, currently not an issue as no backup process exists.

No Security Verification for the ”Zone-Concept”. In (gematik, 2007b), the HTI is divided into several zones to allow a separate view of each specific security zone. These zones are treated as closed areas as mentioned in (gematik, 2007b, p. 32), meaning that security vulnerabilities in one zone shouldn't affect adjacent zones. But the zones of the HTI are physically connected for data transfer, and thus there is still a possibility of unauthorized traffic between zones. The statement itself is still present in (gematik, 2008k, p. 40) but (gematik, 2007a, p. 9) explains that it is possible to break into the HTI network and compromise adjacent systems, which contradicts statements about closed zones. Therefore, this statement should be replaced by a more accurate one explaining the connection between zones.

Adjustment of Security Standards. According to (gematik, 2007b, p. 28), the minimum security standards for the HTI have to be checked and adjusted once a year. This time span remains unaltered in the current version of the document, but considering the CERT (http://www.cert.org/stats) statistics of about 8,000 vulnerabilities per year, a time span of one year seems unnecessarily long. A shorter period between minimum security standard adjustments would improve the security of the HTI.

Inadequate Security Assumptions about the HTI. gematik considers all systems inside the VPN of the HTI to be secure (gematik, 2006b, p. 60). Therefore, the time servers within the HTI are used by the connector without any authentication. In fact, there are no completely secure IS systems (Sharman et al., 2004), so the argument is not valid.

Nevertheless, it is still used in (gematik, 2008e, p. 114). There is also contradicting information regarding the time servers. While (gematik, 2008a, p. 49) explains that the time sync is mainly for chronological logging purposes and therefore no authentication is needed, (gematik, 2008c, p.15) points out that electronic prescriptions on the eHC use the primary system's time, which is synced with connector time, which is synced with the time server's time. This leads to the conclusion that the time server's time is used for time stamps of secure medical data on the eHC. If a manipulated time server could be used to manipulate timestamps on the eHC, there must be authentication to prevent such a scenario.

Security by Obscurity. The concept of *security by obscurity* isn't a proper way of securing medical IS systems, as pointed out by gematik in (gematik, 2007b, p. 246). However, parts of the software used within the HTI are classified as highly confidential by the same document, due to copyright issues, as the programs remain the intellectual property of the developing companies.

While copyright is important, Shannon’s maxim and Kerckhoff’s principle (Schneier, 1996) should be considered and program code that contains security-related processes should be published.

4.2 Analysis of the Connector

Security Issues Concerning Communication with the Primary System. For communication between primary system and connector, none of the gematik documents requires authentication other than the general demand for SSL usage between HTI components (cp. (gematik, 2007b, p. 137 and p. 172)). As the primary system doesn't possess a cryptographic identity, an authentication between the two components would at best be one-sided. With only one-sided or no authentication at all, man-in-the-middle attacks are possible between the connector and the primary system. In order to verify the connector's identity the primary system would need some kind of service by the HTI to perform the necessary id check, something which is not possible as (gematik, 2007b, p. 177) forbids direct access of the HTI for an outside component.

Although this deficiency is still present, in (gematik, 2008e, p. 41) an optional server authentication for TLS/SSL connections between connector and primary system is considered. In (gematik, 2008i, p.167) an obligatory initialization of a secure channel between the two components is proposed. Therefore this deficiency may be dealt with in the next document release.

4.3 Analysis of the Primary System

Security Aspects of Primary Systems. The current security measures used in present primary systems are, according to (IBM et al., 2004, p. 21), sufficient to provide a “*normal”* level of security for processed data, based on the categorization of IT-Grundschutz[2] (security guidelines).

In (gematik, 2008k, p. 28), the security level for medical data is raised to “*very high”,* but this only affects the well-secured HTI components. As the primary system is not part of the HTI, no security requirements for it are found within the specification, which leaves the primary system as the least secure part of the eHC-related network. To ensure the safety of private data at all times, it might be necessary to reconsider the security level of primary systems and provide concurrent security requirements.

4.4 Deficiencies of the Current Security Concept

Missing Specification for Services to manage eHC Data by the Insured. An important and basic requirement of the HTI and eHC is to enable the insured to exercise his right to view and administrate his own medical data (cp. (gematik, 2008k, p. 27)). Therefore, two services are planned to privately manage data on the eHC. The so called *eKiosk* will be a terminal positioned in public places like hospital lobbies, where every insured person can insert his eHC and view or change permissions on data stored on the card. Another service, called *Versicherter@home*, will enable the insured to manage eHC data at home using the internet.

However, neither of these services can be found in the gematik documents, as they belong to the services to be introduced last. Since both of them access medical data on the eHC and are less secure than other HTI components due to their exposed position, they have to be thoroughly tested and secured, so it may be unwise to specify such critical components last.

Missing Backup Processes for Important HTI Processes. As mentioned earlier, one of the security requirements for services within the HTI is to provide backup processes in case the HTI experiences technical difficulties and is unavailable, as stated in (gematik, 2008d, p. 40) and (gematik, 2008k, p. 41). But so far, no backup processes are described in the specification documents. Because of attacks or technical problems, one-hundred percent availability for components in the HTI can't be guaranteed. Hence, backup processes have to be defined before the eHC is introduced nation-wide in Germany.

Possibility of Health Insurance Number Readout by Unauthorized Persons. The health insurance number of an insured person issued together with the eHC remains the same throughout the life of every insured person, so it could be used for identification purposes and should be kept strictly confidential. In (gematik, 2008k, p. 247), a requirement defines that the use of the insurance number stored on the eHC for purposes not related to healthcare *should* be avoided and access to the number on the eHC *should*

[2] German Federal Office for Information Security - http://www.bsi.de/gshb/index.htm

be restricted to MSPs and authorized personnel to prevent the leakage of social data. RFC 2119[3] states that *should* defines a recommendation with room for exceptions. As no reasonable exceptions are stated by gematik, there is no reason to use *should* instead of *must*. The insurance number must not be accessed by unauthorized users.

Logs for SMC Access on the Primary System may not be Reliable. To protect medical data on the eHC, access is only possible through authentication with an HPC or a Security Module Card (SMC). SMCs are used to create secure connections between components (e.g. between a connector and the HTI) or between smart cards. SMCs can be used by MSP's to gain access without a personal HPC. It is stated in (gematik, 2008k, p. 249) that the primary system must generate a reliable access log for all users with SMC access. This can only be done using software encryption on the log file, as the primary system lacks hardware key material. Software encryption tends to be less secure as key material may be reverse engineered by an attacker gaining control over the primary system. SMC access is part of the HTI use cases, so the logging should be done on a HTI component (e.g. connector) instead of the primary system.

4.5 Deficiencies of the Current Security Concept for Peripheral Parts

Environment of the Medical Service Provider. In (gematik, 2008i, p. 27) it is assumed that the primary system will provide sufficient security for stored medical data until the data is transferred into the HTI. It is further assumed that the MSP's LAN is hardened against unauthorized access through relevant measures based around security guidelines provided by the German Federal Office for Information Security. The MSP's LAN and the computer containing the primary system consist of standard electronic parts and no temper-evident casing, so security measures outside of the peripheral HTI tend to be significantly lower than within. Security and penetration tests on LANs and primary systems would help to detect vulnerabilities and enhance the local security (Sunyaev et al., 2009b).

In (gematik, 2008i, p. 29) it is assumed that the MSP personnel will regularly (at least annually) check the HTI components and the trusted viewer (trusted viewer is a trustworthy component that enables the verification of signatures and the signed content.) software for manipulation. A manipulated component staying undiscovered for up to a year is not satisfactory given the amount of data that will pass through the HTI per day, so this time span should be shortened.

Insider Attacks from MSP Personnel. The introduction to the threat analysis in (gematik, 2008i, p. 77) states that the MSP and their personnel are regarded as trustworthy and are not considered as possible attackers. However, insider attacks performed by healthcare personnel are entirely possible, and lead to several million Euro damage per year for health insurance companies (Wright et al., 2008). Larger companies have special agents to hunt down persons responsible for fraud within the healthcare sector. Therefore, the threat of attacks on the HTI by MSP personnel should be acknowledged.

MSP's LAN Security. The introduction to the threat analysis also assumes that the potential for an attack on the peripheral HTI is higher than the potential for an attack on the MSP's LAN (cp. (gematik, 2008i, p. 27)). As already mentioned, the non-HTI components generally have a lower security level than HTI components, so an attacker would most likely concentrate on breaking into the primary system rather than into the connector, for example.

Missing Best-practices Recommendations for Software Keys. (gematik, 2008i, p. 109) explains the security functions of the eHealth-card terminal. In this context, best-practices recommendations for software keys are to be noted. However, no specific recommendations and no specific source of information are given to the reader. This information should be supplemented for the cause of a complete specification of the HTI.

Missing Emergency Plans for HTI Components and Cryptographic Methods. In (gematik, 2008i, p. 130), gematik states that there is no complete defense against the emergence of new attacks on components and cryptographic algorithms used within the HTI. The remaining risk can be reduced by defining emergency measures to be taken in the event of a successful attack. Currently, no such emergency measures exist. In order for the specification to be complete, gematik must define emergency measures, including the exchange of key material, the exchange of HTI components not patchable with a software update, emergency software updates for a swift reaction to new threats

[3] http://www.ietf.org/rfc/rfc2119.txt

or program errors, and the exchange of smart cards (eHC, HPC, SMC) whenever cryptographic or technical issues emerge that pose a security risk.

5 DISCUSSION AND CONCLUSIONS

In the course of this work, using the current specification documents of German healthcare telematics, 19 deficiencies within the security concept of the system currently being developed were identified and described. These include weaknesses, inconsistent, conflicting or incomplete development and specification documents and violations of various security demands. The identified security issues are the first results and experiences from the introduction of the healthcare telematics in Germany. More than any other results, the privacy and security concepts analyzed and the vulnerabilities discovered within the German healthcare telematics plans might be helpful for other healthcare telematics projects and could potentially prevent possible vulnerabilities in future healthcare information systems.

One problematic factor, not discussed during this paper, is human interaction with the HTI. Social engineering is a serious problem for modern secure systems, as an attack carried out by influencing authorized users to give out confidential passwords or authentication credentials can't be prevented with technical measures. Only if the users, insured people and MSP personnel alike, are properly instructed and remain vigilant, will medical data within the HTI system remain secure.

As far as technical security is concerned, further security analyses, attack simulations and penetration tests performed by both IS security companies and scientific institutions would help to detect issues and weaknesses within the healthcare information systems currently being tested, and also improve the practical security of the HTI as demanded by many MSPs not only in Germany. For future work, the discover weaknesses will be verified in practice. By the time of the conference we hope to provide results from a practical security analysis.

REFERENCES

BDSG (2003) Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970).

gematik (2006a) Einführung der Gesundheitskarte - Gesamtarchitektur. Version 0.2.0. Gematik.

gematik (2006b) Einführung der Gesundheitskarte - Konnektorspezifikation - Teil 1 Allgemeine Funktionen und Schnittstellen des Konnektors.

gematik (2006c) Einführung der Gesundheitskarte - Spezifikation Infrastrukturkomponenten: Zeitdienst. Version 1.0.0.

gematik (2007a) Spezifikation Netzwerksicherheit. Version 1.1.0. Gematik.

gematik (2007b) Übergreifendes Sicherheitskonzept der Telematikinfrastruktur. Version 1.9.0.

gematik (2008a) Einführung der Gesundheitskarte - Spezifikation Infrastrukturkomponenten: Zeitdienst. Version 1.3.0.

gematik (2008b) Facharchitektur Verordnungsdatenmanagement (VODM). Version 1.5.1.

gematik (2008c) Fachkonzept Verordnungsdatenmanagement (VODM). Version 2.6.0.

gematik (2008d) Gesamtarchitektur. Version 1.4.0.

gematik (2008e) Konnektorspezifikation. Version 2.8.0.

gematik (2008f) Mehrwertanwendung Fachkonzept - Mehrwertkommunikation Leistungserbringer 0.9.0.

gematik (2008g) Prüfvorschriften Primärsystem Rel. 2.2.3. Version 2.0.0.

gematik (2008h) Spezifikation eHealth-Kartenterminal. Version 2.6.1.

gematik (2008i) Spezifisches Sicherheitskonzept der dezentralen Komponenten - Einboxkonnektor-Szenario. Version 0.9.0 Kandidat.

gematik (2008j) Übergreifendes Datenschutzkonzept der Gesundheitstelematik. Version 0.9.0. Gematik.

gematik (2008k) Übergreifendes Sicherheitskonzept der Gesundheitstelematik. Version 2.3.0.

Guah, M. & Fink, K. (2008) Cost of Controlling Modern Healthcare With Information Systems. *Proceedings of the Fourteenth American Conference on Information Systems.* Madison, Omnipress.

Huber, M., Sunyaev, A. & Krcmar, H. (2008) Security Analysis of the Health Care Telematics Infrastructure in Germany. *10th International Conference on Enterprise Information Systems.* Barcelona, Spain, Vol. ISAS-2, pp. 144-153.

IBM, Dr. Biltzinger, P., Dr. Bunz, H. & Dr. Neeb, J. (2004) Erarbeitung einer Strategie zur Einführung der Gesundheitskarte - Sicherheitsanforderungen.

Lorence, D. P. & Churchill, R. (2005) Incremental adoption of information security in health-care organizations: implications for document management. *Information Technology in Biomedicine, IEEE Transactions on,* 9**,** 169-173.

Mandl, K. D. & Kohane, I. S. (2008) Tectonic Shifts in the Health Information Economy. *The New England Journal of Medicine,* 358**,** 1732-1737.

Marschollek, M. & Demirbilek, E. (2006) Providing longitudinal health care information with the new

German Health Card—a pilot system to track patient pathways. *Computer Methods and Programs in Biomedicine,* 81**,** 266-271.

Schabetsberger, T., Ammenwerth, E., Andreatta, S., Gratl, G., Haux, R., Lechleitner, G., Schindelwig, K., Stark, C., Vogl, R. & Wilhelmy, I. (2006) From a paper-based transmission of discharge summaries to electronic communication in health care regions. *International Journal of Medical Informatics,* 75**,** 209-215.

Schneier, B. (1996) *Applied Cryptography,* New York, Chichester, Brisbane, Toronto, Singapore,, John Wiley & Sons, Inc.

Schweiger, A., Sunyaev, A., Leimeister, J. M. & Krcmar, H. (2007) Information Systems and Healthcare XX: Toward Seamless Healthcare with Software Agents. *Communications of the Association for Information Systems,* 19**,** 692-709.

SGB (2007) *Sozialgesetzbuch*, DTV-Beck.

Sharman, R., Rao, H. R., Upadhyaya, S. J., Khot, P., Manocha, S. & Ganguly, S. (2004) Functionality Defense by Heterogeneity: A new paradigm for Securing Systems. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04).*

SigG (2001) Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) - Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 3 Abs. 9 des Gesetzes vom 7. Juli 2005 (BGBl. I S. 1970; änderung durch Art. 4 G v. 26.2.2007 I 179 zukúunftig in Kraft).

SigV (2001) Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) - Signaturverordnung vom 16. November 2001 (BGBl. i S. 3074), geändert durch Artikel 2 des Gesetzes vom 4. Januar 2005 (BGBl. I S. 2).

StGB (2005) *Strafgesetzbuch*, DTV Deutscher Taschenbuch Verlag.

Sunyaev, A., Göttlinger, S., Mauro, C., Leimeister, J. M. & Krcmar, H. (2009a) Analysis of the Applications of the Electronic Health Card in Germany. *Proceedings of Wirtschaftsinformatik.* Vienna, Austria, 25-27 February, to appear.

Sunyaev, A., Kaletsch, A., Mauro, C. & Krcmar, H. (2009b) Security Analysis of the German electronic Health Card's Peripheral Parts. *ICEIS 2009 - Proceedings of the 11th International Conference on Enterprise Information Systems, Volume ISAS***,** 19-26.

Wright, D., Friedewald, M., Schreurs, W., Verlinden, M., Gutwirth, S., Punie, Y., Maghiros, I., Vildjiounaite, E. & Alahuhta, P. (2008) The Illusion of Security. *Communications of the ACM,* 51**,** 56-63.