ATTACK SCENARIOS FOR POSSIBLE MISUSE OF PERIPHERAL PARTS IN THE GERMAN HEALTH INFORMATION INFRASTRUCTURE

Ali Sunyaev, Alexander Kaletsch, Sebastian Dünnebeil and Helmut Krcmar
Chair for Information Systems, Technische Universität München, Boltzmannstraße 3, Garching, Germany

Keywords: Security Analysis, Electronic Health Card, Health Information Infrastructure.

Abstract: This paper focuses on functional issues within the peripheral parts of the German health information infrastructure, which compromise security and patient's information safety or might violate law. Our findings demonstrate that a misuse of existing functionality is possible. With examples and detailed use cases we show that the health infrastructure can be used for more than just ordinary electronic health care services. In order to investigate this evidence from the laboratory, we tested all attack scenarios in a typical German physician's practice. Furthermore, security measures are provided to overcome the identified threats and questions regarding these issues are discussed.

1 INTRODUCTION

Currently, German authorities are building up a nationwide health information infrastructure, called health telematics infrastructure (TI), which should have been finished in 2006 (SGB V, 2007, § 291a). Although there are still delays which evolved as a consequence of various problems with the introduction, the new electronic health card (eHC) will be launched within the next few years (Sunyaev et al. 2009a, p.19).

Bales (2003, p. 5) expects an improvement in efficiency of the health care system and better protection of patient's rights after its introduction. The eHC will contain administrative data as well as information about a patient such as illnesses and treatments. As this data is to be highly protected by the physician-patient confidentiality and strictly protected by law (Berg, 2004, pp.412-413), its handling requires adequate care. Especially complete data protection has to be ensured because issues concerning privacy, safety, security and availability directly apply to the patients (Sunyaev et al. 2009b). The eHC, a smart card, is able to guarantee this. Moreover, it can encrypt and sign documents containing valuable information in order to share them with trusted third persons and systems.

Based on ISO 27001 Standard for Information Security Management Systems and BSI Security Guidelines (BSI, 2004) as well as by extensive laboratory experiments and an extensive review of gematik's specifications, we have provided a security analysis (Sunyaev et al. 2009b), which showed that open security issues, e.g. missing authentication or unencrypted transmissions, can result in making all peripheral parts of the telematics infrastructure vulnerable.

In this paper, we present the continuation of that security analysis. Possibilities for misuse of functions provided by the peripheral parts of the German health information infrastructure are explained. The concerns are enriched with detailed attack scenarios. Solutions and upcoming questions to these issues are provided and discussed.

2 THE GERMAN HEALTH TELEMATICS INFRASTRUCTURE

Gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH), which was created according to the law (SGB V, 2007, § 291b), is conducting the introduction of the electronic health card in Germany. Gematik has created all specifications used in the health care telematics infrastructure (these can be found at the organization's website - http://www.gematik.de) and

Sunyaev A., Kaletsch A., Dünnebeil S. and Krcmar H. (2010).
ATTACK SCENARIOS FOR POSSIBLE MISUSE OF PERIPHERAL PARTS IN THE GERMAN HEALTH INFORMATION INFRASTRUCTURE.
In *Proceedings of the 12th International Conference on Enterprise Information Systems - Databases and Information Systems Integration*, pages 229-235
DOI: 10.5220/0002900102290235

is responsible for their compliance.

Figure 1 presents the German health care telematics infrastructure, which is divided into central and peripheral parts. While the central part consists of central databases stored in data centres, the peripheral parts are used at the different providers of service – e.g. in physicians' practices, hospitals or pharmacies (Schweiger et al. 2007, p. 694-695; gematik, 2008d, p.8).

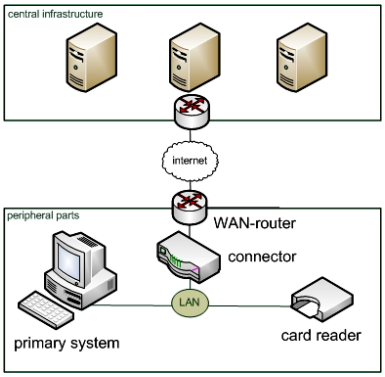

Figure 1: German health care infrastructure.

In this paper, we focus on the usage of the peripheral parts. The connector, which is the core of the peripheral systems, manages all local connections. It interacts with primary systems and card readers. A primary system is a piece of software, which offers the eHC's functionality to the renderers of service. A primary system can only access a card reader through the connector, which establishes a secure connection with the card reader using the Secure Interoperable ChipCard Terminal (SICCT) protocol.

Any connections onto the central part are managed by the connector. When connecting peripheral parts and central part, the connector establishes a protected VPN connection to the VPN concentrator on the central side (Schweiger et al. 2007, p. 694-695; gematik, 2008d, p.8).

There will be two different kinds of cards. The electronic Health Card (eHC), which will be obligatory for all insurants, and the Health Professional Card (HPC), which is for health care staff only. Both are smartcards, i.e. each card type has its own microprocessor with its own instruction set (Caumanns et al., p.343). This clearly distinguishes it from the present health insurance card, which is only a memory card. Therefore, not only administrative data about the insurant can be stored. The insurant can decide whether information for medical emergencies, pharmaceutical documentations, prescriptions and medical reports will be stored. Furthermore, one can decide whether information is to be directly stored on the eHC or in central databases (Neuhaus et. al., p.1).

Moreover, the card can perform different functions on its own, e.g. secure signing and encryption or decryption of documents. As the card contains a so-called qualified signature (SGB V, 2007, § 291b), an electronic document signed by that signature, is treated equally to hand signed document before the law. Therefore, certificates used by the electronic health card must be protected.

Figure 2 displays different classes of attack. In ICEIS 2009, we already presented *disruption of card usage* and *spy on personal data*. Disruption is possible by compromising actions like *permanent card ejection*, *automatic filling or deletion of prescriptions* or even *blocking a card*. Personal data can be stolen by retrieving *administrative data, prescriptions* or *medical emergency information* (Sunyaev et al. 2009b).

In this paper we focus on abuse of functions of the peripheral parts. Section 3 shows how to *pair a card reader without explicit administrator permission* with the connector**.** After that, a scenario is provided, which illustrates the *misuse of the connector's and cards' encryption and signing functions*. Finally, the *creation of inconsistent prescriptions* is explained in detail in section 5.

3 ATTACHING UNSECURE CARD READERS TO THE CONNECTOR

As mentioned earlier, a patient's eHC, which is attached to a card reader, is only reachable through the connector over the local area network in a physician's practice. No other type of connection between card reader and connector is designated. Furthermore, gematik (2008a, p. 26) enforces that the card reader must only communicate with inserted cards and with the connector. Therefore, it is not possible that primary systems, which are the interfaces to the physicians, connect directly to the card reader and its attached cards. Thus, in order to obtain patient information from an eHC, a data flow from the primary system to the card reader has to be established via the connector.

Gematik (2008a, p. 66) enforces that the card reader initially has to be securely paired with the connector by the administrator responsible. It has to be ensured that the card reader is in the administrator's personal area. During the initial pairing process the card reader has to be guarded, so it cannot be accessed by any third party.

Admission is usually granted at the administra-

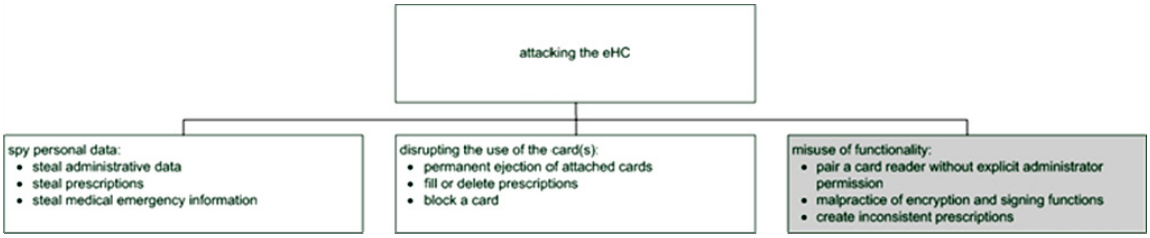

Figure 2: Attack tree.

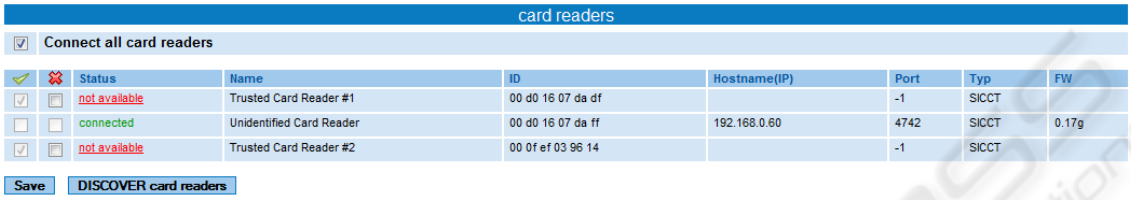

Figure 3: Administrator web interface for granting admission to card readers.

tion website of the connector. The administrator can select trusted card readers and put them to a whitelist. Moreover, detailed information about every card reader is provided to support his decision.

The connector used is part of the Futro S400 series by Siemens, version V1.07R4.8; hpscV1.07R4_build_2533_R13907. Figure 3 shows a table with all card readers attached. Each row contains one card reader as well as its status, e.g. *connected*, *not connected* or *not available*. Furthermore, name of the card reader, MAC address, IP, port, protocol and firmware-version are listed. The administrator can approve a card reader by checking a box in front of its representation in the table.

The webpage of the connector offers the possibility to set the connector into a mode, which allows the automatic connection of every card reader existing in the LAN. When "Connect all card readers" is checked at the top-left of figure 3, every card reader connected to the local area network will be accepted automatically. Therefore, there is no more need to activate card readers manually at the bottom table.

This enables two different ways of proceeding. In one case, the administrator hand selects every card reader manually and approves each. In the other case, all card readers are automatically accepted. Therefore, the connector will gain access to every card reader attached, which makes the security check itself completely needless.

Insecure card readers in the peripheral parts of the German health care information system acting as regular ones constitute a threat. Those can be utilized via the connector in order to access patient's data for reading or writing.

There are different possible scenarios which could lead to serious security violations. First, an additional card reader could be plugged into the system without any notification. On the one hand, it could just confuse patients and staff; on the other hand, a foreign HPC plugged into the card reader would enable an attacker to gain full access to all cards plugged to any card reader in the physician's practice. Thus, it could be possible for the attacker to read and write at any eHC wanted.

Secondly, a card reader could be exchanged with a modified duplicate, which grips or modifies data in a mischievous way. As no further approval exists, the exchange most likely would not be detected.

Finally, after updating a currently approved card reader to a new firmware version, there would be no need to reinitiate the pairing manually, which could be dangerous if the new firmware is modified in a mischievous way.

This loss of control over the card readers attached to the LAN is dangerous as shown in the scenarios above. Furthermore, it violates gematik's regulations (gematik 2008a, p. 66). Therefore, the automatic paring functionality has to be removed from the connector.

4 MISUSE OF CRYPTING AND SIGNING

In this section, we show how to abuse the functions of connector and card to crypt and sign documents. We show that it is possible to build up a secure network with eHCs or HPCs. By doing so we state

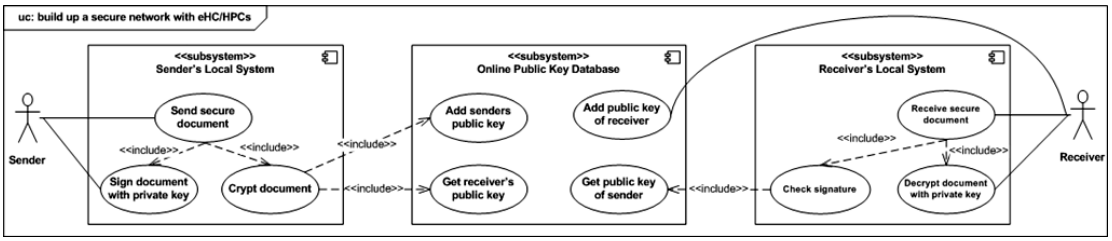

Figure 4: Secure message transportation scenario.

that the system can be used against its purpose and therefore, against German law (SGB V, 2007, § 291a).

Figure 4 shows such a scenario in a simplified way. It contains a sender which transmits a confidential message. By encrypting the message with the receiver's public key, one can assure that it can only be read by the receiver. The sender identifies himself by signing the document with his private key. Later on, the receiver can make sure to have received the confidential message from the right person by checking the message against the sender's public key.

All functionality, e.g. encrypting, decrypting, signing and the signature check, are provided by the sender's and receiver's local systems. Those consist of standard modules of the peripheral parts of the German health care telematics system.

Sender and receiver share an online system which stores their public encryption keys and can encrypt messages using them. It ensures the secure key exchange between sender and receiver and can prevent man-in-the-middle attacks in this phase.

Table 1: Used functions of the connector.

Function	PIN needed	Supported card types	required parameters	gematik's specification
Sign Document	Signature PIN (PIN.QES)	All	• Card Handle • Signature Policy • Document	gematik 2008d, 283f; chapter 5.5.6.3.1
Verify Document	None	All	• Document with signature • Signature policy	gematik 2008d, 287f; chapter 5.5.6.3.2
Encrypt Document	None	All	• Document • Public key certificate or Card Handle	gematik 2008d, 296f; chapter 5.5.7.2.1
Decrypt Document	Decrypt Pin (PIN.CH)	HPC, (eHC)	• Encrypted document • Card Handle	gematik 2008d, 299f; chapter 5.5.7.2.2

The sequence of actions in this scenario is the following: At first the sender signs the document. The signed document and its signature part then get encrypted. After completing transportation the receiver first decrypts the message and is then able to check the document against its signature.

All functions used by the sender and receiver are part of the peripheral systems of the German health infrastructure. Table 1 lists all of them and their required parameters, supported card types, PIN requirements and their description in gematik's specification. The following sections (4.1-4.4) explain these functions in detail.

4.1 Signing a Document

For the signing of a user document the function *SignDocument* of the connector is used (see table 1). It uses the document to sign, a corresponding signature policy and a card handle, which refers to the smart card that will sign the document, as parameters. When signing the document, the card will require the user to enter the corresponding signature PIN at the keypad of the card reader.

Since the signing functionality of the connector is limited to special xml structures by signature policies (gematik 2008d, 506) a workaround becomes necessary. A closer look into the signature policies reveals such a workaround. In the emergency signature policy a version attribute is set as an unlimited string. Therefore, we can store user data, which is base64 encoded for integrity reasons, in there. Figure 5 shows how this works.

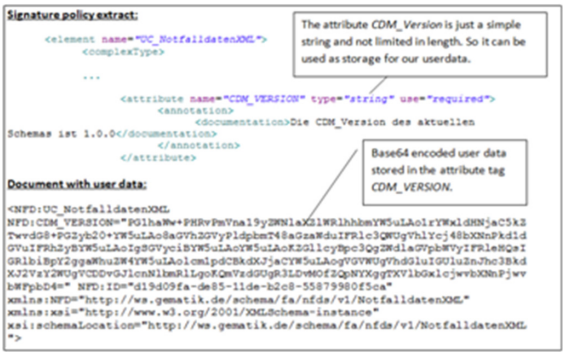

Figure 5: Hiding user data in an XML attribute.

4.2 Encrypting a Document

In order to encrypt a document the function *EncryptDocument* of the connector, is used. All it

takes to encrypt the document is the public key certificate. This functionality could be implemented at the online key storage presented above, too.

In our scenario we decided to encrypt the already signed document. Hence, the document is to base64 encode with its signature in order to hide both from the encrypting module. It has to be mentioned that the function expects XML documents, so a surrounding root XML structure is created, too. After encryption, the document can be safely sent to the recipient.

4.3 Decrypting a Document

In order to decrypt a document, the function *DecryptDocument* is called. It requires the encrypted document and a card handle as parameters. If the private key found on the card corresponds to the public key, which encrypted the document, the document will get successfully decrypted. The card holder will have to enter his PIN at the card reader in order to start decrypting. After removing the base64 encoding, the receiver will be able to see the plain text, the sender transmitted to him.

It has to be stated that gematik (2008d, p. 299f) does not allow decrypting with an eHC via the *DecryptDocument* function. But in the context of special applications it will be possible in future (2008d, p. 299f).

4.4 Checking the Signature of a Document

Finally, the signature of the document has to be validated. Therefore, the function *VerifyDocument* of the connector is called. As table 1 shows, *VerifyDocument* requires the document with its signature and the signature policy. If the integrity of the signed document is verified, a confirmation message will be shown.

4.5 Transmitting a Secure Document

Figure 6 summarizes four steps to secure a document. The onion diagram shows in detail how the original data document is modified and embedded. It gives a good impression, of how the data is modified while sending and receiving.

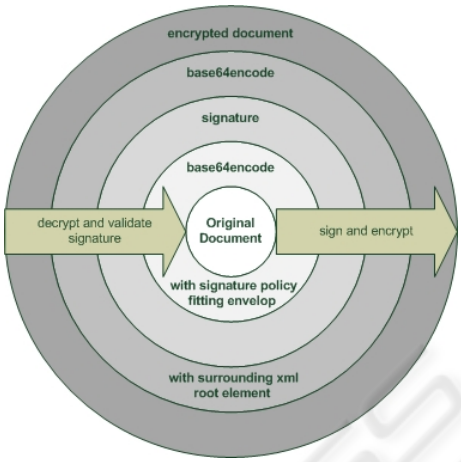

Figure 6: The data onion.

How Robust is such a Secure Transmitting System?
Secure storage of private keys is most important for the security of the system. They are stored securely on the eHC and HPC. The backup, which exists at the manufacturer for card-recreation and private keys stored in the central parts of the telematics system, can compromise security.

As those storages are well protected against unauthorized access, we can still assume the transmitting system to be secure.

How can One Obtain eHCs or HPCs?
Every German insurant will receive one eHC. Some of them could try to misuse their cards for functions like the ones mentioned above. But it is conceivable that healthcare staff use their HPCs accordingly.

Moreover, criminals might try to simply steal cards. E.g., it has to be assumed that the physician is not the only one knowing the *PIN.QES* for a HPC. Often nurses often do so, too. Therefore, thieves might be able to obtain the HPC and its *PIN.QES* with some social engineering.

Does Black-listing Private Keys from Stolen Cards impRove the Situation?
It will work quite well, if access to the blacklist is not prevented. But gematik (2008c, p. 78) explicitly stipulates that access to private keys must be continued, if there is no reachable blacklist. Therefore, it will be quite easy to overcome this feature, if one uses the offline mode of the connector.

What would be a Possible Solution to Prevent this Scenario?
One possible solution would be the enforcement of a present global authentication server, which provides

blacklists for decrypting. But this would add a single point of failure to the system.

Would not a More Restricted Signing and Encryption Policy Help to Fix this Problem?
We are well aware that such security breaches, like the XML specification gap, can be easily closed when uncovered. But there would still be other possible strategies to hide user data conforming to the signature policy. E.g., an algorithm could split user data into fitting parts which are then distributed all over the conform document. Although the message space would be quite limited, it would mostly be enough to transmit confidential text messages.

Can you give a Concrete Example of Usage?
We were able to encrypt and sign emails, which were then sent to an Internet mail server. Later on, the emails could be received and successfully be decrypted and verified.

Therefore, two web interfaces were created. One is used for encrypting and signing emails. The user can grab a public key of the card or choose any user-defined certificate. A sender's and receiver's email-address can be chosen as well as the title of the message and the document. The other contains the interface to the receiver. After selecting the designated email account and email message, the corresponding card for decrypting is chosen. The user will be shown the encrypted message as well as the plain text message. Moreover, the interface offers the functionality to verify an email which was signed before.

5 CREATING INCONSISTENT PRESCRIPTIONS

In ICEIS 2009, we presented the possibility to delete or fill prescriptions without any effort of a pharmacist by calling the function *DeleteVO* or *DispenceVO*. In this section we take a closer look at the prescription itself, which we are going to write to an eHC by using *WriteVO*.

A prescription consists of information about the insurant and his insurance coverage as well as the dispensing institution and the drug prescription itself. Both pieces of information about the insurant and the dispensing institution contain the names and addresses of the corresponding persons and are equipped with one unique id each.

According to gematik (2008b, p. 19-27) and verified by our tests, the XML document is checked against a strict scheme before being signed and then written on the eHC. Unfortunately, the plausibility of the content written is not checked sufficiently. Except for the insurant's id, which is checked for consistency with the id of the eHC, no other value is validated. Therefore, we are able to write a XML document containing fake data onto an eHC.

On the front side of the card there are patient-related information, a picture of the insurant and the microchip. Furthermore, some recognition features are placed there, e.g. braille, the name and logo of the providing insurance company. On the back, there is the European health insurance card (EHIC) (Drees, 2007, p. 1).

When analyzing figure 7 and comparing the image of the HPC with the data presented on the right sight of the figure, one will notice two out of three of the following inconsistencies:

1) Wrong patient name
2) Wrong insurance company id and name
3) (Wrong dispensing institution)

Especially when the prescription data is displayed on the pharmacist's computer, it is quite likely that these differences will not be recognized.

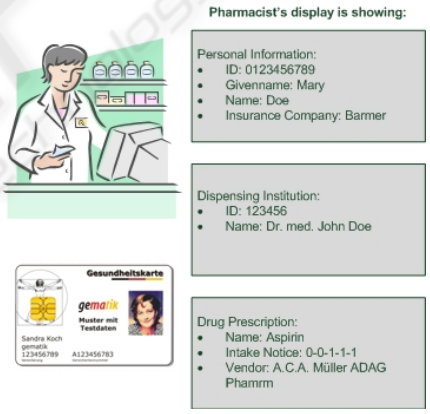

Figure 7: Pharmacist reading inconsistent prescription.

Why is this Dangerous?
When a pharmacist serves a patient, there probably would not be enough time to compare every field of the eHC to the document fields of the prescription. Therefore, it is quite likely that inconsistencies will not be recognized. Especially when considering, that the card will be plugged into the card reader while the prescription document is shown, there even will not be a possibility of comparison.

Can the Real Values be Restored?
They can, but only at some administrative costs. As the dispensing person's certificate is attached to the prescription and is delivered to the pharmacist it is actually no problem to restore the correct physician.

The patient's real name and address can be restored by tracking his insurant's id. With the id and the timestamp from the signature of the prescription it should be possible to receive the right insurance company's information. Therefore, backtracking and reconstruction is always possible, however it will take some time and hence be costly.

How can these Costs be Saved?
Actually, there is no need to copy patient's personal information, insurance data or dispensing person's data into the prescription as it is already stored at the eHC. Therefore, the avoidance of creating duplicate information would not only save storage space, but also reduce risks.

How to Deal with Prescriptions for Third Persons and Consumables for a Doctor's Surgery?
In these special cases, a flag should be set which informs the pharmacist. Only then it should be allowed to add extra information about the receiving third persons.

6 CONCLUSIONS

In this paper, we presented different scenarios, which show that the functions of the German electronic health card's peripheral parts can be abused. Three possible attacks were presented:

- Automatic pairing of card readers and connector without administrative guidance
- Misuse of encryption and signing
- Creating inconsistent prescriptions

Possible solutions were given and further questions discussed. The automatic pairing function would need to be deactivated at the connector, which will hardly cost anything. Therefore, this should be done immediately. Preventing misuse of functionality and creation of inconsistent prescription might prove to be more costly. The scenarios mentioned in this paper should be included in the overall security specification in order to make people aware of the possible risks.

As the German electronic health card is currently on hold and redesigned in parts, security related parts will have to be reconsidered and newly checked once the moratorium ends. As presented in this paper, there is not only a need for proving information security, but the absence of possibilities to abuse functions must be checked, too. Furthermore, a security analysis concerning the central parts as well as the use and play of value-added-applications has to be performed.

REFERENCES

Bales, S., 2003. *Die Einführung der Telematik im Gesundheitswesen als Herausforderung für die Weiterentwicklung der Patientenrechte in Deutschland*. [Talk] Bonn: gematik. Available at: http://www.dimdi.de/dynamic/de/ehealth/karte/downloadcenter/veroeffentlichungen/vortraege/bagh-bonn-bal-031107.pdf [Accessed 9 September 2008].

Berg, W., 2004. Telemedizin und Datenschutz. *Medizinrecht*, 22 (8), pp. 411-414.

BSI, Bundesamt für Sicherheit in der Informationstechnik, 2004. Studie zu ISO-Normungsaktivitten ISO/BPM - *Anforderungen an Information Security Management Systeme*.

Caumanns, J. et al., 2006. Die eGK-Lösungsarchitektur Architektur zur Unterstützung der Anwendungen der elektronischen Gesundheitskarte. *Informatik-Spektrum*, 29 (5), pp. 341-348.

Drees, D., 2007: The Introduction of Health Telematics in Germany. In: European Commission Directorate General Information Society, *Information Security Solutions Europe/SECURE 2007 Conference*. Poland, Warsaw 25 27 September 2007. Vieweg: Wiesbaden.

gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008a. *Spezifikation eHealth-Kartenterminal*. Version 2.8.0.

gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008b. *Facharchitektur Verordnungsdatenmanagement (VODM)*. Version 1.5.1.

gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008c. *Übergreifendes Sicherheitskonzept der Gesundheitstelematik*. Version 2.3.0., Anhang B.

gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 2008d. *Konnektorspezifikation*. Version 3.0.0.

Neuhaus, J., Deiters, W. & Wiedeler, M., 2006. Mehrwertdienste im Umfeld der elektronischen Gesundheitskarte. *Informatik-Spektrum*, 22 (5), pp.332-340

SGB V, 2007. *Sozialgesetzbuch*. Fünftes Buch. DTV-Beck.

Schweiger, A., Sunyaev, A., Leimeister, J.M., Krcmar, H. 2007. Information Systems and Healthcare XX: Toward Seamless Healthcare with Software Agents. In: Communications of the Association for Information Systems (CAIS), Vol. 19 (2007) Nr. Article 33, pp. 692-709.

Sunyaev, A. et al., 2009a. Analysis of the Applications of the Electronic Health Card in Germany. In: WI 2009, Proceedings of Wirtschaftsinformatik 2009, Austria, Vienna 25-27 February 2009.

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, pp. 19-26.