A Note on the Security in the Card Management System of the German E-Health Card

Marcel Winandy

Horst Görtz Institute for IT Security
Ruhr-University Bochum, Germany
marcel.winandy@trust.rub.de

Summary. The German compulsory health insurance system will introduce an electronic health card (eHC) in the near future. The eHC is supposed to enable new applications like securely storing electronic health records of patients in a central data center infrastructure so that health professionals can access these data via a common network. In this context, the card management system (CMS) is of special interest since it is used to personalize, issue, and maintain the cards. In this paper, we analyze the functional requirements specification of the CMS in Germany and identify several conflicting and ambiguous requirements. As the most important result, the specification defines technical measures that are insufficient to protect the data and data sovereignty of the patient. We discuss the resulting consequences, which might be helpful to improve the system design before its final deployment.

Key words: Electronic health card, card management system, security

1 Introduction

In the German compulsory health insurance system each insured person currently has a health insurance card that stores administrative data for the usage of health care services (name, date of birth, details of insurance, insurance number). This simple memory card will be replaced by an advanced smartcard, the Electronic Health Card *eHC* [4, 6]. The eHC has a programmable microprocessor chip that provides not only the facility to store small amount of data directly on the chip but also provides cryptographic functions to encrypt and sign data that can be securely stored outside the chip. This is assumed to enable a number of new applications, e.g., storing medical emergency data on the card, issuing and filling of electronic prescriptions, and protecting the access to Electronic Health Records (EHRs) that are stored in a central healthcare telematics infrastructure.

Since personal health data are very sensitive information about the patient, data privacy is a very important aspect in this context. In many countries, and in particular in Germany, privacy laws require that patients must have the *sovereignty* on their data. This means that only the patients can define who may access their personal data, and that the data has to be protected from unauthorized access to prevent misuse and to maintain privacy. Disclosure of personal health data may have severe (social) consequences. For instance, individual persons or groups of people could be discriminated based on their health data, e.g., when applying for health insurance, bank loan, or a job.

To protect the privacy of health data, the German eHC system defines basic security requirements [5]: The authentication, authorization, and audit mechanisms have to be chosen in a way that the data sovereignty of the insured party can be taken for granted. This means that by using the eHC the insured person can solely control the access to the health data. Technically, this is realized by a hybrid encryption mechanism: The health data are encrypted with a random symmetric key before they are uploaded to the EHR server, and this key is encrypted with the public key of the patient's eHC [1, 4]. This ensures that only the patient's eHC can decrypt the data again. Moreover, the patient has to authenticate to the eHC by entering a PIN in the card reader terminal at, e.g., the doctor's practice, when the patient wants to authorize access to health data.

Gematik, a company organization founded by leading institutions of the German health care system, is responsible for defining, maintaining, and developing the specifications of the telematics infrastructure and the electronic health card. Researchers have analyzed various security aspects of the telematics infrastructure, including network security and access control policies [7], peripheral parts such as end-user systems [9], and criticized open security issues in general [10]. However, one aspect has not been analyzed in depth and publicly discussed until now: the security of the Card Management System (CMS) of the eHC. Besides data privacy, data availability is another important basic requirement: If the eHC as root of trust gets lost or damaged, the medical data needs to be re-encrypted for a new eHC [5]. In this context, the CMS is of special interest since it is used to personalize and issue the cards as well as to provide and maintain the card data. This includes issuing of replacement cards, which may require to perform the re-encryption process of health data that is associated with the old card.

In this paper, we analyze the functional requirement specification [3, 2] of the card management system of the German electronic health card and examine whether the specified security requirements are sufficient to guarantee the data sovereignty of the patient. As a major result, we can identify conflicting requirements (Section 3), which finally lead to a violation of the required data sovereignty (Section 4). Additionally, there are other ambiguous requirements (Section 5), which make a correct implementation difficult, if not impossible.

2 About the Requirements Specification of the CMS

We start with an overview of the functional requirement specifications of the CMS [3]. The CMS is responsible for the life-cycle management of the health cards. This includes personalization and issuing of cards, application management (i.e., which applications are stored or activated on the card), locking and unlocking of cards (e.g., in case of theft), and in particular management of cryptographic keys. The objective of the specification [3] is to provide a consistent definition of the functional requirements for the CMS. The health care insurance providers (the card issuers) should have a certain degree of freedom in the implementation since they will have to provide and maintain the CMS [3, p. 5]. However, technical realizations have to fulfill all requirements, especially security and privacy requirements [3, p. 13].

The card management of the eHC comprises the following use cases:

- **Card Life Cycle**: producing, issuing, locking, and unlocking the eHC.
- **Card Validity**: lock/unlock eHC, lock/unlock applications. If a card (or a single application) is locked, it cannot be used in the telematics infrastructure.
- **Card Application Management**: management of potentially and actually available applications on the eHC (add/delete, activate/deactivate).
- **Data Preservation**: in case of issuing a replacement card, determine applications of the old eHC and maintain capabilities for accessing existing application data on the new card.
- **Key Management**: management of cryptographic keys.

Figure 1 shows the interaction of the stakeholders with the CMS: The **Card Manufacturer** is a service provider that produces the card, including personalization and initialization of the chip. The card is then given to the **Card Issuer**, a health insurance provider, who registers the card in the CMS and issues it to the **Insured Party**, who is a natural person (the patient). When the patient visits a **Health Care Provider**, e.g., a medical doctor, he/she shows the card for administrative purposes, and also to encrypt data that the doctor wants to send to an **Application Operator**, e.g. an EHR server. In case an eHC has to be replaced by a new one, the Card Issuer invokes an update process at the Application Operator to re-encrypt the data for the new card.

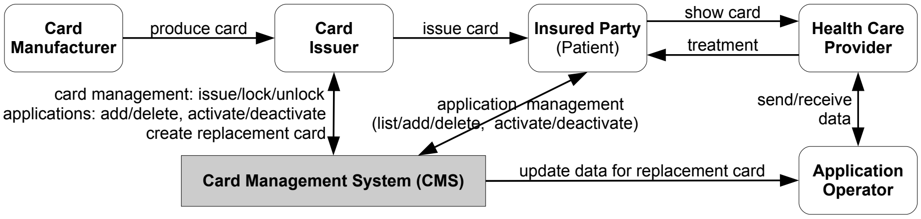

Fig. 1. Interaction diagram of the Card Management System.

The requirements specification gives detailed descriptions of all use cases, including a separate section specifying the security requirements for each use case. At the end of the document all security requirements are listed again. This shows a strong emphasis on security aspects during the development process.

However, we can find in the specification several conflicting and ambiguous requirements which have an important impact on the basic security requirement of data sovereignty of the insured party. In the following sections, we analyze the problems in more detail and point out their consequences.

3 Conflicting Requirements

3.1 Two valid cards at the same time?

Within the domain of the card life cycle management, we can already find a conflict in the overview of the use cases. For the use case "issue eHC", it says: *If a renewal card has to be issued, the old eHC should still be active over a specific period. Only after expiry of a given time period, the old card SHOULD be unusable. [3, p. 16]* In contrast, it says on the same page for the use case "unlocking eHC": *Before unlocking the eHC, it MUST be assured that there are not two valid cards afield. [3, p. 17]*

The difference between SHOULD and MUST in the specification is that MUST is an absolute requirement, whereas SHOULD allows deviation in case of valid reasons [3, pp. 9-10]. According to those requirements above it is not possible to clearly decide whether it is allowed or not to have two valid cards of an insured person at the same time. The definition of SHOULD in the first use case implies possible implementations that can have two coexistent valid cards.

3.2 Unauthorized access to unencrypted data?

While the conflict described above may be a result of a mistake in writing and could possibly be fixed, there is another conflict, pertaining card application management, data preservation, and key management, which cannot be resolved without major changes in the whole requirement specification.

On the one hand, there are the following postulations: *At any time, the card management is not allowed to obtain information about application contents in a readable style for which it is not authorized. This holds especially for medical data. [3, p. 24] The card issuer MUST NOT get possession of unencrypted medical application data. [3, p. 27]* The medical (application) data mean the personal health data of an insured party. For secrecy and privacy reasons, those data will be encrypted using cryptographic keys of the insured person's eHC. Of course, an unencrypted representation of those data should only be visible to the insured person and authorized care providers, e.g., the family doctor.

On the other hand, the keys to decrypt the data should not get lost if an eHC gets lost or damaged. Therefore, there is the requirement of data preservation: *When a replacement or renewal card is created, it MUST be assured that application data stored at a server (e.g., the electronic health record) can be accessed using the new eHC. [3, p.28]*

However, instead of leaving the technical realization of those requirements to the design specification of an implementation, the requirement specification requires a particular realization by specifying a central key management: *Management of cryptographic keys is essential within the card management. The following secret keys MUST be presently managed in the context of the card management: [a list of keys follows] [3, p. 29]* This means that, on the one hand, the card issuers should not be able to decrypt medical data, but on the other hand, they should know and manage the secret keys for reasons of re-encrypting data due to a card replacement. This is definitely a contradiction.

4 Violation of Data Sovereignty of the Insured Party

In this section, we want to go further into the question why Gematik specifies a central key management in the CMS as a requirement. If we look at the overview of use case "locking eHC", we can find the following requirement: *As far as locking the eHC causes the insured party to be unable to use the data, the card issuer MUST make sure that further access to the data is possible by using a replacement card. [3, p. 17]* Moreover, further access to health data is not only required after locking an eHC, but also after switching to another health insurance company, which results in issuing a new eHC [3, p. 27]. In this case, the CMS must be able to somehow transfer the applications and their data contents from the old eHC to the new one. Data that is stored on a server and encrypted with a key protected by the old eHC have to be re-encrypted for the new eHC, which of course does not possess the old key. If the old eHC is lost or damaged, the keys stored in the eHC will be lost as well. Thus, we need an appropriate method of reconstructing lost keys. We examine in the following how the specification addresses this issue.

4.1 Specifications about handling of secret keys

The functional requirements specification does not leave the definition of the method of re-encryption to a design specification. Instead, it requires to store copies of all secret keys in a central place, namely, the card management system of the card issuers, cf. [3, pp. 28-29]. However, the specification does not describe the details of the key management, but leaves this to the respective card issuers: *The key management use cases do not have an interface to the telematics infrastructure currently, and, therefore, their realization can be left to the card issuers on their own. [3, p. 14]*

The specification of this requirement results in the possibility that the card issuer is in possession of the secret key used to encrypt the medical data of the patient. But we can prove this finding further. For instance, there are requirements stating that the card issuer knows the secret key already at the time of its generation [3, p. 30]: *Principally, the key management MAY be used to generate the keys needed by the eHC. Depending on where the keys of an eHC are generated, the key management MUST support the export or import of keys into the key management. The reason for this is that externally generated keys must be known by the key management if it is necessary to use them in operation.*

The specification mentions the deletion of keys as another use case. Keys that were generated by the key management should be deleted irrecoverably *after they have been successfully used for the production of eHCs* [3, p. 30]. However, it is doubtful how the insured party can reliably verify that the card issuer is not any more in possession of the keys afterwards. Furthermore, the deletion of the keys can only be effective if holding the keys in the CMS *is not necessary any more* [3, p. 30]. Due to the requirement of re-encrypting data during the process of issuing a replacement card, this case will never happen though.

As a consequence, the key management requirements of the CMS do violate the data sovereignty of the insured party since the encryption keys are not under control of the insured party alone. Implementations of the CMS cannot choose a different technical method for re-encryption because the method is already fixed in the requirements specification.

4.2 The process of creating a replacement card

The detailed description of the "create eHC" use case names the card issuer as the involved actor. One of the triggering events for this use case occurs when the *insured person reports the loss, malfunction, or theft of his/her eHC* [3, p. 32]. The precondition for this use case is the following: *All data required for the production of the card are available. [3, p. 32]* According to the definition of Card Manufacturer, the participation of this actor is obvious in the "create eHC" use case. However, this actor is neither mentioned in the overview [3, pp. 14-15] nor in the detailed use case description [3, p. 32]. We can find the following notice in the annotations of the use case instead: *The card issuer may assign the creation of the card to one ore more service providers. [3, p. 33]* Since we must assume the card issuer already to be in possession of the secret keys (see Section 4.1), the statement above expands the number of potential "key holders" since the card issuer could give the keys to those service providers. Although there is a special security requirement according to this, it is too vague: *The confidentiality of data MUST be ensured for a part of the personalization data (e.g., keys). [3, p. 33]* It is not specified towards whom the data shall be confidential and, more importantly, which data exactly are meant. The formulation of "e.g." in a requirement specification allows too much tolerance for an implementation.

The detailed description of the data preservation use case [3, pp. 52-53] requires again explicitly that the insured person can access encrypted data stored on a server if he or she uses a replacement card of the eHC. Interestingly, the input data required for this use case are merely the identification number ("ICCSN") of the insured party's eHC. From this we can infer again that the CMS of the card issuer must already know the keys used to (re-)encrypt the medical data because they would need more input data otherwise.

Again, this violates the required data sovereignty of the insured party. If the card issuer possesses the secret key, it is not possible to technically enforce the basic security requirement, which the same use case mentions though [3, p. 53]: *Plaintext of medical data MUST NOT be available to the card issuer.*

Furthermore, the use case description contains the statement that the card issuer *transmits the ICCSN of the insured party and other data to the application operator*, whereas the application operator *processes the application data* [3, p. 52]. In case the application operator is responsible for managing the server storing the encrypted health data of the insured party, we can deduce that the application operator is another actor who has access to the secret keys since he has to re-encrypt the data. Note that, while the above security requirement holds for the card issuer, there is no such requirement for the application operator – neither in the use case [3, pp. 52-53], nor in the rest of the specification.

As a consequence, we can identify three parties – the card issuer, the card manufacturer, and the application operators – who can potentially be in possession of the secret keys and, hence, access the health data of patients although there are not authorized to do so. In order to enable data preservation in case of replacement cards, the data sovereignty of the insured party is dismissed.

5 More Ambiguous Requirements

Besides conflicting requirements leading to a violation of data sovereignty of the patient, the specification of the CMS contains other ambiguous requirements that may be a problem for realizing a correct implementation.

(i) The use cases "locking eHC" [3, pp. 35-36] and "locking eHC for online usage" [3, pp. 37-38] mention the insured person reporting the lost or theft of the eHC as triggering event. However, locking the eHC requires that the eHC is available via telematics infrastructure [3, p. 35]. How could this be possible when the card is lost or stolen?

(ii) The use cases "locking/unlocking eHC" require an identification of the insured person and exclusion of external card issuers in the process [3, pp. 35-37]. However, the use cases "locking/unlocking eHC for online usage" do not have these requirements. Hence, is it possible that someone who has stolen the eHC could unlock the card after it was locked for online usage?

(iii) Modifications of the eHC are possible, e.g., to download, update, activate, or delete applications, but require a mutual authentication between the eHC and the card issuer [3, p. 44-51]. This implies a demand for integrity of the stored data. However, only the use case for downloading applications has such a requirement [3, pp. 46, 55]. Thus, it is not clear whether the integrity of data has to be preserved when an application is updated.

(iv) Furthermore, the eHC is an individual-related identification card [3, p. 58]. But a representative of the insured person can also be the card holder [3, pp. 12]. Unfortunately, there is no further description of the role of the representative and the technical implications, respectively. For instance, this leaves the question whether the representative should also know the PIN, which is needed to authorize access to medical data. But if the representative knew the PIN, this would challenge the role of the eHC of being an identification card. Moreover, the data sovereignty of the insured person would be doubtful in this case, too.

6 Conclusion

Gematik developed specifications [3, 2] for the card management system of the German electronic health card. We have analyzed the specifications and identified several conflicting and ambiguous requirements, which make an implementation of all requirements impossible. As a most important result, the specification requires technical measures that are insufficient to protect the data and data sovereignty of the patient. Unauthorized parties may be able to read sensitive data. Misuse of personal health data caused by malfunction, intent, or bribery must be considered as potential threats. A realization of the CMS can only rely on organizational and legal measures to resolve the conflicting requirements.

In order to avoid those conflicts and to allow technical measures to enforce the data sovereignty, the functional requirement specification of the CMS would greatly benefit from explicitly defining potential threats and assumptions about the security environment. The requirement of centrally storing copies of the secret keys should be omitted and other technical solutions, e.g., secret sharing [8], should be allowed to technically enforce the data sovereignty of the insured party.

References

1. Gematik. The Specification of the German Electronic Health Card eHC. `http://www.gematik.de`, February 2006. The English version of the specification is outdated. More recent versions are available in German only.
2. Gematik. Einführung der Gesundheitskarte - Facharchitektur Kartenmanagement eGK, Version 1.6.0. `http://www.gematik.de/cms/media/dokumente/release_2_3_4/release_2_3_4_kartenmanagement/gematik_CMS_Facharchitektur_Kartenmanagement_eGK_V1_6_0.pdf`, July 2008.
3. Gematik. Einführung der Gesundheitskarte - Fachkonzept Kartenmanagement eGK, Version 1.3.0. `http://www.gematik.de/cms/media/dokumente/release_2_3_4/release_2_3_4_kartenmanagement/gematik_CMS_Fachkonzept_Kartenmanagement_eGK_V1_3_0.pdf`, June 2008.
4. Gematik. Einführung der Gesundheitskarte - Gesamtarchitektur, Version 1.7.0. `http://www.gematik.de/cms/media/dokumente/release_4_0_0/GA_ZentraleDienste.zip`, August 2009.
5. German Federal Ministry of Health. Entscheidungsvorlage - Festlegung der Authentisierungs-, Autorisierungs- und Auditmechanismen der Telematikinfrastruktur für die Fachanwendungen, Version 0.9.0, March 2006.
6. German Federal Ministry of Health. The Electronic Health Card. `http://www.bmg.bund.de`, October 2006. Order No. BMG-G-G430EN.
7. M. Huber, A. Sunyaev, and H. Krcmar. Security analysis of the health care telematics infrastructure in germany. In *ICEIS 2008 - Proceedings of the 10th International Conference on Enterprise Information Systems, Volume ISAS-2, Barcelona, Spain, June 12-16, 2008*, pages 144–153, 2008.
8. B. Schneier. *Applied Cryptography.* John Wiley & Sons, 1996.
9. A. Sunyaev, A. Kaletsch, C. Mauro, and H. Krcmar. Security analysis of the german electronic health card's peripheral parts. In *ICEIS 2009 - Proceedings of the 11th International Conference on Enterprise Information Systems, Volume ISAS, Milan, Italy, May 6-10, 2009*, pages 19–26, 2009.
10. A. Sunyaev, J. M. Leimeister, and H. Krcmar. Open security issues in german healthcare telematics. In *HEALTHINF 2010 - Proceedings of the 3rd International Conference on Health Informatics*, pages 187–194. INSTICC, 2010.