Identity Management in Telemedicine

Christoph Meinel, Matthias Quasthoff
Hasso-Plattner-Institut, University of Potsdam, D-14440 Potsdam, Germany

***Abstract*—Electronic health insurance cards are introduced in regions all over Europe. Many of them will either carry sensitive patient data or grant access to online health records. Thus, effective data protection measures have to be taken with strong forms of authentication and encryption incorporated. The solution for Germany is described in this paper. The architecture features service orientation and allows for the constitution of a nationwide public key infrastructure.**

***Index Terms*—Attribute Certificate, Authorization, Digital Identity Card, Health Insurance Card, Health Professional Card, Identity Management, Public Key Infrastructure**

I. Introduction

MEDICAL professionals around the world heavily rely on modern information technology. Since years technologies like image processing play a major role in modern medicine. With the rise of broadband internet, radiographic images are transmitted around the country and are analyzed remotely. ECG data are collected at home and are transmitted via wireless connections. The amount of electronic communication and data on patients' issues—medical and administrative—grows and causes more cost and effort to manage. On the other hand, legislation and ethics demand that storage of and access privileges to these data are well organized.

In the last years, many of countries in the EU set up programmes for electronic health insurance cards, which are also designed to support processes around healthcare. Since this introduction consolidates the telemedicine processes also from a legal point of view, governments decide to put an integrated identity management in place. Experience in identity management in service oriented architectures (SOA) delivers some of the answers needed to fulfil the pressing demand for such an identity management solution in telemedicine.

However, the new system needs incorporate the many existing IT solutions around, be it in hospitals, medical practices, pharmacies or in the offices of the many health insurance funds. As workers in health care do lots of different jobs and bear lots of different responsibilities, it is important to design an access control scheme that matches legal and practical needs. According to the German government, in Germany there are 2.200 hospitals, 65.000 dentists, 123.000 licensed practical doctors, 21.000 pharmacies and about 290 statutory health insurance funds. Many of these institutions have again many employees themselves. Furthermore German legislation requires that each of the around 80 million people insured can specify highly individual permissions for any subset of their medical record. Designing an architecture of that size and complexity requires deep thought and a good understanding of what management of identity-related data means in healthcare, in legislation and in IT. [15]

From the traditional information technologies point of view, identity management was about managing access control. Access for certain operations (create, read, update, delete) on certain resources (files, records, etc.) could be granted or denied. Users were basically names plus some attributes, which could easily differ depending on where the user logged in. Often in IT environments it was not necessary that a user was given an all-embracing digital identity.

As the number of online applications grew with a different login mask each, first single sign-on (SSO) solutions appeared. Most of them were directory-based and permissions—mostly group membership or role descriptions—were stored in that directory. [14] With an ever-growing user base, administration efforts for these directories did not come handy. And with the arrival of service-oriented architectures, applications performing authentication with different directories started talking to one another. New access control paradigms arose, mimicking national identity management: In the real world, centralized authorities are not permanently asked to verify names or identity cards. So, in the SOA world instead of always performing identity verification against one central repository, tickets were introduced. Valid only for short period of time, but trusted from the different trust domains or independent from trust, they proved practical and are now part of modern SOA like the one forming the modernised German healthcare system.

Identity management in national healthcare is much more than just granting or denying access—protection of sensitive personal data is not just an ethical but a legal must. This paper describes the proposed solutions for the modernisation of the German healthcare system, which will rely on public key encryption, digital signatures and certificates, digital identity cards and a ticket toolkit system. The solution presented is to meet the requirements for an electronic healthcare system, assuring the integrity and authenticity of medical records and prescriptions and the confidentiality and anonymity of personal health records and other sensitive information.

II. Introduction To Digital Identity Management

As said before, identity management in healthcare is more than just managing access control. It also includes managing

personal health records and other medical data of patients according to local legislation. Even more difficult, access control has to be put in place for millions of people at once in a way that allows for continuation of work during loss of connection to the internet in medical institutions. [3]

A. Authentication Factors

As in the real world, in a computer environment there are several ways of proving your claimed identity. On many computer systems, users can log on giving their username and a password. Their username is their claimed identity, whereby the password is to serve as the proof of identity. Besides the fact that passwords can be weak, i.e. easy to guess for an adversary, the computer system handling logon needs access to the password validation service. Thus, a person cannot be identified when isolated from the password database. Instead of typing a password or PIN—something you know—computer systems can be equipped with biometrical sensors, scanning who you are. Still, the scanning system would have to have access to a central repository of biometrical data.

The third choice of proving identity is to do so by showing something you have. In the real world, this is the common choice of access control. Doors open when you have a key that matches the lock. The police will let you drive a car if you have a driving license. The security guard will let you pass if you have a ticket.

Digital security tokens model this behaviour for computer environments. Those are little pieces of hardware the user carries with him/her. To log in, the computer system obviously has to offer a possibility to use the security token. E.g. some type of token display ever-changing pseudo-random numbers that can be verified by a service but cannot be reproduced. If a user enters the correct pseudo-random number and the system knows how to verify the number, the use proved to be in possession of the security token.

If a computer system requires a combination of different types of authentication factors, the process is called **Two Factor Authentication** (**TFA**). TFA is considered a strong form of authentication, as synchronous theft of those different authentication factors happens less likely and is more likely to be detected.

B. Digital Signatures and Digital Certificates

Public key encryption offers another elegant way of identification. Everyone taking part in public key encryption has a pair of public and private keys (e, d), often called encryption and decryption key. It is possible to protect the decryption key with a pass phrase or PIN. Given a message m, everyone can encrypt m using e, but only the owner of the matching decryption key d can decrypt m. On the other hand a user can prove authenticity of a message by decrypting a hash value of the message. The decrypted hash value is called a **digital signature**. Everyone reencrypting the signature can now verify that the hash value matches the encrypted signature. [1]

Digital signatures are heavily used in today's computer infrastructure. Similar to the act of signing a message, if person A wants to authenticate with system B, A can use its private key to prove ownership of it. If B knows the public key of A and identity information related to the key, A has successfully authenticated. One drawback of this approach is that B has to know A's public key which seems like B either has again to be connected to a central repository or needs to have exchanged the public key of A before.

But instead, it is enough for B to know the public key of a **trusted third party** (**TTP**). When proving ownership of the private key, A would present a document containing all relevant information (public key, name, organizational role etc.). If this document is signed by a TTP that B trusts, B would use the public key stored in the document to verify A's authenticity. These signed documents are called **digital certificates**.

A widespread format for digital certificates is the one according to the ITU-T X.509 standard. Those X.509 certificates consist of three fields:

- tbsCertificate
- signatureAlgorithm
- signatureValue

The tbsCertificate field contains all the user data of the certificate, among them the identifier for the subject of the certificate, i.e. the owner of the public key being signed, the public key itself and the issuer of the certificate, i.e. the entity having signed the certificate, and a validity period of the certificate. [1]

The X.509 standard furthermore defines how to verify the validity of certificates. Instead of, as in the example above, requiring all certificates being signed by the same trusted third party, **public key infrastructures** (**PKI**) are established. A PKI specifies a root **certificate authority** (**CA**), which all participants need to trust. This root CA then certifies other CAs or possibly individuals and so on. A participant is now being validated using his/her certificate by establishing a trusted certification path to the common root CA. Important to note is the fact, that PKI have to be designed. Because the identifiers of the participants—individuals as well as certification authorities—reference to organizations, countries and other real-world names, migrations, merges and other restructuring of PKI is difficult or even impossible. However, if a PKI is to be designed in a proper manner, there is no need for such restructuring.

C. Legal Aspects of Digital Signatures

Not all digital signatures are legally equivalent to a hand-written signature. In the last six years, many countries have adopted regulations to specify under which circumstances digital signatures may be used instead of hand-written ones. Possible constraints as found in e.g. Germany are:

- the certificate issuer has to meet rigid physical security restrictions
- the certificate subject needs to be identified successfully, e.g. by showing a valid identity card
- the user data in the certificate needs to be sufficient to uniquely identify the certificate subject

For applications to process legally relevant data, it is nec-

essary to register with a so-called accredited certification authority. Legally binding signatures are then called "qualified signatures".

D. Digital Identity Cards

Digital Identity Cards are microprocessor cards designed for cryptographic applications. Instead of merely storing identity information or a digital certificate, they contain a microprocessor and the private key for the certificate in a tamper-proof manner. [1] By design, it is ensured that the private key cannot leave the card, at least not without causing observable physical damage to the smart card.

That way, smart cards are perfectly suitable to perform two factor authentication: The user inserts the card (the token) into the terminal. By entering the private key's pass phrase—most often a PIN, the authentication factor you have to know—into to terminal's keypad, the pass phrase is sent to the smart card. The smart card will use this pass phrase to perform the actual authentication with the terminal. No one can authenticate successfully without stealing the card and revealing the pass phrase or PIN.

In addition to the authentication function, the smart card might store additional data. That data could either be arbitrary user information (e.g. medical data) or administrative data helpful for authorization processes.

E. Attribute Certificates

In password- or biometry-based environments, all authentication data needs to be stored and managed in central locations. This causes huge administrative efforts and most likely, the system administrators will actually be able to manipulate permission control. In certificate-based environments, it is possible to include authorization information (e.g. role names) in the according certificates. However, authorization to sensitive data should have a shorter lifetime than is desired for the certificate of the respective individual.

One solution is to issue separate certificates besides the "identity certificate". Those separate, **attribute certificates** [1], [14] reference to the respective certificate and specify administrative information (e.g. validity period, attribute authority's identifier) and the attributes themselves. Those attributes could be

- service authentication information
- access identity
- charging identity
- group or role
- authorization information

Authorization information will often be valid for a minimal period of time only, maybe just a couple of minutes. The use of attribute certificates reduces the costs of digital identity card redistribution for authorization reasons. Instead, attributes will not be accepted after their validity period and new attributes can be created easily.

III. Access Control

A. Role Based Access Control

Access Control in password- or biometry-based environments is often based on access control lists (ACL), which either mention identifiers of individuals or groups, which are a sets of individuals. Instead of groups, in service oriented architectures (SOA) individuals would be assigned roles, and authorization decisions would happen based on these role information. [9] A role name could be a job description, a role in a process or a profession. In a certificate-based environment, these group or role information would be put in attribute certificates, thus would not necessarily be stored centrally. [15]

B. Authorization Based Access Control

Sometimes identity- or role-based access control is not sufficient. In fragmented environments, environments where responsibility is delegated on a regular basis or permission control happens decentralized, an authorization based model is more suitable for access control. [9] In those environments access is not granted upon presentation of a document of identity or because of group or role membership. Instead, the relevant users are issued **authorizations** (often called **tickets**) to the respective resources. An authorization needs to be unforgeable, i.e. signed by some trusted party or most unlikely to be reconstructed.

When requesting a resource (a file, log in etc.) presenting an authorization, access will be decided solely based on the authorization, but not on the identity of the presenter. Typically, authorizations are issued with a very limited validity period only, but this is not a necessity. By issuing fine-grained authorizations for different resources, there is no "super user" having full or nearly full access to large sections of the system.

One major advantage of authorization based access control can be found across trust domains. In identity- or role-based access control environments, the domain of a service provider needs to trust the identity or role information of the requestor and then base the access decision upon these information. That way, the provider's domain would have to maintain information about the individuals or roles of all possible requestors' domains. In the authorization based environment, each domain needs to maintain information about the authorizations for domains of possible providers. According to [9], authentication based access control significantly decreases the hassle of cross-domain authorization.

IV. Digital Identity Cards in German Healthcare

With the modernization of the German Healthcare System, three types of digital identity cards will be issued: Health Insurance Cards (**elektronische Gesundheitskarte**) for patients, Health Professional Cards (**elektronischer Heilberufsausweis**) for medical practitioners and pharmacists and Secure Module Cards for medical practices and pharmacies to be used by their employees.

A. Electronic Health Insurance Cards In Europe

According to the EC eHealth Action Plan (COM (2004) 356) an Electronic European Health Insurance Card (eEHIC) is to be introduced in 2008. [10] On the other hand, many countries across the EU already chose to introduce electronic health insurance cards or electronic identity cards in piloting regions or nationwide. In Austria a social security card was introduced, allowing for several eGovernment processes. One application using medical data is the ePrescription. In Andalusia, electronic health cards are being tested since 2004. The cards also provide access to a patient's electronic health record. This Spanish project is considered one of the most advanced in Europe. A similar piloting project takes place in Lombardy, Italy. Besides those projects, many other projects are running: In Belgium, already in 1998 an electronic social security (SIS) card was introduced. The insurance data required no further authentication to read. In contrast, using a health professional card medical data could be stored to and read from the SIS card. Until 2009, an electronic id card for general eGovernment applications is planned, which should include the functionality of the SIS card. Similar projects can be found in Estonia, Finland, France, Slovenia and other countries. [10]

B. Health Insurance Card

The ***elektronische Gesundheitskarte*** (***eGK***) is the new health insurance card carrying a photograph of the insurant. Technically, it will be a smart card designed for so-called mandatory and voluntary applications [10]. Every card will carry insurant's master data, i.e. his/her

- full name, birthday, gender, address
- health insurance fund's name
- health insurance number
- start time (and end time, if applicable) of insurance protection
- health insurance and extra payment status

By law, extra payment status data are subject to special protection. [6] Thus, only authorized personnel will have access to these data. Whenever the patient uses the eGK in an online environment, the data will be updated with the actual data from the health insurance fund. In the case of an update, the patient will be presented both the expired and updated master data, as it is required by law. Although the patient is granted full read access to his/her master data, of course he/she is not allowed to alter, hide or delete any of this data.

The second mandatory application is that the eGK should carry electronic prescriptions, digitally signed by the relevant practitioner. Because of the limited storage capacity of the eGK, a link to a central prescription repository might be stored on the card instead of the prescription itself. As the practitioner will be able to produce qualified digital signatures, the pharmacist will be able to verify the signature of the prescription. Also, prescriptions cannot be reused after being invalidated by the pharmacist. This allows for more fraud prevention and detection than current paper-based prescriptions do.

Additionally, each patient can choose for the voluntary applications of the eGK. For emergencies, the eGK can carry unencrypted medical emergency data. To improve or simplify medical treatment, other medical data like drug interaction and contraindication checks can be carried out with the help of the eGK. Furthermore, the eGK grants access to the patient's personal electronic health record. Some of these applications, like disease management programme (DMP) data, require special protection by law, whereby others, like the emergency data set, need to be accessible ad-hoc.

As legislation grants patients the ownership on their medical data, health professionals always need authorization of the patient for read or write access to these data. To manage these access rights and their granularity, kiosks will be put in public places (**eKiosk**). [3] From there, or from their home internet connection, patients will use their eGK to view access protocols, their master data, and to manage permissions and the visibility of records. The option to integrate the eGK in a nationwide PKI is still considered for the future; but at the time of this writing, it is not planned for patients to receive a qualified digital certificate with their eGK. However, it is required by law, that the eGK has to be technically able to carry a qualified digital certificate in the future.

The eGK will be a smart card according to ISO/IEC 7816-2 and of normal ID-1 size. [5] The eGK's file system will contain [4]

- card-verifiable certificates
- the Healthcare Application (HCA) to hold and process medical data
- the ESIGN application for public key encryption, decryption and authentication protocols
- the Cryptographic Information Application (CIA) related to ESIGN
- the Qualified Electronic Signature (QES) application (being disabled at the moment)

The private key stored on the eGK PrK.eGK.AUT which is used for card-to-card authentication is a RSA key. For local authentication between eGK and HBA and between eGK and SMC, no session keys are negotiated. For remote interactions between eGK and SMC, the eGK needs to support authentication protocols with session keys. The public key PuK.eGK.AUT corresponding to PrK.eGK.AUT is located in the card-verifiable certificate CVC.eGK.AUT on the eGK.

In addition, the eGK stores two PIN; the PIN.CH consisting of 6–8 digits is used to unlock the voluntary applications of the eGK. PIN.home, consisting of 6–8 digits either, is used for the so-called "passive" applications the patient can use from their home internet connection. Both PINs can be mistyped three times and have to be reset by an 8-digit unlocking code afterwards. However, the eGK only allows for access to the voluntary applications after entering the PIN.CH. Any functions concerning the data protection rights of the patient can only be accessed from the eKiosks but not from a healthcare institution's systems. The authorization from the HBA is required by the security constraints of the eGK's file system. [4]

The estimated amount of data to be stored on the eGK is about 58 KiB. The HCA will consume 42 KiB thereof; the ESIGN application another 9 KiB. The rest will be distributed among the QES application, the master file and the card-verifiable certificates. [8]

C. Health Professional Card

Medical practitioners, dentists and pharmacists will receive an **elektronischer Heilberufsausweis** (**HBA**). This will be a contact based smart card similar to the eGK, carrying a photo outside and healthcare information inside. The HBA will be a normal-size ID-1 card according to ISO/IEC 7816-2. [12] The HBA will serve for authentication to the electronic healthcare system and to patients' eGK. For identification of the health professional, the HBA will carry all information needed. All HBA will carry a digital certificate which allows for creation of qualified digital signatures, as required by German legislation for legal effect. Those qualified signatures will be used e.g. for signing medical prescriptions.

The kind of health professional (practitioner, pharmacists, etc.) is stored on the HBA via attribute certificates. Those attribute certificates are used when permission to certain functions of the health care system or the eGK is checked. For these purposes, the Heilberufsausweis contains

- card-verifiable certificates and global keys for authentication—for verification of the authenticity of an eGK and for proving access rights to the eGK
- the Health Professional Application (HPA) being used to access health professional data
- the Qualified Electronic Signature (QES) application for signature computations according to German legislation
- the ESIGN application for secure client/server authentication and document decryption
- the Cryptographic Information Application (CIA) related to ESIGN

In order to achieve strong authentication for the HBA, the card is protected by a PIN. This PIN has a length of 5–8 digits; it can be changed but needs to be unlocked by an 8-digit resetting code when entered wrongly three times. The private key PrK.HPC.AUT stored on the HBA for card-to-card authentications—that is to patients' eGK and to SMC—is a 1024 bit RSA key. The according card verifiable certificate used for card-to-card authentication is CVC.HPC.AUT. The specification defines to secure environments at the card's master file level:

- SE#1 as a general level for all purposes except those of SE#2
- SE#2 is reserved for the usage of the HBA's private key PrK.HPC.AUT for trusted channel establishment between the HBA and SMC

For usage of PrK.HPC.AUT in SE#1, i.e. authentication against an eGK, the health professional's PIN needs to presented to the HPC. For usage of the key in SE#2, no PIN is required.

For interaction between a HBA and an eGK, the eGK has to prove its authenticity. It does so with the help of its own card-verifiable certificate. In the opposite direction, the health professional has to prove his access rights. He/she does so with the HBA's card-verifiable certificate and the PIN. Authentication happens in SE#1 as no secure messaging is involved in the further communication with the eGK. The logic allowing that authentication against an eGK can happen only after presentation of the health professional's PIN will be stored on the HBA.

For the Qualified Electronic Signature application, a separate private key PrK.HP.QES, again protected by a PIN, is found on the card. It has not yet been decided if with each presentation of the PIN the number of signatures to be created will be limited or unlimited. Processes in hospitals require physicians to issue many prescriptions in short periods of time. Having to enter the PIN for each single signature might either lower the acceptance of new electronic processes or lead to distribution of the health professional's PIN among unauthorized personnel. For the electronic signature itself, hashing happens outside the HBA. Depending on the hash algorithm used, the last text block might be hashed on the HBA. The hash value is then padded and the signature is computed from the padded hash value. [12]

D. Secure Module Card

Business processes in medical practices, pharmacies and hospitals require many more people to have access to healthcare information than just the health professionals like practitioners or pharmacists themselves. Receptionists, nurses and even administrative personnel might require access to certain patient or healthcare data. It is neither desired to issue each of these employees an own HBA-similar card with qualified digital signatures for scalability reasons, nor to have them use their respective health professional's HBA for security and legal reasons.

As a solution, each health care institution is issued a **Secure Module Card** (**SMC**). These SMC allow access to the patient's eGK and to the healthcare system. But, it does not convey a qualified digital certificate for a single individual, and only identifies the respective health care institution, not any single employee. The SMC will also accord to ISO/IEC 7816-2, but will not be a full ID-1 sized card. Usually, it will be a small ID-000 plug-in card to be put in electronic equipment like a card terminal or one of the connector to the German healthcare infrastructure. [13]

Two different types of SMC are specified. SMC-A allow for card-verifiable authentication and trusted channels, but do not convey PKI keys nor X.509 certificates. These SMC will be used to authenticate against eGK after the respective SMC-A being authorized by a HBA. For this authorization the SMC also has to authenticate against HBA. A trusted channel can be established between the HBA and the SMC to access services of the HBA remotely. SMC-A will typically be used in different workplaces around the healthcare institution and are referred to as "workplace cards".

In contrast, SMC-B have additional capabilities. They are configured with PKI keys and X.509 certificates, which are issued for the institution. With the help of this keys and cer-

tificates, encrypted documents addressed to the healthcare institution can be decrypted. These keys are also used for client/server authentication within the healthcare infrastructure. Typically, one SMC-B per institution can be found e.g. in the connector to the healthcare infrastructure. SMC-B are referred to as "institution cards".

On both types of SMC, the private key used for card-to-card authentication PrK.SMC.AUT can only be used if external authentication of the respective HBA happened before. As in the HBA, PrK.SMC.AUT is a 1024 bit RSA key, and as in the HBA there are two security environments SE#1 and SE#2 for the same purposes on the SMC. In order to authenticate a SMC for interaction with a eGK, the public key of the HBA PuK.HPC.AUT will be imported and the HBA's card verifiable certificate CVC.HPC.AUT is verified. After successful verification, the security status for usage of PrK.SMC.AUT is set according for interaction with an eGK. If e.g. an internet pharmacy is to process an electronic prescription, the interaction between the SMC and the eGK need to happen over a trusted channel. For those purposes, SE#2 will be used.

In addition, the SMC-B contains three more private keys PrK.HCI.DSIG, PrK.HCI.ENC, and PrK.HCI.AUT, each of them a 1792 bit RSA key and protected by a PIN instead of requiring a health professional's authorization. Those keys serve digital signatures, document encryption and authentication. [13]

V. Identity Management In German Healthcare

The digital identity cards in German healthcare—eGK, HBA, and SMC—are all used to authenticate for access to the digital healthcare system, while the eGK additionally serves as a storage for patient data. This authentication, as well as management of decentralized patient data, make up identity management in health care. Access and potential risks are subject to rigid legal restrictions. It has to be impossible for a system administrator to reconstruct the link between a patient's medical record and his/her identity. Even more, given some record of some anonymous patient, it should be impossible to obtain all records concerning the same patient, as this would maybe allow for reconstruction of the patient's identity.

Another difficulty arises as the patient is required to allow health professionals access to his/her medical records. For process reasons, this permission management has to be decoupled from the access of the health professional, as the patient might be under anaesthetic at access time. [2] In this scenario, the patient should have granted access to his/her patient record at the hospital's reception. In order to meet all this difficulties, a ticket system has been suggested [2] that solves the issues mentioned above and is compatible with a modern service-oriented approach.

A. X.509 certificates on the Health Insurance Cards

The eGK will contain more than just one X.509 certificate. The main certificate CVC.eGK.AUT serves for authentication of the eGK and is used as a proof of presentation of the card. The commonName of this certificate contains the full name and some insurance data of the patient. While the same applies for the one ENCV certificate of the two additional certificates, the second additional AUTN certificate does not contain a human readable name of the patient, but a re-computable pseudonym based on some of the patients data and a hashing algorithm. [7]

The subjectDN for the non-pseudonym certificates consists of the following fields:

commonName

The commonName consists of a concatenation of the title, the given name and the surname of the patient. As the commonName attribute must not contain more than 64 letters, additional parts of the given name and surname may be abbreviated. On the front of the eGK, the commonName attribute will be printed split in two lines.

title

This field will carry any academic title of the patient.

surname

This field will carry the surname of the patient. As the surname attribute must not contain more than 64 letters, for few people with surnames consisting of multiple parts it might be necessary to abbreviate parts starting with the last part.

givenName

This field will carry the given name of the patient. As the givenName attribute must not contain more than 64 letters, for few people with given names consisting of multiple parts it might be necessary to abbreviate parts starting with the last part.

organizationalUnitName

Along with the modernization of the German healthcare system, a new type of health insurance number is being introduced. The new health insurance number will consist of three digit blocks with ten, nine and ten digits plus one error checking number. The first block is to uniquely identify the insurant. This block would stay the same if the insurant decided to change his/her health insurance fund and thus would be issued a new eGK with still the same first digit block. The first block is used as organizationalUnitName and does not need any abbreviation.

organizationalUnitName

The second 9-digit block in the health insurance number uniquely identifies the health insurance fund. This identifier is used for the organizationName. Again, this field is not subject to abbreviation.

organizationName

The name of the issuer of the eGK, i.e. the health insurance fund of the card holder, will be used as the organizationName of the certificate.

countryName

The countryName on the eGK certificates is always the two-letter ISO 3166 code of the Federal Republic of Germany, "DE".

For the pseudonym certificate, each health insurance fund has to maintain a periodically changing random number RND. This number RND is to be kept secret by the respective health insurance fund, should be changed periodically and be archived for more then ten years. For an insurant, his/her surname, his/her identifying first part of his/her health insurance number and RND are concatenated and hashed with SHA256. The first 20 hexadecimal digits of the hash value will be taken as the commonName of the pseudonym certificate.

By this construction, the health insurance fund can verify whether a given pseudonym certificate belongs to a given insurant. But given the pseudonym certificate only, no-one can reconstruct the identity of the insurant. The subjectDN of the pseudonym certificate will consist of:

commonName

The previously described hash value will be used as commonName.

organizationalUnitName

As for the other certificates, the identifying block of the health insurance fund in the health insurance number of the insurant is used as organizationalUnitName for the pseudonym certificate

organizationName

The name of the issuer of the eGK is used as the organizationName of the certificate.

countryName

The countryName of the pseudonym certificate will be "DE", too. [7]

B. A Service-Oriented Healthcare Architecture

As a basic requirement, the storage and management of health care data should be as flexible as possible as it is intended to transfer this task to external providers on the one hand. On the other hand, the flexible design of the voluntary applications on the eGK require a flexible architecture themselves.

The architecture suggested by FhG [3] builds upon the proven scalability of service-oriented architectures, but chooses to drop some of their features like UDDI as they are either not required in the healthcare system or would introduce unnecessary complexity. As one variation of the SOA paradigm, the business logic happens in the decentralized client systems, i.e. the health professionals' systems, the eKiosks and the patients' software at home. The architecture specified is split-up into five layers:

- presentation layer
- business process layer
- service layer
- application layer
- infrastructure layer

As mentioned before, the business logic happens on the client systems. The service layer is split and resides both on the client and server systems. The lower layers reside in the telematics infrastructure. The client- and server-side parts of the service layer are joined by connectors ("Konnektoren"), which connect all the decentralized services on the systems in healthcare institutions with the central services of the German healthcare system. From a requestors point of view, the connectors mirror the architecture from the other side of the connector. The specification allows the connectors to act as a proxy service. As another option, the connector can rely on services of the infrastructure but offer a more fine-grained service itself. As an example, a connector could retrieve a collection of unique identifiers which have not yet been associated with any entities. But the service in the connector would not pass on the whole collection but with each request just one of the unique identifiers. [3]

All services offering functionality on patient data—prescriptions or health records—have to offer a generic interface for data manipulation—create, read, update, delete—and another interface to allow for permission control on the single health records. The storage of health records can happen decentralized. Thus, existing health records in health institutions around the country can be integrated into the nationwide healthcare infrastructure via those interfaces.

The services are not located dynamically, but are specified by localization services. The addresses of this localization services are configured in the connectors; the configuration is protected by certificates. Thus, the risk of forgery of localization services is decreased. The communication itself can happen via SOAP, but is not restricted to. The authors argue that the potential loss of flexibility is fairly compensated by the gains in security.

The architecture is divided in three security zones. The primary zone contains all the systems in the various healthcare institutions. Those are considered potentially unsecure. Systems in the access zone are considered secure and are connected to the services via virtual private networks (VPN). Infrastructure and PKI services are located in this access zone. The systems from the primary zone connect via their connectors to access gateways, which provide connection to the access zone. Finally, the service providers themselves are located in the telematics zone, which is again a secure zone connected to the access zone via service gateways.

As the specification requires every component to be located in exactly one of these zones and interaction between the zones can only happen across very few, exactly defined interfaces, the architecture is to deliver a maximum in security. The connectors themselves have to authenticate against the access gateway. Thus, not only is access to sensitive medical data is regulated by fine-grained permission control techniques, but so is access to the telematics infrastructure as well. No-one can access the infrastructure without a proper connector and proper authorization, i.e. from one of

the digital identity cards.

Once a connector connects to the infrastructure, according to the type of connector (in hospital, a medical practice, a pharmacy or an eKiosk) the connector is connected to a VPN dedicated to its type. This ensures on a technical level, that e.g. a patient's health record cannot be accessed from a pharmacy, or that a medical practitioner cannot force a patient to grant access to data in the practice or hospital. Permission management is generally only allowed from the eKiosk VPN. [3]

C. Secure Storage of Patient Data

In order to store patient data possibly decentralized and unlinkable to the patient's identity, upon creation of a new medical document the following steps are taken: [2]

- creation of a "data id" (DID)
- creation of two separate symmetric keys (SeKT and SeKD)
- creation of a random number (RND)

The combination (RND, DID) is called a ticket. Now, instead of directly storing some data signed with the eGK's public key (PuK), for confidentiality reasons at least two records are stored on the server:

- hash(RND, DID)—the ticket verifier
- (DID, e(SeKD, data))—the encrypted data

If a client asks for (RND, DID), it will receive e(SeKD, data) if the appropriate ticket verifier hash(RND, DID) could be found. In order not to have to redistribute RND upon each document creation, the patient can choose to store ticket toolkits on the server:

- (e(PuK, (SeKD, SeKT)), e(SeKT, (RND, DID)))

The owner of the private key corresponding to the public key PuK can now decrypt both symmetric keys, and thus decrypt both the ticket (using SeKT), and after retrieval, the data (using SeKD).

Along with the ticket verifier, an access control list (ACL) will be stored, granting or revoking the different permissions for roles (practitioners, pharmacists) or individuals. [2] The respective professional would then prove his/her role by use of the attribute certificate stored on the HBA.

This architecture comprises another big advantage with regards to data availability: in the case of loss of a patient's public key, no data will be lost, if the patient has access to another ticket toolkit via another private key. The authors emphasize that this second pair of private and public keys has to be related in no way to the German healthcare system, but could be any type of private and public keys. Thus, only new ticket toolkits have to be generated for a reissued eGK and the ticket toolkits for the old eGK can be deleted. This re-encryption can happen without actually decrypting the real medical data. [2]

VI. Conclusion

Identity management plays a major role in the design of an integrated electronic healthcare system. Obviously, access control to the telematics infrastructure is essential. But also, people want to be sure that their medical and other sensitive data is stored safely. The best way of assuring this is allowing everyone full permission control on their own data. Furthermore, some applications require to uniquely identify individuals associated with a data record or an operation while others require strict anonymity of the individuals involved.

Public key encryption is a key technology for achieving these goals. Digital signatures and digital certificates are widely used and accepted and are credited a high amount of trust by the public. Therefore, lots of software and hardware tools exist supporting the associated protocols. Like in many other countries, the digital identity cards to be used in the healthcare sector—elektronische Gesundheitskarte, Heilberufsausweis and Secure Module Card—will be smart cards relying on digital signatures and certificates.

Additionally the architecture proposed for the telematics infrastructure of the German healthcare sector features a flexible modular design. This is required as not all features of the infrastructure will be in place at once. Thus, all components allow for the subsequent introduction of new applications. New applications are classified as internal or external applications. [11] Internal applications rely on the telematics infrastructure, whereby external applications use the digital identity cards for identification or authentication, but the application itself exists outside the telematics infrastructure and does not even need to be related to healthcare at all.

One example of such an additional application is the preparation of the elektronische Gesundheitskarte for the Qualified Electronic Signature application. If an individual decides to obtain this application for the elektronische Gesundheitskarte, he/she will be able to sign arbitrary documents legally effective. Maybe people are inspired by the way health professionals use their QES application to sign prescriptions and other documents. Another side-effect of the QES application will be that many individuals would take part in a nationwide, reliable PKI. It remains to be seen if this development results in a boost for PKI-based IT security applications in the consumer sector.

A. References

[1] Torsten Becker, Christoph Meinel: Security in Telemedicine – Certificates and Digital Identity Cards. In Proc. XII Wintercourse of the CATAI, La Laguna, Tenerife, Spain, 2004, pp. 44–47

[2] Jörg Caumanns: Der Patient bleibt Herr seiner Daten, in Informatik-Spektrum Volume 29 No. 5, pp323–331. October 2006

[3] Jörg Caumanns, Herbert Weber, Arne Fellien, Holger Kurrek, Oliver Boehm, Jan Neuhaus, Jörg Kunsmann, Bruno Struif: Die eGK-Lösungsarchitektur, in Informatik-Spektrum Volume 29 No. 5, pp341–348. October 2006

[4] Die Spezifikation der elektronischen Gesundheitskarte. Teil 2: Anwendungen und anwendungsspezifische Strukturen, Version 1.2.1. gematik, 7.9.2006

[5] Die Spezifikation der elektronischen Gesundheitskarte. Teil 3: Äußere Gestaltung, Version 1.2.1. gematik, 7.9.2006
[6] Fachkonzept Versicherungsstammdatenmanagement (VSDM), Version 1.1.0. gematik, 19.9.2006
[7] Festlegungen zu den X.509 Zertifikaten der Versicherten, Version 1.2.0. gematik, 2.10.2006
[8] Speicherbedarf der eGK, Version 1.1.1. gematik, 7.10.2006
[9] Alan H. Karp: Authorization-Based Access Control for the Service Oriented Architecture. In the Fourth International Conference on Creating, Connecting and Collaborating through Computing. HPL-2006-3, 3.1.2006
[10] Reinhold A. Mainz: Electronic health cards – European perspectives. 1st national eHealth conference, Bulgaria. Federal Ministry of Health, Germany. 1.2.2006
[11] Jan Neuhaus, Wolfgang Deiters, Markus Wiedeler: Mehrwertdienste im Umfeld der elektronischen Gesundheitskarte, in Informatik-Spektrum Volume 29 No. 5, pp332–340. October 2006
[12] Bruno Struif (Ed.): German Health Professional Card and Security Module Card. Part 2: HPC Applications and Functions. Version 2.1.0, 21.2.2006
[13] Bruno Struif (Ed.): German Health Professional Card and Security Module Card. Part 3: SMC Applications and Functions. Version 2.1.0, 21.2.2006
[14] Wei Zhou, Christoph Meinel, Vinesh H. Raja: A Framework for Supporting Distributed Access Control Policies, iscc, pp. 442-447, 10th IEEE Symposium on Computers and Communications (ISCC'05), 2005.
[15] Wei Zhou, Vinesh H. Raja, Christoph Meinel, Munir Ahmad: Label-Based Access Control Policy Enforcement and Management, snpd-sawn, pp. 395-400, Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'06), 2006.