published as: T. Becker, Christoph Meinel: Security in Telemedicine - Certificates and Digital Identity Cards;
La Laguna (Teneriffa), 2004, pp. 44-47.

Security in Telemedicine – Certificates and Digital Identity Cards*

Torsten Becker, Christoph Meinel
FB IV – Informatik, University of Trier, D-54286 Trier, Germany

***Abstract*— In health care confidentiality of data is an ethical necessity. Hence data must be stored and transmitted according to high level security standards, at best under control of the concerned people. Moreover, data with legal meaning must be digitally signed. Certificates and cryptographic keys stored on digital identity cards are suitable means to fulfil these requirements.**

***Index Terms*— Attribute Certificates, Health Insurance Card, Health Professional Card, X.509.**

I. Introduction

THE increasing networking in health care make high demands on data security. Data security covers in first line availability, integrity, authenticity, liability, and confidentiality.

Availability concerns network and system stability primarily. Without a 7-24 availability of the resources telemedicine is severely limited. Integrity means that the stored and transmitted data can not be manipulated. The authenticity of a person is the basis to protect the access to confidential information. Liability concerns verifiability and non-repudiation of therapeutic arrangements and prescriptions for instance. Confidentiality in this context stands for professional discretion and obligation of secrecy. It has to be ensured that each concerned person only can get access to those data which he/she needs on behalf of the patient. Confidential data have to be strictly secured during the transmission. Anonymity can be considered as a characteristic of confidentiality - the confidentiality of someone's identity.

Cryptography is the basic security technology for open networks and systems. With encryption methods the confidentiality of stored and transmitted data can be guaranteed. In addition, cryptography is the premise for digital signatures which ensure integrity and liability as well as secure authentication of users.

Digital identity cards are helpful to introduce high-level cryptographic methods on a very convenient level. For this purpose certificates stored on smart cards are advisable. In Germany the "Health Professional Card" (HPC) will be introduced as a professional identity card for physicians, pharmacists, and other health professionals. These cards offer cryptographic functions to guarantee data security: integrity, authenticity, liability, and confidentiality by using digital cryptographic methods and keys.

II. Certificates

A public-key certificate is digital signed by a certification authority (CA). Thus, the certification authority authenticates that the specified public key belongs to a specific user (person or host computer). To obtain a public-key certificate the user (the operator of the host computer respectively) has to appear by a registration authority (RA) personally, and has to prove his identity.

Certificates have a temporary validity. Because of the high administrative effort to prepare a certificate certificates are normally issued over a longer period (e.g. for 2 years).

The disadvantage is that in many cases access rights are accorded for a shorter period (e.g. some days or weeks). For this reason there are attribute certificates (AC). Attribute certificates contain information about the rights of the user and should be linked to a public-key certificate. An attribute certificate can be issued easily. Nevertheless, it is a secure instrument for authentication.

A. Public-Key Certificates

The normally used certificate is a public-key certificate in X.509 format. This standard is described in [1]. A X.509 certificate consists of three fields:

- ***tbsCertificate***,
- ***signatureAlgorithm***, and
- ***signatureValue***.

The user data of the certificate are contained in the field *tbsCertificate*. The certification authority digitally signs this data with its private key. The signature is stored in the field *signatureValue*. The field *signatureAlgorithm* contains the used signature algorithm.

The specific data of the field *tbsCertificate* for a public-key certificate are described in the following:

version: is the version of the certificate. Normally v3 is used. If the *extensions* component is present in the certificate, version shall be v3. If the *issuerUniqueIdentifier* or *subjectUniqueIdentifier* component is present version must be v2 or v3.

serialNumber: is an integer assigned by the certification authority to each certificate. The value of *serialNumber* must be unique for each certificate issued by a given certification authority (i.e., the issuer name and serial number identify a unique certificate).

signature: contains the algorithm identifier for the algorithms and hash functions used by the CA in signing the certificate (e.g. *md5WithRSAEncryption*, *id-dsa-with-sha1*, *sha-1WithRSAEncryption*, etc.). This identifier is registered in

* in Proc. XII WINTERCOURSE OF THE CATAI, La Laguna, Tenerife, Spain, 2004, pp. 44-47

the field *signatureAlgorithm,* too, but for security reasons it is stored in the signed data in addition.

issuer: identifies the entity that has signed and issued the certificate (i.e., the certification authority).

validity: is the time interval during which the certification authority warrants that it will maintain information about the status of the certificate.

subject: identifies the entity associated with the public key found in the *subjectPublicKeyInfo* field.

subjectPublicKeyInfo: is used to carry the public key being certified and to identify the algorithm which this public key is an instance of (e.g. *rsaEncryption*, dhpublicnumber, *id-dsa*, etc.).

issuerUniqueID: is used to uniquely identify an issuer in case of name re-use.

subjectUniqueID: is used to uniquely identify a subject in case of name re-use. CAs can use the unique identifier to distinguish between reused instances. However, if the same user is provided certificates by multiple CAs, it is recommended that the CAs coordinate on the assignment of unique identifiers as part of their user registration procedures.

extensions: This field allows addition of new fields to the structure. An extension field consists of an extension identifier, a criticality flag, and a data value. When an application does not recognize an extension, it may ignore that extension, if the criticality flag is FALSE. If the criticality flag is TRUE, unrecognized extensions shall cause the structure to be considered invalid, i.e. in a certificate, an unrecognized critical extension would cause validation of a signature using that certificate to fail. Specific extensions may be defined in ITU-T Recommendations and International Standards or by any organization which has a need. The object identifier (OID) of an extension shall be defined in accordance with [2].

The binding of a privilege to an entity is provided by an authority through a public-key certificate containing an extension defined explicitly for this purpose. But in most cases it will be better to use a digitally signed data structure called an attribute certificate.

B. Attribute Certificates

Privileges will have lifetimes that do not match the validity period for a public-key certificate. They will often have a much shorter lifetime. The authority for assignment of privilege will frequently be other than the authority issuing the public-key certificate. Furthermore, different privileges may be assigned by different attribute authorities (AA).

The use of attribute certificates provides a flexible Privilege Management Infrastructure (PMI) which can be established and managed independently from a Public Key Infrastructure (PKI). At the same time, there is a relationship between the two whereby the PKI is used to authenticate identities of issuers and holders in attribute certificates.

An attribute certificate is a separate structure from a subject's public-key certificate. A subject may have multiple attribute certificates associated with each of its public-key certificates.

An attribute certificate consists of three fields:

- ***acInfo***,
- ***signatureAlgorithm***, and
- ***signatureValue***.

The user data of the certificate are contained in the field ***acInfo***. The certification authority digitally signs this data with its private key. The signature is stored in the field ***signatureValue***. The field ***signatureAlgorithm*** contains the used signature algorithm.

The specific data of the field *acInfo* for an attribute certificate are described in the following:

version: This number differentiates between different versions of the attribute certificate. If holder includes *objectDigestInfo* or if issuer includes *baseCertificateID* or *objectDigestInfo*, version must be v2.

holder: conveys the identity of the attribute certificate's holder. This field can have three components optional:

The ***baseCertificateID*** component, if present, it identifies a particular public-key certificate that has to be used to authenticate the identity of this holder when asserting privileges with this attribute certificate.

The ***entityName*** component, if present, it identifies one or more names of the holder. If *entityName* is the only component present in holder, any public-key certificate that has one of these names as its subject can be used to authenticate the identity of this holder when asserting privileges with this attribute certificate. If *baseCertificateID* and *entityName* are both present, only the certificate specified by *baseCertificateID* may be used. In this case *entityName* is included only as a tool to help the privilege verifier locate the identified public-key certificate.

The ***objectDigestInfo*** component, if present, is used directly to authenticate the identity of a holder, including an executable holder (e.g. an applet). The holder is authenticated by comparing a digest of the corresponding information, created by the privilege verifier with the same algorithm identified in *objectDigestInfo* with the content of *objectDigest*. If the two are identical, the holder is authenticated for purposes of asserting privileges with this attribute certificate.

issuer: conveys the identity of the attribute authority (AA) that issued the certificate.

signature: identifies the cryptographic algorithm used to digitally sign the attribute certificate. As mentioned above, this identifier is registered in the field *signatureAlgorithm* too, but for security reasons it is stored in the signed data in addition. The algorithms and identifiers are defined in [3].

serialNumber: is the number that uniquely identifies the attribute certificate within the scope of its issuer.

attrCertValidityPeriod: conveys the time period during which the attribute certificate is considered valid.

attributes: contains the attributes associated with the holder that are being certified (e.g. the privileges).

Examples for attributes are:

- Service Authentication Information
- Access Identity
- Charging Identity
- Group
- Role

issuerUniqueID: may be used to identify the issuer of the attribute certificate in instances where the issuer component is not sufficient.

extensions: allows addition of new fields to the attribute certificate.

C. References

[1] ISO/IEC 9594-8, "The Directory: Public-key and attribute certificate frameworks," 2001

[2] ISO/IEC 9834-1, "Procedures for the operation of OSI Registration Authorities: General procedures," 1993

[3] W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile," RFC 3281, Apr. 2002

III. Digital Identity Cards

A. Health Insurance Cards in Europe

In Europe all countries have a system for identifying persons covered by social insurance. But at the moment not all of them have a card-based system. In some countries projects are under way. Other countries have no national cards, but there are plans of region authorities or sickness insurance bodies to distribute them.

Functions of existing sickness insurance or health cards (or of those cards which will soon be available on an operational or experimental basis) of different EU Member States vary widely. They may, for example:

- serve solely to identify the insured,
- enable acquired rights to be verified and facilitate payment or reimbursement procedures,
- carry identification data which provide access to online services,
- extend beyond the field of social security: they may, for example, carry medical emergency data, enable the individual's legal status in respect of labour law to be verified to combat undeclared working, provide access to public services such as public libraries or employment agencies.
- Finally, some Member States plan to integrate medical data (diseases, treatment received, medical or surgical history, etc.) into a secure health network.

The nature and scope of the data stored on the various cards depends on the purpose for which they are intended. Some carry only the information necessary to identify the insured, and possibly to allow online access to resources and services. Others also store information on acquired rights (e.g., the basic scheme of which the holder is a member, any supplementary scheme, the rate of reimbursement for various types of care). So far there is no European standard for the information to be included on such cards.

The technology used obviously depends on the card's functions. Some have a microprocessor chip, others a memory chip or magnetic strip. At the moment, therefore, these cards are not compatible. They also require different kinds of reader depending on the "intelligence" carried on the cards themselves, which sets additional limits on their capacity to dialogue (or their "interoperability").

Like technological developments, changes in health systems entail constant adaptation. The internet, for example, with its data transmission protocol and network security and cryptography systems (Public Key Infrastructure), provides new opportunities for developing online services for all those involved in care provision. The European landscape is therefore in constant evolution, which makes it difficult to contemplate harmonizing the technologies and functions associated with the cards. Efforts should focus rather on card "interoperability". This approach would seem both realistic and appropriate to achieving the coordination of Member States' social security schemes under Regulation 1408/71 [1].

B. Introduction of an European Health Insurance Card

The eEurope 2005 Action Plan [2] seeks to support European cooperation on electronic health cards.

This health card represents an essential stage in the possible development of new services or functions using information technologies, such as storing medical data on a smart card or secure access to the medical file through the insured's identifier.

To ensure that the card is readable, at the beginning it should only carry data that are absolutely necessary for the provision of care and reimbursement of the cost to the institution in the place of stay. The paper E111 form already contains this essential information, but also certain redundant or superfluous data. So the obligatory information on the European health insurance card should be cut down to the following:

- surname and first name of the cardholder,
- identification number of the cardholder,
- card validity date,
- ISO code of the Member State of registration,
- identification number, or, if none, name of the competent institution,
- the logical number of the card, which must enable the information it carries to be checked against the information held by the insuring organisation for the same logical number, to reduce the risk of fraud.

For the countries distinguishing between different types of acquired rights, (e.g. hospital treatment only or all health care), this could be indicated.

C. The Health Professional Card (HPC) in Germany

Already in 1997 all participants in health care in Germany argue for an interoperable electronically identity card for health professionals to provide a functional and secure infrastructure for data exchange in health care. In 1999 a first specification of the "Health Professional Card" (HPC 1.0) was published. Last year a new specification (HPC 2.0) [3] was accepted and released for implementation.

In 2006 a new health insurance card with cryptographic functions and the possibility to store data on the card (e.g. blood type, diagnostic findings, etc.) should be introduced in Germany. It must be guaranteed that only health profession-

als (physicians, pharmacists, etc.) have access to these cards. This can be done by using a digital identity card for health professionals. HPC 2.0 permits a diversified technical infrastructure So that all required applications can be realized with the health professional card.

The HPC contains the personal data of the health professional, for example the name and a picture of the holder, the area of expertise, and the card issuer. This data must be available electronically (digital signed but not encrypted) as well as in non-electronic form ("be visible to the naked eye").

As main security features the HPC enables digital signatures, encryption, and client server authentication. For these applications different keys (with different PIN) are used. The associated public-key certificates and attribute certificates where required can be stored on the HPC. The encryption feature is only used for decryption of received (encrypted) data since the HPC is only for key management and not for the encryption and decryption of data in fact. The client server authentication feature allows the health professional to get access to server systems that provide electronic patient files for example.

Of particular importance is the card-to-card authentication. With this feature health professionals can verify their access authorization of an electronic health insurance card. Since the new health insurance card is not specified up to now, the HPC 2.0 specification contains a symmetric as well as an asymmetric authentication method. The card-to-card authentication is a verification of the HPC and the health insurance card together.

All the cryptographic functions of the HPC have to be protected by a PIN in order to prevent non-authorized people from use of HPC if it was stolen or lost.

The HPC 2.0 standard includes the specification of a so-called "Security Module Card" (SMC) which has similar features as the HPC. The main functions of a SMC are card-to-card authentication and encryption functions for an organization so that, for example, each authorized employee of a doctor's surgery or a ward can encrypt or decrypt a document. Moreover, the SMC can enable access for a physician to his HPC from different stations (surgeries).

D. References

[1] Regulation EC No 1408/71 on the application of social security schemes to employed persons and their families moving within the Community, consolidated version OJ L 28, Jan. 1997

[2] "eEurope 2005: An information society for all," Commission of the European Communities, Brussels, May 2002

[3] Bruno Struif, Alfred Giessler, Björn Schneider, "German Health Professional Card and Security Module Card Specification," Version 2.0, Jul. 2003