Applications in Health Care using Public-Key Certificates and Attribute Certificates

Petra Wohlmacher
University of Klagenfurt
System Security Group
9020 Klagenfurt, Austria
petra.wohlmacher@uni-klu.ac.at

Peter Pharow
Otto-von-Guericke University of Magdeburg
Medical Faculty, Medical Informatics Department
39120 Magdeburg, Germany
peter.pharow@medizin.uni-magdeburg.de

Abstract

Security infrastructures are increasingly used in the health care and welfare sector, particularly for providing security, like confidentiality, authenticity, integrity, non-repudiation, and auditing. Especially within the health care sector, there is a need for different kinds of certificates, namely public-key certificates and attribute certificates. This necessity is caused by the huge range of processes and procedures deriving from different application areas within the health care sector. Due to that, this leads to a large amount of specific and different roles, rules, access rights, and permissions for each health professional. An important security token within health care is represented by the smart card, called health professional card (HPC). Existing solutions e.g. the German HPC, prototypes, and European as well as national projects, activities, and initiatives, show the state of the art with respect to certificates. Finally, we point out unsolved problems regarding security infrastructures, jurisdiction, data protection, and advertizing via Internet.

Keywords

Public-key cryptosystem, cipher, digital signature, authentication protocol, public-key certificate, attribute certificate, x.509, security infrastructure, trust center, trusted third party, health care, welfare, health professional, smart card, applet, German health professional card, HARP, European Electronic Signature Directive, European Data Protection Directive.

1. Introduction

Nowadays, large security infrastructures are developed and currently going to be established for meeting security requirements [PKIX99]. Different areas are using these infrastructures to enhance the security of their IT-systems and their applications. A main beneficiary of these developments is the health care sector, where a large number of national and international projects and initiatives are set up (for more information about such activities see conference proceedings e.g. [HC95, HC97, Med98, MIE00]). The basic objectives of these activities are:

- to support high availability of information by using large networks and high-speed connections;
- to reduce costs within the health care and welfare sector by granting cross-border access to digital data in a fast and secure manner;
- to increase the responsibility of health care employees as well as administrative personnel by auditing their actions and activities;
- to realize privacy of both patient data and health professional data by means of cryptographic mechanisms as well as access control mechanisms; and
- to establish multi-media medicine, tele-diagnostics, surgeries using robots, and tele-health at all.

To achieve these objectives in the best possible way, security requirements need to be defined, e.g. confidentiality, integrity, authenticity, and non-repudiation. These requirements can be met by security measures (or security services), whereby most of them use cryptographic mechanisms, e.g. ciphers, digital signatures, and authentication protocols. Substantially, the security depends on the authenticity of data like public keys as well as on the authenticity of special attributes of entities like roles, rights, and authorizations. An authentic link between a public key and its owner can be provided by public-key certificates [ISO93, ISO97], which are particularly suitable for use in such applications, where a large number of entities (persons, institutions, processes or devices) exist and furthermore, entities associated to different institutions have to communicate with each other. Correspondingly, attribute certificates link attributes to an entity in an authentic manner [ISO97].

This paper is organized as follows. In section 2 we motivate the need for public-key certificates and attribute certificates, and particularly justify the necessity for the separation into these two kinds in general. In section 3 we present several procedures and applications within the health care and welfare sector, where distinctive public-key certificates as well as attribute certificates need to be applied. Furthermore, we give more detailed reasons for the separation of the certificates with respect to the health care sector. Finally, in section 4 we point out some unsolved problems and future works.

2. Need for certificates

Initially, we describe the need for public-key certificates, and then we motivate attribute certificates in general. Finally, we show reasons for the need of different certificates, especially why public keys and attributes need to be separated into different kinds of certificates.

2.1. Need for public-key certificates

In most cases, cryptographic mechanisms like ciphers, digital signatures, and authentication protocols are realized by public-key cryptosystems. In comparison to secret-key cryptosystems, public-key cryptosystems are based on the use of key pairs, whereby each key pair consists of a private key *sk* and a public key *pk* corresponding to *sk*. Each user of a public-key cryptosystem owns one key pair or even several key pairs. Given a public key *pk*, it is computationally infeasible to find the private key *sk*. Accordingly, each key *sk* must strictly be kept secret by its owner, and the corresponding key *pk* is usually published.

The use of public-key cryptosystems raises the following problems:

- With respect to ciphers: The public key of the recipient is used for the encryption of the plain text. Here, it cannot be ascertained whether or not the public key actually belongs to the designated entity.
- With respect to digital signatures and signature-based authentication protocols: The public key of the signer is needed for the verification process. By the use of the public key it can be checked whether the signature to particular data was generated by the corresponding private key or not. Thus, the authenticity of data can be proven. However, it is not provable whether or not a certain entity owns the public key.

Obviously, an authentic link between public keys and its owner is needed. Such a link is provided by public-key certificates. Since each public key corresponds to a particular private key, a binding of the private key to its owner is given indirectly. By the use of certificates, a lot of attacks fail like the man-in-the-middle attack, replay attack, masquerade, repudiation, spoofing, and trojan horses. If the public key is not bound to its legal owner, attacks like the following masquerade become possible: An adversary X generates his own key pair (pk_X, sk_X), and publishes the public key pk_X by claiming a wrong identity A. This leads to the following problems:

- Regarding ciphers, since only X knows the right decryption key sk_X, no other entity with the exception of X is able to decrypt the ciphertext. Therefore, X is able to get knowledge of information which is actually designated to an entity possessing identity A.
- Regarding digital signatures, X is able to forge signatures of an entity A. This is due to the fact, that the verifier assumes, that the public key used for the verification process, belongs to its legal owner, namely entity A.

Since 1986, different versions of public-key certificates have been defined [ISO88, ISO93, ISO97] specified in ASN.1-notation. During the past, the practice has shown the need for additional granularity of the specification of certificates. Today, the current version v.3 of X.509 certificates allows to use a lot of extensions, where some of them can be used for propriety purposes, e.g. for defining attributes of an entity like roles, rights or authorizations.

The disadvantage of these degrees of freedom leads to incompatibilities with respect to private extension fields [Lain99]. For example, usually distinctive applications do not recognize the meaning of extensions in each case. If the extensions are marked to be non-critical, the application will ignore them. Otherwise they are set to critical, and therefore, the verification must fail. However, in any case the extensions get useless. Additionally, in some circumstances there is a need to sign these extensions separately (this topic is explained in more detail in section 2.3.). Attribute certificates can alleviate all these problems.

2.2. Need for attribute certificates

In specific situations it is necessary to separate attributes, which are designated to an entity, from their public-key certificate. A certificate containing such attributes, is called attribute certificate. An attribute certificate does not exist autonomously – it is rather bound to a base certificate: the public-key certificate of the entity. Particularly, its validity period must be within the validity period of the public-key certificate but it can also be valid for a short term only. With respect to applications, an entity may possess different attribute certificates related to different validity intervals or even different purposes. Public-key certificates and attribute certificates are linked together either by the serial number of the public-key certificate or

by the distinguished name of the certificate holder, which represents the dedicated entity. After a successful verification process of the certificate, attributes are extracted and handed over to the application, which uses them e.g. for authorization purposes.

Exemplarily, attributes describe some of the following characteristics: general authorizations, international or national specific data, delegations for other persons like procura, kinds of permissions and admissions, temporary rights and access control mechanisms, and, to a certain extend, also roles.

Attribute certificates are specified in a first version v1 [ISO97]. Because of the standardized specification, attribute certificates are appropriated to support interoperability just as good as public-key certificates do. They are structured similar to public-key certificates and are also noted in ASN.1. Due to the different purposes of the attributes, attribute certificates are often specified in more detail and also named more precisely, e.g. attribute certificates for qualifications and attribute certificates for authorizations [HPC99].

2.3. Reasons for separation

With regard to applications in health care, we motivate main reasons why different certificates have to exist. Particularly, we describe reasons for the separation into public-key certificates and attribute certificates.

Considering public-key certificates, for security reasons each security measure must apply an individual key pair. If only one single key pair is used, the following attacks may succeed:

- If the same key pair is used for both security measures, digital signatures and digital signature based authentication protocols, signing a challenge within the authentication protocol is similar to the generation of a signature to specific data within the digital signature scheme.
- Assuming the RSA scheme [RiSA78] is used for both security measures, digital signatures and ciphers, then the decryption of a specific data is similar to the generation of a signature to these data.

Therefore, different key pairs must exist, whereby each key pair is applied to a single security measure. Due to that, different public-key certificates have to be generated with each certificate containing a different public key dedicated to a corresponding private key. Furthermore, a security measure might also be supported by different key pairs or even algorithms. That also increases the number of public-key certificates. With respect to those three security measures mentioned above, at least three different key pairs and therefore, at least three different public-key certificates are needed.

Regarding attribute certificates, an entity may use distinctive applications for different purposes, even in a business or private context. Here, the entity must usually prove in an authentic manner that it possesses specific attributes e.g. the right to perform particular actions. Furthermore, an entity may decide to have – assuming it has the permission to do so – the opportunity to choose which attribute certificate it wants to apply in specific circumstances. Due to that all, similar to public-key certificates the number of different attribute certificates related to a single entity might be large.

Concerning the management of certificates in general, different trustworthy authorities (trust centers – TC, or trusted third parties – TTP) are needed for distinctive purposes. Each TC or TTP operates under its own security policy. A security policy regulates for example the identification process of an entity, the generation of keys, the generation and distribution of certificates, the validity interval of certificates, and also how to ensure the availability of the services. More precisely, a key-generation authority generates key pairs and a certification authority authenticates the link of entities to their designated data like public keys or attributes by issuing certificates. Other parts of TCs or TTPs provide and support further security services like non-repudiation, revocation handling, time stamping, auditing, and directory service.

To establish proper and practical security infrastructures for public-key certificates and attribute certificates some important topics concerning practical, legal and validity aspects have to be taken into account. These topics indirectly contribute reasons for the separation of certificates and have additionally encouraged different projects to decide for splitting [TH97, HPC99]:

Initially, existing bindings between institutions and also individuals, particularly established trustworthy ones, should be exploited. Therefore, these entities should be involved into the security infrastructure. Due to that, the issuer of different kinds of certificates can be in compliance to existing connections, functions, responsibilities, and also liabilities and even legal requirements. Consequently, this leads to the existence of various registration, naming and certification authorities, which are operating under different security policies. Unfortunately, usually their policies do not match. Nevertheless, different authorities can interoperate if they accept each others security policy. Exemplarily, the registration process of entities can be performed by a single appropriated authority if its security policy concerning the registration is accepted by all authorities that need such a registration for entities. Commonly, the validity periods of public-keys and attributes are also different. Especially the validity of public keys might strictly be regulated by law (e.g. [SigV97]). Furthermore, certification paths, certification hierarchies, availability of the directory services, revocation reasons,

and particularly the revocation methods may have different requirements. Due to that, we derive a lot of important reasons for the separation into two types of certificates: public-key certificates and attribute certificates.

3. Applications in health care

Similar to many other business sectors, health care and welfare are challenged by new electronic media. High expectations of both patients and health insurance companies and an even decreasing budget for health purposes request an increasing use of a communication infrastructure. Using this infrastructure, data like images and lab results can be communicated rather fast and particularly cross-border and thus, guarantee an optimized care process. Here, a well-functioning and certificate-based security infrastructure is required.

Nowadays health information systems are designed to support a well-defined access control mechanism. But in most cases, this access is provided by using rather simple and weak access mechanisms, e.g. passwords which are even shared between colleagues rather often. From a data protection and data security point of view, this fact is intolerable. It demands the development and the implementation of strong authentication mechanisms based on secure tokens using strong authentication. Initially, this means in minimum a smart card with a PIN functionality but additionally more and more biometrics mechanisms like fingerprint or iris analysis. Furthermore, the use of a security infrastructure based on different certificates can provide a basis for the necessary access granularity.

Regarding the health care sector, we are going to consider entities which are named health professionals. A health professional (HP) is stated as any person involved in any kind of health care and welfare related services – ranging from doctors to nurses, from administrative staff to support staff, from IT staff to educational staff. Health professionals at all have to provide a very wide range of distinctive services which means definitely not only the "pure" care and treatment functionality. Due to this huge range of processes and procedures, it is impossible to handle all of these roles and rules, access rights, permissions and admissions, etc. within public-key certificates – regardless of the aspects of practical, legal and validity issues (see section 2.3.). A more specific explanation is given in the following section.

3.1. The use of public-key certificates

In the health care sector, there is a clear distinction between the identity-related part of security services, and the professional part, both represented by certificates and related key pairs. Similar to most of the other domains, public-key certificates and especially the private keys corresponding to the certified public keys are bound to a carrier – a secure token. In the health care scene of several European countries this carrier is a smart card, also known as health professional card (HPC). It is quite clear, that the welfare of patients has highest priority, and due to that, it has to be guaranteed, that the infrastructure and particularly the technical equipment need to be available at any time. For this, e.g. a proper emergency management needs to be defined including solutions for backup systems particularly for smart cards.

The security infrastructure within the health care sector mainly supports the following three security measures: confidentiality, integrity, and authenticity. Accordingly, each health professional needs at least three different key pairs (see section 2.3.): to be used for ciphers, digital signatures, and strong authentication.

Public-key certificates used for security measures include all relevant items, which are necessary for a unique identification of the individual. In some cases it might be an advantage to have a general description of a health professional type or role already included here. By this kind of generic statement it just supports simple identity-related functions showing that the owner (holder) of the certificate is a health professional regardless of the more specific definition within the attribute certificate context.

3.2. The use of attribute certificates

Attribute certificates are relevant for very different aspects in health care and welfare. They can be used for any kind of profession and are of course not restricted to doctors or physicians.

In the following, different features of attributes are described, which are used in an attribute certificate for health professionals. A general approach to illuminate several aspects of attribute certificates in the context of health care and welfare is shown in the documents of the specification of a German electronic doctor's license [HPC99].

Firstly, attribute certificates point out the profession of a health professional. Examples for some Europe-wide types of professions have been defined by CEN/TC 251 WG7 N45/46, namely: physician, dentist, pharmacist, midwife, nurse, physiotherapist, psychologist, psychotherapist, speech therapist, chiropractor, optician, dental nurse, dispending pharmacist, administrator, and dental hygienist. Additionally, attribute certificates hold general information about a health professional which means to have a qualification to practice as a specialist with a certain experience on behalf of, and accepted by, regional or national health bodies. Further information might also reflect any kind of knowledge in terms of specific surgeries

or investigation methods using devices as, e.g., tomographical devices (CT), ultra sound devices, X-ray devices, herbal treatment, ancient Asian ways of traditional treatment. Here, attribute certificates illuminate the static roles in health care and welfare including specific knowledge, further education in terms of medical practice, and examinations provided by health authorities. Due to that, this kind of certificate might be called an attribute certificate for qualification.

Beside the medical qualification, information about permissions and admissions include the allowance to practice on behalf of health authorities or health insurance companies within a country, a federal state, a province, or a county. This is an important topic, because in some countries within Europe, a doctor is not allowed to practice without this specific permission given by the health authority. This means that he has to become a member of the regional health authority (health body, chamber) to practice. A typical example for that kind of procedure is Germany where each physician has to belong to the Physicians' Chamber of the federal state as soon as he intends to practice. This membership has to be pointed out by use of a specific attribute. Attribute certificates of this type reflect medical terms and access rights, roles, and even related rules. This includes also whether or not a doctor is allowed to prescribe specific medication including drugs, and whether a pharmacist is allowed to hand over these drugs to a patient. These attribute certificates can (and will) also be used for permissions related to health insurance companies, which at least means billing and, thus, to a certain extend electronic commerce. Thus, they are supporting authorization items which may have lead to the term of attribute certificates for authorization.

Concerning the security infrastructure described here, national or regional health authorities play an important role within the infrastructure because of their knowledge and their amount of information about health professionals practicing in their particular region. This might be a country, a federal state, a province, or a county – always depending on the administrative structure of the related health care and welfare system. Resuming the latter example of Germany: if a health professional moves his residence to another German federal state it would mean to become a member of the other chamber before starting to practice there. Since these chambers have the responsibility to collect both identity-related and profession-related data of their members, they are well-prepared to act as an important entity of the security infrastructure playing their role as a registration authority.

Finally, we will also point out some important future work concerning harmonization efforts: Since there is a growing mobility of people throughout the world in terms of both business and leisure activities, also the roles and professions in health care and welfare in different countries with perhaps different educational and cultural background have to be harmonized or at least adopted and adapted. Based on a framework for different specialization in Europe, it can clearly be stated what a nurse is allowed to do e.g. in Germany and in Sweden. And this role and responsibility framework (as a part of a European health care and welfare security policy) can then be used for describing access rights. So it is more a question of interpretation than an interoperability issue.

3.3. A national German implementation

In the following, some examples are given how the process of issuing attribute certificate types and sets is defined and used in Germany. This concerns two kinds of attribute certificates: the attribute certificates for qualification and for authorization. For a more detailed and specific view on this issue, please refer to [HPC99].

Attribute certificates in the context of the German "Electronic Doctor's License" specification for physicians are issued to denote special attributes of the certificate holder not presented in his public-key certificate used for digital signatures. If the certificate holder signs a document on behalf of an institution or company, or if he signs it playing a certain "role" within an entity he has to use one or even more attributes of his certificates in this given context. This is done by integrating the relevant attribute certificates in the sequence to be signed at the end of the document before signing the document as a whole.

First of all, attribute certificates for qualification should be illuminated, as they contain the information requested for any medical procedure. Attribute certificates for qualification are issued following X.509 [ISO97]. In this type of attribute certificates, the following information items shall be encoded:

- profession,
- specialty type,
- dedicated specialty.

For each specialty type a separate attribute certificate shall be issued. The authority guaranteeing these qualifications is the named Physicians' Chamber of the German federal states. These chambers (at least 17 in Germany) will provide three specialty types of attribute certificates for qualification in German language: specialty, subspecialty, and medical discipline. The coding scheme for this specification is being worked out and will conform to a general format.

The table below gives some examples how the values of information items of attribute certificates for qualification regarding specialty types following the German HPC specification could look like.

Table 1. Attribute certificate for qualifications

specialty type	dedicated specialty
specialty	general practice
specialty	surgery
subspecialty	vessel surgery
subspecialty	thorax surgery
medical discipline	allergies
medical discipline	intensive care surgery

In the following, attribute certificates for authorization will be explained. These certificates are also issued following X.509 [ISO97]. Here, other relevant information items shall be encoded:

- general authorization,
- authorization type,
- dedicated authorization.

For each authorization type a separate attribute certificate might be issued. In Germany, the Association of Office Based Physicians (Kassenärztliche Vereinigung – KV) will provide this type of attribute certificate in German language. The coding scheme is being worked out already. Table 2 shows examples for the authorization type "authorization" of attribute certificates for authorization following the German HPC specification.

Table 2. Attribute certificate for authorizations

authorization type	dedicated authorization
authorization	ultra sound
authorization	x-ray
authorization	manual therapy

In the German national implementation, the security infrastructure employs the following authorities: the admission authority is represented by the entity which is responsible for the assignment of the values of the related components. The naming authority is the entity which defines the code lists containing the allowed values.

All examples mentioned above are taken from the technical guideline provided by the German National Chamber of Physicians (Bundesärztekammer – BÄK). This guideline covers items for IT-based processing of profession-related data of health professional. It consists of 13 chapters ruling e.g. the coding of specialties, subspecialties, medical disciplines, admissions and permissions (see above) but also academic degrees (Dr. med., Prof. Dr. med., etc.), main business areas (GP, head of a department or a clinic, assistant, etc.), and, last but not least, knowledge of foreign languages. After all, about 500 to 600 different items are defined and described. However, several of these information items have absolutely no relation to any other country but are specific for German health care and welfare.

Large trials and pilots with about 2000 health professionals using the German HPC type will be launched end of year 2000 including 5 regions in Germany.

3.4. Medical scenarios

The dynamic progress of communication and cooperation technologies and structures with increasing immediate needs to spread information systems, particularly medical networks, is a great challenge for the health care and welfare sector. Apart from economic and organizational aspects, security and privacy requirements have to be taken more and more into account. As health professionals at all mostly work with highly sensitive medical data appropriate administrative, technical, ethical, and legal solutions have to be developed and implemented. Already existing centralized (Sweden, U.K.) or decentralized structures (Germany) as well as related regulations and tools of the general health care system can be transformed in a way they get a much more important status than they might have currently, act as a motivation and can promote the introduction of a pan-European security infrastructure because of their familiarity.

In the following we intend to explain the basic statements of this paper by introducing two typical examples within the health care sector.

3.4.1. Example 1

Contrary to the banking sector where a clerk is very often allowed to get access to client-related personal data upon request simply by being a clerk of this bank, the health care and welfare sector is managed in a rather different way. Even doctors within the same department of a clinic or hospital are by law not allowed to get access to the same amount of personal data even for the same patient. It depends on the roles they are engaged to play within a very specific care and treatment process, and the related rules and policies.

From the access point of view, example 1 could be seen like two triangles (see figure 1). The top represents a lot of people sharing only a few rather general data items about a patient (even only administrative ones, e.g. for the process of exchanging bills between the clinic or hospital and the health insurance company the patient belongs to). In the middle section, a diagnostic or therapeutic team has to share much more information about the specific patient in order to treat him well. But even this amount of patient-related information is strictly limited to the real process of care they are obliged to deliver. And at the bottom of this triangle, we find the one and only responsible doctor with access to all medical and administrative patient-related information.

So this access aspect could be seen as the major problem of providing

- the right amount of patient-related medical and administrative information (correctness from a medical point of view and integrity from the security point of view)
- to the right person (the person with explicit access rights to read these information items)
- at the right time

in order to achieve the highest possible quality in the care and treatment process.

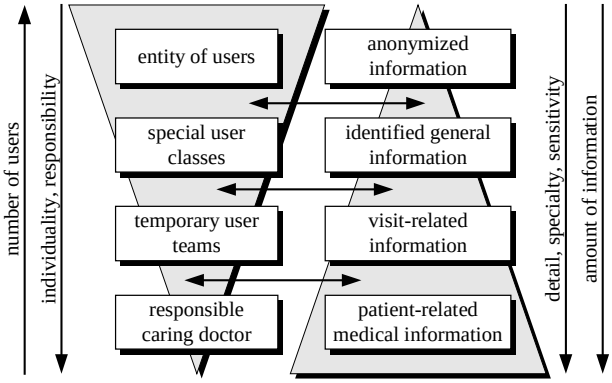

Figure 1. Example 1 – aspects of access

This may seem to be rather simple – but it isn't. Even when it comes to the example explained before (doctors in the same department of a clinic) it very much depends on their roles within the care process. If one of them became the caring doctor of a specific patient, he has of course access to all data. This is both a legal and ethical requirement. If the other doctor is "just" another doctor of this department he may have access to data which are relevant for the services he has to provide for the department. But as soon as he might become the deputy chair of the department (even for a couple of hours if the chair is absent for a surgery or a meeting) he has to have access to the medical data. In this case, he (as the deputy chair) is responsible for all activities provided by his team.

This example might have illuminated that the rights of professionals in health care and welfare consist of both static and very dynamic permissions and admissions. Due to that, the content of attribute certificates varies from case to case (see section 3.2.). Basically, static permissions are issued by health authorities, dynamic permissions may be issued even by employers (hospitals, clinics). Static qualification and authorization attributes can also be connected with dynamic permissions and admission, for example by a supervisor or administrator within the IT environment of a hospital. This kind of realizing application security functions is even possible only identity-based.

Furthermore, attribute certificates can be used for exchanging data between hospitals more efficiently, where there is no administrator ruling access rights between two health establishments. This has to be done certificate-based, of course supported by local access policies. But even in a national context, data exchange including related access rights is a difficult issue because of often decentralized structures with organizations belonging to different business models facing a different legal basis. There are public hospitals and private ones, denominated clinics and GPs, health insurance companies and health providers, and much more. Nevertheless, attribute certificates are used to control access in an efficient way.

3.4.2. Example 2

In the aforementioned context, the handling of access rights based on attribute certificates is rather simple compared with data exchange cross-border. There is no general model of trust in healthcare just based on a profession or a title. There is only a model of trust based on functions of health professionals, their qualifications, and their local (in this context national) authorizations. But even here, a secure exchange of highly sensitive patient-related medical data and furthermore, the growing mobility of people must be taken into account.

Secure access to patient-related medical and administrative data guaranteeing both security and privacy is one of the main challenges of nowadays data exchange procedures within health care and welfare. One way of getting access to this kind of data even crossing national borders could be managed by using specific trustworthy applets.

To obtain further experience of this idea, a European project called HArmonisation for the secuRity of web technologies and aPplications – HARP [HAR00] recently started including experienced partners from Greece, Israel, the Netherlands, Norway, the U.K., and Germany. The project shall demonstrate the WWW-based exchange of medical data using downloadable software applets. In this context both public-key certificates and attribute certificates play an important role. The former ones are used for strong authentication as well as to sign and to encrypt files (applets, documents, images, etc.) whereas the latter ones let the communication partners rely on the profession of each other concerning qualification and authorization. This is especially true for any kind of communication and co-operation between hospitals in far regions or even for data exchange crossing national borders. In the following, we will explain the benefit of the project by regarding a common fact.

Nowadays, it is very familiar and usual to spend holidays in another country, getting there for business reasons for a few days or even longer, or getting cured in another country. An example for the latter one is the use of the very healthy conditions close the Dead Sea in Israel for patients from European countries suffering from asthmatic diseases. The mobility of even "sick" persons leads to

regular visits in the context of the treatment and sometimes also to unexpected emergency cases not only caused by accidents.

Initially, we sketch a typical scenario that demonstrates the basic idea and concept of exchanging patient-related medical data between countries in a secure and trustworthy manner: Consider the situation, that a German tourist visits a Greek island. A motorcycle accident is the reason for the tourist to go the Greek local clinic. His health insurance card provides administrative data and contact details of the patient. Additionally, in a German Hospital a patient-related electronic patient record with all historical data exists. Based on the patient's consent, the local Greek doctor is granted limited access in order to download and execute various Java applets from the patient's German hospital site for the treatment (see figure 2).

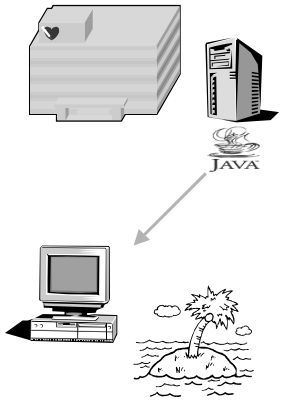

Figure 2. Secure download of applets

As shown in figure 3, the Greek doctor uses these applets for visualization of medical data, for annotation of visual data (e.g., medical images), for a remote database access, for an update of medical records, for any assistance in reaching diagnosis, or to examine and annotate an X-ray image of the patient and store back the annotated image.

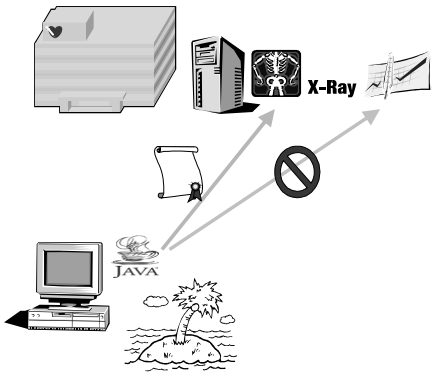

Figure 3. Secure access to medical data

In order to provide a well-functioning security infrastructure for the scenario above, different aspects have to be considered in more detail. First of all, a very fast access to a restricted amount of medical data is very essential for the life and the health of patients. But this cannot be achieved easily, having both the different time zones and also often different work-related behaviors in mind.

To provide medical data, initially a national or regional health insurance provider, a health care provider, or even a company starts developing a piece of software – here: an applet. The applet is designed to give other health care actors access to specific data within a medical database via Internet using WWW and is based on national or regional policies. Both for integrity and for non-repudiation of origin reasons, this applet has to be signed by its originator. Additionally, the provider adds the related attribute certificates attesting the professional qualification (here, e.g., a qualification as a well-established provider of medical software) and the professional authorization (here, e.g., as a provider accepted by health insurance companies). So both public-key certificates and related, bounded attribute certificates get involved.

In a next step, the source code of this applet can be checked and proven by an official authority, perhaps by a TC or TTP. In some of the European countries, this kind of authority already exists. In Germany, a similar authority is, e.g., responsible for checking, proving, and certifying all software and hardware components for a trustworthy system creating digital signatures.

After the software might have been proven to be trustworthy and to be without obvious software bugs, the official authority issues a specific public-key certificate for the software as this may be requested for SSL or TLS end-to-end connections, and an attribute certificate stating whether the source code and the software itself has been checked or not. Then, the same authority signs the applet for both integrity and non-repudiation of origin reasons. And again, beside the public-key certificate(s) related attribute certificate(s) are used stating the role of the signing authority as a trustworthy and well-established official (public or private) authority. Finally, all related certificates for the applet are communicated to a publicly available directory service.

The certified applet will then be uploaded to the trustworthy server of a clinic, a hospital, or a health care provider in order to allow controlled access to the data of this organization. Based on both the signatures of the software provider and the official authority, the user can rely on the content and the integrity of the applet. Finally, the piece of software is again signed, this time by the clinic or hospital. Adding their own signature for non-repudiation of origin reasons, this states that the applet is seen as being acceptable and reliable for data access controlled by the software.

Last but not least this example includes the health professional himself who is willing or requested by the patient to get access to the medical and administrative information items of this person. Based on his set of attribute certificates and the overall professional framework ruling access rights and permissions throughout Europe, he signs an order to download the aforementioned software applet. The related download or access procedure is of course securely logged and audited. After having checked all relevant public-key certificates and attribute certificates (of provider, authority, and hospital) the doctor is able to use the software providing him with a controlled access to exactly the data items he needs for the treatment of the patient.

This example explicitly shows how both public-key certificates and attribute certificates could be used in the context of software for medical applications. As already mentioned, in most of the real cases more than one key pair and one certificate are requested.

Of course the example tried to simplify access rights issues and the professional framework to handle these rights. The procedure of exchanging patient-related medical data between countries in a secure and trustworthy manner has to be based on existing legislation and related regulations both on the technical (signature) and the professional site (professional acting schemes). In the following, beside conclusions and future work we will also explain the legal status in more detail.

4. Conclusions and future work

In the previous sections we focused on existing solutions, prototypes, and European as well as national projects, activities, and initiatives. A lot of work has already been done establishing a European security infrastructure for the health care and welfare sector. But of course the existing problems should not be underestimated, as there are:

- unequal jurisdiction with respect to the borders;
- related to the latter: different systems for accounting, billing, and reimbursement of treatment procedures crossing national borders;
- national health policies which are still contrary to the European perspective from an administrative point of view;
- both centralized and de-centralized health care systems in the different European countries, and
- more than one actor (group concepts) in terms of diagnostic or therapeutic teams, teams within a pharmacy, or teams within a department of a clinic, as well as
- the lack of existing applications using attribute-certificate-based security infrastructures.

In the following paragraphs we try to explain at least a few aspects in a more detailed manner, and the intention is to start with the legal basis.

There is a huge difference in the viewpoints between the Internet technology mainly used and the established laws and regulations. Internet means a global market place in the world of bits and bytes based on multi-media techniques whereas laws are always (and still) related to a national situation in the material world of papers using uni-media techniques.

Several European countries have already adopted and adapted existing European law (e.g. Sweden, Norway). From this point of view they do not distinguish between electronic communication within a country or between countries. But that is not yet common because some of the countries including Germany have a delay in this process of making European law a national one. So in Germany, most of the pending items concerning data exchange with other countries are ruled by national data protection and data security legislation, e.g., the German Data Protection Law [BD99]. At least for all kind of data storage and exchange the consent of the patient is requested by law.

To overcome these gaps, Europe has started several initiatives, with some that should be shortly mentioned here. First of all it is the Electronic Signature Directive [ESD99] to be illuminated along with a Draft, and furthermore, it is the Data Protection Directive [DPD95]. They all have in common that they reflect European law with national implementations. All of them affect the health care and welfare sector directly or indirectly because even e-commerce is just a new way to serve the billing procedures between the actors of a treatment process.

The European Electronic Signature Directive has been established in 1998. It is technology-independent and tries to serve a free market for products and services. A legal recognition is provided by specifying requirements for signature products and related services. Together with new Draft Directives on the Issuance of Electronic Money, established in 1998, they provide a basis for e-commerce not only for health care and welfare. The draft mentioned is focussing on a supervisory framework for non-bank issuance of electronic money. A definition of the term “electronic money” as some sort of a monetary value is given there which

- is stored electronically on an electronic device such as a chip card or a computer memory;
- is accepted as means of payment by undertakings other than the issuing institution;
- is generated in order to be put at the disposal of users to serve as an electronic surrogate for coins and notes, and

- is generated for the purpose of effecting electronic transfers of limited value payment orders.

In addition to that, another Directive ruling electronic commerce [ECD99] by liability of intermediaries, codes of conduct, and the out-of-court settlement of disputes is already in place.

On the other hand, the European Data Protection Directive of 1995 directly affects the exchange of medical information as it rules the protection of individuals with regard to the processing of any personal data and on the free movement of such data.

Last but not least, the European Commission tried to rule the aspect of advertizing via Internet. This did lead to a framework to fine misleading, corruptive, harming, confusing, and comparative advertizing issues. Also this directive has an influence on the health care and welfare sector as far as new methods of treatment, new medication, curing, and general health-related information are concerned.

To conclude from the aforementioned it has to be said clearly that Europe is characterized by a diversity of different national rules slowly developing towards a harmonized European legal framework. This includes both the necessity of such a legal framework and a highly developed threat and risk management.

The most critical point indeed seems to be the applications aspect (even if most of the problems related to definition, specification, development, implementation, and installation of a security infrastructure are already solved) as one of the key issues for any kind of installation of new services is the user awareness and acceptance issue. And both awareness and acceptance can only be achieved by providing all partners of the security infrastructure with up-to-date services and with applications which really focus on their daily work including improvement of time-consuming processes.

References

[BD99] Der Bundesbeauftragte für den Datenschutz: Bundesdatenschutzgesetz, 1999. (German Data Protection Law) http://www.bfd.bund.de/information/info1 /info1.htm

[DPD95] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 of 23/11/1995. http://europa.eu.int/comm/ dg15/en/media/dataprot/ law/index.htm

[ECD99] Electronic Commerce Directive of the E. C. COM (1998) 586 final, O.J. 1999/30/04. http://www.ispo.cec.be/Ecommerce/legal.htm

[ESD99] Gemeinsamer Standpunkt (EG) des Rates im Hinblick auf den Erlass der Richtlinie 1999/EG des europäischen Parlaments und des Rates über die gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Stand 8. Juni 1999. Engl. Version (Electronic Signature Directive): http://www.accurata.se/QC/index.html

[HAR00] European Project HARP. 2000-2001. www.telecom.ntua.gr/~HARP/HARP/HARP.htm

[HC95] Claus O. Köhler, Otto Rienhoff, and Otfried P. Schaefer (Eds): Health Cards ’95, Frankfurt. IOS Press Amsterdam, Berlin, Oxford, Tokyo, Washington D.C., 1995. Vol. 26 of Studies in Health Technology and Informatics.

[HC97] Laurens van den Broek and Anne J. Sikkel (Eds): Health Cards ’97, Amsterdam. IOS Press Amsterdam, Berlin, Oxford, Tokyo, Washington D.C., 1997. Vol. 49 of Studies in Health Technology and Informatics.

[HPC99] Gemeinsame AG der Kassenärztlichen Bundesvereinigung (KBV) und der Bundesärztekammer (BÄK): Deutsche HPC-Spezifikation Ärzte (The German specification of an electronic doctor’s license) Version 1.0, July 1999. http://www.hcp-protocol.de

[ISO88] ISO/IEC 9594-8 | ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection – The Directory. Part 8: Authentication Framework, 1988.

[ISO93] ISO/IEC 9594-8 | ITU-T Recommendation X.509: Information technology – Open Systems Interconnection – The Directory. Part 8: Authentication Framework, 1993.

[ISO97] ISO/IEC 9594-8 | International Telecommunication Union: ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, 6-1997.

[Lain99] Simon G. Laing: Attribute certificates – a new initiative in PKI technology. Baltimore – Library – Whitepapers 1999. http://www.baltimoreinc.com/library/whitepapers/acswp-hm.htm

[Med98] Branko Cesnik, Alexa T. McCray, and Jean-Raoul Scherrer (Eds.): MedInfo ’98 – Proceedings of MedInfo ’98, Seoul, Korea. IOS Press Amsterdam, Berlin, Oxford, Tokyo, Washington D.C., 1999. Vol. 52 of Studies in Health Technology and Informatics.

[MIE00] Arie Hasman, Bernd Blobel, Joachim Dudeck, Rolf Engelbrecht, Günter Gell, Hans-Ulrich Prokosch (Eds): Medical Infobahn for Europe – MIE 2000 Hannover, Vol. 77 of Studies in Health Technology and Informatics, IOS Press 2000.

[PKIX99] Public-Key Infrastructure (X.509) (pkix). http://www.ietf.org/html.charters/pkix-charter.html

[RiSA78] Ronald L. Rivest, Adi Shamir, Leonard A. Adleman: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, Vol. 21, Nr. 2, Feb 1978, pp. 120-126.

[SigV97] Bundesamt für Sicherheit in der Informationstechnik: Verordnung zur digitalen Signatur (Signaturverordnung – SigV), 1997. http://www.iid.de/iukdg

[TH97] TRUSTHEALTH I/II: Trustworthy Health Telematics, 1997-2001. http://www.ehto.org/ht_projects/ html/dynamic/130.html resp. 131.html