MEDINFO 2001
V. Patel et al. (Eds)
Amsterdam: IOS Press

Electronic Signature and Certification Models in Health Care

F. De Meyer[a], G. J. E. De Moor[a], F. H. Roger France[b]

[a]Dept. of Medical Informatics, University Hospital of Ghent, 9000 Ghent, Belgium

[b]Centre for Medical Informatics, Université Catholique de Louvain-UCL, 1200 Brussel, Belgium

Abstract

Recently, Belgian legislation has enabled the practical use of electronic signatures. Several implementation options are still open and different models for deployment on a wide scale are possible. This document describes two models that can be applied to the healthcare domain and summarises the recommendations as issued by the Belgian Health Telematics Standards Committee

Keywords:

Medical Informatics, Security, Electronic Signature, Digital Signature, Trusted Third Party.

The legal context

Electronic signature legislation has been introduced for the first time in Belgian history in the social security Royal Decree of 16th October 1998. This decree was put in place to allow the use of the so-called SIS card or social security card. The goal of the introduction of the SIS card is to reduce the administrative formalities for the socially insured, the employers, care-providers and the administrations of the social security services. The card serves mainly as a means to unambiguously identify the socially insured in an electronic way and as a proof and indication of the social insurance status of the holder of the card. It is not a smartcard because it has no processing capabilities. It is a storage card. Nevertheless, the SAM card that is used to access the SIS card is a smartcard but is not a health professional card as such. Moreover, use of the card is limited to social security purposes.

On a European level, the directive on a community framework for electronic signatures is a reference document that all European countries have to implement [1]

Moreover, Belgian civil law has been adapted so that article 1322 expands the meaning of the term 'signature' to include a digital collection of data that can be created electronically.

The terminology used in legislation is 'electronic signature' in order to stay as generic as possible and to avoid adaptations in legislation as technology evolves.

It should be stressed that the European directive does not make accreditation of certification authorities compulsory.

PKI models

Centralised ID card model with decentralised role attribution

The starting point for the centralised ID card model is that an electronic national identity card is issued to all citizens and residents. This ID card has the form factor and functionality that can be expected from smartcards and could include:

- signature function,
- encryption function,
- authentication function.

Such an ID card normally contains the name, a national identification number, gender, date of birth and nationality of the card holder and identification of the issuer. On the outside, it should contain a clear picture of the holder. A Belgian ID card does not necessarily mean that the holder has the Belgian nationality. It can, for instance, be a permit that allows a person to stay in the country for a specific reason and a predetermined period of time.

Signatures created with this card have nationwide (and possibly even cross border) legal value. The card is used whenever the cardholder has to authenticate himself or sign a document, be it in the private or public domain.

The certificate that contains the public key part associated with the user is put on one or more directory servers that can be accessed publicly and without charge by any verifying entity.

The certificate only contains the identity and key related information of the cardholder.

The meaning of an electronic signature as described above is equivalent to the handwritten signature that is currently used. It proves an identity and not a role.

Such model assumes that each health professional in Belgium holds a Belgian ID card. This card can be used for signature and authentication purposes. Authentication means that the holder can prove his identity electronically by means of the card.

Health professional specific functions can be built on top of this platform. For health professionals the following elements could be needed as well:

- certification and statement of the professional or qualities of the holder. For instance: "Mr. X. is a Medical Doctor, cardiologist",
- license to practice and by whom it is issued,
- one or more roles.

The first two elements are generic and usually invariable for a long time. The administration can be done nationally or regionally by e.g. the Council of Physicians or a governmental institution. The requirement is that these organisations maintain (or obtain) registration information about all health professionals under their control.

The role of a health professional may have significance over a large geographic area but is usually assigned by a local organisation. A few examples of roles are:

- a general practitioner employed by an insurance organisation,
- a physician that is head of a hospital department,
- a self employed nurse,
- a self employed physiotherapist or dentist, ...

The granting and revoking of role certificates is a function that should be done locally by the organisation that assigns the role to the health professional. A role is expressed in a certificate. The main elements of a role certificate are:

- The identity of the certificate holder.
- The identity of the organisation issuing the certificate.
- The signature and identity of the person within the local organisation that is responsible for the issuing of role certificates.
- Proof or reference (i.e. a certificate or certificate identifier) that the issuing organisation is allowed to issue role certificates.
- The role that is attributed to the certificate holder.
- The validity period of the role certificate.

All these elements need not be very long, so that the size of a certificate can be kept rather small. The role can be given by a role identifier that references a policy document that describes in extenso the details and constraints of the role.

Authorisation to local sources is a local matter. The signature and authentication functions of the health professional card support the authorisation process but the card does not contain authorisation information as such.

Decentralised key issuing model

If health professionals do not already hold a smartcard (issued by a central organisation) that contain signature and authentication keys, the decentralised issuing organisations have to deliver smartcards that are personalised and that contain the necessary keys. On top of that, role certificates have to be issued and maintained as well, depending on the variant of the decentralised model.

Two variants on this model are possible:

- Role, identity and signature key are combined
- Identity and keys are kept separate from the roles.

In both variants, a complete PKI infrastructure has to be set up by the decentralised organisations for the issuing of smartcards to health professionals. Moreover, the identity related information only has significance within the issuing domain, in casu health care. In the case where ID and role are combined a health professional will produce a different signature for each of his roles. This can make the process of verification and role management more complicated.

Some practical scenarios

This section contains some scenarios that relate to various aspects of the deployment and use of digital signatures. Some parts in the scenarios are specific to digital signatures; others are generic and apply to any type of electronic signature. The scenarios are based upon the assumption that a public key infrastructure, based on smartcards, is used. This document concentrates on signatures but large parts are equally valid for keys used to encrypt or to authenticate.

The scenarios will highlight differences between the various model described above.

Obtaining a signature key pair

Before a person can digitally sign a document, he has to possess a smartcard containing at least a private signature key. A smartcard is a tamperproof environment in which the cryptographic key used to sign is securely stored and where the actual encrypting part of the signature is executed. The public key part of the signature key pair has to be associated to the identity of the key holder, which is done in the public key certificate, and made publicly available.

If a health professional already has an ID card that enables him to sign electronically, he already has a signature key pair and this step can be skipped. This reduces the complexity of signature support significantly since all effort can be concentrated on the roles of the cardholder. This scenario further deals with the model where the health professional already has a centrally issued electronic ID card.

If not, the health professional has to go to the registration authority (or to the certification authority if both functions are combined into one organisation) and present his credentials. What credentials are needed, including form and content requirements need to be stated in a written policy document. The policy statement can e.g. contain the following requirements:

- Handover of an authentic birth certificate.
- Presentation of the paper based ID card and handover of a copy of it.
- A handwritten signature of the health professional on a document stating that he has read and understands the policy requirements for the use and handling of the smartcard that he is applying for.

Obtaining an attribute certificate

Once a user has an electronic ID and a smartcard that can be used for signatures, certificate issuing and application becomes quite simple. Some examples:

1. A health professional has finished his studies and has obtained the diploma of physician. He submits this paper document to the Council of Physicians. The Council of Physicians issues a registration number. Supposing that the applicant already has a nationally registered electronic ID and that the Council of Physicians has access tot a trusted source for verification of the electronic ID and the ID on the diploma, it could automatically issue an electronic certificate stating the qualifications of the health professional. The certificate is sent by e-mail to the health professional and is optionally published on a directory server.
2. A health professional is employed by a hospital. The following procedure is followed.
    - He inserts his electronic ID card into a card reader of the personnel department. He signs (i.e. he pushes an 'accept' button and inputs his pincode) an electronic statement saying that he is about to receive a role certificate of the hospital and that he has read and understood the role certificate policy stating the use and constraints of the role certificate.
    - He withdraws his ID smartcard.
    - The hospital checks his certificate that states his role as health professional (e.g. a medical doctor, nurse, ...)
    - He receives an electronic copy of his certificate(s), a paper copy of the policy and perhaps some practical information like his e-mail address at the organisation.

Signing a document

Once a health professional has received his smartcard he can put his electronic signature on an electronic document or on a message, provided of course that the applications he is using have signing capabilities.

Signing a document consists of the following steps:

- Either the user clicks a 'sign' button or the application prompts the user automatically to sign.
- The user selects the role(s) he wants to include in the signature.
- He verifies what he is about to sign.
- He inserts his smartcard (if not already done) and inputs his pin code via the keyboard of the pc or via a separate keypad.

Verifying a signature on a document

When an application is signature enabled, it will automatically check all incoming documents for signatures.

- When a document has not been signed or when the signature is invalid, it will issue a warning and state the reason. Warnings are also displayed if a role or key certificate is not valid anymore.
- When the signature is valid it will display information about the author.

The most critical element in the verification process of signatures and roles are the key and role certificates. The policy of the organisation should also specify the acceptable period during which certificates and revocation lists can be held locally without refreshing (i.e. downloading up-to-date information from a directory service).

Revoking a key pair

- A health professional cannot find his smartcard anymore. He informs the personnel department and requests a new card. The policy requires that the card and certificates are revoked from that moment on and new ones are issued.
- A health professional quits the hospital he is working for. From that moment on, the personnel department revokes his locally issued role certificates.

It is only at verification time that can be discovered if a certificate was revoked at the time the signature was made. Therefore a regular updating of certification revocation lists should be defined in the verification policy.

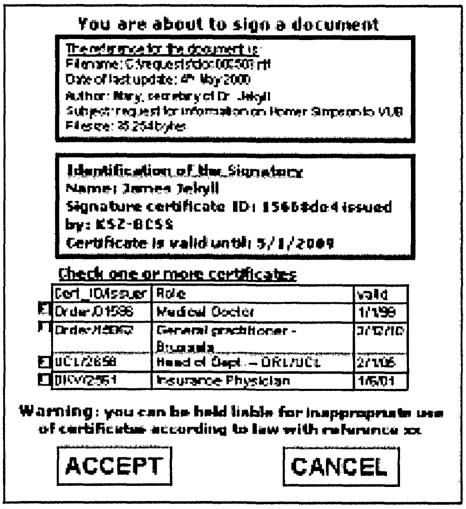
There are schemes that allow a stepwise revocation in which the certificate can be put on-hold in an early step and where the revocation can still be undone as long the final revocation has not been done.

When key and attribute certificates are distinct, it is possible to revoke specific attribute certificates without having to revoke the other certificates as well. This can be particularly interesting when certificates contain relatively volatile information, such as employment data.

User interaction with security services

Security services should be as transparent as possible to the users. Figure 1 shows how an interface for signing an electronic document could look like.

- The user needs to know what he is signing. That can be done by showing the document or message he is signing, but also by reference to the document itself (name, size, date of latest edit, ...).
- The user needs to recognise his identification and the information on the certificates.
- The user has to be given the choice in which capacities he is going to sign. When a conflict of roles can arise, he must be aware of the ethical rules and legislation that exist.



You are about to sign a document

The reference for the document is:
Filename: C:\request\doc00507.rtf
Date of last update: 4th May 2000
Author: Mary, secretary of Dr. Jekyll
Subject: request for information on Homer Simpson to VUB
Filesize: 35 254 bytes

Identification of the Signatory
Name: James Jekyll
Signature certificate ID: 1566#do4 issued by: KSZ-BCSS
Certificate is valid until: 5/1/2009

Check one or more certificates

	Cert_ID/Issuer	Role	valid
☒	Order/01586	Medical Doctor	1/1/98
☒	Order/45062	General practitioner - Brussels	3/12/10
☒	UCL/2658	Head of Dept. – ORL/UCL	2/1/05
□	DKV/2561	Insurance Physician	1/6/01

Warning: you can be held liable for inappropriate use of certificates according to law with reference xx

Figure 1 – signature interface

Generating a signature should always be a conscious act. Misuse of mandates cannot be prevented technically (for this would limit correct use in other situations). The user has to be aware that he is liable for misuse and that all misuse is considered deliberate.

Recommendations

Recommendations on digital signatures

The digital signature techniques and procedures offer more guarantees and advantages (e.g. in terms of integrity and authentication) than hand-written signatures. Digital signatures should therefore be recognised as valid signatures and their use should be - when appropriate - encouraged in the healthcare sector.

The provision of registration and certification services is an essential requirement for achieving the levels of trust, security and quality in electronic communication as demanded by the healthcare sector.

In order to get the 'best practice', compliance is recommended with international laws, standardised rules and agreements applicable to such services (cf Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, published in the Official Journal of the European Communities, 19.1.2000). Liaison will also be established with the mixed national committee "Information Society for the Public Sector".

A distinction has to be made between identity certificates and attribute certificates. The assessment of the identity and of attributes can be executed by different registration authorities. Several certificates can be associated with one pair of keys. The owner of certificates should be able to use every certificate separately.

By Belgian Law, the Chamber of Physicians and the Chamber of Pharmacists are the responsible authorities for the registration and revocation of physicians and pharmacists. In Belgium, there should be an agreement on the choice of the organisation(s) maintaining a complete directory with appropriate identification data on healthcare professionals in order to assess e.g. their identity and professional qualifications. The Ministry of Health and Social Affairs could undertake such an initiative together with other relevant organisations (eg. Chamber of Physicians/National Medical Council, Council of Pharmacists...) and in co-operation with the Third Party Payer (RIZIV-INAMI). Such platform could serve as national registration authority for the professional qualifications and as interface with certification service provides (i.e. private companies acting as Trusted Third Parties).

A framework should define the roles, the rights, the responsibilities and the obligations of the different actors involved in secure services implementing digital signatures (cf. liability issue).

Where digital signatures are going to be used, healthcare information flows and communication scenarios (with type and purpose of message, type of sender and receiver, identity certification need, attribute certification need,) should be identified.

A key pair used for digital signature purposes should never be used for other purposes.

Proof of identity should be stored as close as possible to the person as such. Private keys used for digital signatures can be stored on smartcards which are considered safe.

Access rights to resources should be kept close to the system and managed by the organisation responsible for the decision and/or implementation of access.

Multifunctionality should be promoted; i.e. it should be made possible of having several attribute-certificates linked with one single identity.

In the case a conflict of interest might arise from the different qualifications of a single person it is the responsibility of that person to use the right attribute-certificate(s) (the inclusion of a certificate should be a 'conscious'act: this is a non-technical issue). User applications should nevertheless follow procedures to warn, ask and incite, where appropriate, to include the 'right' certificates.

Attribute-certificates can – under certain circumstances – be used without identity-certificate or with pseudonyms.

Certificates should never be delivered behind one's back. Verification should be made possible. The person should be informed.

Recommendations on Trust Services

In the Health Care sector there is an absolute need for services from Trusted Third Parties (TTPs). The roles of such trust service providers can be very diverse as they can offer services in various security domains such as Public Key Infrastructure (PKI)- support (key management, smartcard personalisation and distribution, directory services etc.)Anonymisation/Pseudonymisation services (Privacy Enhancing Techniques, PET), Notary services (eg time and date stamping,proof of delivery).

Priorities are amongst others the PKI services (to enable the implementation of digital signatures in Healthcare) as well as anonymisation and pseudonymisation services through TTPs (to enable the unlocking of data for eg medical research and management purposes). Guidelines for such TTP services in Healthcare should therefore be drafted (eg for PKI- and PET-services).

Conclusions

Health care is only one domain where electronic signatures are introduced. Health care has its specific requirements and procedures for the signing of documents. Electronic signatures will only provide sufficient proof when they are supported by adequate registration and certification infrastructures [7]. It is also necessary to develop message and document formats that allow the use of efficient and open structures for including attribute certificates and a flexible attachment of signatures. It is recommended that the electronic world follows the traditional paper based world in its method of signing and communication roles. The person signing should be able to choose in which role(s) he is signing. Legislation is needed as an incentive to prevent misuse of role certificates by health professionals when signing a document or message.

A costly infrastructure can be saved and flexibility gained if health care specific applications can build on top of already existing PKI services, e.g. nationally provided [8]. In that case, health care could concentrate on the specifics of its domain, dealing with authentication and roles of health professionals. Rules for authorisation should be locally administered by the healthcare enterprise the health professional is associated with. Local authorisation and certification applications however could make use of the electronic ID smartcard of the health professional.

Electronic signatures are only trustworthy when the certificates needed to verify signatures [9] and roles have been provided through services delivered by Trusted Third Parties.

References

[1] Directive 1999/93/EC of the European Parliament and of the ^{council} of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, 19.1.2000.

[2] Draft TR 101 xxx v.0.4.2(1998-11), Telecommunications Security ; Electronic signatures standardization report, ETSI, 1998

[3] Cryptography and Data Security, DER Denning, Addison- Wesley 1982

[4] Social Security Royal Decree of 16.10.98

[5] Recommendations for Internation Action, Ray Rogers et al.,IOS press, 1999, pp.86-91

[6] Personal Medical Information, Ross Anderson, Springer Verlag UK, 1996, pp. 19- 26

[7] Spécifications techniques de l'infrastructure de sécurité AGORA, Partie III, 30/6/98

[8] Ministry of Social Affairs, Public Health and Environment. 3 May 1999. Royal Decree on Telematics Standards for the Healthcare Sector Belgisch Staatsblad 30.07.1999, pp 28464-69, pp 28501-502.

[9] F. De Meyer, F. Allaert, G. De Moor. Argument faveur de la reconnaissance de la valeur juridique de la signature électronique. Informatique et Santé, 1996 (8): 23-25. Springer-Verlag.

Address for correspondence

F. De Meyer

<Filip.DeMeyer@rug.ac.be>