The New Navigators: from Professionals to Patients
R. Baud et al. (Eds.)
IOS Press, 2003

Electronic Signatures for Long-lasting Storage Purposes in Electronic Archives

Peter Pharow and Bernd Blöbel

Institute for Biometry and Medical Informatics, University of Magdeburg, Germany

Abstract

Communication and co-operation in healthcare and welfare requires certain Trusted Third Party (TTP) services describing both status and relation of communicating principals as well as their corresponding keys and attributes. Additional TTP services are needed to provide trustworthy information about dynamic issues of communication and co-operation such as time and location of processes, workflow relations, and system behaviour. Electronic signatures based on asymmetric cryptography are important means for securing the integrity of a message or file as well as for accountability purposes including non-repudiation of both origin and receipt. These electronic signatures along with certified time stamps are especially important for electronic health records (EHR), electronic archives in general, and other typical purposes of a long-lasting storage. Apart from technical storage problems (e.g. lifetime of the storage devices), this paper needs to look for mechanisms of e.g. re-signing of messages, archive details, or whole archives.

Keywords

Public Key Infrastructure, Trusted Third Party, Electronic Signature, Time Stamp, Electronic Archive

1. Introduction

For nowadays high quality and efficient care requirements (generally called Shared Care principle), a well-developed communication and co-operation between all partners within the health care and welfare domain is an inevitable prerequisite. Such communication and collaboration relationship has to be provided in a trustworthy and secure way. The category of trustworthiness is related to both communication security services and application security services. The former comprise several categories like strong mutual authentication of communicating principals, integrity of messages exchanged, confidentiality of the content of these messages and availability of information communicated, accountability of principals (including non-repudiation services) for both data and actions provided, and finally different notary's services.

Application security services concern a specific authorisation of principals with access to the system, integrity of data within data bases or electronic archives, confidentiality of stored data, availability of information recorded, stored, and processed, and accountability of principals (including non-repudiation services) acting within the system, and again several notary's services. This document intends to specifically deal with electronic signatures for integrity and accountability reasons. A more detailed description of the mentioned security categories as well as related – and implemented – solutions can be found in [1].

The paper does not intend to explicitly deal with the aspects of creation and verification of an electronic signature and a digital one in particular. Instead of, it document is mainly focused on the use of digital signatures for purposes of long-lasting archives. The following paragraphs including figure 1 simply intend to describe the mechanisms of creation and verification of both the hash value and the digital signature itself.

2. Integrity and Accountability

The majority of nowadays security services are based on a Public Key Infrastructure (PKI) using asymmetric cryptographic algorithms (in general it's the well-known RSA algorithm). In that particular context, a Trusted Third Party (TTP) is needed to assure the correctness and validity of certain statements about status and relation of the principals. Such assurance is normally provided via certificates or certificate revocation lists (CRL) respectively, and is of rather static nature. Because information and processes in the context of interoperability in the health care and welfare domain are often highly dynamic, there is a strong need for characterising the (informational) workflow. Among others, this includes the informational context, the identification of information and messages as well as the time and partly also the location of the informational process. Such "information about information" is very important indeed.

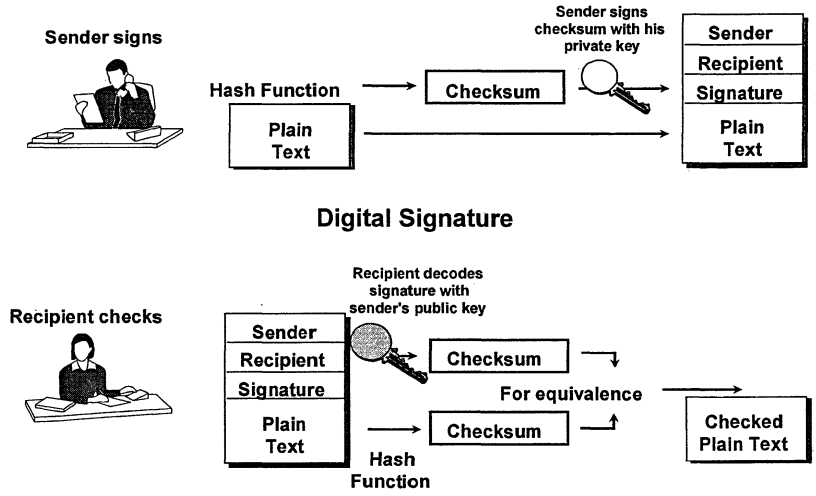

Figure 1: General Description of Digital Signature Creation and Verification

Regarding collaboration and co-operation within or even between health care and welfare organisations, the categories of integrity and accountability need to be considered especially important for electronic archiving of person-related administrative and medical data. From the electronic health record (EHR) point of view, this specific kind of data collection shall contain all person-related information with regard to health. This could mean that a certain information item might be accessed even 30 and more years after it had been stored – and it needs to be kept unchanged all that time. So both the technical integrity of the information items (by the hash value) and the accountability of the information items (the signature created by the person or system that has stored the information long time ago) need to be verifiable. This requires specific electronic signature mechanisms and procedures that are long-lasting and long-verifiable – and therefore long-provable – ones. A digital signature ensures integrity, authenticity and accountability of information. Encoding ensures confidentiality of information. The combination of both services ensures data security and privacy. This is an important security aspect not only for the health care and welfare domain.

3. Requirements for long-lasting Data Storage

Mankind has long been very familiar with aspects and requirements for a long-lasting documentation of important information, such as some very old paintings in caves, on walls and on rocks, the well-known stony plates in ancient Egypt and Greece, and the papyrus documents. This kind of documentation has often been accompanied by ancient forms of time stamps in paper form, such as data marks on theses plates or papyrus rolls, on ancient "newspapers" and letters, or – in the late centuries – by the traditional post marks. They are a specific kind of proof of the actuality of a piece of information.

However, nowadays more and more business and private activities are performed electronically via the open Internet or via companies' Intranet architectures. Here too, a reliable proof of integrity and accountability is required in order to establish security concerning the validity of electronic transmissions and electronic storage of information. In particular in the case of contract-relevant or content-relevant messages and files, orders and purchases, the aspect of archiving any kind digital data, or the exchange of extremely sensitive medical data, the aspect of electronic signatures for all these specific activities plays a major role.

An electronic signature means data in electronic form that are attached to, or logically associated with, other electronic data in a unique way and that therefore serve as a method of authentication. An advanced electronic signature is uniquely linked to signatory and is capable of identifying the signatory. It needs to be created using means the signatory can maintain under his sole control. So an advanced electronic signature is always linked to the data so that any subsequent change of data is detectable. This specific feature of electronic signatures has both a technical and a legal meaning.

The current legislation in most of the European countries – based on the European Electronic Signature Directive (EESD) [2] and the related and technically supporting European Electronic Signature Standardisation Initiative (EESSI) [3] – has defined or at least given an orientation towards electronic signature algorithms that are able to guarantee a certain security level up to 5 years depending on the available key length of, e.g., 1024 or 2048 bit. This aspect is mirrored in certain regulations with regard to certification service providers and their responsibility in terms of liability. In Germany, the aforementioned European Electronic Signature Directive has been adopted by the German Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations ("Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, SigG") and the related German Electronic Signature Ordinance ("Signaturverordnung, SigV") [4].

Contrary to this more general and domain-independent legislation related to electronic signatures, the health care and welfare domain has a lot of specific requirements with regard to any kind of archives for health documents and images. With regard to the development of the future electronic health record (EHR) architectures and their demand for covering the whole history of life of a human being, these both health-related and person-related information items need to be stored and processed in a very secure and trustworthy manner. As another specific example, X-ray images must be stored unchanged for at least 30 years in most of the European countries. This requires certain mechanisms of archiving, signing, and re-signing these information items either on item level or on group level.

Based on legislation in some EU countries as well as on experts' calculations with regard to the proposed "lifetime" of asymmetric algorithms and their keys, TTP service providers normally create key pairs and certificates for signature purposes with a validity

time of up to 5 years. Contrary to that, specific health-related regulations (e.g. for X-ray images) require the storage of patient-related information for up to 30 years and more.

4. Aspects of a Possible Solution

As said already, electronic signatures normally expire after a certain number of years, and so do their related public key certificates and keys. As mentioned in the previous paragraphs, a typical interval for a signature lifetime is 5 years. This restriction is not related to the asymmetric cryptographic algorithm itself but rather to the key length on the one hand and to the fast development on the technical security level on the other as far as new methods of possible attacks are concerned. This means that before the official expiry date the data items stored in electronic archives or registries need to be signed again in order to ensure the requested security level for the next few years.

4.1 Options for the Re-Signing Process

There are at least two different options to perform this kind of re-signing. Either the file content must be completely unwrapped (which very often means decrypted) and afterwards wrapped and signed again using the new encryption key and the new signature key. In this case, only the newly created keys need to be archived in order to guarantee access Or the file content is used in its wrapped (encrypted) form just adding another signature. Both the new signature key and the old keys for encryption and signature need to be archived in this case. The latter model could easily be compared with the aspect of an onion adding a few new shells.

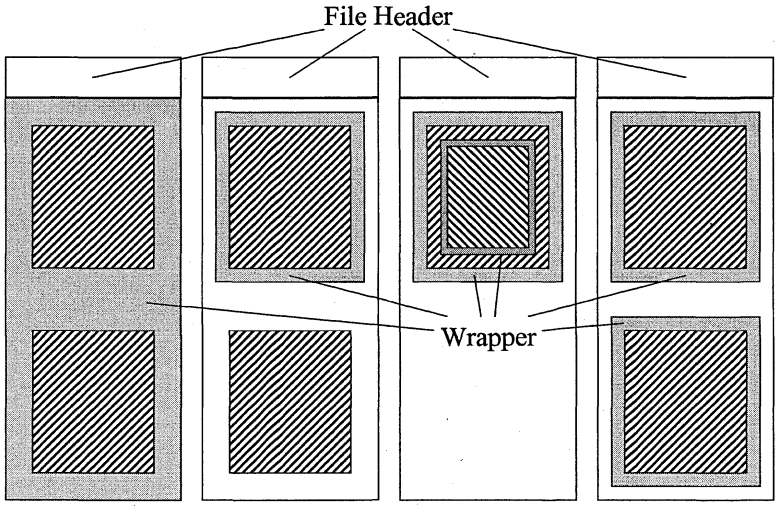

Figure 2: General Description of Wrapping Mechanisms

4.2 Preferred Re-Signing Mechanism

For legal and technical reasons, only the second option of re-signing shall be taken into consideration [5]. This re-signing procedure explained before needs to be performed using a wrapping mechanism (see figure 2 above). Several methods of wrapping are possible. As illustrated above, either a number of items can be easily wrapped in just one single

"envelop", or an envelop might contain a certain number of wrapped and unwrapped items in parallel depending on the level of their own security requirements.

Generally this second method of re-signing means that the content remains unchanged and untouched, and another valid signature is added as a second (third, fourth, fifth, etc.) shell. The advantage of this procedure is obvious. The content could remain encrypted, if necessary, without any confidentiality problems. The electronic (here: digital) signature of the originator remains unchanged so the origination of the medical content can be proved after 20 or even 30 years. The only requirement for this aspect is the obvious need to keep all certificates in a special part of the public directory tree even if they need to be revoked after having expired.

Moreover, another legal questions arises in this context. Who is legally allowed to re-sign medical and administrative information in an electronic health record or an electronic archive? This is mainly an organisational aspect that deals with privilege management and access control of the acting principals. New standards are needed to solve this upcoming problem [6]. From both the technical and the legal point of view it's is not necessary that Health Professionals (HP) become the re-signers of health-related information. It is rather proposed to add the aspect of re-signing to the long list of activities that are performed by an independent notary (in general a trustworthy third party organisation).

The re-signing mechanism described above is similar to the mechanism of co-signatures or group signatures but has nonetheless considerable differences. Co-signing normally means that the co-signer has the responsibility for the content of the signed document or data item whereas the notary can never ever have this responsibility. The notary is not able to "prove" that especially the medical content (letters, images, audio and video streams, single data items, etc.) to be re-signed is correct. He rather acts in the sense of a responsible party for the technical integrity of the document (e.g. by verifying hash values) as well as for the inviolacy of the current electronic (digital) signature of the originator also in terms of the validity of his or her current signature certificate.

Among other organisations and initiatives, the German initiative "Forum Info 2000" has dealt with certain aspects of electronic archiving and related security aspects like long-lasting validity and re-signing, and has provided guidelines and hints on how to perform both integrity and accountability for long-lasting storage of medical person-related information [7].

5. Conclusions

Shared care solutions all over the world have to be based on trustworthy communication and application security services provided by Trusted Third Parties. Beside the well-known TTP services certifying processes and process interoperability (workflow), security services certifying state and relations of principals in longer terms are needed in order to guarantee accessibility of electronic health record architectures and electronic archives in general. This is especially true for the upcoming fast development on electronic health record (EHR) architectures, their requirements, their design, their policy details, and their instantiation and implementation strategies [8].

Provable and auditable mechanisms for the provision of long-lasting electronic signatures and in particular digital ones in the health care and welfare domain are required along with secure and reliable time stamps. Wrapped signatures fulfil both technical and legal requirements as they guarantee both the technical integrity of the signed document or items and the accountability of the originator even decades later. Notaries as re-signing parties act as the responsible partner for the proof of integrity and inviolacy of information

content (hash algorithms) and security shell (digital signature) without a need to tackle aspects of confidentiality of patient-related information because of the absence of a given requirement to unwrap the documentation items in either electronic archives or electronic health record architectures.

6. Acknowledgement

The authors are in debt to the European Commission for the funding of several European research projects and especially to the project partners within "HARP" and "RESHEN" as well as the other regional, national and international partners and organisations for their support and their kind co-operation.

7. References

[1] B. Blobel, F. Roger-France: A Systematic Approach for Analysis and Design of Secure Health Information Systems. International Journal of Medical Informatics **62** (3) (2001) 51-78.

[2] 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 L 013 , 19 / 01 / 2000 p. 0012 – 0020. http://europa.eu.int/ISPO/ecommerce/legal/digital.html

[3] The European Electronic Signature Standardization Initiative (EESSI) – an Industry Initiative in Support of the European Directive on Electronic Signature. http://www.ict.etsi.fr/eessi/EESSI-homepage.htm

[4] The German Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften – SigG): English version, May 16th, 2001. The German Electronic Signature Ordinance (Signaturverordnung – SigV): English version, November 2001. http://www.iid.de/iukdg/english.html

[5] ISO TC 215 Health Informatics: Public Key Infrastructure: Part 1: Framework and overview; Part 2: Certificate Profiles; Part 3: Policy Management of Certification Authority. Technical Specification ISO / TS 17090-1

[6] B. Blobel, R. Nordberg: Privilege Management and Access Control in Shared Care Health Information Systems and EHR. Proceedings of MIE 2003. This volume, Studies in Health Technology and Informatics. IOS Press, Amsterdam, 2003

[7] Forum Info 2000: Forum Informationsgesellschaft 2000; AG 7 Gesundheitswesen (German language). http://www.forum-informationsgesellschaft.de/fig/extern/VorlagenDownload/gesundheitswesen.pdf

[8] B. Blobel: Analysis, Design and Implementation for Secure and Interoperable Distributed Health Information Systems. Volume 89: Studies in Health Technology and Informatics. ISBN 1-58603-277-1. IOS Press, Amsterdam, 2002

8. Address for Correspondence

Address: University of Magdeburg, Institute for Biometry and Medical Informatics
Leipziger Str. 44, D-39120 Magdeburg, Germany

Email: Peter.Pharow@Medizin.Uni-Magdeburg.DE

URL: http://www.med.uni-magdeburg.de/fme/institute/ibmi/dmi