INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS 76 (2007) 442–448

journal homepage: www.intl.elsevierhealth.com/journals/ijmi

Long-term verifiability of the electronic healthcare records' authenticity

Dimitrios Lekkas[a,*], *Dimitris Gritzalis*[b]

[a] *Department of Product and Systems Design Engineering, University of the Aegean, Syros GR-84100, Greece*
[b] *Information Security and Critical Infrastructure Protection Research Group, Department of Informatics, Athens University of Economics and Business (AUEB), 76 Patission Ave., Athens GR-10434, Greece*

ARTICLE INFO

Keywords:
Security
Digital signatures
Notarization
Archiving
Electronic healthcare record (EHR)

ABSTRACT

Purpose: To investigate whether the long-term preservation of the authenticity of electronic healthcare records (EHR) is possible. To propose a mechanism that enables the secure validation of an EHR for long periods, far beyond the lifespan of a digital signature and at least as long as the lifetime of a patient.

Approach: The study is based on the fact that although the attributes of data authenticity, i.e. integrity and origin verifiability, can be preserved by digital signatures, the necessary period for the retention of EHRs is far beyond the lifespan of a simple digital signature. It is identified that the lifespan of signed data is restricted by the validity period of the relevant keys and the digital certificates, by the future unavailability of signature-verification data, and by suppression of trust relationships. In this paper, the notarization paradigm is exploited, and a mechanism for cumulative notarization of signed EHR is proposed.

Results: The proposed mechanism implements a successive trust transition towards new entities, modern technologies, and refreshed data, eliminating any dependency of the relying party on ceased entities, obsolete data, or weak old technologies. The mechanism also exhibits strength against various threat scenarios.

Conclusions: A future relying party will have to trust only the fresh technology and information provided by the last notary, in order to verify the authenticity of an old signed EHR. A Cumulatively Notarized Signature is strong even in the case of the compromise of a notary in the chain.

1. Introduction

Modern healthcare environments exploit the immense advances in Information and Communication Technologies (ICT) in order to increase the quality and the quantity of the healthcare services provided. Several privacy and security problems become much more intense in such shared environments, where healthcare services are offered by multidisciplinary teams of healthcare professionals, to patients and other stakeholders through web-based applications or at least through remote interconnected Health Information Systems (HIS) [1,2]. Besides the privacy and the access control issues, which emerge in a HIS, we will focus on the long-term preservation of the integrity and the origin verifiability (i.e. the authenticity) of electronic healthcare records (EHR). EHR must be preserved at least for the lifetime of a patient or even longer for research or other purposes. The preservation of electronic data for a lifetime is not a straightforward task,

* *Corresponding author*. Tel.: +30 2281097100; fax: +30 2281097009.
E-mail addresses: dlek@aegean.gr (D. Lekkas), dgrit@aueb.gr (D. Gritzalis).

1386-5056/$ – see front matter © 2006 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.ijmedinf.2006.09.010

since ICT are under intense development and are subject to continuous changes. The long-term preservation of EHR may be approached and analyzed from various perspectives, such as future data readability, storage media longevity and security [3]. The value of the archived EHR depends on the existence of a digital signature, which is the principal expression of an author's intent, while it ensures the integrity of the signed data. The preservation of the readability, the verifiability and the validity of the digital signature are, thus, crucial for the future value of the healthcare data.

As of today, several electronic signature schemes have been proposed. The main procedure is common and it is based on public key cryptography, where the signer encrypts (signs) a sequence of data using her private key, and the verifier of the signature ensures the originality of the data by decrypting the signature using the public key of the signer and obtaining the original data [4]. From the first steps of public key cryptography till today, several methods have contributed new features to the basic signature capability. The hash algorithms gave a solution to the computational efficiency of the signatures, the digital certificates and the self-certified keys provided the means for effective identification of the signer, the Public Key Infrastructure (PKI) architectures built the necessary trust relationships and the time-stamping and notarization schemes made a digital signature stronger [5,6]. However, the lifespan of a digital signature is restricted by the validity period of the relevant keys and digital certificates, by the future unavailability of signature-verification-data, as well as by cryptanalysis advances and by suppression of trust relationships. The paradigms of time-stamping and notarization have been used to extend the lifespan of a digital signature, either by indicating that a signature was created at a time before a subsequent compromise, or by transferring the trust against the signed data to a new entity, the Notary. Yet, timestamps and notarizations consist of digital signatures and therefore will become invalidated in some, not long, period of time.

The objective of the paper is to present a digital signature scheme for EHR, where the signature verification process is based on trust relationships, data, and technologies that are available in the distant future, at the moment of verification. The basic idea is the elimination of any dependency on obsolete trust relationships, data, and technologies that may have existed in the past, but are subsequently invalidated. The idea focuses on the preservation of trust in the information needed to verify the identity of an EHR signer in a ceaseless way. This is achieved by a continuous *successive trust transition* to new entities, data, and technologies, and the proposed solution is a *cumulative notarization scheme*.

2. The requirement for long-term digital signatures

2.1. The importance of healthcare data signing

Data authenticity is defined as the preservation of the integrity of the data (i.e. data is not modified during storage or transmission) plus the possibility of origin verification (i.e. the secure identification of the creator or the owner of the data). Both properties are assured by means of digitally signing. Authenticity of EHR is crucial for the trustworthiness of a HIS, especially in distributed environments where data is transmitted over insecure channels and stakeholders have never physically met [7]. We may identify several risks that may endanger the preservation of healthcare data authenticity [8]:

2.1.1. *Central archiving attacks*

EHR are stored in central repositories at institutional level, and can be accessed over open networks by remote healthcare professionals. Such a centralized multi-user inter-networked environment is subject to remote exploits and attacks putting in danger the confidentiality and integrity of medical information.

2.1.2. *Ownership of medical records dilemma*

The question is whether the EHR belong to the hosting healthcare unit, to the related patients, or to the healthcare professional who created them. Proof of record origin contributes to the protection of the intellectual property of healthcare professionals, who then feel more comfortable to share their data for the common good.

2.1.3. *Communication channels tampering*

The information transmitted over a communication channel can be deliberately or accidentally modified, thus sacrificing data integrity. Any modification on signed content is immediately detectable.

2.1.4. *Data repudiation*

In cases where liability for the information provided is a legal requirement, repudiation of data origin must be avoided. Digital signatures assure the non-repudiation of having created (or at least published) a healthcare record.

2.2. Restrictions on the longevity of digital signatures

There is a considerable gap, in the existing technology, between the required longevity of an EHR and the longevity of its digital signature. While the longevity of the EHR itself depends only on the preservation of its content readability, the longevity of its digital signature depends on multiple factors, which considerably restrict its lifespan. For example:

- The keys used for signature creation and verification must have limited lifespan in order to avoid long exposure to security threats. A common practice of Certification Authorities (CA) is to impose a limit of 1–2 years in the lifespan of certificates based on a 1024 bit RSA key pair.
- The algorithms used for signature creation may be broken, or signing keys may be compromised before the completion of their lifespan, rendering the signature of an EHR vulnerable to modification attacks.
- The information needed for the verification of a digital signature, such as digital certificate chains and certificate revocation status, may be not available at a future time.
- The Trusted Third Party (TTP), which binds the signature-verification data to a specific identity, may be not trusted in the future, either because it ceased operation, or because it does not fulfill the necessary requirements any more.