

This is an HTML working draft that led to an article publication. A reference to this work should always be done using the following citation:

[Dimitrios Lekkas](#), [Dimitris Gritzalis](#), "Long-term verifiability of healthcare records authenticity", *International Journal of Medical Informatics*, Vol.76, No.5-6, pp.442-448, 2007 (doi:10.1016/j.ijmedinf.2006.09.010)

This material is presented to ensure timely dissemination of research and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by all the copyright holders. In most cases, these works may not be reposted or distributed without the explicit permission of the copyright holders.

Long-term verifiability of healthcare records authenticity

Dimitrios Lekkas¹ and Dimitris Gritzalis²

¹ Dept. of Product and Systems Design Engineering, University of the Aegean
Syros GR-84100, e-mail: dlek@aegean.gr

² Information Security and Critical Infrastructure Protection Research Group
Dept. of Informatics, Athens University of Economics and Business (AUEB)
76 Patisson Ave., Athens GR-10434, e-mail: dgrit@aueb.gr

Abstract

The paper deals with the long-term validation of the authenticity of electronic healthcare records (EHR). 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 EHR is far beyond the lifespan of a simple digital signature. This lifespan 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. The paper proposes a successive trust transition towards new entities, modern technologies, and refreshed data. According to the paper, a future relying party will have to trust only the information provided by the last notary, in order to verify the validity of the initially signed EHR, thus eliminating any dependency on ceased entities, obsolete data, or weak old technologies.

Keywords

Security, Digital Signatures, Notarization, Time-Stamping, Electronic Healthcare Record (EHR).

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). 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). HER

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, 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 [1]. 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 [2]. 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 [3] [4]. 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 at 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 HER 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 [5]. We may identify several risks that may endanger the preservation of healthcare data authenticity [6]:

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.

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 commonwealth.

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.

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.

Some technical solutions to this problem are presented in [7] [8]. These solutions are mainly based on document time stamping, which proves the existence of a sequence of data before a specific moment in time. This time stamp is refreshed before the used algorithms or keys become (or are likely to be) compromised or rendered vulnerable, thus ensuring its validity through the years. However, the validation process in such schemes still requires the successful validation of the initial signature and timestamp, therefore it is based again on information, such as digital certificates and Certificate Status Information (CSI) [9] that may be unavailable in the future. Thus, these solutions focus on the problem of algorithm decay, not on the preservation of trust.

3. Solution framework overview

The basic idea of our approach is that a digitally signed EHR has to be regularly verified by a trusted entity (called the 'Notary'). This entity attests its validity, signs it, and "refreshes" the strength of the initial digital signature. At the next period, the Notary has to check only the attestation made by the previous notary, without validating the initial signature. This "cumulative notarization" scheme may theoretically continue forever. According to this idea, the verifiability of EHR is a successively transited transition towards new trusted entities, newer technologies, and refreshed data. A future relying party will have to trust only the information provided by the last notary, in order to verify the validity of the initially signed EHR, thus eliminating any dependency on ceased entities, obsolete data, and weak old technologies.

The actors involved in the proposed model of cumulative notarization are the following:

- The *initial signer* who creates the *initial digital signature* on the EHR.
- The *Certification Services Provider (CSP)* that provides the necessary trust mechanisms (e.g. digital certificates) to authorize the signer to act as such and to bind her keys to her identity.

- The *Notaries* (or *Confirmers*) acting as TTP, which make specific attestation on the content and the characteristics of a data collection (e.g. on the validity of a digital signature at a specific moment), and then sign digitally the data and the attestation.
- A *Relying Party* (RP) (or *Verifier*), who relies on the information provided by a CSP or a Notary, that enables her to verify the validity, the origin and other characteristics of a digital signature. A short-term RP and a long-term RP may be distinguished.

3.1 Assumptions and Requirements

Again, the focus of the paper is the preservation of the verifiability and the validity of digital signatures for long periods, assuming that the readability of the EHR itself is assured [10]. Technology obsolescence, different data representation formats, limited storage media longevity, special software and hardware required, are some factors that may reduce the future readability of EHR. Some solutions to this problem are based on the existence of metadata [11], but this is a different part of the problem, which is outside the scope of this paper.

The entity providing notary services in our proposed framework must be a trusted entity for acting so, either on national level or within a closed medical group. Legally, the notary is a TTP and should abide by law and regulations concerning a regular notary service. At the moment, when a notary confirms a signed EHR, it attests that:

- The signature of the EHR is algorithmically valid for a given public key and the related algorithm is valid and strong.
- The signer possesses a valid digital certificate that binds the signer's keys to her identification details.
- The issuer of the signer's certificate is a trusted, officially qualified entity, acting legally within the scope of medical applications, adhering to published policies and abiding by the current national or international law and regulations. It is therefore assumed that the notary trusts the CSP of the signer at the moment of the notarization.
- All the relevant information, such as the status of certificates, the validity of trust chains and the policies and regulations in force are properly checked.
- The validity of the optionally included timestamp is properly verified.

The successful verification of the last notarization indicates that the initial signature is valid. It is required that this verification must not have any dependency on past technologies and on data, which are not necessarily archived or attached to the initially signed healthcare record (e.g. keys or certificates of the initial signer). Therefore, it is required that the verification of the *Cumulatively Notarized Signature* (CNS), as described in the next sections, is based only on the last notarization, which does not have any dependency on:

- The existence of the CSP, which issued the certificate for the initial signature.
- The existence and the operational status of intermediate notaries.
- The algorithm and key characteristics of the initial signature or the intermediate notarizations
- The existence of keys, certificate chain and Certificate Status Information (CSI) for the validation of initial signature and intermediate notarizations.
- The subsequent expiration or compromise of the keys of the initial signature or the intermediate notarizations.

Finally, the framework does not require a secure archiving system. Notarization tokens are tamperproof signed data structures and may be stored in personal storage media or in publicly accessible archives and directories. The inclusion of the initial healthcare record in the CNS is not required, depending on the confidentiality level of the content. The CNS may be an autonomous public structure that contains only the hash value of the healthcare record as a reference (detached form) or contain the whole signed data (attached form) [12].

3.2 Transition of Trust

The proposed solution, apart from its technical aspects, is mainly based on the notion of trust within the PKI. A notary acts as a TTP for the services she offers. The notion of trust against a third party assumes that the TTP is part of the social system, expresses the faith of the relying party in specific operational, ethical, and quality characteristics, while it also includes the acknowledgement of a minimum (and acceptable) risk factor [13].

Trust has the property of *transitivity*. A trust relationship is transitive [14] when the fact that an entity A trusts an entity B and the entity B trusts an entity C, leads us to the conclusion that entity A is bound to trust entity C. The property of trust transitivity is essential for the proper functionality of the proposed framework; however there is a need of establishing specific restrictions and requirements in trust transition. In fact, it is hereby assumed that when a relying party trusts a Notary, it is bound to trust any other party that the Notary declares as a TTP and, thus, it trusts the information that this TTP publishes. However, the acceptance of this trust transitivity remains to the discretion of the relying party. The trust model, which results as a consequence of trust transitivity, is illustrated in Figure 4. A short-term relying party trusts directly the CSP that certifies and authorizes the initial signer. As a result, it trusts the signature-verification-data and consequently the created signed EHR. The first Notary validates and notarizes the signature data, since it trusts the signer's CSP. Subsequent Notaries are continuously refreshing the trust against the signature data by applying the cumulative notarization. A long-term relying party trusts directly the last notary, only. Therefore, a trust relationship against the signature data is derived.

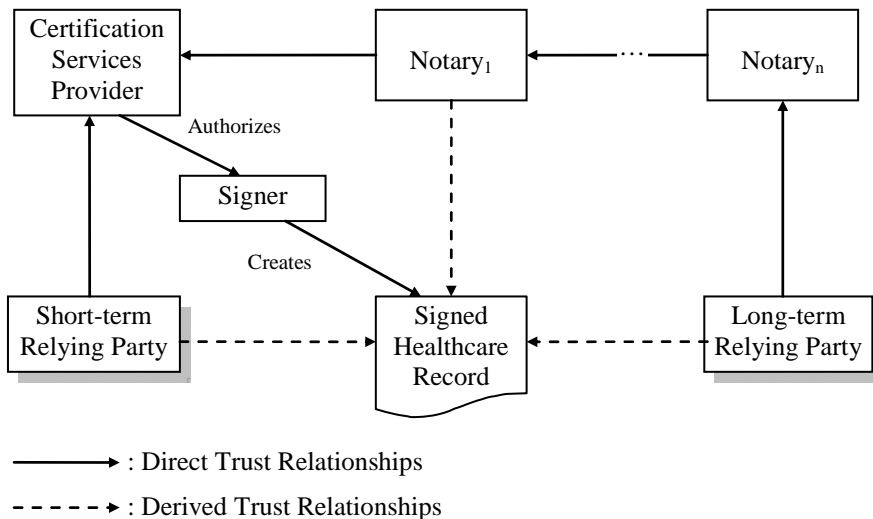


Figure 4: Trust Model in a cumulative notarization framework

After a long-term cumulative notarization on a digitally signed EHR, it is likely that the resulting trust chain between the initial signer and the relying party will become unexpectedly long. This long “*trust distance*” may introduce new risks and weaken the trust relationships, since the relying party has no control on this successive transitivity and in most cases cannot follow up the policies and practices of all the intermediate Notaries and CSP. The restriction of the length of trust chain is not an acceptable solution, since a limit on the steps of trust transitions would reduce the potential longevity of the initial signature. The restriction of security domains of consecutive notaries (i.e. all notaries belong to the same group or organization), as well as the requirement for policy compatibility between notaries, may mitigate the effects of long trust distance [15].

4. Technical implementation

4.1 Generic Mechanism

The mechanism of cumulative notarization for signed EHR is summarized below:

1. The EHR is signed by the *initial signer*. The EHR content, the metadata describing its content and format, the signature, the signature metadata, and the distinguished name of the signer form the ‘signedEHR’ element.
2. The metadata included in ‘signedEHR’ consists of two elements; they refer to the document and the signature, respectively. Since the objective is the long-term preservation of data, the inclusion of metadata for the accurate description of the subject data is crucial.
3. A Notary attestation is also included in the ‘signedEHR’ element. This field contains the details of the verification process that the notary performs before the signing (notarization) of the data structure. The ‘notaryAttestation’ field may appear multiple times and its indicative values are: (a) Signer’s CSP is trusted, (b) algorithm is valid and strong, (c) key length is acceptable, (d) CSI checked, (e) certification chain is valid, (f) signature is algorithmically valid, and (g) CSP policy is compatible and/or acceptable
4. The first Notary signs the ‘signedEHR’, forming the first Notarized Signature (‘firstNS’ element) structure. This structure includes the notarized data (‘signedEHR’), the notary signature, its metadata, and the distinguished name of the first Notary.
5. The second Notary forms the ‘previousCNS’ element; it contains the ‘firstNS’ and its attestation on the verification process it performed on the previous notarization token.
6. The second Notary signs the ‘previousCNS’ element, forming the Cumulatively Notarized Signature (CNS - ‘cumulativeNS’ element) structure; it includes the notarized data (‘previousCNS’), the notary signature, its metadata, and the distinguished name of the second Notary.
7. Consecutive Notaries similarly encapsulate the last CNS into the ‘previousCNS’ element (instead of the ‘firstNS’ element), and perform steps 6-7, producing each time a new CNS.

The entities referred to as “second Notary” or “consecutive Notaries” are not necessarily distinct and different from the previous ones. They are named as such, in order to emphasize the fact that each and every notarization process is a stand-alone and independent procedure that may be performed by repeated or distinct notaries. The proposed mechanism of cumulative notarization and the relevant transition of trust are illustrated in Figure 1.

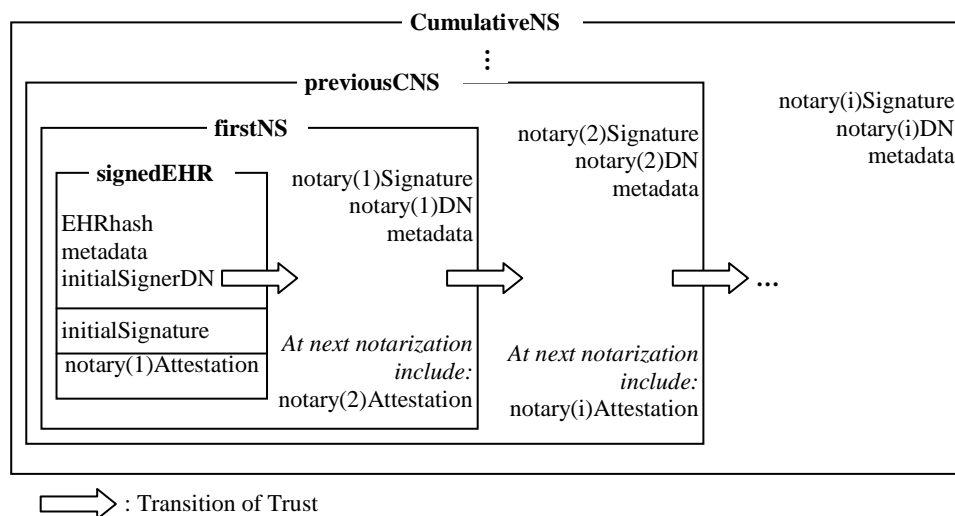


Figure 1: Successive signature encapsulation in Cumulative Notarization

4.2 Data Structures

The Extensible Markup Language (XML) provides the means for the construction of an open cumulative notarisation scheme that ensures effectiveness, readability, and applicability for a long period of time. We present a simplified XML schema that implements the generic mechanism proposed previously. The schema uses signature elements XML-signature namespace [16]. It is worth-noticing that the realization of a cumulative data structure is achieved by means of *recursive XML elements*. Specifically, the element ‘cumulativeNS’ contains the element ‘previousCNS’ which in turn is a choice of either another ‘cumulativeNS’ or a ‘firstNS’ element.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://mynotary.org"
<xmlns="http://www.w3.org/2001/XMLSchema" xmlns:n="http://mynotary.org"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

  <!-- signed initial Electronic Healthcare Record -->
  <complexType name="signedEHR">
    <sequence>
      <element name="EHRHash" type="base64Binary"/>
      <element name="signerDN" type="string"/>
      <element name="signerSignatureValue" type="base64Binary"/>
      <element ref="ds:keyInfo"/>
      <element name="timeStamp" type="base64Binary" minOccurs="0"/>
    </sequence>
  </complexType>

  <!-- the first notarization on the initial signed Healthcare Record -->
  <complexType name="firstNS">
    <sequence>
      <element ref="n:signedEHR"/>
      <element name="notaryDN" type="string"/>
      <element name="notaryAttestation" type="string" minOccurs="0"
maxOccurs="unbounded"/>
      <element name="notarySignatureValue" type="base64Binary"/>
      <element ref="ds:keyInfo"/>
    </sequence>
  </complexType>

  <!-- previously notarized data that will be notarized again -->
  <complexType name="previousCNS">
    <sequence>
      <choice>
        <element ref="n:cumulativeNS"/>
        <element ref="n:firstNS"/>
      </choice>
      <element name="notaryAttestation" type="string" minOccurs="0"
maxOccurs="unbounded"/>
    </sequence>
  </complexType>

  <!-- the resulting Cumulatively Notarized Signature-->
  <complexType name="cumulativeNS">
    <sequence>
      <element ref="n:previousCNS"/>
      <element name="notaryDN" type="string"/>
      <element name="notarySignatureValue" type="base64Binary"/>
      <element ref="ds:keyInfo"/>
    </sequence>
  </complexType>

</schema>
```

4.3 Verification of a CNT

Provided that the assumptions described above (3.1) are in effect, the verification of the initial signature contained in a CNS depends on the verification of the last notarization. Specifically, a

Relying Party will validate the last CNS by confirming that: (a) the signature of the last notary is algorithmically correct, (b) the notary is trusted to perform the operation, (c) the certificate of the last notary is validated, by checking its chaining up to a TTP, and (d) the attestation declaration included in the token is satisfactory for the relying party.

5. Security considerations

Some threat scenarios, which may arise with the proposed framework, as well as the way they are dealt with, follow:

Alteration of a cumulatively notarized EHR: The integrity of the whole structure is protected by the signature of the last notary.

Forged initial signature: The sequential consistency of the consecutive notarizations and the attestations of the first notary ensure that the initial signature was created at a time where the signature algorithms and the signature-creation-data were strong and secure.

Compromise of intermediate notary keys or algorithms: It does not affect the validity or the overall security of the CNS, since it depends only on the validity of the last notarization.

Compromise of last notary keys or algorithms: One solution to this is the rollback to a previous notarization in the chain, provided that there exists at least one valid and strong past notarization in the CNS. If this does not apply, then the CNS must be notarized by another valid and operational notary service.

Faulty attestation by a notary: Since it is assumed that the notary is a properly trusted and authorized authority, a fault attestation on the characteristics of the notarized data would breach laws and regulations. Such a situation has to be addressed with by legal means.

6. Conclusions

The authenticity of EHR is crucial for the trustworthiness of a HIS and, thus, for the whole healthcare process. Data authenticity is even more significant in distributed environments, where data is transmitted over insecure channels and stakeholders have never physically met. Digital signatures constitute an effective tool for assuring the integrity, the originality, and the non-repudiation of the data contained in EHR. However, digital signatures have a short lifespan compared to the requirement of preserving healthcare records at least for the lifetime of the relevant patient.

We propose an open, practical, and efficient framework, based on the digital signature notarization paradigm, which ensures that a relying party at the distant future will efficiently verify the authenticity of a signed EHR, without the need to rely on ceased entities, obsolete trust relationships, or data and technologies that may have already been invalidated.

The solution to the problem is the continuous successive trust transition to new entities, data, and technologies. This is achieved by a mechanism of cumulative notarization that encapsulates and refreshes previously signed or notarized data. As a result, a relying party will have to verify only the newest notarization and, thus, it will always depend on current trusted entities, on state-of-the-art technologies, and on available data for the verification of a digital signature. The proposed framework copes efficiently with various possible threats. It has a comparative advantage against other signatures schemes, since it preserves the strong security characteristics of a digital signature and, additionally, eliminates the requirement to trust the CSP of the initially signed HER. Also, it does not require a secure archiving system, and it has the ability of technology refreshing.

References

- [1] P. Maniatis, M. Baker, "Enabling the Archival Storage of Signed Documents", in *Proc. of the FAST Conference on File and Storage Technologies*, pp. 31-45, USA, 2002.

- [2] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Com. of the ACM*, pp. 120-126, Vol. 21, No. 2, 1978.
- [3] M. Atreya, et al., *Digital Signatures*, RSA Press 2002.
- [4] A. Ansper, A. Buldas, M. Roos, J. Willemson, "Efficient long-term validation of digital signatures", in *Proc. of 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001)*, pp. 402-415, Korea, 2001.
- [5] S. Gritzalis, D. Gritzalis, K. Moulinos, J. Iliadis, "An integrated architecture for deploying a virtual private medical network over the Web", *Medical Informatics and the Internet in Medicine*, Vol. 26, No.1, pp.49-72, 2001.
- [6] S. Gritzalis, C. Lambrinouidakis, D. Lekkas, S. Deftereos, "Technical Guidelines for Enhancing Privacy and Data Protection in Modern Electronic Medical Environments", *IEEE Transactions on Information Technology in BioMedicine*, Vol. 9, No. 3, pp. 413-423, 2005.
- [7] D. Pinkas, J. Ross, N. Pope, "Long term electronic signatures", *IETF Request For Comments*, No.3126, available at <http://www.ietf.org/rfc/rfc3126.txt>
- [8] C. Wallace, S. Chokhani, "Trusted Archive Protocol (TAP)", *IETF Internet Draft*, available at <http://www.ietf.org/internet-drafts/draft-ietf-pkix-tap-00.txt>
- [9] J. Iliadis, S. Gritzalis, D. Spinellis, D. De Cock, B. Preneel, D. Gritzalis, "Towards a framework for evaluating certificate status information mechanisms", *Computer Communications*, pp. 1839-1850, Vol. 26, No. 16, 2003.
- [10] T. Wright, "Secure digital archiving of high-value data", *BT Technology Journal*, pp. 60-66, Vol. 19, No. 3, 2001.
- [11] D. Alemneh, S. Hastings, C. Hartman, "A metadata approach to preservation of digital resources: The University of North Texas libraries' experience", *First Monday Journal*, Vol. 7, No. 8, August 2002.
- [12] N. Ferguson, B. Schneier, *Practical Cryptography*, Wiley, 2003.
- [13] D. Lekkas, "Establishing and managing trust within the Public Key Infrastructure", *Computer Communications*, pp. 1815-1825, Vol. 26, No. 16, 2003.
- [14] A. Fernandes, "Risking trust in a public key infrastructure: Old techniques of managing risk applied to new technology", *Decision Support Systems*, pp. 303-322, Vol. 31, 2001.
- [15] S. Kokolakis, E. Kiountouzis, "Achieving interoperability in a multiple-security policies environment", *Computers and Security*, pp. 267-281, Vol. 19, No. 3, 2000.
- [16] M. Bartel, J. Boyer, B. Fox, B. LaMacchia, E. Simon, "XML-Signature Syntax and Processing", W3C Recommendation, available at <http://www.w3.org/TR/xmlsig-core/>.