

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](#), [Stefanos Gritzalis](#), Lilian Mitrou, "[Withdrawing a declaration of will: Towards a framework for Digital Signature Revocation](#)", *Internet Research*, Vol.15, No.4 (2005) pp.400-420 [PDF] (doi:10.1108/10662240510615173)

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.

Withdrawing a Declaration of Will: Towards a Framework for Digital Signature Revocation

Dimitrios Lekkas

*Department of Product and Systems Design Engineering
University of the Aegean, Syros Island GR-84100, Greece,
Tel: +302281097100, Fax: +302281097009, e-mail: dlek@aegean.gr*

Stefanos Gritzalis

*Department of Information and Communication Systems Engineering,
University of the Aegean, Karlovassi, Samos GR-83200 Greece,
Tel: +302273082234, Fax: +302273082009, e-mail: sgritz@aegean.gr*

Lilian Mitrou

*Department of Information and Communication Systems Engineering,
University of the Aegean, Karlovassi, Samos GR-83200 Greece,
Tel: +302273082250, Fax: +302273082009, e-mail: L.mitrou@aegean.gr*

Article Type

Research paper

Structured abstract

Purpose

To identify and justify the cases where a signer has the right to legally withdraw the declaration of will she made by a previously created digital signature. To propose a technical framework for establishing a signature revocation mechanism and for disseminating the Signature Status Information (SSI) to the relying parties

Design/methodology/approach

We identify various intrinsic problems of the digital signature creation process that arise several questions on whether the signer performs a conscious and willful act, although she is held liable for this action. The Law faces the eventual right of the signer to claim a revocation of a previously made declaration of will, especially in cases of an error, fraud or duress. In our technical approach we propose a solution based on special data structures, the Signature Revocation Tokens (SRT) and we analyze the possible mechanisms for disseminating SRTs to the relying parties.

Findings

A relying party has to perform a sequence of actions, taking into consideration the possible existence of a signature revocation, in order to decide on the validity of a digital signature. A scheme based on a central public repository for the archival and distribution of Signature Revocation Tokens exhibits significant advantages against other alternatives.

Research limitations/implications

The future design of digital signature standards and applications must be seen under a new perspective, taking into consideration the possibility of signature revocation.

Originality/value

The paper identifies and fulfils a new legal, practical and technical requirement that adds value to the digital signature deployment.

Keywords

Security, Non-repudiation, Public Key Infrastructure, Signature Revocation Token, XML signatures

1. Introduction

Digital signatures are increasingly gaining momentum in our everyday electronic transactions. Signed documents in digital format have become commonplace for a wide range of information types, such as transaction records, books, scientific work, contracts and even governmental decrees. Digital signatures preserve basic security characteristics of a digital document, such as integrity and authenticity, while it is the principal expression of an author's intent. European law, the electronic signatures directive (European Union, 1999), further increases the value of electronic signatures, by granting them legal validity equivalent to traditional hand-written signatures. Similar legislation exists in the U.S, Japan and the United Nations rendering the digital signatures legally binding (Broderick 2001).

Various electronic signature schemes have been proposed. The main procedure 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 (Rivest, 1978). From the first steps of public key cryptography until today, many value-added characteristics are enhanced, by integrating new technologies in the digital signature process. Hashing algorithms gave a solution to the computational efficiency of the signatures; digital certificates (Kohnfelder, 1978) and self-certified keys (Girault, 1991) provided the means for effective identification of the signer; the Public Key Infrastructure (PKI) architectures build the necessary trust relationships and finally the time-stamping (Adams, 2001) and notarization (Ansper, 2001) techniques providing additional proofs that add value and longevity (Lekkas, 2004) to a digital signature.

The creation of a digital signature cannot be denied as an action, since it can be algorithmically proved, using cryptographic techniques. However, there are many weak points in the procedure of digitally signing data. The questions arising relate to *who is using the signature-creation-data, whether she performs a willful act and whether the software and hardware used for this action can be trusted*. The objective of this paper is to investigate the legal and technical reasons why a declaration of will, denoted by a digital signature, can be cancelled and how this cancellation can be technically achieved. In section 2 we identify the weaknesses of the signature creation process and in section 3 we justify the necessity for a digital signature revocation mechanism from a legal and a technical view. In section 4 we examine previous works that relate to sorts of signature cancellation. In section 5 we propose technical solutions for establishing a signature revocation mechanism and for disseminating the relevant Signature Status

Information (SSI) to the relying parties. For a relying party, a digital signature is considered as revoked (and thus not valid) if revocation information exists and this information is properly validated. We finally present, in section 6, a comparison between the alternative proposals for signature revocation.

2. Weaknesses and risks on the signature creation process

2.1 *Can we trust the signature-creation-devices?*

Within the PKI it is generally assumed that a signer provided with a qualified certificate binding his identity to his public key, cannot ever deny having created a digital signature for a specific electronic document, using his corresponding private key (Herda, 1995). In fact, this assumption is not absolutely accurate. A more precise technical statement would be that ‘one cannot deny that a specific private key was used for the creation of a digital signature for an electronic document’. Furthermore, one may deny the intent of creating a digital signature or state that this action was not a willful act.

A fundamental intrinsic problem of digital signatures (Mauer, 2003) is that the action of their creation (i.e. the usage of a private key) is not directly bound to a physical entity, but only indirectly through a machine and an application. The risk lies in the fact that the calculation of a digital signature is performed transparently by hardware and software (the signature-creation-device) that is mostly unknown and non-trusted for the end-user and that may also be malicious or at least unreliable. In more risky cases, a software agent may have been charged by its creator to apply a digital signature on behalf of a person. Although this approach contradicts to the nature of digitally signing, which has to be a purely personal activity, we often meet the existence of such signature-proxy agents in resource-restricted environments, such as mobile systems (Park, 2003). In any case malicious software agents may, for example, exploit the recently discovered vulnerability of collisions in hash functions (Wang, 2004) or violate the principle of ‘What you see is what you sign’ (Sceibelhofer, 2001). As a result, one may be held liable for a signature created by his private key, without his awareness or consent.

In spite of the existence of a secure binding between a key and a physical entity, assured by a Trusted Third Party, by means of a digital certificate, it is inherently impossible for a relying party to determine when, how and by whom a digital signature was generated, unless it is time-stamped and notarized by a properly authorized notary within a trusted environment (Rivest, 2001). In other words there is no means to prove that the creator of a digital signature guarantees his awareness and that he performs a conscious and willful act. This fact is the basic weakness of digital signatures comparing to the hand-written signatures – which although are easy to forge, sometimes not-recognizable and not securely bound to one person – their creation is under the direct control of the signer and directly bound to material (a piece of paper).

2.2 *Do Smart cards solve the problem of untrustworthy systems?*

Although regular computing systems may be considered rather untrustworthy for the creation of digital signatures (see section 2.1) it is generally accepted that PKI-enabled smart cards provide a high level of security in the cryptographic operations needed for digitally signing data. They conform to the European directive on digital signatures that requires secure signature-creation-devices that remain under the control of the signer (European Union, 1999). Smart cards are generally considered as tamper-proof devices, while their usage is authorized by means of a personal identification number (PIN). The private key is generated and securely stored within the smart card, with strict access conditions declining any kind of export or usage of the private key outside the chip of the smart card.

However, a smart card has no direct I/O interface to the user and its operation depends on a computer with the necessary APIs. Due to this fact, we may identify two major problems that lead us again to the problem of untrustworthy systems:

- When a signer creates a digital signature she must trust the operating system, the user interface and the card API, that they present the correct data to the smart card for signing.
- Although the private key is used within the trusted environment of the smart card, the PIN is given to a dialog presented by the terminal. Thus, malicious software may be able to reuse the PIN to sign another portion of data within the smart card.

The provision of vendor-signed software for the smart-card subsystem and APIs and the usage of ‘signature counters’ informing the owner of the times and the purpose of private key usage, are two indicative proposals that may mitigate (but not eliminate) the risks described above and render the smart card a real trustworthy signature-creation-device.

3. **The emerging need for digital signature revocation**

3.1 *A legal view*

Since the creation of a signature (digital or handwritten) is given, a revocation does not cancel this action itself, but the declaration of will or the contract on which the signer binds his signature. Consequently, the term ‘signature revocation’ as it is used in this context concerns the eventual right of the signer to claim a revocation of a previously made declaration of will and not the revocation of the creation or the function of the digital signature itself. According to the principles and common provisions embedded in the central European civil law, we may identify the following generally accepted legal reasons of revocation (Stathopoulos, 1995; Brox, 1995):

- *Revocation of a declaration of will*: In most legal orders a declaration of will produces legal effects only as from the time it has reached the person to whom it must be directed. The declaration has no effect if a revocation of this declaration reaches the addressee prior or together with the declaration. Such provisions apply to unilateral legal acts/ legal transactions as well as to contracts.
- *Annulment of a legal act/contract*: As neither the autonomy of the will , nor the security of transactions and the confidence principle can be entirely sacrificed the law adopts in-between positions permitting the parties to invoke the fact that their genuine will was absent or defective in certain circumstances and on certain conditions such as the cases of a simulated declaration, an error (as to the declaration, the will, the qualities etc.) fraud or erroneous dispatching of the declaration or duress. The party concerned is entitled to apply for the annulment of the act.
- *Modification/Abrogation of a legal act*: An act/a contract is usually necessary in order to create or to modify an obligation through an act, without prejudice to any differing provision of the law.

A legal act or a contract is the expression of private autonomy and the (valid) declaration of will is the main condition for a conclusion of a contract. The law had to face the problem of the defects of consent/ declaration on the one side and the protection of the recipient on the other side and seek for an appropriate balance of interests (Dumortier, 2003; Reidenberg, 1996). Technology must provide the necessary solutions for coping with the relevant cases in the digital world.

3.2 *Non-repudiation vs. Signature revocation*

One of the strongest characteristics of digital signatures is that of *non-repudiation*. According to a definition given in ISO 7498-2, non-repudiation is the property of an electronic transaction that prevents a person from denying that she/he enters into this transaction. Non-repudiation was not a traditional technical legal term. Legally it refers to a rule, which defines circumstances in which a person is treated for legal purposes as having sent/received a message, whether in fact he/she did it or not (Laurie, 2003).

More specifically, in a message-centric system, non-repudiation is a security service that protects against the denial by one of the entities involved in a message exchange of having participated in all or part of the exchange. This service provides both proof-of-origin to the recipient (i.e. authentication) and proof-of-receipt to the sender (Herda, 1995). For a digitally signed document, non-repudiation means that the signer can be held liable for the attestation he made on this document when he created the signature. This attestation may include, but not limited to, content comprehension, agreement, authoring or legal contractual binding. It generally guarantees the awareness of the signer of performing a conscious and willful act (Mauer, 2003).

In any case, the signer is the one who is granting the non-repudiation property to the relying party, according to his intention when creating a digital signature. In a more generic approach we could define non-repudiation as *“the process that establishes a trust model, such that any event that is deemed non-repudable is beyond question”*. Hardware, software, people, procedures and legal environment are integral parts of this trust system, each of them incorporating special security characteristics.

In the case of handwritten signatures, each signed document is a distinct entity with a distinct unique signature. Consequently, a revocation of its signature is straightforward and it is equivalent to the destruction of the original signed document (although this action does not always imply the annulment of the relevant legal consequences). Even in the case where a document is signed (by hand) in multiple original copies, it is theoretically possible to destroy each one of them, since they are distinct and finite. If, however, the signed document is distributed and has already reached its addressees, the revocation of signature is not trivial and it does not stand as a legal case itself. Instead, a revocation of the signer’s declaration of will, may be possible and legally acceptable by means of an annulment or a contract (see section 3.1).

In the digital world things are slightly different. Digitally signed documents can be copied and distributed unlimited times, without the consent or the control of the signer. Every copy of digitally signed data is an original and these originals are not finite and not even distinct. It is obvious that the revocation of a signature by deletion of data is a non-solution. A special mechanism must be established *enabling the signer to revoke his signature and ensuring proper and prompt dissemination of this revocation to any interested party*.

As described in section 2, the problem of untrustworthy information systems (even with the use of smart cards) may lead the alleged signer to the repudiation of having created a signature. There are several reasons why one may *deny the creation of a signature*, such as:

- The signature is created without the full consent or awareness of the owner of the private key, due to a virus, a malicious application or an unauthorized usage of her personal computer. Such malware may, for example, exploit the recently discovered vulnerability of collisions in hash functions (Wang, 2004) or violate the principle of ‘What you see is what you sign’ (Sceibelhofer, 2001)
- The private key is compromised and a false signature is created by an unauthorized entity, before the key compromise is detected, reported to the certification authority and published by means of certificate revocation mechanisms (Iliadis, 2004).
- A digital certificate proved to be invalid, due to Certification Authority’s fault on identity

verification or due to algorithm compromise, thus binding a digital signature (precisely, the signature-verification-data) to the wrong physical person.

In all the above cases the creation of a signature may be denied by the legitimate user, since it is a result of *simulated declaration, error or fraud*. We may identify several additional cases where a signer would have to revoke his signature, *without necessarily denying its creation*. Most of the listed cases below match to the legally defined cases of revocation, as described in the previous section, but they are placed into the digital world context, in a more practical approach:

- Revocation of a digital signature, which is proved to have been created as *a result of duress*.
- Annulment of a binding digital declaration on a document, contract or legal act, *imposed by a legally authorized entity*, who is acting as a proxy or a delegate and expresses the will of the signer.
- *Mutual annulment* of a contract by all the contracting parties, without the intervention of a third party.
- *Unilateral annulment* of a contract, in case such a possibility is clearly stated as a term within the contract.
- *Cease of a trust relationship* in a web-of-trust scheme, such as openPGP (Callas, 1998). In this case a trust relationship is established by one party who digitally signs the keys of another party. It is absolutely necessary to have a mechanism for revoking such signatures.
- *The revocation of a digital certificate* by a Certification Authority is in fact a widely deployed revocation mechanism, enabling a CA to withdraw its attestation on the previously signed data included in the certificate. It denotes that the initial (signed) declaration of the CA on binding a public key with a subject does not stand any more.
- A signing party may be *legally entitled to withdraw a declaration* she made by previously signing a document, as a result of either a relevant legislation or a bilateral agreement.
- *Conditional cancellation of a signature* if not confirmed within a specified period of time or under other event-driven circumstances.
- *Cancellation of a compromised, stolen or lost digitally signed token*, such as an electronic cheque in an e-payment scheme.
- *Expiration of an agreed period* for the validity of a contract or a declaration (this case is straightforward, as a relevant expiration statement within the signed data is sufficient).

It is now clear that the revocation of digital signatures is an important functional and legal requirement

within the Public Key Infrastructure. In the next sections we will record any related work and we will investigate the various technical alternatives in establishing a signature revocation framework.

4. Related work

4.1 *Technology related to signature revocation*

The notion of digital signature revocation does not appear in any of the well-established international standards such as the X.509 digital certificates, the Secure Multipurpose Internet Mail Extensions (S/MIME) protocol or the Public Key Cryptographic Syntax (PKCS) standards (Oppliger, 2000).

A signature revocation provision exists in some extend in openPGP (Callas, 1998) but it is limited only on revoking a trust relationship with another entity and it does refer to the revocation of a signature on arbitrary data.

The conditional signatures proposed by (Berta, 2004) are initially invalid, until they are properly endorsed by a Trusted Third Party. This mechanism gives a ‘second chance’ to the signer to repudiate an unintended attestation she made by creating a digital signature. This approach may be considered as a kind of signature cancellation, although it is nothing more than imposing a requirement for signature notarization.

(Zhang, 2002) introduces the notion of signature revocation. However, the approach is very limited, since it addresses the problem only for the data exchange between two entities. Besides, there is one more major weakness, being the requirement that the signers have to perform handshaking of secret data prior to the creation of their initial signatures, something which renders the proposed solution inefficient and almost infeasible in a large public scale.

As already mentioned, the Certificate Revocation Lists and other online protocols (Iliadis, 2003) that enable the revocation of digital certificates, is an example of an established technique for the ‘*withdrawal of a previously signed declaration*’. Also, *revocability of anonymity* appears as an important security requirement in anonymous communication systems (e.g. Internet payments and auctions) and in anonymous certification services (Claessens, 2003).

4.2 *A positive rather than a negative approach*

In line with the principles of *honesty* and *transparency* in information systems, one would prefer only to be supplied with ‘positive statements’ rather than checking for ‘negative statements’. In other words a signature acceptor would prefer to see a signature together with the evidence that this signature is valid and not to search for information indicating that it has been revoked. Since the relying party is the party who is running the risk of a wrong decision, he is the one to pose the requirements on the necessary evidence that

must be supplied in order to decide for the validity of a signature (Rivest, 2001). However, there is no feasible solution toward this positive approach, since the actions of creating and revoking a digital signature are independent and asynchronous. In general, there is no way to attach validity evidence to a digital signature, since such evidence may dynamically and unforeseeably change.

The only way to implement such an approach is to impose a limited life-span in a digital signature, upon its creation. According to this approach, it is assumed that a digital signature is definitely valid for a short time, similarly to the SPKI/SDSI (Ellison, 1999) paradigm for digital certificates, without the need to check any Signature or Certificate Status information. If such a mechanism is acceptable by a relying party, then the relying party is able to determine the validity (in respect of revocation) of a digital signature based on a convenient statement such as “This signature is good until its expiration date” rather than on a statement such as “This signature is good unless you find out that it has been revoked”. However, although this approach is rather convenient for a transaction-based system (e.g. web banking) based on short-lived messages, it is not suitable for general purpose document signing, for archiving and generally for applications requiring long-term verifiability of digital signatures (Lekkas, 2004) due to its intrinsic short-living function.

5. A proposed solution framework

5.1 *Alternatives for enabling signature revocation*

As a result of the examination of the need for a signature revocation scheme and the related work, we may identify the following possible generic solutions for the revocation of a digital signature:

- *Signature deletion*: This is the trivial case where the signer destroys his digital signature immediately after its generation and before its distribution or archiving to other systems. (section 3.1)
- *Signature Revocation Token*: The signer revokes one of its own signatures by making and signing a necessary attestation.
- *Signature Revocation Authority*: A Trusted Third Party acting as a ‘Signature Revocation Authority’ produces, signs and distributes Signature Status Information, after proper request and authorization by the signer or by another party.
- *Conditional signature*: A signature is not initially valid and it is automatically revoked after a specified period of time, unless an authority intervenes and confirms it (Berta, 2004). (see section 4.1)
- *Expiring signature*: A signature is valid until a predetermined period of time (i.e. it expires)

as part of a contractual agreement (e.g. payment cheques, privilege delegation, expiring contracts, etc.- see section 4.2).

The solution framework for digital signature revocation presented in the next sections, focuses on the second approach where the signer revokes his own signature by making a relevant secure declaration, the Signature Revocation Token (SRT). The justification of this choice is emerging within the following sections and is concluded in section 6, where a technical comparison of the proposed solution with all the abovementioned alternatives shows its comparative advantage.

5.2 *Entities entitled to revoke a signature*

In most of the cases described in sections 3.1 and 3.2, the signer himself must revoke her own signature. In the cases involving fraud or duress the revocation should be addressed by legal means (i.e. by means of a judicial annulment or a contract) in addition to the technical means described in this paper. In the general case, we consider that a signer creates a signature by means that remain under her absolute control and that the same condition should apply in the case of signature revocation, where a signer should be the only entity entitled to revoke his own signature.

Another reason that leads us to conclude that the signer is the only entity entitled to revoke her own signature is that signature revocation is usually an action that denotes a commitment as strong as the initial signature. For example, by revoking a signature one may disclaim any right derived by the initially signed document and this is an action that cannot be later repudiated. Furthermore, in most contractual cases, the signer has the right to revoke a signature, provided that she is aware of and agrees with the *conditions* and the *consequences* of withdrawing such a previously made declaration.

Our proposed framework presented in the next sections, is built on the assumption that the following basic conditions or principles must apply:

- Only the signer is entitled to revoke (or to request revocation for) his own signature, by creating and signing a declaration claiming the withdrawal of the intent that led to the initial signature.
- The acceptance of the signature revocation by a Relying Party must not be considered as a given fact, but depends on the type of the signed document and on related terms and conditions that may apply.
- A RP must be able under any circumstances to check whether a signature is valid or revoked.
- The signer must be able to prove that she revoked her signature at a specified moment.

5.3 *Distribution of Signature Status Information*

In the paradigm of Certification Authorities, which are centralized authorities, the information on the status of the issued certificates can be easily disseminated to the relying parties by automated procedures through the Internet. Digital certificates include an extension pointing to ‘Authority Information Access Methods’ that enable the end-user applications to check transparently whether a certificate is valid or revoked. This dissemination procedure is not so straightforward in the case of signature revocation by end-users, since there is no central authority that hosts the signatures and the relevant revocation information nor there is a standard format for digital signatures with fields pointing to signature status information.

Signatures are usually bound to the signed content in form of either an integrated file format containing both content and signatures (attached signature) or in two separate files distributed simultaneously (detached signature) (Bartel, 2002). The basic advantage of attached signatures is that the signature accompanies the document and thus there is no effort needed for retrieving or distributing the signature that is bound to a specific document. The difficulty, on the other side, is that an integrated file has to be in a special format (usually proprietary with no clear verification procedures that cannot be controlled by the relying party). The benefit from the detached scheme is that the signed document may be kept in its initial format. However in a large scale distribution (e.g. not just an exchange between two parties but a public document for example) a file may be distributed or copied without the related signatures. This is the reason why a detached scheme is preferably used only in centralized archiving systems, where document retrieval and signature verification are synchronously and centrally performed.

In the case of Signature Revocation Tokens we may technically follow either the paradigm of attached or detached signatures. However, there is a basic difference: since the signature revocation process is asynchronous (i.e. it is executed at a later time - even years - after a signature is created) the attached method would be a rare case. It applies only to the case where a document is signed and the signature is revoked before it is distributed or in case it is required to re-distribute a signed document together with its revocation token.

A detached method for the creation and distribution of signature revocation tokens is obviously preferred, since the revocation is produced at a time subsequent to the digitally signed document. The key issue here is to ensure that a relying party will have access to that information in order to determine the validity of the signature. This requirement is easily achieved in case of centralized archiving systems, where documents, signatures and revocation tokens may be stored together. It is also easy to achieve in low-scale cases where a very small number of contractors decide to revoke their signatures and distribute their signature revocation tokens between themselves (see section 5.7.2). Difficulties arise in the case where a digital signature that must be revoked is already distributed in large scale without central document archiving. The only acceptable solution is an on-line retrieval system where one can retrieve signature status information and determine the validity of a signature.

Summarizing, we may identify the following alternatives for the distribution of the information related to signature revocation:

- *Detached revocation token*: The signer is responsible for the distribution of this stand-alone secure token.
- *Attached revocation token*: The signer distributes the initially signed document together with the revocation information.
- *Central repository of revocation tokens*: The revocation tokens are centrally archived stand-alone secure data structures, publicly available through a widely deployed service, such as LDAP or HTTP.
- *Online SSI responder*: Provided as a value-added service, described in section 5.7.1
- *Mutual signature revocation*: Another value-added option for the exchange of signature revocation information between a closed group of signers, described in section 5.7.2

5.4 Basic user requirements

In order to determine the functional characteristics and the basic data structures of the proposed solution, we identify the following rules and user requirements that must be fulfilled:

- The relying party must always be able to reach a *deterministic decision* on whether a specific signature is valid or revoked.
- A signature revocation token must be *uniquely linked to a specific signature*. This can be achieved by the inclusion of a unique signature identifier (e.g. a signature thumbprint value) within the revocation token data structure.
- The revocation token must be *digitally signed by its creator*. Since we assume that the signer is the only one who can revoke his signature, it is required that the identity of the revocation signer (proved by means of digital certificate) matches the identity of the initial signer. However, it is not necessary that the initial signature and the revocation token are created by the same keys.
- The revocation of a signature can be claimed as *definite* or *non-definite* according to the relevant policies and rules that apply. Since the revocation is a binding signature itself, *a revocation of a revocation* would stand as a legal and technical case, in exactly the same way as a digital signature. Even if a revocation is claimed to be definite, it is possible to legally repudiate this signature revocation in case it is proved to be a result of an illegal or malicious action of a third party, against the will of the signer. In case a signature revocation must be cancelled, the

solution is the creation of a fresh signature by the same signer on the same document. However, we have to mention that the recreated signature of the document is not absolutely equivalent to the initial signature, since their signature-creation-times differ.

- *Timestamp* of revocation data is a value-added characteristic that is necessary in critical applications. Time-stamping prevents a signer from fraudulently claiming that he has revoked his signature at a past time whenever he benefits from such repudiation.

Additionally, the following requirements relate to the establishment of a basic Signature Status Information (SSI) distribution service, as described in the previous section:

- A trusted, preferably centralized *archive of signature revocation tokens* is necessary. The archive may be maintained by a Certification Services Provider as a value-added service or by a directory service (e.g. LDAP) used to store identities and digital certificates.
- *On-line public client access to SSI* is necessary. It can be achieved either by a common protocol such as LDAP and HTTP for accessing a public repository of digitally signed Revocation Tokens or by a special online protocol that responds to relevant requests (based on the Online Certificate Status Protocol paradigm (Myers, 1999)).
- A *referral to the SSI* archive or service must be made available to all Relying Parties. It can be achieved by the inclusion of an extension either in digital certificates (signer specific) or within the signature data structure (signature specific). This extension indicates a '*signature revocation access point*' in form of a URL, which leads to an online database containing SSI.

5.5 *Data Structure of the Signature Revocation Token*

We exploit the eXten-sib-le Markup Language (XML) and the XML-signature syntax (Cowan, 2001) to present a generic signature revocation XML schema that ensures openness, readability, and applicability for a wide range of applications. The following schema includes the necessary data structures to implement either an attached or a detached signature revocation token. The schema uses some elements from the xml-signature namespace (Bartel, 2002).

Based on the previously recorded user requirements we propose the basic element of the schema, the '*sRT*' (Signature Revocation Token) structure, which includes the '*sRTSignedData*' structure and the relevant signature of the entity that creates the revocation token. It optionally includes the '*keyInfo*' containing information (keys, certificate chains etc.) that enable the relying party to easily obtain the information needed to validate the signature of the SRT. It may also optionally include a secure timestamp ('*timeStampValue*') obtained by a trusted time-stamping authority, in case that a proof on the existence of the SRT at a specific time is critical.

The data that are signed within a SRT (*sRTSignedData*) include a digest of the signature to be revoked (*signatureThumbprint*) as a unique identifier of the initial signature. The structure includes also the *signatureMethod* of the SRT signature (as defined in XMLdsig) and the time recorded by the client application (*clientTime*) when creating the SRT.

The SRT in its 'attached' form is the structure *attachedSRT* which includes the signed document (*signedDocument*) the signature that is revoked (in XMLdsig form) the SRT and the *documentMetaData* that describe the signed document (MIME type and encoding).

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

  <!-- Signature Revocation Token -->
  <complexType name="SRT">
    <sequence>
      <element ref="sr:SRTSignedData"/>
      <element name="SRTSignatureValue" type="base64Binary"/>
      <element ref="ds:keyInfo" minOccurs="0"/>
      <element name="timeStampValue" minOccurs="0"/>
    </sequence>
  </complexType>

  <!-- Signature Revocation Signed Data -->
  <complexType name="SRTSignedData">
    <sequence>
      <element name="signatureThumbprint" type="base64Binary"/>
      <element name="thumbprintAlgorithm" type="string"/>
      <element ref="ds:signatureMethod"/>
      <element name="clientTime" type="dateTime"/>
    </sequence>
  </complexType>

  <!-- Attached Signature Revocation Token -->
  <complexType name="attachedSRT">
    <sequence>
      <element name="signedDocument" type="base64Binary"/>
      <element ref="sr:documentMetaData"/>
      <element ref="ds:signature"/>
    </sequence>
  </complexType>

```

```

    <element ref="sr:SRT"/>
  </sequence>
</complexType>

<!-- metadata for the recognition of the signed document -->
<complexType name="documentMetaData">
  <sequence>
    <element name="mimeType" type="string" use="optional"/>
    <element name="encoding" type="anyURI" use="optional"/>
  </sequence>
</complexType>

<!-- XMLdsig data element definitions -->
<element name="signature" type="ds:signatureType"/>
<element name="signatureMethod" type="ds:signatureMethodType"/>
<element name="keyInfo" type="ds:keyInfoType"/>

<!-- New data element definitions -->
<element name="SRT" type="sr:SRTType"/>
<element name="SRTsignedData" type="sr:SRTsignedDataType"/>
<element name="attachedSRT" type="sr:attachedSRTType"/>
<element name="documentMetaData" type="sr:documentMetaDataType"/>
</schema>

```

5.6 Extending XML signatures to support signature revocation

As already stated in section 5.4 it is required to extend the initial signature data structure (or the signer certificate) and to include a URL referral, pointing to Signature Status Information. Furthermore, the initial signature may optionally include the proper revocation scheme that is acceptable for a relying party, according to the type of the data signed and the applicable policies. We propose the following indicative schema element as an extension to XML signatures (Bartel, 2002):

```

<!-- Extended XML Signature -->
<complexType name="extendedXMLdsig">
  <sequence>
    <element ref="ds:signature"/>
    <element name="sSIIDistributionPoint" type="anyURI"/>
    <element name="revocationAcceptableMethod" type="revMethods"
      minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
</complexType>

```

The ‘*revMethods*’ type is an optional choice of the following non-exhaustive list: ‘Mutual revocation

only', 'Revocation within time-limit', 'Personal revocation', 'Revocation by authority', etc. This is a non-binding condition that merely indicates the wish of the signer and reflects the relevant terms and conditions that apply.

5.7 *Value-added options*

5.7.1 Online Signature Status responder

Another value-added service is the construction of an on-line protocol for updating and retrieving the current status of a specific signature. A service supporting the Online Signature Status Protocol (OSSP) must be able to give a definite reply (i.e. good or revoked) on the status of a signature for which it is authorized to respond. A procedure of archiving every digital signature produced, together with its status, would obviously be non-scalable and rather inefficient. Instead, only the revocation tokens produced by the signers should be archived. Consequently, in order to produce a definite response, it must be assured that each and every revocation token, must be uploaded and archived in the central archive of the service. This is an obligation for a signer and the uploading of the revocation token must be an integral part of the revocation procedure. The actions of creating a revocation token and its upload must be considered as an integrated transaction, where failure of uploading renders the revocation invalid. In a more efficient approach, the service is supplying an online tool for producing and uploading a revocation token.

Such a protocol must be able to perform the following two basic procedures:

1. Request and response for signature revocation token upload by a signer
2. Request and response for signature status retrieval by a relying party

The analogous paradigm of OCSP (Myers, 1999) can be used as a very close example of how such a request/response protocol may be implemented. In such an online system, the signature validation is performed on the server's side and therefore a *trusted service* is required. Specifically, it is required that: a) the provider of the service must be trusted and b) the service must respond in a secure manner.

A promising scenario is the case where the OSSP service is provided as a value-added service by the TTP for the community bound by its policy and to whom it is providing certification services. In this case the search for signature status information becomes straightforward for a community under a TTP, as the location of this information can be pre-determined and included within the digital certificates, as an additional extension (e.g. sSIDistributionPoint) or as an additional value in the AuthorityInfoAccess field, together with the certificate status information points. This eliminates the need to include an SSI field within the SRT structure.

As an example, the following lines are an excerpt from the OpenSSL configuration file, where a SSI distribution point is included in the authorityInfoAccess field together with the certificate chain retrieval point and the certification status retrieval point:

```
authorityInfoAccess = caIssuers;URI:http://www.pki.gr/SUB_CA.crt
authorityInfoAccess = OCSP;URI:http://www.pki.gr/ocsp
authorityInfoAccess = OSSP;URI:http://www.pki.gr/oss
```

5.7.2 A protocol for mutual signature revocation

The contractual parties of a digitally signed contract may decide to mutually cancel their agreement. A protocol for this mutual cancellation case must be based on a *fair exchange of signature revocations* between the contractors. This exchange must be completed as a whole transaction; otherwise it is not valid for any party. The following steps in order must be completed for this mutual signature revocation: 1) Each party produces its own signature revocation token and distributes them to the other parties. 2) Each party receives the revocation tokens of the other parties and signs them (declaring agreement) thus producing a proof of receipt for every token. 3) Each party returns the receipts to the owners of the tokens. Now each party holds the revocation tokens and the revocation receipts from every other party. Consequently each party alone is able to prove the cancellation of the contract by presenting the revocation tokens of every party, plus the acceptance of its own revocation by the other parties.

The basic principles met in the above protocol are:

- Every contractual party must revoke his signature and distribute that revocation to all the other parties.
- Every contractual party must be provided with secure receipts by all the other parties that they have received and accepted his signature revocation.

5.8 Relying party obligations

Based on the proposed framework with the ‘signature revocation tokens’ approach, a relying party who wishes to determine the status of a digital signature has to perform the following checks:

1. Verification of the initial signature, based on the classic procedure (i.e. algorithmic correctness, valid certificate chain, trust relationships, certificate revocation lists, key usage, etc.)
2. Retrieval of information related to possible signature revocation (i.e. SSI distribution point, location of online service or attached SRT). If there is such information indicating that the initial signature is revoked, then this information has to be validated as described in the next steps, otherwise the signature must be considered as *valid*.

- 3a. Verification of the signature of the revocation information (e.g. the signature of the XML structure representing the SRT as described in section 5.5).
 - 3b. Inspection of the identity of the revoking party. It must either match the identity of the initial signer or be a trusted party acting as a ‘Signature Revocation Authority’.
 - 3c. Examination on whether the signer is entitled to withdraw the declaration of will made by her initial signature. Such a decision will determine the final acceptance of the revocation by the relying party and it must be based on relevant policies, regulations, bilateral agreements or on relevant declarations included in the signed data.
4. Failure to verify one of the steps 3a-3c renders the revocation *invalid* and as such, the initial signature must be considered as *valid*.

The above procedure is depicted in a UML sequence diagram in Figure 1.

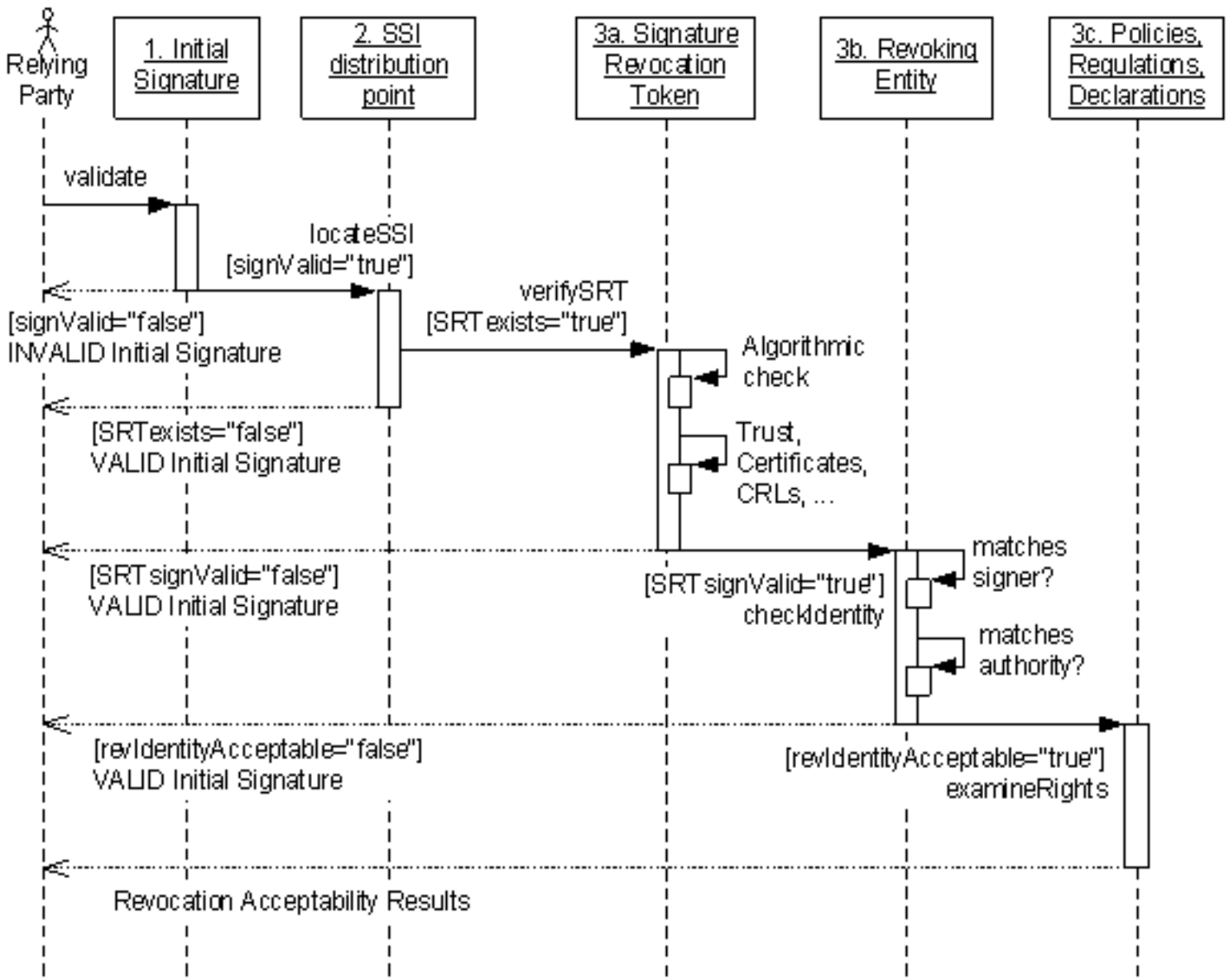


Figure 1: Signature status verification procedure

6. Technical comparison of signature revocation alternatives

A comparative summary of the proposed signature revocation framework against other alternatives, discussed in the previous sections, is presented in Table I. The alternatives taken into consideration are the generic signature revocation mechanisms described in section 5.1. The comparison includes (a) the trivial case of signature deletion (b) the Signature Revocation Tokens in their stand-alone detached form, (c) the case of a ‘Revocation Authority’ (see section 5.1) (d) the conditional signatures and (e) the expiring signatures (see section 4.1). The comparison continues further in Table II, focusing on the SRT solution (labeled ‘b’ in Table I) with the SSI distribution alternatives presented in section 5.3. The four variations of SSI taken into consideration are: (b1) the attached SRTs (see section 5.3), (b2) the existence of a central repository of SRTs (see section 5.3), (b3) the online SSI responder (see section 5.7.1) and finally (b4) the protocol for mutual signature revocation (see section 5.7.2).

The *applicability* of the revocation scheme refers to the basic type of signed data for which the scheme is more suitable. The criteria for the applicability are the criticality of the data, its scope, its lifespan and the number of addressees.

Some revocation schemes such as the ‘expiring signature’ are addressed to *short-lived signed data* (e.g. buying a ticket) while the rest of the schemes are addressed to data preserved for long periods (e.g. a governmental decree).

Another diversifying characteristic of the revocation schemes is the requirement for an *online directory* or service in order to obtain the Signature Status Information. The *SSI distribution efficiency* depends on the ability of an arbitrary relying party to easily and quickly determine the status of a signature. Similarly, the characteristic of *scalability* refers to the limitations on the distribution of the SSI to a large number of relying parties.

Some of the schemes require the establishment of *additional protocols* (further than a simple signature structure and its verification algorithm) either for the interpretation of a special data structure (e.g. attached signature revocation) or for the communication with an online request-respond service (e.g. online SSI protocol).

Finally, some schemes require the existence of a *trusted ‘revocation authority’* either for executing the revocation procedure itself or for the provision of trusted Signature Status Information.

Characteristic	Applicability	Life-span of	Need access to central	SSI distribution efficiency	Scalability (in terms of relying	Requires special protocol	Requires trusted ‘revocation

Revocation scheme		signed data	repository		parties involved)		authority'
(a) Signature deletion	Non-distributable data	Short	No	Not needed	None	No	No
(b) Signature Revocation Token (detached - without repository)	Transactions, Documents	Short & Long	Yes	Low	Low	No	No
(c) Revocation by a 'Signature Revocation Authority'	Trust relationships, Documents, Legal acts	Long	Yes	High	High	No	Yes
(d) Conditional signature	Contracts	Long	No	Not needed	High	Yes	Yes
(e) Expiring Signature	Transactions	Short	No	Not needed	High	Yes	No

Table I: Comparison of signature revocation alternatives

Characteristic	Applicability	Life-span of signed data	Need access to central repository	SSI distribution efficiency	Scalability (in terms of relying parties involved)	Requires special protocol	Requires trusted 'revocation authority'
SSI distribution scheme							
(b1) Attached SRT	Documents, Contracts	Long	No	Medium	Low	Yes	No
(b2) Central repository of SRTs	Documents, Contracts	Long	Yes	High	High	No	No
(b3) Online SSI responder	Documents, Contracts	Long	Yes	High	High	Yes	Yes

(b4) Mutual signature revocation	Contracts	Short & Long	No	Not needed	Low	Yes	No
----------------------------------	-----------	--------------	----	------------	-----	-----	----

Table II: Comparison of SSI distribution alternatives

Based on the above technical comparison of the various alternatives, we may now draw up a conclusion that a scheme based on the proposed ‘Signature Revocation Tokens’ with a central repository for their archival and distribution (labeled ‘b2’ in Table II) is the most efficient solution for an average digital signature application. This variation is superior in terms of data longevity, SSI distribution efficiency, scalability and additionally it does not require the existence of trusted authorities or the establishment of special protocols.

7. Conclusions

Although the creation of a digital signature is deemed non-repudable there are questions arising on whether the signer performs a conscious and willful act, since the signature-creation-devices cannot always be trusted even if they are based on tamper-proof devices such as the PKI-enabled smart cards. There are several cases where a signer has to withdraw the declaration of will she made when creating a signature, such as delusion or fraud during the signature creation process, mutual cancellation of a contract or cease of a trust relationship. From the legal perspective, the revocation of a declaration of will and the cancellation of a legal act are identified in the civil law. The need for a signature revocation mechanism is emerging and technology must provide the necessary solutions.

Related research has not provided any efficient solution to the problem as a whole. The proposed solution framework for digital signature revocation is based on the creation of a secure declaration by the signer that withdraws her initial intend, namely the Signature Revocation Token. The key issue of this solution is the establishment of a proper mechanism for the dissemination of the signature status information to the relying parties, enabling them to reach a deterministic decision on whether a specific signature is valid or revoked.

XML signatures may be extended to support the proposed solution, by incorporating into the signature data structure a referral to SSI. An online repository of Signature Revocation Tokens or a relevant responder is deemed necessary. A relying party has to check the existence and the validity of a signature revocation, further to the validation of the digital signature itself, in order to conclude on the status of the signature. A solution based on the ‘Signature Revocation Tokens’ with a central public repository for their archival and distribution proved to be the scheme with the most comparative advantages against other

alternatives. As a future work, a case study on the large scale implementation of this solution will be performed and the relevant experimental results will be presented.

8. References

- Adams C., Cain P., Pinkas D., Zuccherato R., (2001), “Internet X.509 Public Key Infrastructure Time-Stamp Protocol”, IETF Request For Comments 3161, Available at: <http://www.ietf.org/rfc/rfc3161.txt>
- Ansper A., Buldas A., Roos M., Willemsen J. (2001), “Efficient long-term validation of digital signatures”, in Proceedings of 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC2001), Cheju Island, Korea, pp. 402-415.
- Bartel M., Boyer J., Fox B., LaMacchia B., Simon E. (2002), “XML-Signature Syntax and Processing”, W3C Recommendation, Available at: <http://www.w3.org/TR/xmlsig-core/>
- Berta I.Z., Buttyan L., Vajda I. (2004), “Mitigating the untrusted terminal problem using conditional signatures”, in Proceedings of the International Conferences on Information Technology 2004 (ITCC’04), IEEE, Las Vegas, pp.12.
- Broderick M.A., Gibson V.R., Tarasewich P. (2001), “Electronic signatures: they're legal, now what?”, *Internet Research*, Vol. 11, No. 5, pp. 423-434.
- Brox H. (1995), Allgemeiner Teil des Bürgerlichen Gesetzbuchs, Köln-Berlin-Bonn-München.
- Callas J., Donnerhacke L., Finney H., Thayer R. (1998), “OpenPGP Message Format”, IETF Request for Comments 2440, available at: <http://www.ietf.org/rfc/rfc2440.txt>
- Claessens J., Díaz C., Goemans C., Preneel B., Vandewalle J., Dumortier J. (2003) “Revocable anonymous access to the Internet?”, *Internet Research*, Vol. 13, No. 4, pp. 242 – 258.
- Cowan J., Tobin R. (2001), “XML Information Set”, W3C Recommendation, Available at: <http://www.w3.org/TR/xml-infoset>
- Dumortier J., Kelm S., Nilson H., Skouma G., Van Eecke P. (2003), “The legal and Market Aspects of Electronic Signatures”, Study for the European Commission - DG Information Society, Contract Nr. C 28.400.
- Ellison C., Frantz B., Lampson B., Rivest R., Thomas B., Ylonen T. (1999), “SPKI Certificate Theory”,

IETF Request for Comments 2693, Available at: <http://www.ietf.org/rfc/rfc2693.txt>

European Union (1999), Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

Girault M. (1991), “Self-certified public keys”, in *Advances in Cryptology: Eurocrypt'91*, LNCS 547, Springer-Verlag, pp. 490-497.

Herda S. (1995), “Non-repudiation: Consisting evidence and proof in digital cooperation”, *Computer Standards & Interfaces*, Vol. 17, pp.69-79.

Iliadis J., Gritzalis S., Spinellis D., De Cock D., Preneel B., Gritzalis D. (2003), “Towards a framework for evaluating certificate status information mechanisms”, *Computer Communications*, Vol. 26 No.16, pp.1839-1850.

Kohnfelder L. (1978), “Towards a practical public-key crypto-system”, Thesis, MIT.

Laurie B., Bohm N. (2003) “Signatures: an Interface between Law and Technology”, Available at: <http://www.apache-ssl.org/tech-legal.pdf>

Lekkas D., Gritzalis D. (2004), “Cumulative notarization for long-term preservation of digital signatures”, *Computers & Security*, Vol.23 No.5, pp.413-424.

Maurer U. (2003), “Intrinsic limitations of digital signatures and how to cope with them”, in *Proceedings of the 6th Information Security Conference (ISC'03)*, LNCS-2851, pp.180-192

Myers M., Ankney R., Malpani A., Galperin S., Adams C. (1999), “X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP”, IETF Request for Comments 2560, Available at: <http://www.ietf.org/rfc/rfc2560.txt>

Oppliger R. (2000), *Security Technologies for the World Wide Web*, Artech House Publishers, USA.

Park H.U., Lee I.Y. (2003), “A Digital Nominative Proxy Signature Scheme for Mobile Communication”, in *Proceedings of 3rd International Conference on Information and Communications Security: ICICS 2001*, LNCS 2229, Springer, pp.451

Reidenberg J. (1996) “Governing Networks and Rule-Making in Cyberspace”, *Emory Law Journal*, Vol. 45, Issue III, pp. 911.

Rivest R. (2001), “Issues in Cryptography”, MIT Laboratory for Computer Science, Available at: <http://>

theory.lcs.mit.edu/~rivest/Rivest-IssuesInCryptography.pdf

Rivest R.L., Shamir A., Adleman L. (1978), “A method for obtaining digital signatures and public-key cryptosystems”, *Communications of the ACM*, Vol.21 No.2, pp.120-126.

Sceibelhofer K. (2001), “What You See is What you Sign – Trustworthy display of XML documents for signing and verification”, in *Proceedings of Communications and Multimedia Security, CMS’01*, Darmstadt, pp.3-13

Stathopoulos M. (1995), *Contract Law in Hellas*, Kluwer Law International – Sakkoulas, Athens.

Wang X., Feng D., Lai X., Yu H. (2004) “Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD”, rump session, CRYPTO 2004, Cryptology ePrint Archive, Report 2004/199, Available at: <http://eprint.iacr.org/2004/199>

Zhang H., Kudo M., Matsuura K., Imai H. (2002), “A model for signature revocation” in *Proceedings of 2002 International Symposium on Information Theory and Its Applications (ISITA 2002)*, Xi'an, PRC, pp.455-458