ETSI TR 102 046 V1.1.1 (2003-02)

Technical Report

Electronic Signatures and Infrastructures (ESI); Maintenance Report

Reference

DTR/ESI-000007

Keywords

e-commerce, electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Introduction

Electronic commerce is emerging as a way of doing business and communicating across public and private networks. An important requirement of electronic commerce is the ability to identify the originator of electronic information in the same way that documents are signed using a hand-written signature. This is commonly achieved by using electronic signatures which are supported by a certification-service-provider issuing certificates, commonly called a certification authority.

For users of electronic signatures to have confidence in the authenticity of the electronic signatures they need to have confidence that the CA has properly established procedures and protective measure in order to minimize the operational and financial threats and risks associated with public key crypto systems.

The Directive 1999/93/EC [7] (of the European Parliament and of the Council on a Community framework for electronic signatures) (hereinafter referred to as "the Directive") identifies a special form of electronic signature which is based on a "qualified certificate". Annex I of the Directive 1999/93/EC [7] specifies requirements for qualified certificates. Annex II of the Directive specifies requirements on certification-service-providers issuing qualified certificates (i.e. certification authorities issuing qualified certificates). Annex III of the Directive specifies requirements for the use of a secure-signature-creation device.

The ETSI TC on Electronic Signatures and Infrastuctures, along with CEN ISSS, has published a number of Technical Specifications for the implementation of services and infrastures supporting the requirements of the Electronic Signatures Directive, as well as to meet the general commercial requirements for Electronic Signatures. As a result of experience in implementing these specifications a number of comments and issues have been raised on the sepcifications. The present document records these issues and in some cases proposes resolutions. These comments may result in new versions of some or all of these specifications in the future. It should be noted, however, that until new versions of new Technical Specifications are released the existing requirements stand.

1 Scope

The present document records comments and issues raised with the ETSI TC ESI on Technical Specifications published for Electronic Signatures and Infrastructures, and in some cases proposes resolution for these issues.

These comments may result in new versions of some or all of these specifications in the future. It should be noted, however, that until new versions of new Technical Specifications are released the existing requirements stand.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI TS 101 456: "Policy requirements for certification authorities issuing qualified certificates".

[2] ETSI TS 102 042: "Policy requirements for certification authorities issuing public key certificates".

[3] ETSI TS 101 733: "Electronic signature formats".

[4] ETSI TS 101 861: "Time stamping profile".

[5] ETSI TS 101 862: "Qualified certificate profile".

[6] ETSI TS 102 023: "Policy requirements for time-stamping authorities".

[7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[8] CEN/ISSS WS/E-Sign Workshop agreement CWA 14167-1: "Security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System security requirements".

[9] CEN/ISSS WS/E-Sign Workshop agreement CWA 14170: "Security requirements for signature creation applications".

[10] ITU-T Recommendation X.520: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[11] IETF RFC 2247: "Using Domains in LDAP/X.500 Distinguished Names".

[12] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (obsoletes RFC 2459).

[13] IETF RFC 3039: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

3 Definitions and abbreviations

For the purposes of the present document, the terms, definitions and abbreviations given in TS 101 456 [1], TS 102 042 [2], TS 101 733 [3], TS 101 861 [4], TS 101 862 [5] and TS 102 023 [6] apply.

4 TS 101 456 - Qualified Certificate Policy and TS 102 042 - Normalized Certificate Policy

4.1 Keys Certified Under Multiple Policies

Comment

We have not looked at possible conflicts, which may arise when there are more than one certificates issued to a key pair, e.g. generated and residing on a card. These certificates may be issued by different CAs, under different CPs.

I have, so far, identified one potential conflict. Assume that two CAs issue two different certificates to the same key, one specifying key usage for el. signatures only, the other for encryption. The two CAs don't know about each other, users can hardly made responsible for things they don't have a clue about. Without a flag in the CP the situation is not transparent to auditors either.

We should consider to look at:

a) whether there are other potential conflicts for the configuration described above, and

b) how to address them.

Maintenance of the policies is probably the right place to deal with this.

Discussion

Key multiple usage:

Providing a framework to support the use of e-signatures and creating an environment which will promote trust, and protecting the interests of consumers relying on e-signatures; is an objective under EESSI and the Directive.

It is technically possible that the same public key may be included in more than one certificate. (This could well be the case, for example, where the key pair is generated by the subscriber, which he sends to more than one certification authority.) In general, there may be nothing objectionable in this, but for some applications, this may be undesirable, particularly where higher levels of assurance are required.

Issue revolves around:

a) the quality of the key pair generated; and

b) the creation of a close association between the key pair and an application for which it is to be used.

Qualified certificates are designed to offer a high level of assurance which needs to be maintained in all aspects of the service. TS 101 456 [1] does not prohibit subscriber generation of keys. It should be preferred that the certification authority takes responsibility for generating the keys. This is not currently part of Electronic Signatures Directive, nor conformance guidance.

Qualified certificates may be used to support an article 5.1 e-signature; they may also be used for authentication in general use.

Article 5.1 signatures must be recognized in legal proceedings as the equivalent of hand written signatures. Other electronic signatures may be recognized as such, although probably only if they satisfy at least the definition of an advanced electronic signature under article 2.2.

It is suggested, therefore, that subscriber key pairs issued for the purpose of creating any type electronic signature which is intended to fulfil the function of a hand written signature, i.e. one which is to be treated as a handwritten signature by a relying party, should be restricted to that purpose.

In respect of both qualified certificates AND any e-signature which is intended to be a handwritten signature equivalent, there is a need that they should provide a high level of assurance to any third party who may reasonably rely on this.

Signatures in the real world perform two main functions:

- they indicate a will or intention by the signer to take on a commitment. (The exact nature of the commitment may be ambiguous except by reference to the document to which it is applied, or to some other evidence); and
- a signature is ***evidence*** of itself, i.e. of the act of signing.

Therefore, there are two elements which electronic signatures cannot prove:

a) the ***intention*** to express a commitment; and

b) the ***intention*** to create the signature.

Even an Article 5.1 electronic signature created using public key cryptography, i.e. digital signatures, are ***not*** (unless there is other evidence) capable of demonstrating the signer's intentions. However, ***intent*** is an essential element of signing and there is an urgent need to find a means of incorporating this factor into an electronic signature, which is intended as a handwritten signature.

One factor which could provide evidence of the intention to create a signature equivalent to a h/w one, is to "bind" the signing key to the application. This could be achieved by restricting the use of a key to a "signing" application, i.e. by including it in a certificate (qualified) which specifies a key usage.

The relying party needs to know (in order to rely on a "e-signature equivalent to handwritten signature") that the signer will not be able to deny his intention to make the signature as a handwritten one. This requires two steps:

- making it clear to the signer that his key, certificate, must only be used to create an e-signature, enforcing that obligation either by technical or (second best) by legal means;
- ensuring a means of signature creation which makes it clear to the signer that he is creating is equal to a h/w one; preventing (as far as possible) the use of his key pair for any other purpose.

As a preference, the sscd on which the keys are stored should also be dedicated to a hw sign, but this may carry unrealistic costs implications. The reason is that will give an opportunity to include something on the casing of the sscd which will alert the signer to its significance as a signing device.

The fact that:

- key usage is restricted, and
- the signer probably knew that key usage was restricted

will provide prima facie evidence that the signer knew what kind of electronic signature he was making, i.e. that a commitment that may be enforced by law was being undertaken as a result.

Enforcement:

It has been argued that certification authorities should be free to decide for themselves whether to enforce obligations against a subscriber. There may be many reasons for **NOT** taking any enforcement action:

- the certification authority does not regard the breach as being significant;
- the certification authority itself has not suffered any loss, neither will its inaction is not (currently) in contravention of any auditing criteria, or guidance;
- the subscriber is a customer, there is a real conflict of interest - it is not a good marketing practice to bring legal proceedings against customers; and
- ***cost*** of legal proceedings.

The reliability of signatures = to h/w signatures is a matter of public interest, therefore, the responsibility for ensuring their effectiveness should not just be left to the discretion of a certification authority. The role of the certification authority should be to take such steps as are reasonably within its competence and power to ensure a single use of keys used to create such signatures. This could be provided for by including appropriate requirements in TS 101 456 [1] and TS 102 042 [2] (or for the time being, in any appropriate maintenance document).

In due course, it is to be hoped (and expected) that national laws will impose the same level of responsibility of a signer as currently exist in relation to a handwritten signature. However, this cannot happen for so long as there is ambiguity surrounding the electronic signature creation.

Jane Hill

Proposed Resolution

To be resolved.

4.2 Advise on use of SSCD

I am wondering whether we ommited a clause in TS 101 456 [1] to state that the CA shall inform their subscribers about the kind of environnment that he shall use for the SSCD, pointing to CWA 14170 [9]: Security requirements for Signature Creation Systems.

Proposed Resolution

Add to clause 7.2.9:

"NOTE: It is recommended that the CA advises subscribers as to the environments in which the SSCD should be used. This includes the characteristics of the devices and applications used, and the purpose or intention of the act of signing."

4.3 Use of CA key for multiple policies

Comment

I think it is not very feasible to require CSPs not to use same signing key for QCPs and NCPs. That's because I cannot see why that would nesessarily compromise security. Probably we could advice CSPs to use dedicated keys (use should instead of shall), but not make that as a requirement.

Proposed Resolution

a) Replace text in clause 7.2.5 with:

The signing keys(s) used for generating certificates, as defined in clause 7.3.3, and/or issuing revocation status information, shall not be used for any other purposes if this results in the violation of ***THE SECURITY MEASURES OR ANY OTHER SPECIFIC LIMITATIONS PROVIDED FOR*** in this policy.

NOTE: It is recommended that different CA keys are used to issue certificates under different policies.

b) An alternative resolution is to delete this clause.

Jan Sauer comment: With the proposed new wording of clause 7.2.5 a), the QCP will contain a requirement that something should not be done if it would result in violation of the QCP. Same for NCP.

This is not a requirement that can be understood easily. Actually, I think that the new wording is meaningless.

4.4 Reference to CWA 14167-1 in clause 7.4.7

Comment

Update clause 7.4.7, note 1 to explicitly reference CWA 14167-1 [8] and add the reference to the bibliography/references.

RGW comment: "however, any such reference should not be to the exclusion of any other means of adequately satisfying the requirements of Directive 1999/93/EC Annex II (f)".

4.5 Proposed Amendments from Italian UNINFO on TS 101 456

Introduction

The present document means to give suggestions in order to modify TS 101 456 [1] V1.2.1: the proposed changes concern both document's stylistic aspects (spelling/syntax) and the content of the deliverable.

For each paragraph to be modified the numeric reference is given and a new statement is proposed (highlighted in bold): those parts of statement that have to be deleted are highlighted in bold and struck out.

a) Spelling/Syntax corrections

✓ **2 References**

[9] FIPS PUB 140-2 (2001): "Security Requirements For Cryptographic Modules".

✓ **4.1 Certification Authority**

(first section) "The Certification Authority has overall responsibility for the provision of certification services identified in **clause 4.2**. **The certification authority is identified in the certificate as the issuer and its private key is used to sign qualified certificates**. "

(second section) "However, the **private** key used **to sign** the certificates, ..."

b) Content corrections

✓ **4.2 Certification services**

"Dissemination service: disseminates certificates to subjects, and if subject consents, **makes them available** to relying parties. This service also **makes available** the CA's terms and conditions….to subscribers ad relying parties."

✓ **6.2 Subscriber Obligations**

The paragraph 6.2 is proposed to be modified in the following way:

The CA shall oblige, through agreement (see clause 7.3.1 h)), the subscriber:

1) to make the subject aware (in the case the subscriber and the subject are not the same person) of the CA's terms and conditions as provided for in section 7.3.1.a);

2) to ensure that the subject fulfils the following obligations:

   a) submit accurate and complete information to the CA, **directly or through the subscriber**, in accordance with the requirements of this policy, particularly with regards to registration;

   b) only use the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber (see clause 7.3.4);

   c) exercise reasonable care to avoid unauthorized use of the subject's private key;

   d) idem;

   e) idem;

   f) idem;

   g) notify the CA without any reasonable delay, **directly or through the subscriber,** if any …;

   h) idem.

✓ **7.2.1 Certification authority key generation**

b) CA key generation shall be carried out….

   - meets the requirements identified in FIPS PUB 140-1 **[5]** or **140-2 [9]** level 3 or higher

✓ 7.2.2 Certification authority key storage, backup and recovery

a) "The CA…."

- ... FIPS PUB 140-1 **[5] or FIPS PUB 140-2 [9]**

✓ 7.2.9 Secure-Signature-Creation device

NOTE 2: "Separation may be achieved by ensuring distribution **of activation data** and delivery **of secure signature creation device**…"

✓ 7.3.1 Subject Registration

f) This comma should be cancelled from this section (Subject registration) and inserted in "Subscriber's obligations" (this kind of information is provided at the moment of signing the agreement by the subscriber).

NOTE 7: The item above…

i) "…legal proceedings according to the national law of the country where the Certification Service Provider is established."

✓ 7.3.3 Certification generation

a) "if the CA generated the **subject's** key:

- the procedure of issuing….
- the private key is securely passed to the registered subject"

✓ 7.3.6 Certificate revocation and suspension

g) Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least daily and:

- every CRL shall state a time for next CRL issue; and
- a new CRL may be published before the stated time of the next CRL issue;
- the CRL shall be signed by **the** certification authority or an authority designated by the CA.

✓ 7.4.4 Physical and environmental security

Certificate generation, subject device provision and revocation management

e) Physical protection shall be achieved through the creation of clearly defined security perimeters (…) around the certificate generation, subject device provision and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.

NOTE 1: As defined at the beginning of the document, a "subject device provision service <u>prepares</u> and <u>provides</u> a signature-creation device to subjects". In the case the CA gives Registration authorities the responsibility <u>to provide</u> signature devices to subjects comma e) is applicable only to subject device preparation (and NOT provision).

g) idem.

NOTE 2: …

NOTE 3: …

✓ 7.4.5 Operations management

c) **Media used within the CA shall be securely handled to protect media from damage, theft,** and **unauthorized access.** Media life cycle management shall be such to proactively prevent obsolescence.

✓ **7.4.8 Business continuity management and incident handling**

Revocation status

a) In the case of compromise….

- **Inform all subscribers** (and these one in turn will inform the subjects) and any entity with which it has agreements or other form of established relations, among which relying parties and CAs …

✓ **7.4.9 CA Termination**

CA general

a) before the CA terminates…the CA shall

- inform all subscribers (and these one in turn will inform the subjects) and any entity with which it has agreements or other form of established relations, among which relying parties and CAs**.**

✓ **7.4.11 Recording of Information Concerning Qualified Certificates**

The CA shall ensure that all relevant information concerning a qualified certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings **according to the national law of the country where the Certification Service Provider is established**."

Registration

i) The Ca shall ensure that all registration information…

any specific choices in the subscriber agreement (e.g. subjects' consent to publication of certificate)**.**

4.6 Proposed Amendments from Italian UNINFO on TS 102 042 v.1.1.1 (2002-04)

Introduction

The present document means to give suggestions in order to modify TS 102 042 [2] V1.1.1: the proposed changes concern both document's stylistic aspects (spelling/syntax) and the content of the deliverable.

For each paragraph to be modified the numeric reference is given and a new statement is proposed (highlighted in bold): those parts of statement that have to be deleted are highlighted in bold and struck out.

Because of TS 102 042 [2] includes much text that is in common with TS 101 456 [1] the proposed amendments are roughly the same as those proposed to TS 101 456 [1].

a) Spelling/Syntax corrections

✓ **2 References**

[6] FIPS PUB 140-2 (2001): "Security Requirements For Cryptographic Modules".

✓ **3.1 Definitions**

Extended Normalized Certificate Policy: normalized certificate policy requiring use of a secure user device.

✓ **3.2 Abbreviations**

NCP+ Extended Normalized Certificate Policy.

✓ **4.1 Certification Authority**

(first section) "The Certification Authority has overall responsibility for the provision of certification services identified in **clause 4.2**. **The certification authority is identified in the certificate as the issuer and its private key is used to sign certificates**. "

(second section) "However, the **private** key used **to sign** the certificates…."

a) Content corrections

✓ 4.2 Certification services

"Dissemination service: disseminates certificates to subjects, and if subject consents, **makes them available** to relying parties. This service also **makes available** the CA's terms and conditions….to subscribers ad relying parties."

✓ 6.2 Subscriber Obligations

The paragraph 6.2 is proposed to be modified in the following way:

The CA shall oblige, through agreement (see clause 7.3.1 h)), the subscriber:

1) to make the subject aware (in the case the subscriber and the subject are not the same person) of the CA's terms and conditions as provided for in section 7.3.1.a);

2) to ensure that the subject fulfils the following obligations:

   a) accurate and complete information is submitted to the CA, **directly or through the subscriber**, in accordance with the requirements of this policy, particularly with regards to registration;

   b) the key pair is only used in accordance with any other limitations notified to the subscriber (see clause 7.3.4);

   c) reasonable care is exercised to avoid unauthorized use of the subject's private key;

   d) idem;

   e) idem;

   f) idem;

   g) idem;

   h) notify the CA without any reasonable delay, **directly or through the subscriber,** if any …;

   i) idem.

✓ 7.2.1 Certification authority key generation

b) [CHOICE]

[LCP] CA key generation shall be carried out….

- meets the requirements identified in FIPS PUB 140-1 **[2]** or **140-2 [6]** level 2 o higher

[NCP] CA key generation shall be carried out within a device which either:

- meets the requirements identified in FIPS PUB 140-1 **[2]** or **140-2 [6]** level 3 o higher;

✓ 7.2.2 Certification authority key storage, backup and recovery

a) [CHOICE]

[LCP] "The CA…."

- ... FIPS PUB 140-1 [2] or FIPS PUB 140-2 [6]…

[NCP] "The CA private signing key…":

- meets the requirements identified in FIPS PUB 140-1 **[2]** or **140-2 [6]** level 3 o higher;

✓ 7.2.8 CA provided subject key management services

e) [CONDITIONAL] If a copy of the subject's **private** key is no required…

✓ 7.2.9 Secure user device preparation

d) Where the secure user device has associated user activation data ….separately from the **secure user device**.

NOTE: "Separation may be achieved by ensuring distribution **of activation data** and delivery **of secure user device**…"

✓ 7.3.1 Subject Registration

b) [CONDITIONAL]: If the subject is a person and not the same as the subscriber, the subject shall be informed of his/her obligations.

j) **This comma should be cancelled from this section (Subject registration) and inserted in "Subscriber's obligations" (this kind of information is provided at the moment of signing the agreement by the subscriber).**

l) The CA shall record the signed …

- if required by the CA, agreement by the subscriber to **use** secure user device;
- confirmation that the information held in the certificate **is** correct.

m) "…legal proceedings **according to the national law of the country where the Certification Service Provider is established.**"

✓ 7.4.4 Physical and environmental security

Certificate generation, subject device provision and revocation management

e) Physical protection shall be achieved through the creation of clearly defined security perimeters (…) around the certificate generation, subject device provision and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.

NOTE 1: As defined at the beginning of the document, a "subject device provision service **prepares** and **provides** a signature-creation device to subjects". In the case the CA gives Registration authorities the responsibility **to provide** signature devices to subjects comma e) is applicable only to subject device preparation (and NOT provision).

g) idem.

NOTE 2: …

NOTE 3:…

✓ 7.4.5 Operations management

c) Media used within the CA shall be securely handled to protect media from damage, theft, and unauthorized access. Media life cycle management shall be such to proactively prevent obsolescence.

✓ 7.4.8 Business continuity management and incident handling

Revocation status

a) **In the case of compromise….**

- **Inform all subscribers** (and these ones in turn will inform the subjects) and any entity with which it has agreements or other form of established relations, among which relying parties and CAs …

✓ 7.4.9 CA Termination

CA general

a) before the CA terminates…the CA shall

- inform all subscribers (and these one in turn will inform the subjects) and any entity with which it has agreements or other form of established relations, among which relying parties and CAs.

✓ **7.4.11 Recording of Information Concerning Qualified Certificates**

The CA shall ensure that all relevant information concerning a qualified certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings **according to the national law of the country where the Certification Service Provider is established**."

Registration

i) The Ca shall ensure that all registration information…

any specific choices in the subscriber agreement (e.g. subjects' consent to publication of certificate)**.**

4.7 Suggested Amendments from EESSI Evaluation see EESSI #21(2002)04 - section 6

i) Mandate that either a formal assessment or a claim supported by an audit is required before a CSP is allowed (by the relevant Supervisory Authority) to issue its first qualified certificate.

5 TS 101 733 - Electronic Signature Format

5.1 Archive Timestamp

The Archive Timestamp attribute is a timestamp of the user data and the entire electronic signature. If the Certificate values and Revocation Values attributes are not present these attributes shall be added to the electronic signature prior to the timestamp. The Archive Timestamp attribute is an unsigned attribute. Several instances of this attribute may occur with an electronic signature both over time and from different TSAs.

The following object identifier identifies the Nested Archive Timestamp attribute:

```
id-aa-ets-archiveTimestamp OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 27}
```

Archive timestamp attribute values have the ASN.1 syntax ArchiveTimeStampToken

```
ArchiveTimeStampToken ::= TimeStampToken
```

The value of messageImprint field within TimeStampToken shall be a hash of the concatenated values (without the type or length encoding for that value) of the following data objects as present in the electronic signature:

(a list of 11 different attributes follows)

For further information and definition of TimeStampToken see clause 10.4.

The timestamp should be created using stronger algorithms (or longer key lengths) than in the original electronic signatures and weak algorithm (key length) timestamps.

5.2 Early comments from Italian UNIFO

- References to the various RFCs and Internet Drafts from PKIX (especially RFC 2459/3280 [12]).
- Signing Time optional?
- Time-mark: the use of the time-mark may solve the problems related to the compromission of TSA private key.
- The use of the "Invalidity Date" extension of a CRL entry may invalidate all the formats for long term signatures.
- There is the need for a better specification of the verificationprocesses (initial and usual), even if it is a matter of CWA 14170 [9].

- There is the need for the good practices while using the different formats, in order to give a reader a comprehensive and overall picture of the electronic signature model.
- There is the need to introduce some explanation about the relationship between the rules (some naming and path constraints) included in the Certificate Policy and the ones included in the Signature Policy even if it is a matter of "Signature Policy Report".

6 TS 101 861 - Time Stamp Profile

6.1 Clause 5.2.1 - Accuracy and precision of time

This clause currently includes the requirements:

- "a genTime parameter limited to represent time with one second is required,
- a minimum accuracy of one second is required,"

What is the aim of the first requirement? This could be read to imply that time representation of better accuracy than 1 second is not allowed.

Proposed Change

Replace with:

- "the genTime parameter shall be to the precision of one second or better;
- the time shall be to the accuracy of one second or better;"

6.2 Clause 5.2.1 ordering

This clause states:

- "an ordering parameter missing or set to false is required,"

What is the reason for not allowing ordering if the TSA wants to provide this service. Surely, all that the aim is to not make it mandatory for TSAs to provide ordering.

Proposed Change

Delete item.

6.3 Clause 6 Mandate support for store and forward

It is unclear why the TSA has to support access via store and forward? Most existing time-stamp servers do not support store and forward. Also, with the accuracy currently proposed, the use of store and forward is inappropriate.

Proposed Change

Update as indicated:

One on-line protocol ~~and one store and forward~~ protocol must be supported for every Time Stamping Authority (TSA).

6.4 Clause 7.1.1

It not explicit as to which algorithm identifier this refers to. Presumeably, this is HashAlgorithm in MessageImprint.

It is not common practice for "NULL" to be explicitly included in the algorithms parameters. Why not allow the parameters to be non-present.

Proposed Change

Update as indicated:

"The AlgorithmIdentifier parameters field is optional. ~~If present, the parameters field shall contain an ASN.1 NULL.~~

Implementations should accept SHA-1 AlgorithmIdentifiers with absent parameters ~~as well as NULL parameters~~.

~~Implementations should generate SHA-1 AlgorithmIdentifiers with NULL parameters."~~

7 TS 101 862 - Qualified Certificates Profile

7.1 Country Name

Comment

It is suggested that there are two ways to indicate the country of supervision:

i) by using the countryName attribute type defined in ITU-T Recommendation X.520 [10]; (This is what our standard mandates) or

ii) by using the domainComponent attribute type defined in RFC 2247 [11]. (This is the approach used in Microsoft's Active Directory)

This is not supported in our standard. David would like that to be added to TS 101 862 [5].

7.2 Suggested Amendments EESSI Evaluation see EESSI #21(2002)04 - section 6

A Certificate Revocation List (CRL) is just as complex a data structure as a certificate. Whilst we have a qualified certificate profile in deliverable TS 101 862, we do not have a CRL profile in any of the deliverables. This is a significant deficiency that could impede interworking.

Proposed Change

This is to be addressed by CEN ISSS activity on CRL profiles.

7.3 Italian: UNINFO STT Area # 4 Proposed amendments to TS 101 862 v1.2.1

Introduction

TS 101 862 [5], clause 1 specifies: "The present document defines a technical format for Qualified Certificates that can be used by issuers of Qualified Certificates to comply with annex I and II of the Directive." Amendments are hereafter suggested in order to better achieve compliance with Directive requirements.

Additionally, since TS 101 862 [5] is based upon RFC 3039 [13], some comments to RFC 3039 [13] are also made, which lead to some proposed TS 101 862 [5] amendments.

7.3.1 References to be updated

Since TS 101 862 has been published, RFC 2459 has been replaced by RFC 3280 [12]. Thus it is suggested to accordingly modify reference [3] in the next TS version.

7.3.2 CSP identifier

a) Annex I of Directive 1999/93/EC, specifies: "Qualified certificates must contain:

….

(b) the identification of the certificate-service-provider and the State in which it is established".

TS 101 862 specifies that the name of the issuer (clause 4.1): "MUST contain a country name stored in the countryName attribute", but nothing is said about the CSP Identifier. It is therefore herewith proposed the organizationName attribute to be also mandatory:

b) Additionally, since one single CSP may set up different Certification Authorities (e.g. for issuing qualified certificates on behalf of different client organizations or for issuing qualified certificates with some different extensions) it is proposed that an attribute is used to identify the single CA.

From the above comments stems the following proposed amendment to clause 4.1 text:

"The name of the issuer contained in the issuer field (as defined in clause 3.1.1 in RFC 3039 [4]) MUST contain:

1) a country name stored in the countryName attribute. The specified country SHALL be the country in which the issuer of the certificate is established;

2) the organizationName attribute specifying the relevant CSP identifier.

If one CSP sets up different CAs, each one specific to issue a different qualified certificate type, it is also RECOMMENDED that the issuer field contains the serialNumber attribute with a value which SHALL be unique for each CA within the same CSP. Optionally, the CSP MAY use the organizationalUnitName attribute to specify further details of the specific CA."

7.3.3 Identity of the signer

Article 2.9 of the quoted Directive states: "certificate" means an electronic attestation which links signature-verification data to a person and **confirms the identity of that person**". In order to "confirm the identity" of the signer the following data are commonly deemed necessary and used:

- Date of birth
- Place of Birth
- Gender
- Country of Citizenship

For this reason it is suggested that insertion in subjectDirectoryAttributes of the corresponding attributes, as listed in RFC 3039 section 3.2.1, is at least RECOMMENDED in TS 101 862, unless a pseudonym is used "which shall be identified as such" (Directive Annex I, item c). Please see subsequent item 4).

Proposed text

"4.2 SubjectDirectoryAttributes extension

4.2.1 Identity relevant fields

(NOTE: Renumbering of the subsequent sections is required.)

In order to provide reliable information on the qualified certificate subject's identity, consistently with Directive [1] definition of certificate, the name is not sufficient. Actually the following data are commonly deemed necessary: date of birth, place of birth, gender, country of citizenship.

It is therefore RECOMMENDED that a subject's certificate bears at least the following fields in the subjectDirectoryAttributes extension:

- dateOfBirth;
- placeOfBirth;
- gender;
- countryOfCitizenship.

Where necessary, the countryOfResidence field MAY also be used.

Signature verification applications SHALL be able to handle the previously mentioned fields."

7.3.4 Pseudonyms

A requirement is needed on how the pseudonym is to be "identified as such". RFC 3039 [13] allows both "commonName" or "pseudonym" attributes to carry the pseudonym. This could lead to misunderstandings, even malicious ones, if a commonly agreed manner to identify pseudonyms is not defined. In fact a fictitious name like "John Doe" recorded in the "commonName" and furnished with date and place of birth, gender and citizenship, could be misinterpreted as being a "real" name. To avoid mistakes it is then proposed to add a requirement in TS 101 862 [5] that pseudonyms MUST be inserted in the "pseudonym" attribute.

Proposed text

"4.3 Subject field

4.3.1 Pseudonym attribute

In order to avoid misinterpretation of the data held in the "commonName" attribute, the "pseudonym" attribute SHALL be used when the subject field is to hold the subject's pseudonym. The pseudonym SHALL NOT be held in the "commonName" attribute.

Signature verification applications SHALL be able to handle this attribute as above specified."

7.3.5 SerialNumber attribute

Even the data mentioned in the previous item 2) may not be enough to uniquely identify one person: in fact in small towns or villages many people happen to share the same surname and quite a few of them have the same given name too, so it is possible to find two persons with the same name born in the same place on the same day. Therefore it is suggested that TS 101 862 [5] at least MANDATES usage of the serialNumber attribute in the subject field. This field, SHALL hold at least "`an identifier assigned by a government or civil authority",` as per RFC 3039 [13], section 3.1.2. In addition to such identifier and where necessary to comply with RFC 3039 [13] following sentence: "`It is the CA's responsibility to ensure that the serialNumber is sufficient to resolve any subject name collisions`", each CA SHALL add a code it assigns itself, which SHALL be unique for each certificate of that subject. A printableString character separator (e.g. "/") could be used between the two data. As an example: "RGGFNC42H30A952P/0001".

When the "pseudonym" attribute is used, a fictitious identifier MAY be used in the serialNumber attribute, e.g. "PseudonymA/00001".

Proposed text

"4.3.2 Serial Number attribute

The serialNumer attribute SHALL be used in the subject field to carry an identifier assigned by a government or civil authority.

If one CA issues the same subject several certificates for different usages or roles, it SHALL ensure the serialNumber "differentiate[s] between names where the subject field would otherwise be identical" (as stated in RFC 3039 [4], section 3.1.2), by adding, to the previously mentioned authority assigned identifier, one code which is unique for each certificate of that subject. The authority assigned identifier and the CA assigned code SHALL be separated with a printableString character separator that is not used within any of the two code types (e.g. "/"). As an example: "RGGFNC42H30A952P/0001".

When the "pseudonym" attribute is used, the serialNumer attribute MAY contain a fictitious code, e.g. "PseudonymA/00001".

Signature verification applications SHALL be able to handle this attribute as above specified."

7.3.6 The key usage

There has been a long debate on RFC 3039 [13] section 3.2.3 following text: "If the key usage nonRepudiation bit is asserted then it SHOULD NOT be combined with any other key usage, i.e. if set, the key usage non-repudiation SHOULD be set exclusively."

In order to settle it, it is suggested to mandate the unique use of the non-repudiation bit into TS 101 862 [5].

Additionally, since also authentication certificates can be "qualified certificates", it is suggested to add the following statement: "Should the key usage digitalSignature bit be asserted, the RFC 3280 provisions SHALL be complied with."

It is also suggested that TS 101 862 [5] mandates the keyUsage extension to be marked critical, to avoid any possible malicious misuse of the non-repudiation and of the authentication certificates.

Proposed text

"4.4 Key Usage extension

If the key usage nonRepudiation bit is asserted then it SHALL NOT be combined with any other key usage, i.e. if set, the key usage non-repudiation SHALL be set exclusively.

Should, instead, the key usage digitalSignature bit be asserted, the RFC 3280 provisions SHALL be complied with.

The keyUsage extension SHALL be marked critical to avoid possible malicious misuse of different certificate purposes.

Signature verification applications SHALL be able to handle this attribute as above specified."

8 TS 102 023: Time-stamping Policy

8.1 UNINFO Italian Comments

Introduction

The present document means to give suggestions in order to modify TS 102 023 [6] v.1.1.1: the proposed changes concern both document's stylistic aspects (spelling/syntax) and the content of the deliverable.

For each paragraph to be modified the numeric reference is given and a new statement is proposed (**highlighted in bold**): those parts of statement that have to be deleted are highlighted in bold and struck out.

f) Spelling/Syntax corrections

✓ Introduction

"…The quality of this evidence is based **on** the process of creating and managing the data structure that **represents** ….and **on** the quality of the parametric data points…In this instance this **is** the time data and how…".

"….Another one consists to use….Policy requirements to cover **this** case …."

✓ 4.3 Subscriber

(second section) "…In any case the organization will be responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization…"

✓ 4.4.3 Approach

"A time-stamp policy may be defined by the user of time-stamp services …"

✓ 7 Requirements on TSA practices

"The requirements ... where considered necessary to provide the necessary confidence that those objectives…"

g) Content corrections

✓ Scope

"…The current document addresses requirements for TSAs issuing time stamp tokens **digitally signed by the TSA itself that is synchronized with** Coordinated universal time (UTC)"

✓ 2 References

[7] FIPS PUB 140-2 (2001): "Security Requirements For Cryptographic Modules".

✓ 6.1.1 General

"…The TSA shall also ensure adherence to any additional obligations indicated in the time-stamp **token..."**

✓ 6.2 Subscriber obligations

"NOTE: It is advisable that, when obtaining a time-stamp token, the subscriber verifies that the **time-stamp token's digital signature is a valid one**, particularly that the private key used to sign the time-stamp token has not been compromised".

✓ 6.3 Relying party obligations

a) verify that the time-stamp token's **digital signature is a valid one**, particularly that the private key used to sign the time-stamp token has not been compromised;

b) Take into account any limitations on the usage of the time-stamp **token** indicated by the time-stamp policy**;**

✓ 7.1.2 TSA disclosure statement

d) The expected life-time of the signature **associated to** the time-stamp token

j) The period of time during which TSA event logs (see clause **7.4.11**)

✓ 7.2.1 TSA key generation

"The TSA shall ensure that any cryptographic keys are generated under controlled circumstances "

b) The generation of the TSA's signing key(s) shall be carried out within a cryptographic module(s) which either:

- Meets the requirements identified in FIPS 140-1[4] or **FIPS 140-2 [7]** level 3 or higher, or...

✓ 7.2.2 TSA private key protection

a) The TSA private signing key shall be held and used within a cryptographic module which:

- Meets the requirements identified in FIPS 140-1 [4] or **140-2 [7]** level 3 or higher; or

✓ 7.2.4 Rekeying TSA's Key

NOTE 1: The following additional considerations apply when limiting that lifetime:

- Clause **7.4.11** requires that records concerning time-stamping services shall be held for a period of time after the expiration of the validity of the TSA's **signature verification (public) key as appropriate for providing necessary legal evidence and as notified in the TSA disclosure statement**. The longer the validity period of the TSA certificate will be, the longer the size of the records to be kept will be.

✓ 7.2.5 End of TSA key life cycle

a) Operational or technical procedures shall be in place to ensure that a new key is put in place when a TSA's key expires **or is substituted for other reasons (e.g according to what established by national law)**

c) The TST generation system SHALL reject any attempt to issue TSTs if the signing private key **is not valid anymore (e.g. because it has expired or has been substituted).**

✓ 7.2.6 Life cycle management of cryptographic module used to sign time-stamp tokens

✓ 7.3.1 Time-stamp token

NOTE 2: A protocol **for requests/responses of time-stamp tokens** is defined in RFC **3161** and….

h) The name of the issuing TSA….

- an identifier for the **time-stamping unit** which issues the **time-stamp tokens**.

NOTE 4: The name of the issuing TSA can be gained from the TSA's public key certificate (if present) or from a TSTInfo field (in particular TSA field within TSTInfo), if RFC 3161 is used.

✓ 7.3.2 Clock Synchronization with UTC

NOTE 2: **Subscribers** and relying parties…

✓ 7.4.5 Operations management

c) Media used within the TSA trustworthy systems shall be securely handled to protect media from damage, theft **and** unauthorized access. **Media life cycle management shall be such to proactively prevent obsolescence.**

✓ 7.4.6 System Access Management

e) TSA personnel shall be accountable for their activities, for example, by retaining event logs (see clause **7.4.11**)

✓ 7.4.8 Compromise of TSA Services

c) In the case of compromise to the TSA's operation (e.g. **TSA private signing key** compromise)…

✓ 7.4.9 TSA termination

a) <u>Before the TSA terminates its time-stamping services the following procedures shall be executed as a minimum:</u>

<u>The TSA shall transfer obligations to a reliable party for maintaining event log and audit archives (see clause **7.4.11**) necessary to demonstrate the correct operation of the TSA for a reasonable period;</u>

✓ 7.4.11 Recording of Information Concerning Operation of Time-stamping Services

f) "Records concerning time-stamping services ... after the expiration of the validity of the **TSA's signature verification (public) key** as appropriate…"

History

Document history		
V1.1.1	February 2003	Publication