ETSI TR 102 046 V1.2.1 (2004-06)

Technical Report

Electronic Signatures and Infrastructures (ESI); Maintenance report

Reference

RTR/ESI-000020

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2004.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

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 [11] (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 [11] 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 specifications. 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 and on Technical Reports 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. Comments on Technical Reports will be taken into account in any subquent Technical Specification based on the Technical Report. It should be noted, however, that until new versions of new Technical Specifications are released the existing requirements stand.

Clause 4 contains the explanation of the maintenance process and describes the document structure; clause 5 collects the comment in a tabled style; the Annex A collects the comments in their original format keeping also the original text

The comments contained within the present document were maintained using a database and software tools (see TR 102 317 [1] for details).

2 References

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

[1] ETSI TR 102 317: "Electronic Signatures and Infrastructures (ESI); Process and tool for maintenance of ETSI deliverables".

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

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

[4] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); Electronic signature formats".

[5] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

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

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

[8] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

[9] ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

[10] ETSI TR 102 041: "Signature Policies Report".

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

[12] CWA 14167-1: "Security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System security requirements".

[13] CWA 14170: "Security requirements for signature creation applications".

[14] CWA 14167-2: "Security requirements for trustworthy systems managing certificates for electronic signatures - Part 2: Cryptographic module for CSP signing operations - Protection profile (MCSO-PP)".

[15] CWA 14168: "Secure signature-creation devices - Evaluation assurance level 4; English Version".

[16] CWA 14169: "Secure Signature-Creation devices "EAL 4+"".

[17] ISO/IEC 15408 (all parts): "Information technology - Security techniques - Evaluation criteria for IT security".

[18] ISO/TS 17090-1: "Health informatics - Public key infrastructure - Part 1: Framework and overview".

[19] ISO/TS 17090-2: "Health informatics - Public key infrastructure - Part 2: Certificate profile".

[20] ISO/TS 17090-3: "Health informatics - Public key infrastructure - Part 3: Policy management of certification authority".

[21] ISO/IEC 17799: "Information technology - Code of practice for information security management".

[22] ETSI TS 102 158: "Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates".

[23] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

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

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

[26] IETF RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (Obsoleted by RFC 3280).

[27] IETF RFC 2526: "Reserved IPv6 Subnet Anycast Addresses".

[28] IETF RFC 2527: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" (Obsoleted by RFC 3647).

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

[30] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

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

[32] FIPS PUB 140-2: "Security Requirements for Cryptographic Modules" (Supersedes FIPS PUB 140-1).

NOTE: These references relate to versions to which the issues apply. More up to date versions may be available through the ETSI and CEN web sites.

3 Definitions and abbreviations

For the purposes of the present document, the terms, definitions and abbreviations given in TS 101 456 [2], TS 102 042 [3], TS 101 733 [4], TS 101 903 [5], TS 101 861 [6], TS 101 862 [7], TS 102 023 [8], TR 102 038 [9] and TR 102 041 [10] apply.

4 Role and structure of the present document

4.1 Role of the present document in the maintenance process

The current document is the resolute of an ongoing maintenance process for ETSI Technical Specifications and Technical Reports in the area of Electronic Signatures and Infrastructures.

The document:

a) Provides a means of tracking the contributions received.

b) Organizes the contributions under the relevant document heading.

c) Processes the comments to identify a resolution.

The comments recorded in the present document will be taken into account in future work on ETSI deliverables. Until, the relevant specification has been revised the requirements of the current version applies.

4.2 Structure of the present document

4.2.1 Clause 5: fields and structure

Clause 5 constitutes the main part of the present document, it is the outcome of the organizing the contributions under the relevant heading and records the proposed resolution of the comment. The elementary comments and their metadata will be inserted in a database; the tables for each deliverable included in the clause 5 are automatically generated from the data stored in the aforementioned database.

Clause 5 collects the elementary comments grouped by deliverable. The set of comments related to a single deliverable are put in a single table. If the original contribution is a complex comment or a set of comments, the contribution is splitted into a number of single elementary comments. In the table, the comments are grouped and ordered by the number of the section they apply to. When the comments are effectively applied to a target deliverable, they are retained in the new version of the present document soon after their application, then in the subsequent version these comments will be removed.

The data and the metadata for each elementary comment are:

- *deliverable ID, version and section which the comments are applied to* (are the ones defined in annex A for each contribution);
- *source* (person and organization or group) *and date of the comment*;
- *ID of the elementary comment* (<deliverable_ID>-<unique_code>: e.g. "TS1015456-001"; the <unique_code> is a per-deliverable unique alphanumeric code and it consists of three characters; the progression of the codes is: from "000" to "999" then from "AAA" to "ZZZ" using the twenty six letters of the English alphabet);
- *reference to the original contribution*;
- *elementary comments text*;
- *elementary comments type; the values for this field may be only*:
    - *editorial*;
    - *technical*;
- *original proposal for comment resolution*;
- *resolution comment* (only for the following status values: *provisionally approved, applied, already applied, rejected, no change*);
- *resolution text* (only for the following status values: *provisionally approved, applied, already applied*);
- *resolution date* (only for the following status values: *provisionally approved, applied, already applied, rejected, no change*);
- *source of the comment resolution*: person and group (general maintenance STF, specific maintenance STF, TC-ESI group);
- *status of comment resolution*: the values for this field may be only:
    - *not yet processed*;
    - *in process*;
    - *provisionally approved* (*resolution date* field shall be filled in; the *resolution comment* field may be filled in);

  - *applied* (*resolution date* and *target version* fields shall be filled in; the *resolution comment* field may be filled in);
  - *already applied* (*resolution date* and *target version* fields shall be filled in; the *resolution comment* field may be filled in);
  - *rejected* (*resolution date* and *resolution comment* - with the reason - fields shall be filled in);
  - *no change* (*resolution date* and *resolution comment* - with the reason - fields shall be filled in);

- *version of the target deliverable*.

4.2.2 Annex A: Fields and structure

Annex A collects all comments received in their original format grouped by originator, then by deliverable. Annex A is the outcome of the tracking phase and could be intended as a historical section. If the text received as a whole includes comments on more deliverables, the text is splitted into blocks, each related to only one deliverable. This is the only elaboration done on the comments received. Every block of comments (at least one comment) received as a whole and related to only one deliverable is called contribution and is identified by a unique code. If received in different times, two (blocks of) comments have different identifier even if have been originated by the same source and are related to the same deliverable. In this case they are placed in different clauses in annex A.

The data and the metadata for each contribution are:

- *ID of the contribution* (with a unique prefix for each source: <Source_ID>-<unique_code>:
  e.g. "TC-ESI_1-001"; the <unique_code> is a per-source unique alphanumeric code and it consists of three characters; the progression of the codes is: from "000" to "999" then from "AAA" to "ZZZ" using the twenty six letters of the English alphabet) *to be referenced in the clause 5*;
- *source* (person and organization or group that originates the contribution) *of the contribution*;
- *date of the contribution*;
- *version which the contribution is referred to*;
- *original text of the contribution keeping also the original format* (as best as possible, minimizing the changes applied but being compliant with the ETSI drafting rules);
- *original proposed solution, if any*.

NOTE 1: The e-mail threads (mail exchanges) are treated as follows: every thread is considered as a whole contribution and the source and date contribution metadata are the ones of the thread's first message. Only the first message is kept both in annex A and clause 5. If this message has character and paragraph formatting, this is preserved; otherwise the Courier font is used.

NOTE 2: In order to respect the privacy, all the personal names have been removed from the present document; only the name of organizations, bodies and groups are retained.

5 Comments

This clause collects all the elementary comments obtained by pre-processing the original contributions in a structured format.

5.1 TS 101 456 - Qualified certificate policy

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-001	1.2.1	7.4.8	TC-ESI_1-001	14/03/2003	technical			not yet processed	
	Comment text	In clause 7.4.8 subsection CA General an additional sub-sub-section could be added, named "System backup and recovery", covering the need for these backups in order to resume functions upon disaster. This clause should specify that while the system data backup may be performed by one officer provided they have sufficient privileges, restore must be performed under at least dual control.							
	Original resolution proposal	To add a sub-sub-section named "System backup and recovery" in clause 7.4.8 subsection CA General. To be further specified.							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-002	1.2.1	7.4.3 g)	TC-ESI_1-002	30/01/2003	technical			not yet processed	
	Comment text	Clause 7.4.3.g) last bullet reads: "System Auditors: Authorized to view and maintain archives and audit logs of the CA trustworthy systems". IMO auditors must just look at archives and log files 'handcuffed'. If they can play with them, then their audit function is devoid of trust. If I am wrong please say it clear. If you, instead, agree, the sentence should read: "System Auditors: Authorized to view archives and audit logs of the CA trustworthy systems" performed under at least dual control.							
	Original resolution proposal	Clause 7.4.3.g) last bullet change the sentence "System Auditors: Authorized to view and maintain archives and audit logs of the CA trustworthy systems" to "System Auditors: Authorized to view archives and audit logs of the CA trustworthy systems".							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-003	1.2.1	2	UNSTT-001		editorial			not yet processed	
	Comment text	Update the reference FIPS PUB 140-1 (1994): "Security Requirements For Cryptographic Modules".							
	Original resolution proposal	New reference: FIPS PUB 140-2 (2001): "Security Requirements For Cryptographic Modules".							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-004	1.2.1	4.1 (1st para)	UNSTT-001		editorial			not yet processed	
	Comment text	Modify the text: "The certification authority has overall responsibility for the provision of the certification services identified in clause 4.1. The certification authority's key is used to sign the qualified certificates and it is identified in the certificate as the issuer".							
	Original resolution proposal	New text: "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".							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-005	1.2.1	4.1 (2nd para)	UNSTT-001		editorial			not yet processed	
	Comment text	Modify the text: "However, the key used to generate the certificates ..."							
	Original resolution proposal	New text: "However, the private key used to sign the certificates, ..."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-006	1.2.1	4.2	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "Dissemination service: disseminates certificates to subjects, and if the subject consents, to relying parties. This service also disseminates the CA's terms and conditions, and any published policy and practice information, to subscribers and relying parties".							
	Original resolution proposal	New text: "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".							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-007	1.2.1	6.2	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "The CA shall oblige, through agreement (see clause 7.3.1 h)), the subscriber to ensure that the subject fulfils the following obligations: a) submit accurate and complete information to the CA 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) if the subscriber or subject generates the subject's keys: - generate subject's keys using an algorithm recognized as being fit for the purposes of qualified electronic signatures; - use a key length and algorithm which is recognized as being fit for the purposes of qualified electronic signatures; NOTE 1: It is currently proposed that the recognition of algorithms, with associated key length, being fit for the purposes of qualified certificates is through a cryptographic advisory panel under the committee identified in article 9 of the Directive [1]. - only the subject holds the private key once delivered to the subject. e) if the certificate policy requires use of an SSCD (i.e. QCP public + SSCD), only use the certificate with electronic signatures created using such a device; NOTE 2: The above item is NOT applicable to qualified certificate policy: QCP public. f) if the certificate is issued by the CA under certificate policy QCP public + SSCD and the subject's keys are generated under control of the subscriber, generate the subject's keys within the SSCD to be used for signing; NOTE 3: The above item is NOT applicable to qualified certificate policy: QCP public. g) notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate: - the subject's private key has been lost, stolen, potentially compromised; or - control over the subjects private key has been lost due compromise of activation data (e.g. PIN code) or other reasons; and/or - inaccuracy or changes to the certificate content, as notified to the subscriber. h) following compromise, the use of the subject's private key is immediately and permanently discontinued."							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
	Original resolution proposal	New text: "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 clause 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."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-008	1.2.1	7.2.1	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "b) CA key generation shall be carried out within a device which either: - meets the requirements identified in FIPS PUB 140-1 [5] level 3 or higher"							
	Original resolution proposal	New text: "b) CA key generation shall be carried out... - meets the requirements identified in FIPS PUB 140-1 [5] or FIPS PUB 140-2 [9] level 3 or higher"							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-009	1.2.1	7.2.2	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "a) The CA private signing key shall be held and used within a secure cryptographic device which: - meets the requirements identified in FIPS PUB 140-1 [5] level 3 or higher;"							
	Original resolution proposal	New text: "a) "The CA..." - ... FIPS PUB 140-1 [5] or FIPS PUB 140-2 [9]"							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-010	1.2.1	7.2.9	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "NOTE 2: Separation may be achieved by ensuring distribution and delivery at different times, or via a different route."							
	Original resolution proposal	New text: "NOTE 2: Separation may be achieved by ensuring distribution of activation data and delivery of secure signature creation device..."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-011	1.2.1	7.3.1	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "f) The subscriber shall provide a physical address, or other attributes, which describe how the subscriber may be contacted. ... NOTE 7: The above item above does not apply for QCP Public. ... i) The records identified above shall be retained for at the period of time as indicated to the subscriber (see a) and b) above) and as necessary for the purposes for providing evidence of certification in legal proceedings."							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-012	1.2.1	7.3.3	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "c) if the CA generated the subjects key: - the procedure of issuing the certificate is securely linked to the generation of the key pair by the CA; - the private key (or SSCD - see clause 7.2.9) is securely passed to the registered subscriber or subject."							
	Original resolution proposal	New text: "c) "if the CA generated the subject's key: - the procedure of issuing... - the private key is securely passed to the registered subject"							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-013	1.2.1	7.3.6	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "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;"							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-014	1.2.1	7.4.4	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "e) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) 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. f) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CA's physical and environmental security policy for systems concerned with certificate generation, subject device provision and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc. g) Controls shall be implemented to protect against equipment, information, media and software relating to the CA services being taken off-site without authorization. NOTE 1: See ISO/IEC 17799 for guidance on physical and environmental security. NOTE 2: Other functions may be supported within the same secured area provided that the access is limited to authorized personnel."							
	Original resolution proposal	New text: "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:..."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-015	1.2.1	7.4.5	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "c) Media used within the CA shall be securely handled to protect media from damage, theft and unauthorized access."							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-016	1.2.1	7.4.8	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "Revocation status b) In the case of compromise the CA shall as a minimum provide the following undertakings: - inform all subscribers, relying parties and other CAs with which it has agreements or other form of established relations of the compromise;"							
	Original resolution proposal	New text: "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 ..."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-017	1.2.1	7.4.9	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "CA General a) Before the CA terminates its services the following procedures shall be executed as a minimum: - the CA shall inform all subscribers, relying parties and other CAs with which it has agreements or other form of established relations."							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-018	1.2.1	7.4.11	UNSTT-001		technical			not yet processed	
	Comment text	Modify the text: "i) The CA shall ensure that all registration information including the following is recorded: - type of document(s) presented by the applicant to support registration; - record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents, if applicable; - storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.3.1 h)); - any specific choices in the subscriber agreement (e.g. consent to publication of certificate);"							
	Original resolution proposal	New text: "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)."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-019	1.2.1	4.3	JCPKI-001	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	In clause "4.3 Certificate policy and certification practice statement", will it be better to add the specifications of the relations between them and the cross authentication?							
	Original resolution proposal								
	Resolution comment	Cross certificates not specifically addressed by current TS 101 456							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-020	1.2.1	7.2.4	JCPKI-001	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	"7.2.4 Key escrow", how to handle the problem of "legal monitor" in the wireless communications?							
	Original resolution proposal								
	Resolution comment	The present document only applies to signing keys (not data encryption keys) for which data monitoring and Escrow is not applicable.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-021	1.2.1	7.2	JCPKI-001	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	In clause "7.2 Public key infrastructure - Key management life cycle", why it doesn"t mention the operation of "certification authority key update" like the protocols in PKIX?							
	Original resolution proposal								
	Resolution comment	Issues relating to handling (including changing) CA keys is covered in clause 7.2.1 (generation) and clause 7.2.2 (storage backup etc).							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-022	1.2.1		TC-ESI_3-001		technical			not yet processed	
	Comment text	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 [2] 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.								

<table>
<tr><th>Comment ID</th><th>Deliverable version</th><th>Deliverable clause</th><th>Original contribution reference</th><th>Comment date</th><th>Comment type</th><th>Resolution source</th><th>Resolution date</th><th>Resolution status</th><th>Deliverable target version</th></tr>
<tr><td></td><td></td><td colspan="8">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 [2] and TS 102 042 [3] (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.</td></tr>
</table>

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-023	1.2.1		PR-001		technical			not yet processed	
	Comment text	I will give some comments on a high abstraction level: - For a CSP issuing qualified certificates TS 101 456 is the leading document. It has become a part of our voluntary certification schema and it is more or less copied into or (draft-)law on electronic signatures. Now I know CEN is not responsible for the TS 101 456 document but still I will give you this comments: • TS 101 456 is a set of requirements used by CSP's (technicians, quality managers and internal auditors) to build the CSP-organization and it is used by auditors to audit the CSP-organization. For the purpose it is used for TS 101 456 is too much written by technicians and too less by quality managers and auditors. It is not an easy document to handle. • TS 101 456 contains a lot of redundancy. - In your workshop agreements CEN has written: "This CEN Workshop Agreement can in no way be held as being an official standard as developed by CEN National Members". Nonetheless CWA 14169 Secure Signature Creation Devices has become a part of the Dutch (draft) law on electronic signatures. Can you give me some comments on this matter? - In our guidance on TS 101 456 we refer on the document CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. The problem with CWA 14167-1 however is that it not only specifies requirements on a TWS but it specifies also a lot of requirements on a CSP. In this way CWA 14167-1 doubles with ETSI TS 101 456. The scope of CWA 14167-1 is too wide?							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-024	1.2.1		EESSI-001		technical			not yet processed	
	Comment text	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.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-025	1.2.1	7.2.9	OTHER-001		technical			not yet processed	
	Comment text	I am wondering whether we omitted a clause in TS 101 456 [2] to state that the CA shall inform their subscribers about the kind of environment that he shall use for the SSCD, pointing to CWA 14170 [13]: Security requirements for Signature Creation Systems.							
	Original resolution proposal	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."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-026	1.2.1	7.2.5	OTHER-002		technical			not yet processed	
	Comment text	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 necessarily compromise security. Probably we could advice CSPs to use dedicated keys (use should instead of shall), but not make that as a requirement.							
	Original resolution proposal	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.							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-027	1.2.1	7.4.7	OTHER-003		technical			not yet processed	
	Comment text	Update clause 7.4.7, note 1 to explicitly reference CWA 14167-1 [12] 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)".							
	Original resolution proposal	Update clause 7.4.7, note 1 to explicitly reference CWA 14167-1 [12] and add the reference to the bibliography/references.							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-028	1.2.1	8	OTHER-004		technical			not yet processed	
	Comment text	It is currently not clear when a new certification policy is necessary							
	Original resolution proposal	Add to clause 8: "No changes should be made to a certificate policy which could affect a relying party's consideration on the reliability of the certificate issued by the CA."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-029	1.2.1	Introduction	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Please add the following text after the first paragraph. Another important requirement of electronic commerce is the ability to identify, not only the originator of electronic information in the same way that documents are signed using a hand-written signature, but also their attribute(s), e.g. their role(s) in an organization. This may be achieved using certification services in two ways: - using attributes included in Public Key Certificates (PKCs); - using attributes included in Attribute Certificates (ACs). The former case is covered in the present document. See TS 102 158 for the latter case.							
	Original resolution proposal	Please add the following text after the first paragraph. Another important requirement of electronic commerce is the ability to identify, not only the originator of electronic information in the same way that documents are signed using a hand-written signature, but also their attribute(s), e.g. their role(s) in an organization. This may be achieved using certification services in two ways: - using attributes included in Public Key Certificates (PKCs); - using attributes included in Attribute Certificates (ACs). The former case is covered in the present document. See TS 102 158 for the latter case.							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-030	1.2.1	Introduction	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Please change the following paragraph as subsequently specified. The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [1] (hereinafter referred to as "the Directive") identifies a special form of electronic signature which is based on a "qualified certificate". Annex I of this Directive 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). The mentioned Directive also covers the use of attributes in public key certificates, since it mentions the possibility to include attributes in Public Key Certificates (PKCs) (see annex I, clause d) which refers to the "provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended". The present document specifies baseline policy requirements on the operation and management practices of certification authorities issuing qualified certificates in accordance with the Directive. The use of a secure-signature-creation device, as required through annex III of the Directive, is an optional element of the policy requirements specified in the present document.							
	Original resolution proposal	Please change the following paragraph as subsequently specified. The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [1] (hereinafter referred to as "the Directive") identifies a special form of electronic signature which is based on a "qualified certificate". Annex I of this Directive 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). The mentioned Directive also covers the use of attributes in public key certificates, since it mentions the possibility to include attributes in Public Key Certificates (PKCs) (see annex I, clause d) which refers to the "provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended". The present document specifies baseline policy requirements on the operation and management practices of certification authorities issuing qualified certificates in accordance with the Directive. The use of a secure-signature-creation device, as required through annex III of the Directive, is an optional element of the policy requirements specified in the present document.							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-031	1.2.1	2	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Please add to the list: Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. -> a reference to this is asked to be added in clause 4.3.4							
	Original resolution proposal	Please add to the list: Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. -> a reference to this is asked to be added in clause 4.3.4							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-032	1.2.1	3.1	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Please add the following definitions. attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.							
	Original resolution proposal	Please add the following definitions. attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-033	1.2.1	4.1	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Typo -> Please change reference to clause 4.1 into reference to clause 4.2. Please add the following paragraphs at the end. When a signer signs a document it is of primary importance to be able to identify such signatory in the interest of accountability. This enables the transaction to be traceable. However, in many cases, in order to accept a signature, the acceptance criteria may not necessarily be based on the identity of the signer but instead, or additionally, on the qualification(s) of the signer. Qualifications in this context have the meaning of specific features or attributes that the signatory might possess in order to perform a certain act. Such a qualification may be obtained using attributes within PKCs included or referenced in electronic signatures.							
	Original resolution proposal	Typo -> Please change reference to clause 4.1 into reference to clause 4.2. Please add the following paragraphs at the end. When a signer signs a document it is of primary importance to be able to identify such signatory in the interest of accountability. This enables the transaction to be traceable. However, in many cases, in order to accept a signature, the acceptance criteria may not necessarily be based on the identity of the signer but instead, or additionally, on the qualification(s) of the signer. Qualifications in this context have the meaning of specific features or attributes that the signatory might possess in order to perform a certain act. Such a qualification may be obtained using attributes within PKCs included or referenced in electronic signatures.							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-034	1.2.1	4.3.4	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Please modify the first paragraph as follows. In addition to the policy and practice statements a CA may issue terms and conditions of general commercial purpose. They must follow the requirements of general conditions and comply with the requirements set out in Directive 93/13/EEC -> add reference è as implemented in the national legislation of the member states. In specific, general conditions are non-negotiable and binding to a non-determined number of end users. They have, however, to be brought to the attention of contracting counter parties and especially to consumers. Terms and conditions will only be effective against relying parties, who have no other contractual arrangement with the CA if: - they are easily accessible; and - their existence together with information as to how they can be accessed is brought to their attention in a conspicuous manner; and - they remain in line with the member state law regarding general conditions.							
	Original resolution proposal	Please modify the first paragraph as follows. In addition to the policy and practice statements a CA may issue terms and conditions of general commercial purpose. They must follow the requirements of general conditions and comply with the requirements set out in Directive 93/13/EEC -> add reference è as implemented in the national legislation of the member states. In specific, general conditions are non-negotiable and binding to a non-determined number of end users. They have, however, to be brought to the attention of contracting counter parties and especially to consumers. Terms and conditions will only be effective against relying parties, who have no other contractual arrangement with the CA if: - they are easily accessible; and - their existence together with information as to how they can be accessed is brought to their attention in a conspicuous manner; and - they remain in line with the member state law regarding general conditions.							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-035	1.2.1	4.5	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Add this new clause with title "Certified attributes": "Before being granted, attributes shall be verified in a way that the certification authority is satisfied as to their authenticity. It shall be verified that, at the time of registration for an attribute, the individual was entitled to claim that attribute. The Certification Authority is responsible for verifying the correct attribution of attributes to subjects (see also clause 6.4 Liability)."							
	Original resolution proposal	Add this new clause with title "Certified attributes": "Before being granted, attributes shall be verified in a way that the certification authority is satisfied as to their authenticity. It shall be verified that, at the time of registration for an attribute, the individual was entitled to claim that attribute. The Certification Authority is responsible for verifying the correct attribution of attributes to subjects (see also clause 6.4 Liability)."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-036	1.2.1	4.6	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Add this new clause with title "Attribute semantics": "The semantics of an attribute may be either defined in a standard (e.g. by ISO) or defined by any organization. When the attribute is defined in a standard, it may be used in an open community. NOTE: It may be specified using an OID that has a global international definition. This is in this way that X.509 has defined a set of standard attributes. When it is locally defined by any organization, two approaches are possible: - use an OID located under the OID of the organization; - define the OID of the "issuing authority" (e.g. as called in ISO/TS 17090-2, see Bibliography) and add a definition of the attribute in any syntax (e.g. character string, XML). When the attribute is locally defined by an organization, its use may be restricted to a close community. The semantics of the attribute has then to be interpreted using the identifier of the attribute granting authority (also called sometimes "issuing authority") in combination with the definition of the attribute by that authority."							
	Original resolution proposal	Add this new clause with title "Attribute semantics": "The semantics of an attribute may be either defined in a standard (e.g. by ISO) or defined by any organization. When the attribute is defined in a standard, it may be used in an open community. NOTE: It may be specified using an OID that has a global international definition. This is in this way that X.509 has defined a set of standard attributes. When it is locally defined by any organization, two approaches are possible: - use an OID located under the OID of the organization; - define the OID of the "issuing authority" (e.g. as called in ISO/TS 17090-2, see Bibliography) and add a definition of the attribute in any syntax (e.g. character string, XML). When the attribute is locally defined by an organization, its use may be restricted to a close community. The semantics of the attribute has then to be interpreted using the identifier of the attribute granting authority (also called sometimes "issuing authority") in combination with the definition of the attribute by that authority."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-037	1.2.1	6.3	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Add this new clause with title "Subject obligations" (subsequent clauses must be renumbered accordingly): "The CA shall oblige, through agreement, the subscriber to agree with the subject that the subject is bound to: - use the PKC solely for the usage specified in the CPS; - notify the subscriber without any unreasonable delay, when there is an inaccuracy in the content of an PKC, whatever the reason may be, including a change in the ownership of an attribute."							
	Original resolution proposal	Add this new clause with title "Subject obligations" (subsequent clauses must be renumbered accordingly): "The CA shall oblige, through agreement, the subscriber to agree with the subject that the subject is bound to: - use the PKC solely for the usage specified in the CPS; - notify the subscriber without any unreasonable delay, when there is an inaccuracy in the content of an PKC, whatever the reason may be, including a change in the ownership of an attribute."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-038	1.2.1	7.3.1	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	In "Registration" please replace: c) The service provider shall verify by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation. with: d) The service provider shall verify, at the time of registration, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation.							
	Original resolution proposal	In "Registration" please replace: c) The service provider shall verify by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation. with: d) The service provider shall verify, at the time of registration, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation.							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-039	1.2.1	7.3.1	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	In "Registration" please add: l) The CA shall verify that, at the time of registration of an attribute to be included in a certificate, the individual was entitled to that attribute. That verification shall be done by appropriate means and in accordance with national law. m) The CA shall record all information used to verify the attributes of the subject. n) The CA shall ensure that the subject consents to include attributes in the PKC. o) The CA shall record the information demonstrating that a subject has accepted to have attributes within PKCs.							
	Original resolution proposal	In "Registration" please add: l) The CA shall verify that, at the time of registration of an attribute to be included in a certificate, the individual was entitled to that attribute. That verification shall be done by appropriate means and in accordance with national law. m) The CA shall record all information used to verify the attributes of the subject. n) The CA shall ensure that the subject consents to include attributes in the PKC. o) The CA shall record the information demonstrating that a subject has accepted to have attributes within PKCs.							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-040	1.2.1	7.3.2	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Please add the following clause Attribute Registration: a) The CA shall check by appropriate means that the subject is entitled to the attributes requested to be certified. b) The CA shall record all information used to verify the subjects' rights to exert the attributes to be registered (see item c), including any reference number on the documentation used for verification, and any limitations on its validity. c) The CA shall verify by appropriate means in accordance with national law, the attributes of the person. d) The CA shall record the signed agreement with the subscriber including: - whether, and under what conditions, the subscriber requires the subject's consents to the inclusion in PKCs of the attributes that have been registered; - confirmation that the information registered is correct. NOTE 1: Other parties (e.g. the associated person or legal entity) may be involved in establishing this agreement. NOTE 2: This agreement may be in electronic form, providing all involved parties consent.							
	Original resolution proposal	Please add the following clause Attribute Registration: a) The CA shall check by appropriate means that the subject is entitled to the attributes requested to be certified. b) The CA shall record all information used to verify the subjects' rights to exert the attributes to be registered (see item c), including any reference number on the documentation used for verification, and any limitations on its validity. c) The CA shall verify by appropriate means in accordance with national law, the attributes of the person. d) The CA shall record the signed agreement with the subscriber including: - whether, and under what conditions, the subscriber requires the subject's consents to the inclusion in PKCs of the attributes that have been registered; - confirmation that the information registered is correct. NOTE 1: Other parties (e.g. the associated person or legal entity) may be involved in establishing this agreement. NOTE 2: This agreement may be in electronic form, providing all involved parties consent.							
	Resolution comment								
	Resolution text								

<table>
<tr><th>Comment ID</th><th>Deliverable version</th><th>Deliverable clause</th><th>Original contribution reference</th><th>Comment date</th><th>Comment type</th><th>Resolution source</th><th>Resolution date</th><th>Resolution status</th><th>Deliverable target version</th></tr>
<tr><td>TS101456-041</td><td>1.2.1</td><td>7.3.4</td><td>STF220_4-001</td><td>08/09/2003</td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td rowspan="4"></td><td><b>Comment text</b></td><td colspan="8">Please add the following requirements to item a):
- a clear description of the meaning of each type of attribute that is supported. That description shall be given in readily-understandable terms, and, if appropriate, the law or regulation that defines or assigns the attribute shall be indicated;
- the list of documents the subject must exhibit to prove his/her right to register an attribute and the procedures used by the CA for the verification of such right;
- how each attribute will be represented in the PKC (e.g. a character string and/or an OID);
- any limitations on their use;
- the subscriber's and subject's obligations as defined in clauses 6.2 and 6.3.</td></tr>
<tr><td><b>Original resolution proposal</b></td><td colspan="8">Please add the following requirements to item a):
- a clear description of the meaning of each type of attribute that is supported. That description shall be given in readily-understandable terms, and, if appropriate, the law or regulation that defines or assigns the attribute shall be indicated;
- the list of documents the subject must exhibit to prove his/her right to register an attribute and the procedures used by the CA for the verification of such right;
- how each attribute will be represented in the PKC (e.g. a character string and/or an OID);
- any limitations on their use;
- the subscriber's and subject's obligations as defined in clauses 6.2 and 6.3.</td></tr>
<tr><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution text</b></td><td colspan="8"></td></tr>
<tr><th>Comment ID</th><th>Deliverable version</th><th>Deliverable clause</th><th>Original contribution reference</th><th>Comment date</th><th>Comment type</th><th>Resolution source</th><th>Resolution date</th><th>Resolution status</th><th>Deliverable target version</th></tr>
<tr><td>TS101456-042</td><td>1.2.1</td><td>Annex E</td><td>STF220_4-001</td><td>08/09/2003</td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td rowspan="4"></td><td><b>Comment text</b></td><td colspan="8">Please add the following references:
ISO/TS 17090-1: "Health informatics - Public key infrastructure. Part 1: Framework and overview".
ISO/TS 17090-2: "Health informatics - Public key infrastructure. Part 2: Certificate profile".
ISO/TS 17090-3: "Health informatics - Public key infrastructure. Part 3: Policy Management of certification authority".</td></tr>
<tr><td><b>Original resolution proposal</b></td><td colspan="8">Please add the following references:
ISO/TS 17090-1: "Health informatics - Public key infrastructure. Part 1: Framework and overview".
ISO/TS 17090-2: "Health informatics - Public key infrastructure. Part 2: Certificate profile".
ISO/TS 17090-3: "Health informatics - Public key infrastructure. Part 3: Policy Management of certification authority".</td></tr>
<tr><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution text</b></td><td colspan="8"></td></tr>
</table>

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-043	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment text	A comparison has been carried between the Federal PKI and the ETSI Qualified Certificate Policy (TS 101 456 - QCP), initially put together by a US contractor directed by Federal PKI with subsequent input from members of the ETSI ESI TC. Whilst the resulting conclusion is that the policies are broadly in line, the document identifies a number of areas as "missing" in the ETSI QCP. A significant number of these are issues relating to auditing the conformance of the CA to the policy and practices. It is suggested that this can be covered by reference to the CWA 14167-2 or a comparable national "voluntary accreditation" scheme. There are also other areas which are covered by other EESSI specifications (TS 101 862 and CWA 14168 / CWA 14169).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-044	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment text	FPKI requirement identified as "missing" or partially covered in the QCP: Information about a revoked certificate shall remain in the status information until the certificate expires (table 65).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-045	1.2.1		STF220_2-001	15/05/2003	technical	STF242		not yet processed	
	Comment text	FPKI requirement identified as "missing" or partially covered in the QCP: US feels all CA's should issue CRLs regardless of any other validation capability employed (table 67).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-046	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment text	FPKI requirement identified as "missing" or partially covered in the QCP: The issuance frequency for CRLs and CARLs shall be at least once each day; CRL and CARL issuance for reason of loss or compromise of private key shall take place within 18 hours of notification (table 70).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-047	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment text	FPKI requirement identified as "missing" or partially covered in the QCP: Audit logs shall be reviewed at least once every two months. A statistically significant set of security audit data generated by Agency CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity (table 78). Actions taken as a result of these reviews shall be documented (table 79).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-048	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment text	FPKI requirement identified as "missing" or partially covered in the QCP: Audit processes shall be invoked at system startup, and cease only at system shutdown (table 88). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the Agency authority shall determine whether to suspend Agency CA operation until the problem is remedied (table 89).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-049	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment text	FPKI requirement identified as "missing" or partially covered in the QCP: Routine self-assessments of security controls shall be performed by the entity operating the CA (table 90).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-050	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment text	FPKI requirement identified as "missing" or partially covered in the QCP: Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS (table 121). Backups are to be performed and stored off-site not less than once per week (table 122). At least one full backup copy shall be stored at an offsite location (separate from the Agency CA equipment) (table 123). The backup shall be stored at a site with physical and procedural controls commensurate to that of the Agency CA (table 124).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101456-051	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment text	FPKI requirement identified as "missing" or partially covered in the QCP: The Agency CA Policy Authority shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the Agency CA or its repository not authorized in this CP, the CPS, or other procedures published by the Agency Operational Authority (table 133).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-052	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment text	FPKI requirement identified as "missing" or partially covered in the QCP: Documentation shall be maintained identifying all personnel who received training and the level of training completed (table 136).							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-053	1.2.1	7.2.2 - b)	TC-ESI_1-003	22/10/2003	technical			not yet processed	
	Comment text	CA private signing keys, when exported, can be protected not only by means of encryption, but also by means of other mechanisms, like Shamir's or Blakley's threshold secret sharing mechanism.							
	Original resolution proposal	Change clause 7.2.2 - item b) into "When outside the signature-creation device (see a) above) the CA private signing key shall be protected using cryptographic systems that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key component".							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101456-054	1.2.1	Annex D	TC-ESI_1-006	26/10/2003	technical			not yet processed	
	Comment text	Correct the inconsistencies in annex D, the cross reference between RFC 2527 and TS 101 456.							
	Original resolution proposal	Amendment proposed: * 3.4: change "7.3.5" into "7.3.6" * 4.4: change "7.3.5" into "7.3.6" * 5.2: change "7.4.5" into "7.4.3" (note 1) * 6.3: add "6.2, " before "7.2" * 6.4: add "7.2.7, " before "7.2.9" * 6.5: add "7.4.5, " before "7.4.6" * 6.6: change "7.3" into "7.4" (note 2) * 6.7: add "7.4.5, " before "7.4.6" NOTE 1: The procedural controls, as per RFC 2527, are: - "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role" (22). - For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule) "Identification and authentication requirements for each role may also be defined" NOTE 2: The life cycle security controls, as per RFC 2527, are: - "This subcomponent addresses system development controls and security management controls. - System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design and implementation techniques (e.g. defensive programming) and development facility security. (<- this is not addressed by TS 101 456). - Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation. (<- this is addressed in clause 7.4 of TS 101 456). - This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM) (<- this is not addressed by TS 101 456).							
	Resolution comment								
	Resolution text								

5.2 TS 101 733 - ES electronic signature formats

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-001	1.4.0		UNSTT-003	01/09/2002	editorial	STF242	02/09/2003	already applied	1.5.1
	Comment text	References to the various RFCs and Internet Drafts from PKIX (especially RFC 2459 / RFC 3280).							
	Original resolution proposal								
	Resolution comment	This suggestion has been already applied in the new version 1.5.1.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-002	1.4.0		UNSTT-003	01/09/2002	technical	STF242	02/09/2003	already applied	1.5.1
	Comment text	Signing Time optional?							
	Original resolution proposal								
	Resolution comment	This suggestion has been already applied in the new version 1.5.1.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-003	1.4.0		UNSTT-003	01/09/2002	technical	STF 242	23/01/2004	no change	
	Comment text	Time-mark: the use of the time-mark may solve the problems related to the compromission of TSA private key.							
	Original resolution proposal								
	Resolution comment	The current version includes the time-mark concept and usage for producing the ES with Time Indication (ES-T form). However the current TS focus on usage of time-stamps for archival electronic forms. Usage of time-mark for achieving long term signatures would rely on secure archival technologies that do not fall within the scope of signature formats (although certain data structures specified within the TS 101 733 could certainly be used there). In any case the choice of the various options depends on the applications' scenarios. This issue falls into the one to produce a guidance document that outlines good practices and scenarios.							
	Resolution text	No change.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-004	1.4.0		UNSTT-003	01/09/2002	technical	STF 242	23/01/2004	no change	
	Comment text	The use of the "Invalidity Date" extension of a CRL entry may invalidate all the formats for long term signatures.							
	Original resolution proposal								
	Resolution comment	This is to be addressed by ETSI TC-ESI activity on CRL and OCSP profiles.							
	Resolution text	No change.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-005	1.4.0		UNSTT-003	01/09/2002	technical	STF 242	23/01/2004	no change	
	Comment text	There is the need for a better specification of the verification processes (initial and usual), even if it is a matter of CWA 14170.							
	Original resolution proposal								
	Resolution comment	This is a topic that falls out of the scope of TS 101 733 . It's a matter of CWA 14171.							
	Resolution text	No change.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-006	1.4.0		UNSTT-003	01/09/2002	technical	STF242	25/01/2004	no change	
	Comment text	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.							
	Original resolution proposal								
	Resolution comment	The production of such a set of documents would certainly be worth. This comment could be raised to the ESI group.							
	Resolution text	No change. This comment could be raised to the ESI group.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-007	1.4.0		UNSTT-003	01/09/2002	technical	STF242	25/01/2004	no change	
	Comment text	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".							
	Original resolution proposal								
	Resolution comment	This is a topic that falls out of the scope of TS 101 733, whose purpose is to specify formats for advanced electronic signatures. Relationship between rules in Certification Policy and Signature Policy would be much better to be discussed in details within the Signature Policy Report or other document with broader scope than the current one, which could cover the infrastructure supporting advanced electronic signatures.							
	Resolution text	No change.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-008	1.4.0		UNSTT-004	14/02/2003	technical	STF242	02/09/2003	already applied	1.5.1
	Comment text	Making the SignaturePolicyID signed attribute optional and without the NULL value.							
	Original resolution proposal								
	Resolution comment	This suggestion has been already applied in the new version 1.5.1.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-009	1.4.0		UNSTT-004	14/02/2003	technical	STF242	02/09/2003	already applied	1.5.1
	Comment text	Making the SigningTime signed attribute optional.							
	Original resolution proposal								
	Resolution comment	This suggestion has been already applied in the new version 1.5.1.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-010	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change	
	Comment text	Generalization of the timemark concept (as an external trusted time indication, see ES-Cbis).							
	Original resolution proposal								
	Resolution comment	The current version includes the time-mark concept and usage for producing the ES with Time Indication (ES-T form). However the current TS focus on usage of time-stamps for archival electronic forms. Usage of time-mark for achieving long term signatures would rely on secure archival technologies that do not fall within the scope of signature formats (although certain data structures specified within the TS 101 733 could certainly be used there).							
	Resolution text	No change.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-011	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	already applied	1.5.1
	Comment text	ES as the minimum mandatory format.							
	Original resolution proposal								
	Resolution comment	In its current version, the only attribute that is mandatory to add to the CMS basic format is the SigningCertificate one.							
	Resolution text	No change.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-012	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change	
	Comment text	Signature policy: introducing the minimum mandatory format for a specific application as an additional rule.							
	Original resolution proposal								
	Resolution comment	Do not understand very well the comment. Does it mean that the signature policy format (which is now part of a signature policy report) should include means for specifying the "minimum" ES format that an application should accept as valid? If so, the Signature Policy includes means for identifying attributes required within the signature, although it would be worth to specify shorter mechanisms to mandate specific ES forms already defined. This is a topic that next versions of signature policy reports should deal with. As a quotation: the Digital Signature Services Technical Committee of OASIS is currently dealing with the production of a protocol for requesting generation and validation to a server of different XAdES forms. This protocol will likely include mechanisms for identifying the different Electronic Signature forms that are the XML counterpart to the forms defined in TS 101 733.							
	Resolution text	To be managed in future versions.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-013	1.4.0		UNSTT-004	14/02/2003	editorial	STF242	02/09/2003	already applied	1.5.1
	Comment text	Improving the document structure: a better separation between the mandatory and optional formats; moving the optional formats from the body to an annex.							
	Original resolution proposal								
	Resolution comment	This suggestion has been already applied in the new version 1.5.1.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-014	1.4.0		UNSTT-004	14/02/2003	editorial	STF242	02/09/2003	already applied	1.5.1
	Comment text	Improving the document structure: deleting all text and ASN.1 formal definition about Signature Policies from TS 101 733 and putting it into a specific document as for the XML version of formats and policies.							
	Original resolution proposal								
	Resolution comment	This suggestion has been already applied in the new version 1.5.1.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-015	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change	
	Comment text	Adding some additional explanatory documents: roadmap for the EESSI deliverables EESSI, from a functional perspective and from a new reader perspective: it could be a new version of EESSI DDD.							
	Original resolution proposal								
	Resolution comment	The production of such a set of documents would certainly be worth. This comment could be raised to the ESI group.							
	Resolution text	No change. This comment could be raised to the ESI group.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-016	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change	
	Comment text	Adding some additional explanatory documents: a non-normative (Technical Report) document describing the whole model of the electronic signature generation and verification processes and formats: it could be a new detailed document based on the white papers 'Validation of Electronic Signatures' written by H.N. and D. P.							
	Original resolution proposal								
	Resolution comment	Certainly, such a document giving explanations on the model for signature generation and verification processes for ES forms specified in TS 101 733 would be a valuable outcome. This comment could be raised to the ESI group.							
	Resolution text	No change. This comment could be raised to the ESI group.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-017	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change	
	Comment text	Adding some additional explanatory documents: a new document (Technical Report) about hand-written and electronic signatures interoperability, both from a legal perspective and from a technical perspective, including some case studies with and without signature policies and using different formats.							
	Original resolution proposal								
	Resolution comment	It is not clear the precise meaning of "hand-written and electronic signatures interoperability". Does this comment deal with the co-existence within one environment of both, electronic and hand-written signatures and how to manage both types? (the term interoperability could indicate that ...) or does it deal with the production of a document instructing on the ways electronic signatures should be managed for being equivalent to hand-written signatures? As a quotation, a technical report has been produced within ESI on signature policies which presents different use cases in scenarios where traditionally hand-written signatures have been used (even more than one), where electronic signatures can play a relevant role in an immediate future. Please refer to that ETSI TR.							
	Resolution text	No change.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-018	1.3.1		JCPKI-002	17/02/2003	technical	STF242	25/01/2004	no change	
	Comment text	Rationale: Some comments regarding EESSI Signature Policy Author: Japan Computer Research, 2003/02/17 Scope and Introduction The purpose of the present document is to convey some comments upon the policy aspects of the electronic signature format as specified in [ESF] and [XAdES]. There are at least two obvious reasons to focus on this particular topic: the one is that one of the most distinct features of the specification seems to be incorporation of signature policy; the other is that the policy information issues in general can be regarded as one of the most important milestones in the future evolution of e-business. It is now routine to standardize the encapsulation of signature data. And a number of these formats bind signature with corresponding public key, and often if not all the time, together with its certificate or certificate chain. That policy information can function as a means to validate status of accompanying object is well exemplified in the policy attributes of X.509 certificate profile. Nevertheless, it has to be said that attachment of policy to signature hasn't yet gained the rank of common acceptance. It has to be said, in this sense, that one of the most distinguishing characteristics of [ESF] lies in its introduction of signature policy. However, we anticipate that the policy as proposed in [ESF] can have contextually entirely other use cases than those specific to that for public key certificates. To be more precise, due to more loose semantic constraints associated with digital signature, it is expected that application domain of the signature policy is far more broadly ranged compared to certificate policy. Accordingly, needs to address wider area of practical contexts are felt, and this naturally leads to the necessity of taking into account other policy related development efforts in the Internet community whose shared aim is to promote flexible online transactions (valued or otherwise) while approximating reliability of real world experience. "Policy" has long been traditionally associated, one way or another, with the idea of authority, predominantly centrally and statically perceived at that. The underlying principle of certificate policy closely follows this, essentially due to the way it is bred. Against this, especially to the extent that each individual ought to possess his or her own policy, is a picture in which many policies dynamically interact to form the whole. And this may be thought of as what the "signature policy" might envisage, for signature marks each spatial and temporal lineament of some particular present event. In other words, it should suggest a way to collect disseminated policies in order to proffer a decision suitable to that point of time and space, a way to make feasible Policy Knowledge Interactivity. It is in this spirit that the following comments are delivered, although not always explicit. Comments 1. On the mandated reference to policy. In the data structure, signature policy identifier is made mandatory [ESF; 8.9.1]. This can mean either that: (a) every signature MUST have a non-trivial signature policy available for retrieval in association with the identifier; or that (b) signature policy can have null (i.e. dummy and intentionally empty) signature policy in the case so desired: (a) This case means that validation process refers to and explicitly made dependent on the signing process at each instant. I.e. the action of validation of a signature is determined by the signing of it at the time when the latter took place, so that the temporal medium between the two actions is made frozen. In particular, this allows the users to preserve unaltered the state and quality of signature relatively long time. (b) In this case, the content of the policy can be determined at the time of the validation. Binding between the signature and validation is principally the responsibility of policy source (policy issuer or TSP), and the determination of actual policy content is left to the latter, and the issuance can be protracted to the time of the delivery. (c) In practice, hybrid case is the most likely to be demanded. This is because: (i) Performance wise, a practical computing platform wants to avoid actual communication with the policy source to take place every each time of the signature generation. This is especially so in view that, for some algorithms, signing process is designed more costly in arithmetic operations than validation process. Also, applications serving as a service provider would surely have to process hundreds of requests in a second. All this would imply that signature policy may be cached until the time it is necessary to refresh, and would probably mean that policy content be left empty and signer decides its policy related action in terms of policy qualifiers only. Which in turn would mean that it is desired that policy qualifier carry validity dates or some sort of a recommended best before.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
		(ii) Another reason why it is important to allow empty policy content at the time of signing is that, in encapsulating a transaction message in which signature data is to be attached, one might want to or have to place policy related information outside the signature data, for example using some other policy mechanisms (cf. item 2 below). Practically, this could perhaps mean often that two policy identifiers, that within the signature data and that outside it, are identical, but not necessarily. 2. On policy data or content. The design of [ESF] has that, according to the needs of the singing party and relying party, policy data or content can be obtained from the policy source the reference to which is embedded explicitly in the signature data in the form of mandatory policy identifier. [ESF] does not specify the policy content: "The precise content of a signature policy is not mandated by the present document". This could perhaps mean that not only its data structure but also the protocol through which it is obtained are left to the decision of policy source. Existing similar specification activities along these lines include [SAML], [XACML], and [WS-Policy]. We will examine briefly the possibility of applying these protocols to the purpose of obtaining policy content for the [ESF] signature data here: a) In General. These protocols are specified in terms of XML, while [ESF] data structure is defined in terms of ASN.1. So it would be natural to consider the use of [XAdES] instead of [ESF], to level the networking layer consistent. Similarly, in the following, the reference "[ESF]" is meant to be "[XAdES]", whenever the appropriateness of the context demands, without explicitly mentioned each time. b) SAML. By this, we mean to utilise SAML security assertions as policy content. Which would mean that policy source be SAML authority, messaging protocol be SAML request/response. [SAMLCore] states that SAML "is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subject, where a subject is an entity (either human or computer) that has an identity in some security domain". In order to fit exactly into this description, signature ought to represent the "entity" so intended, which is really the role of public key certificate as the common sense has it presently. However, the practical consideration ensues taking into account that promulgation of SAML is rapidly in place. Whereas, on the other hand, we believe that the signature policy of [ESF] type can act as an "external policy" for SAML, to the contrary. c) XACML. Although termed as "Access Control Markup Language", the motivation of XACML derives from 'a pressing need for a common language for expressing security policy' ([XACML]). It is in this sense that XACML might just be suitable as the policy language for [ESF]. For this, however, we believe that one has to make a careful architectural consideration to cohere the two semantically. (See item 5 for a brief remark on this.) d) Web Services Policy Framework. Similar to applicability of XACML, but with a more restricted context of the web services interoperability. There are on-going investigations as to how [XACML] and [WS-Policy] can be made consistent in practice. Here we would rather insist on the synergy of [ESF] with [XACML] for the reason that semantics of XACML is more general in nature. To add, in conjunction with the overall web services security standards, one might think of applying secure SOAP messaging in the form of Web Services Security, for the signature policy queries (including referencing). We feel that this certainly is a potential. 3. On policy protection. The mechanism for policy protection is provided by the authentication of policy source ([ESF; 6.11]). The latter is rendered in terms of the hash calculation of the policy identifier. Also, binding of the policy source and actual policy seems to be rendered by the same mechanism (although only implicit, cf. [ESF; 11.1]). This may not offer enough level of protection, for a complex distributed policy environment in which, for example, policy source refers to another policy source and so on (which seems to be case with [SAML] in cooperation with [XACML]). Further, signature policy doesn"t seem to carry its own signature explicitly, which means, if it is to be signed, the signature data are to be attached externally. We believe, to complement this, that signing of signature policy has to be described in detail, at least normatively (as XACML TC does). For especially, there may arise possible semantic ambiguities between "signature policy" and "policy signature". And it could well happen that the latter may be provided by some TSP other than policy issuer itself.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
		4. On signature policy data structure. Although not normative, we have a number of reasons that signature policy specified in [ESF] has to be examined closely. The primary one being its position with respect to other policy assertions mentioned above (see item 2), we feel that [ESF] signature policy format has to address either possible interoperability with or definitive differentiation from these other standards. Here are a couple of fragmental comments: a) On Rules. The terminology employed, "Common Rules" ([ESF; 11.3]) and "Commitment Rules" ([ESF; 11.4]), seems to be rather awkward especially when compared with other standards. It is suspected that this was intentionally chosen with some specific application in mind, but we could not have identified the relevant passages in the specification. b) On Extensions. In practice, we believe that heavy usage of SignPolExtensions ([ESF; 11.11]) are expected to be inevitable, for example in embedding signatures or other validation data for further protection depending on the circumstances (see item 3). We feel that it would be a good idea to specify what instances of extensions should be expected as rendered in RFC 3280. 5. On interoperability with XACML. It is often expected that XACML will fill in the gap where it is currently lacking the means to proffer semantic information for establishing secure transactions. It is to this extent that we feel policy framework of XACML should be taken into account in configuring the application domain of signature policy, regardless of whether transaction of the latter takes place through application layer protocols or not. References [ESF] ETSI TS 101 733 "Electronic Signature Formats". [RFC3280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. [SAMLCore] Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML). [XACML] OASIS extensible Access Control Markup Language (XACML). [XAdES] ETSI TS 101 903 "XML Advance Electronic Signatures (XAdES)". [WS-Policy] Web Services Policy Framework (WS-Policy).							
	Original resolution proposal								
	Resolution comment	Comment on (a): The appearance of a signature policy identifier does not preserve unaltered the state and quality of signature relatively long time (if the algorithm or the key are broken, the signature policy identifier does not protect the signature): this has to be achieved by other means, like time-stamping. What a signature policy identifier does is to fix rules that the verifier has to follow to validate the signature. The current version of TS 101 733 does not use the SignaturePolicyImplied with NULL value.							
	Resolution text	No change.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-019	1.3.1		JCPKI-002	17/02/2003	technical	STF242	21/06/2003	already applied	

	Comment text	Pages 49, 67 and 76: "OPTIONAL" should be described after [2] OtherRevVals marked ****.
		RevocationValues ::= SEQUENCE {
		crlVals [0] SEQUENCE OF CertificateList OPTIONAL
		ocspVals [1] SEQUENCE OF BasicOCSPResponse OPTIONAL
		otherRevVals [2] OtherRevVals ****
		}							

	Original resolution proposal	"OPTIONAL" should be described after [2] OtherRevVals marked ****							
	Resolution comment	This problem is fixed in the version 1.4.0.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-020	1.3.1	4.4	JCPKI-002	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	Pages 16 and 17: Timestamp seem unnecessary in ES-X Type1 and ES-X Type2, since ES-X-L is enough. These two should be deleted to avoid being complicacy of specifications.							
	Original resolution proposal								
	Resolution comment	These forms deal with different situations: ES-X Types 1 and 2 are for those environments where verifier has access to all the validation data AND some of the keys of the CAs in the cert path can be compromised. ES-X-L are for those environments where verifier HAS NOT access to all the validation data: then they are added to the signature itself.							
	Resolution text	No change.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-021	1.3.1	8.9.1	JCPKI-002	17/02/2003	technical	STF242	21/06/2003	already applied	
	Comment text	Signature policy is made mandatory in the specification, while it is felt necessary to specify a mechanism that allows dynamic policy referencing, which is presently lacking. At the same time, it is preferable that there is a method to link policy inside signature and that outside signature data.							
	Original resolution proposal								
	Resolution comment	a) In the next version the SignanurePolicyIdentifier attribute will be made OPTIONAL; b) Further clarification is requested regarding what is meant by "a mechanism that allows dynamic policy referencing"; c) If there is an indication of a signature policy outside the signature - in the signed document - and one within the signature they both should certainly not be in contradiction with each other, but we would find difficult in our current specification to say something more about any indication of signature policy.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-022	1.3.1	11.1	JCPKI-002	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	As a part of the policy source protection, we feel it is necessary to consider signature of the signature policy itself, not just its hash value.							
	Original resolution proposal								
	Resolution comment	The standard does not preclude the use of digital signatures as part of the signature policy specification as means of proving its authenticity. The hash mechanism is used to securely bind a specific policy specification to the signature.							
	Resolution text	No change.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-023	1.3.1	11.11	JCPKI-002	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	As the use case demand for the signature policy extension is deemed to increase, it would be nice to have a concrete specification of extension instances as has been done in X.509 certificate profile standard (RFC 3280).							
	Original resolution proposal								
	Resolution comment	We share the author's view of that as signature policies will be used, a number of extensions will appear. Nevertheless, we are facing the start of their usage and specific requirements policy extensions have yet to be identified. Any suggestion will be welcome…							
	Resolution text	No change.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-024	1.3.1	5.4.2	JCPKI-002	17/02/2003	editorial	STF242	21/06/2003	already applied	
	Comment text	"CRI Information" may be a spelling mistake for "CRL Information".							
	Original resolution proposal								
	Resolution comment	Already applied in V1.4.0.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101733-025	1.4.0	5.4.5/5.4.7	JCPKI-002	17/02/2003	editorial	STF242	21/06/2003	in process	
	Comment text	The same clause title "Timestamping for long life of signature".							
	Original resolution proposal								
	Resolution comment	Will be corrected in next release.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101733-026	1.4.0	10.4	OTHER-009		technical	STF242	25/01/2004	already applied	1.5.1
	Comment text	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.							
	Original resolution proposal								
	Resolution comment	This section has been re-written in the current version.							
	Resolution text								

5.3 TS 101 861 - Time stamping profile

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101861-001	1.2.1	5.1.2	JCPKI-004	17/02/2003	editorial	STF242	21/06/2003	in process	
	Comment text	Please add "One of" to the beginning of the sentence, because the sentence uses "must".							
	Original resolution proposal	Please add "One of" to the beginning of the sentence, because the sentence uses "must"							
	Resolution comment	Noted to be considered for next revision.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101861-002	1.2.1	5.2.3	JCPKI-004	17/02/2003	editorial	STF242	21/06/2003	in process	
	Comment text	Please add "One of" to the beginning of the sentence, because the sentence uses "must".							
	Original resolution proposal	Please add "One of" to the beginning of the sentence, because the sentence uses "must".							
	Resolution comment	Noted to be considered for next revision.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101861-003	1.2.1		JCPKI-004	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	This profile is appropriate for common use of time stamp.							
	Original resolution proposal								
	Resolution comment	It is agreed that this profile has general applicability.							
	Resolution text	No change.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101861-004	1.2.1	5.2.1	OTHER-010		technical			not yet processed	
	Comment text	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.							
	Original resolution proposal	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;"							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101861-005	1.2.1	5.2.1	OTHER-011		technical			not yet processed	
	Comment text	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.							
	Original resolution proposal	Delete item.							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101861-006	1.2.1	6	OTHER-012		technical			not yet processed	
	Comment text	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.							
	Original resolution proposal	Update as indicated: One on-line protocol and one store and forward protocol must be supported for every Time Stamping Authority (TSA).							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101861-007	1.2.1	7.1.1	OTHER-013		technical			not yet processed	
	Comment text	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.							
	Original resolution proposal	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."							
	Resolution comment								
	Resolution text								

5.4 TS 101 862 - Qualified certificate profile

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101862-001	1.2.1	2	UNSTT-005		editorial	STF242	09/01/2004	applied	1.3.1
	Comment text	Since TS 101 862 has been published, RFC 2459 has been replaced by RFC 3280. Thus it is suggested to accordingly modify reference in the next TS version.							
	Original resolution proposal	Modify the reference to RFC 2459 into RFC 3280.							
	Resolution comment	Done as per proposed resolution.							
	Resolution text	See TS 101 862 V1.3.1.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101862-002	1.2.1	3.1.1/4.1	UNSTT-005		technical	STF242	09/01/2004	no change	
	Comment text	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) 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."							
	Original resolution proposal	"The name of the issuer contained in the issuer field (as defined in clause 3.1.1 in RFC 3039) 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."							
	Resolution comment	Specific naming requirements incorporated in TS 102 280, X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.							
	Resolution text	No change to TS 101 862, see TS 102 280.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101862-003	1.2.1	4.2.1	UNSTT-005		technical	STF242	09/01/2004	no change	
	Comment text	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 clause 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).							
	Original resolution proposal	Proposed text: "4.2 SubjectDirectoryAttributes extension 4.2.1 Identity relevant fields (NOTE: Renumbering of the subsequent clauses 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."							
	Resolution comment	Specific naming requirements incorporated in TS 102 280 - X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons							
	Resolution text	No change to TS 101 862, see TS 102 280.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101862-004	1.2.1	4.3.1	UNSTT-005		technical	STF242	09/01/2004	no change	
	Comment text	A requirement is needed on how the pseudonym is to be "identified as such". RFC 3039 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 [6] that pseudonyms MUST be inserted in the "pseudonym" attribute.							
	Original resolution proposal	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."							
	Resolution comment	Specific naming requirements incorporated in TS 102 280 - X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.							
	Resolution text	No change to TS 101 862, see TS 102 280.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101862-005	1.2.1	4.3.2	UNSTT-005		technical	STF242	09/01/2004	no change	
	Comment text	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 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, clause 3.1.2. In addition to such identifier and where necessary to comply with RFC 3039 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".							
	Original resolution proposal	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], clause 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."							
	Resolution comment	Specific naming requirements incorporated in TS 102 280 - X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.							
	Resolution text	No change to TS 101 862, see TS 102 280.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101862-006	1.2.1	4.4	UNSTT-005		technical	STF242	09/01/2004	no change	
	Comment text	There has been a long debate on RFC 3039 clause 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. 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 mandates the keyUsage extension to be marked critical, to avoid any possible malicious misuse of the non-repudiation and of the authentication certificates.							
	Original resolution proposal	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."							
	Resolution comment	Specific key usage requirements incorporated in TS 102 280 - X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.							
	Resolution text	No change to TS 101 862, see TS 102 280.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101862-007	1.2.1		EESSI-002		technical	STF242	30/01/2004	no change	
	Comment text	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.							
	Original resolution proposal	This is to be addressed by CEN ISSS activity on CRL profiles.							
	Resolution comment	This is to be addressed by ETSI TC-ESI activity on CRL and OCSP profiles.							
	Resolution text	No change.							
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101862-008	1.2.1		OTHER-014		technical	STF242	09/01/2004	no change	
	Comment text	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 [12]. (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.							
	Original resolution proposal								
	Resolution comment	Specific key usage requirements incorporated in TS 102 280 - X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons							
	Resolution text	No change to TS 101 862, See TS 102 280.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101862-009	1.2.1		TC-ESI_2-001	11/06/2003	technical	STF242	09/01/2004	applied	1.3.1
	Comment text	To the maintenance team of TS 101 862. TS 101 456 defines: a) QCP public + SSCD: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd (1). A certificate policy for qualified certificates issued to the public, requiring use of secure signature-creation devices. b) QCP public: itu-t(0) identified-organization(4) etsi(0)qualified-certificate-policies(1456)policy-identifiers(1) qcp-public (2) A certificate policy for qualified certificates issued to the public. TS 101 862 defines id-etsi-qcs-QcCompliance: An Identifier of the statement (represented by an OID), stating that the certificate is issued according to the EU-Directive [1], as implemented in the country under which law the issuer is operating. esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } -- This statement is a statement by the issuer that this -- certificate is issued as a Qualified certificate according -- Annex I and II of the Directive 1999/93/EC of the European Parliament -- and of the Council of 13 December 1999 on a Community framework -- for electronic signatures, as implemented in the law of the country -- specified in the issuer field of this certificate. id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 } TS 101 862 does not permit to make the same distinction as TS 101 456. In particular if a verifier wants to make sure that the signature is a Qualified Signature, it must be known that an SSCD has been be used. This can currently only be checked when the following CP OID is being used: itu-t(0) identified-organization(4) etsi(0)qualified-certificate-policies(1456)policy-identifiers(1) qcp-public-with-sscd (1) but not when simply using a QCstatement extension. It is thus requested to define an additional QCstatement equivalent to the "QCP public + SSCD" CP. The big advantage would be that the CP under which the certificate is being issued may be kept, while simply adding a QCstatement to mean "QCP public + SSCD". NOTE: The rest of the mail exchange has been removed for privacy.							
	Original resolution proposal								
	Resolution comment	New QC statement for SSCD added to TS 101 862.							
	Resolution text	See TS 101 862 V1.3.1.							

5.5 TS 101 903 - XML advanced electronic signatures (XAdES)

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-001	1.1.1		JCPKI-003	17/02/2003	Technical	STF242	25/01/2004	no change	
	Comment text	Rationale: Some comments regarding EESSI Signature Policy Author: Japan Computer Research, 2003/02/17 Scope and Introduction The purpose of the present document is to convey some comments upon the policy aspects of the electronic signature format as specified in [ESF] and [XAdES]. There are at least two obvious reasons to focus on this particular topic: the one is that one of the most distinct features of the specification seems to be incorporation of signature policy; the other is that the policy information issues in general can be regarded as one of the most important milestones in the future evolution of e-business. It is now routine to standardize the encapsulation of signature data. And a number of these formats bind signature with corresponding public key, and often if not all the time, together with its certificate or certificate chain. That policy information can function as a means to validate status of accompanying object is well exemplified in the policy attributes of X.509 certificate profile. Nevertheless, it has to be said that attachment of policy to signature hasn't yet gained the rank of common acceptance. It has to be said, in this sense, that one of the most distinguishing characteristics of [ESF] lies in its introduction of signature policy. However, we anticipate that the policy as proposed in [ESF] can have contextually entirely other use cases than those specific to that for public key certificates. To be more precise, due to more loose semantic constraints associated with digital signature, it is expected that application domain of the signature policy is far more broadly ranged compared to certificate policy. Accordingly, needs to address wider area of practical contexts are felt, and this naturally leads to the necessity of taking into account other policy related development efforts in the Internet community whose shared aim is to promote flexible online transactions (valued or otherwise) while approximating reliability of real world experience. "Policy" has long been traditionally associated, one way or another, with the idea of authority, predominantly centrally and statically perceived at that. The underlying principle of certificate policy closely follows this, essentially due to the way it is bred. Against this, especially to the extent that each individual ought to possess his or her own policy, is a picture in which many policies dynamically interact to form the whole. And this may be thought of as what the "signature policy" might envisage, for signature marks each spatial and temporal lineament of some particular present event. In other words, it should suggest a way to collect disseminated policies in order to proffer a decision suitable to that point of time and space, a way to make feasible Policy Knowledge Interactivity. It is in this spirit that the following comments are delivered, although not always explicit. Comments 1. On the mandated reference to policy. In the data structure, signature policy identifier is made mandatory [ESF; 8.9.1]. This can mean either that: (a) every signature MUST have a non-trivial signature policy available for retrieval in association with the identifier; or that (b) signature policy can have null (i.e. dummy and intentionally empty) signature policy in the case so desired: (a) This case means that validation process refers to and explicitly made dependent on the signing process at each instant. I.e. the action of validation of a signature is determined by the signing of it at the time when the latter took place, so that the temporal medium between the two actions is made frozen. In particular, this allows the users to preserve unaltered the state and quality of signature relatively long time. (b) In this case, the content of the policy can be determined at the time of the validation. Binding between the signature and validation is principally the responsibility of policy source (policy issuer or TSP), and the determination of actual policy content is left to the latter, and the issuance can be protracted to the time of the delivery.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
		(c) In practice, hybrid case is the most likely to be demanded. This is because: (i) Performance wise, a practical computing platform wants to avoid actual communication with the policy source to take place every each time of the signature generation. This is especially so in view that, for some algorithms, signing process is designed more costly in arithmetic operations than validation process. Also, applications serving as a service provider would surely have to process hundreds of requests in a second. All this would imply that signature policy may be cached until the time it is necessary to refresh, and would probably mean that policy content be left empty and signer decides its policy related action in terms of policy qualifiers only. Which in turn would mean that it is desired that policy qualifier carry validity dates or some sort of a recommended best before. (ii) Another reason why it is important to allow empty policy content at the time of signing is that, in encapsulating a transaction message in which signature data is to be attached, one might want to or have to place policy related information outside the signature data, for example using some other policy mechanisms (cf. item 2 below). Practically, this could perhaps mean often that two policy identifiers, that within the signature data and that outside it, are identical, but not necessarily. 2. On policy data or content. The design of [ESF] has that, according to the needs of the singing party and relying party, policy data or content can be obtained from the policy source the reference to which is embedded explicitly in the signature data in the form of mandatory policy identifier. [ESF] does not specify the policy content: "The precise content of a signature policy is not mandated by the present document". This could perhaps mean that not only its data structure but also the protocol through which it is obtained are left to the decision of policy source. Existing similar specification activities along these lines include [SAML], [XACML], and [WS-Policy]. We will examine briefly the possibility of applying these protocols to the purpose of obtaining policy content for the [ESF] signature data here: a) In General. These protocols are specified in terms of XML, while [ESF] data structure is defined in terms of ASN.1. So it would be natural to consider the use of [XAdES] instead of [ESF], to level the networking layer consistent. Similarly, in the following, the reference "[ESF]" is meant to be "[XAdES]", whenever the appropriateness of the context demands, without explicitly mentioned each time. b) SAML. By this, we mean to utilise SAML security assertions as policy content. Which would mean that policy source be SAML authority, messaging protocol be SAML request/response. [SAMLCore] states that SAML "is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subject, where a subject is an entity (either human or computer) that has an identity in some security domain". In order to fit exactly into this description, signature ought to represent the "entity" so intended, which is really the role of public key certificate as the common sense has it presently. However, the practical consideration ensues taking into account that promulgation of SAML is rapidly in place. Whereas, on the other hand, we believe that the signature policy of [ESF] type can act as an "external policy" for SAML, to the contrary. c) XACML. Although termed as "Access Control Markup Language", the motivation of XACML derives from 'a pressing need for a common language for expressing security policy' ([XACML]). It is in this sense that XACML might just be suitable as the policy language for [ESF]. For this, however, we believe that one has to make a careful architectural consideration to cohere the two semantically. (See item 5 for a brief remark on this.) d) Web Services Policy Framework. Similar to applicability of XACML, but with a more restricted context of the web services interoperability. There are on-going investigations as to how [XACML] and [WS-Policy] can be made consistent in practice. Here we would rather insist on the synergy of [ESF] with [XACML] for the reason that semantics of XACML is more general in nature. To add, in conjunction with the overall web services security standards, one might think of applying secure SOAP messaging in the form of Web Services Security, for the signature policy queries (including referencing). We feel that this certainly is a potential. 3. On policy protection. The mechanism for policy protection is provided by the authentication of policy source ([ESF; 6.11]). The latter is rendered in terms of the hash calculation of the policy identifier. Also, binding of the policy source and actual policy seems to be rendered by the same mechanism (although only implicit, cf. [ESF; 11.1]). This may not offer enough level of protection, for a complex distributed policy environment in which, for example, policy source refers to another policy source and so on (which seems to be case with [SAML] in cooperation with [XACML]). Further, signature policy doesn"t seem to carry its own signature explicitly, which means, if it is to be signed, the signature data are to be attached externally. We believe, to complement this, that signing of signature policy has to be described in detail, at least normatively (as XACML TC does). For especially, there may arise possible semantic ambiguities between "signature policy" and "policy signature". And it could well happen that the latter may be provided by some TSP other than policy issuer itself.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
		4. On signature policy data structure. Although not normative, we have a number of reasons that signature policy specified in [ESF] has to be examined closely. The primary one being its position with respect to other policy assertions mentioned above (see item 2), we feel that [ESF] signature policy format has to address either possible interoperability with or definitive differentiation from these other standards. Here are a couple of fragmental comments: a) On Rules. The terminology employed, "Common Rules" ([ESF; 11.3]) and "Commitment Rules" ([ESF; 11.4]), seems to be rather awkward especially when compared with other standards. It is suspected that this was intentionally chosen with some specific application in mind, but we could not have identified the relevant passages in the specification. b) On Extensions. In practice, we believe that heavy usage of SignPolExtensions ([ESF; 11.11]) are expected to be inevitable, for example in embedding signatures or other validation data for further protection depending on the circumstances (see item 3). We feel that it would be a good idea to specify what instances of extensions should be expected as rendered in RFC 3280. 5. On interoperability with XACML. It is often expected that XACML will fill in the gap where it is currently lacking the means to proffer semantic information for establishing secure transactions. It is to this extent that we feel policy framework of XACML should be taken into account in configuring the application domain of signature policy, regardless of whether transaction of the latter takes place through application layer protocols or not. References [ESF] ETSI TS 101 733 "Electronic Signature Formats". [RFC3280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. [SAMLCore] Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML). [XACML] OASIS extensible Access Control Markup Language (XACML). [XAdES] ETSI TS 101 903 "XML Advance Electronic Signatures (XAdES)". [WS-Policy] Web Services Policy Framework (WS-Policy).							
	Original resolution proposal								
	Resolution comment	Comment on (a): The appearance of a signature policy identifier does not preserve unaltered the state and quality of signature relatively long time (if the algorithm or the key are broken, the signature policy identifier does not protect the signature): this has to be achieved by other means, like time-stamping. What a signature policy identifier does is to fix rules that the verifier has to follow to validate the signature. The current version of TS 101 903 does not use the SignaturePolicyImplied with NULL value.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-002	1.1.1		JCPKI-003	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	Page 17: Timestamp seems unnecessary in XAdES-X, since XadES-X-L is enough. This should be deleted to avoid being complicacy of specifications.							
	Original resolution proposal								
	Resolution comment	These forms deal with different situations: XAdES-X Types 1 and 2 are for those environments where verifier has access to all the validation data AND some of the keys of the CAs in the cert path can be compromised. XAdES-X-L are for those environments where verifier HAS NOT access to all the validation data: then they are added to the signature itself.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101903-003	1.1.1		JCPKI-003	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	It makes sense that signature format, which is designed to incorporates signature policy, is defined in terms of XML, when considered that the worldly policy standards, like SAML, XACML, WS-Security, are specified at the same processing layer using XML. In this sense, it would be preferable (if not normatively, but informatively) for the present standard to investigate its practicable interoperability with these policy related standards.							
	Original resolution proposal								
	Resolution comment	As said before the intentions of the ESI group is to try to be aligned with relevant initiatives on the fields where it develops its documents. And indeed the development of a signature policy format will have to take into account developments in XACML							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-004	1.1.1		JCPKI-003	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	Relative to TS 101 733 ES Formats, a profile of XML long term signature format was introduced assuming a similar use of CMS SignedData last year. Relative to Japan e-Government, Electronic applications are specified to be XML based documents and XML signature will be in use. In this case, XadES matches well than ASN.1 based TS 101 733 from the point of view of long term signature save. To diffuse the use of XadES, test programs for interoperability should be implemented. Some errors are pointed out in some parts of XadES schema so that bug information should be opened to public promptly. The manual of XML time-stamping used in the present document should be described soon after OASIS standard formulation.							
	Original resolution proposal								
	Resolution comment	There is a currently taking place interoperability event within ETSI. Dealing where different implementations are being developed and interoperability among them is being assessed. The group is also building up a number of tests for facilitating developments of such tools. A specialist task force is currently working on maintenance of all the ETSI specifications and will issue a report on all outstanding issues that have yet to be addressed by revised specifications.							
	Resolution text								

<table>
<tr><th>Comment ID</th><th>Deliverable version</th><th>Deliverable clause</th><th>Original contribution reference</th><th>Comment date</th><th>Comment type</th><th>Resolution source</th><th>Resolution date</th><th>Resolution status</th><th>Deliverable target version</th></tr>
<tr><td>TS101903-005</td><td>1.1.1</td><td></td><td>XAdES-PT-001</td><td>25/01/2004</td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td rowspan="4"></td><td><b>Comment text</b></td><td colspan="8">In the clause 7.6.2 of the XAdES specification [1] it says:
OCSP Responses (OCSPValues) consist of a sequence of at least one OCSP Response. The <EncapsulatedOCSPValue> element contains the base64 encoding of a DER-encoded OCSP Response. [1, clause 7.6.2]
During the XAdES-PLUGTESTST it turned out that this section has been interpreted differently by the participating implementers in terms of what the actual content of the <EncapsulatedOCSPValue> has to bee. Some implementers included the whole OCSPResponse others have just included the BasicOCSPResponse (contained in the ResponseBytes of the OCSPResponse as defined in RFC 2560 [21]). Therefore, the specification should be more explicit about what to include into the <EncapsulatedOCSPValue> element.</td></tr>
<tr><td><b>Original resolution proposal</b></td><td colspan="8">Since the additional information that is provided by the OCSPResponse is not needed to be archived, it was first suggested to include the BasicOCSPResponse. The different possibilities are:
- OCSPResponse: On the one hand, the additional information provided by the OCSPResponse—an integer value indicating if the request was successful—is not needed to be archived, however, this is how the actual version of the specification is to be interpreted most likely. On the other hand, the information provided by the <OCSPReferences> element reflects the content of the BasicOCSPResponse. Therefore, any other OCSP response type than the BasicOCSPResponse has to be referenced by a <OtherRef> element, most likely.Thus, an OCSP response containing a different response type will have to be included into a <OtherValue> element.
- ResponseBytes: The ResponseBytes are already in DER-encoded format. They include an additional object identifier indicating the type of the included OCSP response. The Response Bytes may again contain OCSP responses of different types. Therefore, the same arguments apply, as for the OCSPResponse stated in the paragraph above.
- BasicOCSPResponse: The BasicOCSPResponse contains exactly the data that needs to be archived and corresponds to the information provided by the <OCSPRef> element.
At the interop the participants agrred to use OCSPResponse, since this is basically what the standards said, and furthermore the only deployed implementation in Estonia uses that interpretation.</td></tr>
<tr><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution text</b></td><td colspan="8"></td></tr>
</table>

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-006	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	Problem Description The specification of the <TimeStampType> data type is broken in two ways: 1. While it is easy to verify the time-stamp by processing all <HashDataInfo> elements and comparing the resulting hash value to the hash value stored in the time-stamp, it is difficult, time-consuming and possibly even infeasible in the general case to verify, if the time-stamp is applied exactly on the data that is claimed by the XAdES specification. That is, to verify if the time-stamp is applied on the elements that are claimed to be time-stamped. 2. For the <AllDataObjectsTimeStamp>, <IndividualDataObjectsTimeStamp> and the <ArchiveTimeStamp> <HashDataInfo> elements have to be composed that resolve to exactly the same data as the corresponding <ds:Reference>s in the <ds:SignedInfo> do. In the general case it is difficult or probably infeasible to compose such a reference, because the result of resolving depends on the context (e.g. the node it is contained in). Remarks The input for the different time-stamps used in the current XAdES version is formed by means of <HashDataInfo> elements. These <HashDataInfo> elements have to be processed according to the reference processing model specified in the XMLDSig specificaion [3]. This is, in short, resolving the provided URI in the URI-attribute of the <HashDataInfo> element, applying the transforms that are specified by the optional <Transforms> child element of the <HashDataInfo> element and finally canonicalizing the result, if the output of the last transform (or the result of resolving the URI, if there is no transform at all) is a node list. This means that the result of processing one <HashDataInfo> element is octet data in any case. The resulting octets of all the included <HashDataInfo> elements are then concatenated in the order the <HashDataInfos> appear in the document to form the input for the time-stamp. These resulting octets are in fact the information that is time-stamped. The current version of XAdES specification therefore mandates what the result of processing an <HashDataInfo> elements has to be. In the definition of the <SignatureTimeStamp> property it says for instance: The <SignatureTimeStamp> element contains a single <HashDataInfo> element that refers to the <ds:SignatureValue> element of the XMLDSig signature. That is, the input for the time-stamp hash computation is the <ds:SignatureValue> XML element. [1, clause 7.3.1] A verifying application has to make sure that the time-stamp has been applied on the proper input data. This is, to verify somehow that processing the <HashDataInfo> element results in the data that is claimed by the XAdES specification. In case of the <SignatureTimeStamp> for instance, this is the <ds:SignatureValue> element. Thus, the verifying application has to check that the octets that are being time-stamped are a valid representation of the <ds:SignatureValue> element. As an URI and an arbitrary number of transforms can be used to compose such a <HashDataInfo> element, it is infeasible to deduce from the specified URI and the given transforms to the result, in the general case. Thus, the only way to verify what has been time-stamped is to process the <HashDataInfo> element and analyze the result. As one XML structure can have any number of different octet data representations that bear the same information, canonicalization has been introduced. Thus, the only practical way to verify the timestamp input is to compare the canonicalized form of the data that has to be time-stamped according To the specification with the data that results from processing the corresponding <HashDataInfo> element. In this case it would be sufficient to simply create the required input for the time-stamp, compute the digest value and compare it with the digest value in the time-stamp. However, the <HashDataInfo> element was introduced to identify the input of a given time-stamp in cases where the input is ambiguous. But it does not serve this purpose anyway, as has been shown above Therefore, a new solution has to be found to identify the input-data of a given time-stamp in cases were this input cannot be unambiguously defined by the XAdES specification.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
	Original resolution proposal	During the interoperability event the following resolution proposal was discussed and agreed on: The <TimeStampType> data type should be redefined to use an ID-list to identify the elements that have been time-stamped. An optional <ds:CanonicalizationMethod> element should indicate which canonicalization method to use for canonicalizing XML elements. If no canonicalization method is specified the standard canonicalization method as specified by the actual XMLDSig specification MUST be used. In the case of included <ds:Reference> elements an additional referencedData-attribute indicates if the <ds:Reference> element itself or the data resulting from processing the <ds:Reference> should be included. If the referencedData-attribute is omitted or the attribute value is false the element identified by the included URI is included. If the referencedDataattribute value is true the <ds:Reference> has to be processed according to the reference processing model of the XMLDSig specification. The result is then used as input for the time-stamp. The result of the processing must be exactly the same data as that was used in the computation of the <ds:Reference> digest value. <xsd:element name="TimeStamp" type="TimeStampType"/> <xsd:complexType name="TimeStampType"> <xsd:sequence> <xsd:element name="Include" type="IncludeType" maxOccurs="unbounded"/> <xsd:element ref="ds:CanonicalizationMethod" minOccurs="0"/> <xsd:choice> <xsd:element name="EncapsulatedTimeStamp"> type="EncapsulatedPKIDataType"/> <xsd:element name="XMLTimeStamp" type="AnyType"/> </xsd:choice> </xsd:sequence> </xsd:complexType> <xsd:complexType name="IncludeType"> <xsd:attribute name="uri" type="xsd:anyURI" use="required"/> <xsd:attribute name="referencedData" type="xsd:boolean" use="optional"/> </xsd:complexType>							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-007	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	The <ArchiveTimeStamp> definition is broken in two ways: 1. The <ArchiveTimeStamp> includes the <SignedPropertiesElement> twice. 2. The references to the <SignedSignatureProperties> and the <SignedDataObjectProperties> cannot be composed using ID-references, because these elements do not have an xsd:ID-attribute. In clause 7.7.1 of the XAdES specification [1] it says: The XAdES <ArchiveTimeStamp> element contains the following sequence of Hash-DataInfo elements: - One <HashDataInfo> element for each data object signed by the XMLDSIG signature The result of application of the transforms specified each <HashDataInfo> must be exactly the same as the octet stream that was originally used for computing the digest value of the corresponding <ds:Reference>. - One <HashDataInfo> element for the <ds:SignedInfo> element. The result of application of the transforms specified in this <HashDataInfo> must be exactly the same as the octet stream that was originally used for computing the signature value of the XMLDSIG signature. - One <HashDataInfo> element for the <SignedSignatureProperties> element. - One <HashDataInfo> element for the <SignedDataObjectProperties> element. -... In the first paragraph it says to include a <HashDataInfo> element for each <ds:Reference> in the XMLDSig signature. This obviously includes the reference to the <SignedProperties>. In the third and the fourth paragraph it says to include a <HashDataInfo> element for the <SignedSignatureProperties> and the <SignedDataObjectProperties>. These elements are already included by the reference to the <SignedProperties>. Additionally these two elements have no xsd:ID-attribute specified, thus they cannot be referenced using ID-references.							
	Original resolution proposal	Omit the <HashDataInfo> elements for the <SignedSignatureProperties> and the <SignedDataObjectProperties>. Additionally, - either add an <HashDataInfo> element for the <SignedProperties> and omit the <ds:Reference> to the <SignedProperites>, - or simply leave the <ds:Reference> to the signed properties included. Add xsd:ID-attributes to the <SignedSignatureProperties> and the <SignedDataObjectProperties> elements as well as to the <UnsigendSignatureProperties> and the <UnsignedDataObjectProperties> elements							
	Resolution comment								
	Resolution text								

<table>
<tr><th>Comment ID</th><th>Deliverable version</th><th>Deliverable clause</th><th>Original contribution reference</th><th>Comment date</th><th>Comment type</th><th>Resolution source</th><th>Resolution date</th><th>Resolution status</th><th>Deliverable target version</th></tr>
<tr><td>TS101903-008</td><td>1.1.1</td><td></td><td>XAdES-PT-001</td><td>25/01/2004</td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td rowspan="4"></td><td><b>Comment text</b></td><td colspan="8">Within the current version of the XAdES specification, the word "must" is used to indicate a requirement at several places and should therefore say "MUST" according to RFC 2119 [22]. The RFC 2119 defines how the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted in the sense of requirement level. Therefore, the specification should use these key words wherever a requirement is stated.
XAdES specification [1], clause 5, first paragraph:
The XML namespace URI that must be used by implementations of the present document ... [1, clause 5]
XAdES specification [1], clause 6.2, second paragraph:
... The <SignedProperties> must be covered by a Reference element of the XML signature. Alignment with the present document mandates that one <SignedProperties> element MUST exist. [1, secion 6.2]
XAdES specification [1], clause 6.3, second paragraph:
However, the following restrictions apply for using <ds:Object>, <QualifyingProperties> and <QualifyingPropertiesReference>:
- ...
- All signed properties must occur within a single <QualifyingProperties> element. This element can either be a child of the <ds:Object> element (direct incorporation), or it can be referenced by a <QualifyingPropertiesReference> element. See clause 6.3.1 for information how to sign properties.
- ...
XAdES specification [1], clause 7.2.5, last paragraph:
At least one element of <Description>, <ObjectIdentifier> and xmlMimeType must be present within the property. [1, clause 7.2.5]
XAdES specification [1], clause 7.2.8, paragraph 8:
... At least one of the two elements <ClaimedRoles> or <CertifiedRoles> must be present. [1, clause 7.2.8]
XAdES specification [1], clause 7.7.1, paragraph 10:
The <XAdESArchiveTimeStamp> element contains the following sequence of <HashDataInfo> elements:
- One <HashDataInfo> element for each data object signed by the XMLDSig signature. The result of application of the transforms specified each <HashData Info> must be exactly the same as the octet stream that was originally used for computing the digest value of the corresponding <ds:Reference>.
- ...</td></tr>
<tr><td><b>Original resolution proposal</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution text</b></td><td colspan="8"></td></tr>
</table>

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-009	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	Clause 6.2 of the XAdES specification [1] says: "The mandatory Target attribute refers to the XML signature." This should be changed to: "The mandatory Target-attribute MUST refer to the <Id>-attribute of the corresponding <ds:Signature>."							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101903-010	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	For some ASN.1 PKI elements that are included into the XAdES signature the exact ASN.1 encoding mechanism is not specified (clauses 7.1 and 7.2.8 of the XAdES specification [1]). This should be changed to mandate the DER (Distinguished Encoding Rules [12]) encoding mechanism wherever an ASN.1 encoding is required.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101903-011	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	The following proposal was made by members of the ETSI Technical Committee ESI (Electronic Signatures and Infrastructures): XAdES should probably be able to include Trust Status Lists (TSL [23]), beside certification and revocation information in future versions of the specification							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-012	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	In XAdES specification [1] clause 7.2.2, last but one paragraph it says: If the signer uses an attribute certificate to associate a role with the electronic signature, such a certificate MUST be present in the <SignerRole> property. [1, clause 7.2.2] This sentence should be moved to clause 7.2.8 'The <SignerRole> element' of the XAdES specification							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101903-013	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	The following proposal was made by members of the ETSI Technical Committee ESI (Electronic Signatures and Infrastructures): In future versions of the XAdES it should be possible to have archival versions 'references only', 'values only' and 'mixed'. Currently, the XAdES specification mandates to include references to the certification and revocation information as well as the actual certification and revocation values in the XAdES-X-L and XAdES-A forms. For the purpose of archiving all information necessary to validate the signature at a later time it would however be sufficient to just include the actual certification and revocation values and omit the references. Therefore the standard should provide forms to include only the necessary information to avoid redundancies.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-014	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	The following proposal was made by members of the ETSI Technical Committee ESI (Electronic Signatures and Infrastructures): It should be possible in future versions of XAdES to have archival versions that build on XMLDSig signatures without the mandatory <SignedProperties>. With the current XAdES versions it is not possible to create valid XAdES-A archival versions out of a plain XMLDSig signature, because the mandatory <SignedProperties> cannot be added to the signature later. The XAdES specification should therefore provide forms that permit XAdES-A versions without the currently mandatory <SigningTime>, <SigningCertificate> and <SignaturePolicyIdentifier> properties.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101903-015	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	In the actual version of the XAdES specification [1] the <AnyType> data type is defined as follows: <xsd:complexType name="AnyType" mixed="true"> <xsd:sequence> <xsd:any namespace="##any"/> </xsd:sequence> This definition does not allow content that has no schema associated. Therefore the definition of the <AnyType> data type should read like the following: <xsd:complexType name="AnyType" mixed="true"> <xsd:sequence> <xsd:any namespace="##any" processContents="lax"/> </xsd:sequence>							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-016	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	In the current version of the XAdES specification [1] the <CertID> element does not have an URIattribute for pointing to an archived version of the referenced certificate: <xsd:complexType name="CertIDType"> <xsd:sequence> <xsd:element name="CertDigest" type="DigestAlgAndValueType"/> <xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"/> </xsd:sequence> </xsd:complexType> Therefore the definition of the <CertID> element should read like the following to allow pointing to an archived version of the certificate: <xsd:complexType name="CertIDType"> <xsd:sequence> <xsd:element name="CertDigest" type="DigestAlgAndValueType"/> <xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"/> </xsd:sequence>							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101903-017	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	The Microsoft .NET validating XML parser fails to parse the current version of the XAdES schema, although the schema has been validated using the schema validating tools provided by the World Wide Web Consortium (W3C). In order to reach a larger community this issue should be fixed in future versions of the XAdES specification.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

<table>
<tr><th>Comment ID</th><th>Deliverable version</th><th>Deliverable clause</th><th>Original contribution reference</th><th>Comment date</th><th>Comment type</th><th>Resolution source</th><th>Resolution date</th><th>Resolution status</th><th>Deliverable target version</th></tr>
<tr><td>TS101903-018</td><td>1.1.1</td><td></td><td>XAdES-PT-001</td><td>25/01/2004</td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td rowspan="4"></td><td><b>Comment text</b></td><td colspan="8">In the actual version of the XAdES schema which is part of the XAdES specification the import statement for the XMLDSig schema is missing. Since elements from the XMLDSig schema are referenced by the XAdES schema an import statement has to be present. Therefore the XAdES schema should read like the following:

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://uri.etsi.org/01903/v1.1.1#"
     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns="http://uri.etsi.org/01903/v1.1.1#"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
     elementFormDefault="qualified">

<xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
     schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd"/></td></tr>
<tr><td><b>Original resolution proposal</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution text</b></td><td colspan="8"></td></tr>
</table>

<table>
<tr><th>Comment ID</th><th>Deliverable version</th><th>Deliverable clause</th><th>Original contribution reference</th><th>Comment date</th><th>Comment type</th><th>Resolution source</th><th>Resolution date</th><th>Resolution status</th><th>Deliverable target version</th></tr>
<tr><td>TS101903-019</td><td>1.1.1</td><td></td><td>XAdES-PT-001</td><td>25/01/2004</td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td rowspan="4"></td><td><b>Comment text</b></td><td colspan="8">The &lt;QualifyingPropertiesReferenceType> data type introduces a new <Transforms> element in the XAdES namespace for the <ds:TransformsType> rather than using a reference to the element type defined in the XMLDSig schema.
The current XAdES schema definition for the <QualifyingPropertiesReferenceType> data type is:

<xsd:complexType name="QualifyingPropertiesReferenceType">
    <xsd:sequence>
        <xsd:element name="Transforms" type="ds:TransformsType" minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="URI" type="xsd:anyURI" use="required"/>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>

This should be changed to:

<xsd:complexType name="QualifyingPropertiesReferenceType">
    <xsd:sequence>
        <xsd:element ref="ds:Transforms" minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="URI" type="xsd:anyURI" use="required"/>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType&gt;</td></tr>
<tr><td><b>Original resolution proposal</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution text</b></td><td colspan="8"></td></tr>
<tr><th>Comment ID</th><th>Deliverable version</th><th>Deliverable clause</th><th>Original contribution reference</th><th>Comment date</th><th>Comment type</th><th>Resolution source</th><th>Resolution date</th><th>Resolution status</th><th>Deliverable target version</th></tr>
<tr><td>TS101903-020</td><td>1.1.1</td><td></td><td>XAdES-PT-001</td><td>25/01/2004</td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td rowspan="4"></td><td><b>Comment text</b></td><td colspan="8">The XAdES examples in the (non-normative) annex D of the current version of the XAdES specification [1] are not aligned with the specification. These examples should be fixed, or probably replaced by examples produced as test cases for the XAdES-PLUGTESTS TM event.</td></tr>
<tr><td><b>Original resolution proposal</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td><b>Resolution text</b></td><td colspan="8"></td></tr>
</table>

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-021	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	In the XAdES specification [1], clause 7.2.5, second paragraph it says: ... This (the <DataObjectFormat>) is a signed property that qualifies one specific signed data object. In consequence, an XML electronic signature aligned with the present document MAY contain more than one <DataObjectFormat> elements, each one qualifying one signed data object. [1, clause 7.2.5, second paragraph] However, later in the same section the specification speaks about signed data object(s), suggesting that one <DataObjectFormat> applies for more than one signed data object, which it actually does not: This element can convey: - Textual information related to the signed data object(s) in element <Description>; - An identifier indicating the type of the signed data object(s) in element <ObjectIdentifier>; - An indication of the MIME type of the signed data object(s), in element <MimeType>; - An indication of the encoding format of the signed data object(s), in element <Encoding>. This should be changed to say "object" wherever it says "object(s)". Additionally, in XAdES specification [1], clause 7.2.4, fourth paragraph it says: The mandatory ObjectReference attribute refers to the Reference element of the <ds:Signature> corresponding with the data object qualified by this property. [1, clause 7.2.5, fourth paragraph] This should be changed to say The mandatory QbjectReference attribute MUST reference the <ds:Reference> element of the <ds:Signature> corresponding with the data object qualified by this property. in order to indicate that this is a requirement according to RFC 2119 [22]. Additionally, the current version of the XAdES specification mandates the <DataObjectFormat> element to be present when the signed data objects have to be presented to the verifier. In the XAdES specification [1] it says: ... This element (the <DataObjectFormat>) MUST be present when it is mandatory to present the signed data object to human users on verification … [1, clause 7.2.5, second paragraph] The first question is, does it make any sense to mandate the presentation of the signed data objects on verification, at all? Additionally, if it makes sense to mandate the presentation on verification, the data format may be defined implicitly by the application or desired use case, any way. This issue needs further discussion.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-022	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	On the one side the XAdES specification [1] says in clause 7.6.1, third paragraph: In principle, the <CertificateValues> element contains the full set of certificates that have been used to validate the electronic signature, including the signer"s certificate. However, it is not necessary to include one of those certificates into this property, if the certificate is already present in the <ds:KeyInfo> element of the signature. [1, clause 7.6.1] On the other side the <ds:KeyInfo> element is not covered by the <ArchiveTimeStamp>(s). That is, certificates that are present in the <ds:KeyInfo> and are not included into the <Certificatevalues> are not time-stamped for archiving purposes.							
	Original resolution proposal	There are two possible solutions to this issue: - Mandate the inclusion of all certificates in the certificate chain into the <CertificateValues> element. - Mandate to include the <ds:KeyInfo> element into the <ArchiveTimeStamp>(s). This issue needs further discussion.							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS101903-023	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	In the clause 7.4.1 of the XAdES specification it says: The <CertRefs> element contains a sequence of <Cert> elements already defined in clause 7.2.2, incorporating the digest of each certificate and optionally the issuer and serial number identifier. [1, clause 7.4.1, last paragraph] However, the XAdES schema mandates the issuer and serial number identifier to be present in the <Cert> element. Therefore the word "optionally" should be removed from the quoted sentence above.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

5.6 TS 102 023 - Time stamping policy

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-001	1.1.1	Introduction	UNSTT-006		editorial			not yet processed	
	Comment text	Modify the text: "The quality of this evidence is based in the process of creating and managing the data structure that represent the events and the quality of the parametric data points that anchor them to the real world. In this instance this being the time data and how it was applied." "Another one consists to use a time-stamp which allows to prove that a datum existed before a particular time. This technique allows to prove that the signature was generated before the date contained in the time-stamp token. Policy requirements to cover that case is the primary reason of the present document."							
	Original resolution proposal	New text: "... 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 ...".							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-002	1.1.1	4.3 (2nd para)	UNSTT-006		editorial			not yet processed	
	Comment text	Modify the text: "In any case the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore the such an organization is expected to suitably inform its end users."							
	Original resolution proposal	New text: "...In any case the organization will be responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization..."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-003	1.1.1	4.4.3	UNSTT-006		editorial			not yet processed	
	Comment text	Modify the text: "A time-stamp policy may be defined by the user of times-stamp services, whereas the TSA practice statement is always defined by the provider."							
	Original resolution proposal	New text: "A time-stamp policy may be defined by the user of time-stamp services ..."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-004	1.1.1	7	UNSTT-006		editorial			not yet processed	
	Comment text	Modify the text: "The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objective will be met."							
	Original resolution proposal	New text: "The requirements ... where considered necessary to provide the necessary confidence that those objectives..."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-005	1.1.1	1	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "The current document addresses requirements for TSAs issuing time-stamp tokens which are synchronized with Coordinated universal time (UTC) and digitally signed by the TSA..."							
	Original resolution proposal	New text: "...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)"							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-006	1.1.1	2	UNSTT-006		technical			not yet processed	
	Comment text	Update the reference "FIPS PUB 140-1 (1994): "Security Requirements For Cryptographic Modules".							
	Original resolution proposal	New reference: FIPS PUB 140-2 (2001): "Security Requirements For Cryptographic Modules".							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-007	1.1.1	6.1.1	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "The TSA shall also ensure adherence to any additional obligations indicated in the time-stamp either directly or incorporated by reference."							
	Original resolution proposal	New text: "...The TSA shall also ensure adherence to any additional obligations indicated in the time-stamp token..."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-008	1.1.1	6.2	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "NOTE: It is advisable that, when obtaining a time-stamp token, the subscriber verifies that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp token has not been compromised."							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-009	1.1.1	6.3	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "a) verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification; NOTE: During the TSA's certificate validity period, the validity of the signing key can be checked using current revocation status for the TSA's certificate. If the time of verification exceeds the end of the validity period of the corresponding certificate, see annex D for guidance. b) take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy;"							
	Original resolution proposal	New text: "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;"							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-010	1.1.1	7.1.2	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "d) The expected life-time of the signature used to sign the time-stamp token (depends on the hashing algorithm being used, the signature algorithm being used and the private key length). j) The period of time during which TSA event logs (see clause 7.4.10) are retained.							
	Original resolution proposal	New text: "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)							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-011	1.1.1	7.2.1	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "The TSA shall ensure that any cryptographic keys are generated in 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 PUB 140-1 [4] level 3 or higher; or"							
	Original resolution proposal	New text: "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 PUB 140-1[4] or FIPS PUB 140-2 [7] level 3 or higher; or..."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-012	1.1.1	7.2.2	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "a) The TSA private signing key shall be held and used within a cryptographic module which: - meets the requirements identified in FIPS PUB 140-1 [4] level 3 or higher; or"							
	Original resolution proposal	New text: "a) The TSA private signing key shall be held and used within a cryptographic module which: - meets the requirements identified in FIPS PUB 140-1 [4] or FIPS PUB 140-2 [7] level 3 or higher; or"							
	Resolution comment								
	Resolution text								

<table>
<tr><th>Comment ID</th><th>Deliverable version</th><th>Deliverable clause</th><th>Original contribution reference</th><th>Comment date</th><th>Comment type</th><th>Resolution source</th><th>Resolution date</th><th>Resolution status</th><th>Deliverable target version</th></tr>
<tr><td>TS102023-013</td><td>1.1.1</td><td>7.2.4</td><td>UNSTT-006</td><td></td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td></td><td><b>Comment text</b></td><td colspan="8">Modify the text:
"NOTE 1: The following additional considerations apply when limiting that lifetime:
- Clause 7.4.10 requires that records concerning time-stamping services shall be held for a period of time as appropriate for at least 1 year after the expiration of the validity of the TSA's signing key. The longer the validity period of the TSA certificate will be, the longer the size of the records to be kept will be."</td></tr>
<tr><td></td><td><b>Original resolution proposal</b></td><td colspan="8">New text:
"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.</td></tr>
<tr><td></td><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td></td><td><b>Resolution text</b></td><td colspan="8"></td></tr>
<tr><td><b>Comment ID</b></td><td><b>Deliverable version</b></td><td><b>Deliverable clause</b></td><td><b>Original contribution reference</b></td><td><b>Comment date</b></td><td><b>Comment type</b></td><td><b>Resolution source</b></td><td><b>Resolution date</b></td><td><b>Resolution status</b></td><td><b>Deliverable target version</b></td></tr>
<tr><td>TS102023-014</td><td>1.1.1</td><td>7.2.5</td><td>UNSTT-006</td><td></td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td></td><td><b>Comment text</b></td><td colspan="8">Modify the text:
"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.
c) The TST generation system SHALL reject any attempt to issue TSTs if the signing private key has expired."</td></tr>
<tr><td></td><td><b>Original resolution proposal</b></td><td colspan="8">New text:
"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)."</td></tr>
<tr><td></td><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td></td><td><b>Resolution text</b></td><td colspan="8"></td></tr>
<tr><td><b>Comment ID</b></td><td><b>Deliverable version</b></td><td><b>Deliverable clause</b></td><td><b>Original contribution reference</b></td><td><b>Comment date</b></td><td><b>Comment type</b></td><td><b>Resolution source</b></td><td><b>Resolution date</b></td><td><b>Resolution status</b></td><td><b>Deliverable target version</b></td></tr>
<tr><td>TS102023-015</td><td>1.1.1</td><td>7.2.6</td><td>UNSTT-006</td><td></td><td>technical</td><td></td><td></td><td>not yet processed</td><td></td></tr>
<tr><td></td><td><b>Comment text</b></td><td colspan="8">Modify the title: "Life cycle management of cryptographic module used to sign time-stamps".</td></tr>
<tr><td></td><td><b>Original resolution proposal</b></td><td colspan="8">New title: "Life cycle management of cryptographic module used to sign time-stamp tokens".</td></tr>
<tr><td></td><td><b>Resolution comment</b></td><td colspan="8"></td></tr>
<tr><td></td><td><b>Resolution text</b></td><td colspan="8"></td></tr>
</table>

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-016	1.1.1	7.3.1	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "NOTE 2: A protocol for a time-stamp token is defined in RFC 3161 and profiled in TS 101 861. h) The name of the issuing TSA shall be identified in the time-stamp token. This shall include: - an identifier for the unit which issues the time-stamps."							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-017	1.1.1	7.3.2	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "NOTE 2: Relying parties are required to be informed of such events (see clause 7.4.8)."							
	Original resolution proposal	New text: "NOTE 2: Subscribers and relying parties…"							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-018	1.1.1	7.4.5	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "c) Media used within the TSA trustworthy systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence."							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-019	1.1.1	7.4.6	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "e) TSA personnel shall be accountable for their activities, for example by retaining event logs (see clause 7.4.10)."							
	Original resolution proposal	New text: "e) TSA personnel shall be accountable for their activities, for example, by retaining event logs (see clause 7.4.11)."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-020	1.1.1	7.4.8	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "c) In the case of compromise to the TSA's operation (e.g. TSA key compromise), suspected compromise or loss of calibration the TSA shall not issue time-stamp tokens until steps are taken to recover from the compromise."							
	Original resolution proposal	New text: "c) In the case of compromise to the TSA's operation (e.g. TSA private signing key compromise)…"							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-021	1.1.1	7.4.9	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "a) Before the TSA terminates its time-stamping services the following procedures shall be executed as a minimum: - the TSA shall transfer obligations to a reliable party for maintaining event log and audit archives (see clause 7.4.10) necessary to demonstrate the correct operation of the TSA for a reasonable period;"							
	Original resolution proposal	New text: "a) Before the TSA terminates its time-stamping services the following procedures shall be executed as a minimum: - 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;"							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-022	1.1.1	7.4.11	UNSTT-006		technical			not yet processed	
	Comment text	Modify the text: "f) Records concerning time-stamping services shall be held for a period of time after the expiration of the validity of the TSA's signing key as appropriate for providing necessary legal evidence and as notified in the TSA disclosure statement (see clause 7.1.2)."							
	Original resolution proposal	New text: "f) "Records concerning time-stamping services ... after the expiration of the validity of the TSA's signature verification (public) key as appropriate…"							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-023	1.2.1	4.2	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	It should be clearly defined the TSA's key. Because readers cannot distinguish if it is TSA's key or TSU's key.							
	Original resolution proposal								
	Resolution comment	TSUs belong to a TSA. So it could be said that TSU keys also belong to the TSA. However, since the key resides in a specific TSU use of the more specific term TSU key is considered more appropriate. (However, it is not that the heading of clause 7.2.1 should be changed to "TSU key".							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-024	1.2.1	4.2	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	We propose to describe a restriction on key backup. E.g. "TSA's key should not be cloned".							
	Original resolution proposal								
	Resolution comment	It is not exactly clear what "cloned" means. Requirements for security of any backup keys are covered by 7.2.2 b & c.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-025	1.2.1	7.1.2 d)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	Readers easily understand "The expiration date of the time-stamp token, TSA assured,"							
	Original resolution proposal								
	Resolution comment	Time-stamps validity do not expire after this period. It is only necessary to provide additional protection to maintain the integrity of the token (e.g. using additional signatures).							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-026	1.2.1	7.1.2 j)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process	
	Comment text	"See clause 7.4.10" is wrong. "See clause 7.4.11' is right"							
	Original resolution proposal	"See clause 7.4.10" is wrong. "See clause 7.4.11' is right"							
	Resolution comment	Correction noted.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-027	1.2.1	7.2.1 b)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process	
	Comment text	FIPS PUB 140-2 is also required.							
	Original resolution proposal	FIPS PUB 140-2 is also required.							
	Resolution comment	Use of FIPS PUB 140-2 to be considered for next revision.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-028	1.2.1	7.2.2 a)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process	
	Comment text	FIPS PUB 140-2 is also required.							
	Original resolution proposal	FIPS PUB 140-2 is also required.							
	Resolution comment	Use of FIPS PUB 140-2 to be considered for next revision.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-029	1.2.1	7.2.2 b)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process	
	Comment text	Following note is needed. NOTE: When the backup key is recovered, the TSA needs to assure that it does not use previously used serial numbers in the TSTs for new TSTs.							
	Original resolution proposal	Following note is needed. NOTE: When the backup key is recovered, the TSA needs to assure that it does not use previously used serial numbers in the TSTs for new TSTs.							
	Resolution comment	To be considered for next revision. It is recommended that new keys are generated instead.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-030	1.2.1	7.2.4	JCPKI-005	17/02/2003	editorial	STF242	21/06/2003	in process	
	Comment text	NOTE 1: "See clause 7.4.10" is wrong. "See clause 7.4.11" is right.							
	Original resolution proposal	NOTE 1: "See clause 7.4.10" is wrong. "See clause 7.4.11" is right.							
	Resolution comment	Correction noted.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-031	1.2.1	7.3.1 e)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	Following measure is needed. If the TSA's clock has been out of the stated accuracy and TSTs were issued before it was detected, the TSA shall revoke the TSTs.							
	Original resolution proposal	Following measure is needed. If the TSA's clock has been out of the stated accuracy and TSTs were issued before it was detected, the TSA shall revoke the TSTs.							
	Resolution comment	Revocation of time-stamp tokens is not practical. It is preferable to ensure that the TSA stops issuing tokens well before there is a risk that the clock drifts outside accepted accuracy.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-032	1.2.1	7.3.2 a)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process	
	Comment text	The TSA also needs to show to users how it can prove its clock's correctness. For instance, The TSA shall keep and show tractability and authenticity to UTC as its time source to users. An investigation of guideline is required.							
	Original resolution proposal								
	Resolution comment	Noted to be considered for next revision. Synchronization logs may meet this need.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-033	1.2.1	7.3.2 d)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process	
	Comment text	We believe that "the TSA should not issue time-stamps when it is processing for a leap second". Some investigation of guideline is required.							
	Original resolution proposal								
	Resolution comment	Issue noted. However, the importance of availability of time-stamping services needs to be taken into account.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-034	1.2.1	7.4.8	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	It should be provided a way of how to deal with issued TSTs in the following cases. 1. Compromise of the TSA"s signing key 2. Detected loss of calibration							
	Original resolution proposal								
	Resolution comment	Steps required already specified in clause 7.4.8.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-035	1.2.1	7.4.8 c)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	There will be possibility that TST is issued after compromise occurred and it cannot be detected for a while. So we believe that when such cases happened the TSA need to show information of it to relying parties and subscribers (e.g. by time-stamps revocation list). Some investigation of guideline is required.							
	Original resolution proposal								
	Resolution comment	Since the impact of such a compromise is difficult to predict it is not clear whether automatic recovery is practical. It is preferable to measures in place to avoid such a disaster.							
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-036	1.2.1		JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	Referring to TS 102 023, as examples of a specific TSA policy, two operation regulations were created in FY2002 report, "Time-stamping usage guideline". 1. Example of time-stamping service operation regulation using simple protocol. 2. Example of time-stamping service operation regulation using linking protocol. Also in "Time-stamping usage guideline", the important matters on use of time-stamping were summarized. Here we discussed about "Time Authentication" which is not specifically described in the above ETSI TS. A time-stamp token issued by TSA should have the correct time but the token does not have a mechanism to prove that the token itself uses a reliable time source to guarantee the time accuracy. The time included in time-stamp token that TSA insist the accuracy should link to the national standard time based UTC and there should be a mechanism to guarantee the accuracy.							
	Original resolution proposal								
	Resolution comment	The requirements for synchronization with UTC are specified in clause 7.3.2. It is left open to the implementation to decide which mechanism is to be used.							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102023-037	1.2.1		MAINT-001		technical			not yet processed	
	Comment text	The TS 101 733 should be consistent with RFC 3161 and use the "time-stamp token" within a description and "TimeStampToken" for formal definitions (i.e. ASN.1 and XML). The TSA policy should also be consistent.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-038	1.2.1		TC-ESI_2-002	13/06/2003	technical			not yet processed	
	Comment text	To the maintenance team of TS 102 023. In clause 7.2.3. we currently only have: 7.3.2 Clock Synchronization with UTC b) The TSA clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration. Let us consider two scenarios: Scenario A. The clock reference is outside the HSM. It is for example a PCI card placed in a PC with a crystal clock compensated in temperature and synchronized manually every week with UTC by an operator. The operator is able to set any time when performing the synchronization. Someone having an access to the room and knowing some ID and password could set any time. This scenario relies on the security of the environment and on the respect of procedures. Scenario B. The clock reference is within a HSM (Tamper Resistant - Hardware Security Module), this means that both the clock and the TSU signing key are within the same HSM. The clock is based upon a crystal clock compensated in temperature and synchronized every week with UTC. Every week a compensation of only XX microseconds (e.g. 100 microseconds) is allowed. If more is being done, the private key will be zeroized and a new full installation must be done. Someone having an access to the room and knowing *everything* cannot do more that a clock drift of XX microseconds. This scenario only relies on the security features of the HSM. Conclusion I see the need for two different qualities for the protection whether: 1) the security is achieved both by room access control and by procedures to be respected by human-beings, or 2) the security is achieved by security features built-in inside the HSM. This should lead to define two different TSA policies, ... unless we mandate the later only.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102023-039	1.2.1	7.2.2 - b)	TC-ESI_1-005	22/10/2003	technical			not yet processed	
	Comment text	Nothing is said about how long should the exported key protection last.							
	Original resolution proposal	Two possible amendments can apply: 1) Reword the paragraph with the same new text proposed for TS 101 456: - When outside the signature-creation device (see a) above) the CA private signing key shall be protected using systems that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key part. 2) Add the following sentence at the end of the paragraph: "The protection must be capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key part."							
	Resolution comment								
	Resolution text								

5.7 TR 102 038 - XML format for signature policies

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TR102038-001	1.1.1		JCPKI-006	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	To describe about OCSP trust condition, both in CommonRules and CommitmentRules element schema, add following element <xsd:element name="OCSPTrustCondition" type="OCSPTrustConditionType" minOccurs="0"/> This addition should apply on signature policy clause of TS 101 733 in same syntax.							
	Original resolution proposal	To describe about OCSP trust condition, both in CommonRules and CommitmentRules element schema, add following element <xsd:element name="OCSPTrustCondition" type="OCSPTrustConditionType" minOccurs="0"/> This addition should apply on signature policy clause of TS 101 733 in same syntax.							
	Resolution comment	This comment is to be fed into separate activities within ETSI on signature policies - see also response to "comments regarding EESSI Signature Policy".							
	Resolution text								

5.8 TR 102 041 - Signature policies report

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TR102041-001	1.2.1	8.3.1	JCPKI-007	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	In this clause, the Reports describe two types of commitments, which are Common Rules and Commitment Rules. However, meaning difference between these rules are little bit understandable. It is helpful for us if you explain some example of these Rules, especially commitment rules. Also in this clause, description "trust conditions for user certificate, timestamps and attributes" should be added OCSP responder's trust conditions. This addition should apply on signature policy clause of TS 101 733 in same syntax.							
	Original resolution proposal	In this clause, the Reports describe two types of commitments, which are Common Rules and Commitment Rules. However, meaning difference between these rules are little bit understandable. It is helpful for us if you explain some example of these Rules, especially commitment rules. Also in this clause, description "trust conditions for user certificate, timestamps and attributes" should be added OCSP responder's trust conditions. This addition should apply on signature policy clause of TS 101 733 in same syntax.							
	Resolution comment	This comment is to be fed into separate activities within ETSI on signature policies - see also response to "comments regarding EESSI Signature Policy".							
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TR102041-002	1.2.1	8.3.2	JCPKI-007	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	Revocation Requirements Please add CRL Distribution points not only full CRLs.							
	Original resolution proposal	Revocation Requirements Please add CRL Distribution points not only full CRLs.							
	Resolution comment	This comment is to be fed into separate activities within ETSI on signature policies - see also response to "comments regarding EESSI Signature Policy".							
	Resolution text								

5.9 TS 102 042 - PKC certificate policy

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-001	1.2.1	2	UNSTT-002		editorial			not yet processed	
	Comment text	Update the reference "FIPS PUB 140-1 (1994): "Security Requirements For Cryptographic Modules".							
	Original resolution proposal	New reference: FIPS PUB 140-2 (2001): "Security Requirements For Cryptographic Modules".							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-002	1.1.1	4.1 (1st para)	UNSTT-002		editorial			not yet processed	
	Comment text	Modify the text: "The certification authority has overall responsibility for the provision of the certification services identified in clause 4.1. The certification authority's key is used to sign the qualified certificates and it is identified in the certificate as the issuer."							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-003	1.1.1	4.1 (2nd para)	UNSTT-002		editorial			not yet processed	
	Comment text	Modify the text: "However, the key used to generate the certificates ..."							
	Original resolution proposal	New text: "However, the private key used to sign the certificates, ..."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-004	1.1.1	4.2	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "Dissemination service: disseminates certificates to subjects, and if the subject consents, to relying parties. This service also disseminates the CA's terms and conditions, and any published policy and practice information, to subscribers and relying parties."							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-005	1.1.1	6.2	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "The CA shall oblige, through agreement (see clauses 7.3.1a and 7.3.4), the subscriber to ensure that the subject fulfils the following obligations: a) accurate and complete information is submitted to the CA in accordance with the requirements of this policy, particularly with regards to registration; b) the key pair is only used in accordance with any 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) [CONDITIONAL] if the subscriber or subject generates the subject's keys: - subject keys are generated using an algorithm recognized by industry as being fit for the uses of the certified key as identified in the certificate policy; - a key length and algorithm is used which is recognized as being fit for the uses of the certified key as identified in the certificate policy; e) [CONDITIONAL] if the subscriber or subject generates the subject's keys and the private key is for creating electronic signatures only the subject holds the private key once delivered to the subject; f) [NCP+] only use the subject's private key for signing or decrypting with the secure user device; g) [NCP+] [CONDITIONAL] if the subject's keys are generated under control of the subscriber, generate the subject's keys within the secure user device used for signing or decrypting; h) notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate: - the subject's private key has been lost, stolen, potentially compromised; or - control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or - inaccuracy or changes to the certificate content, as notified to the subscriber; i) following compromise, the use of the subject's private key is immediately and permanently discontinued."							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
	Original resolution proposal	New text: "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 clause 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."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-006	1.1.1	7.2.1	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "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;"							
	Original resolution proposal	New text: "b) [CHOICE]: [LCP] CA key generation shall be carried out in a product, application or device which ensures that the keys are generated in a trustworthy manner and do not compromise the security of the private key and which: - meets the requirements identified in FIPS PUB 140-1 [2] level 2 or higher; or - is a trustworthy system which is assured to EAL 3 or higher in accordance to ISO/IEC 15408 [3], or equivalent security criteria. [NCP] CA key generation shall be carried out within a device which either: - meets the requirements identified in FIPS PUB 140-1 [2] level 3 or higher; or - meets the requirements identified in CWA 14167-2 [4], or"							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-007	1.1.1	7.2.2	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "a) [CHOICE]: [LCP] The CA private signing key shall be held and used in a product, application or device which does not compromise the security of the private key and which: - meets the requirements identified in FIPS PUB 140-1 [2] level 2 or higher; or - is a trustworthy system which is assured to EAL 3 or higher in accordance to ISO/IEC 15408 [3], or equivalent security criteria. [NCP] The CA private signing key shall be held and used within a secure cryptographic device which: - meets the requirements identified in FIPS PUB 140-1 [2] level 3 or higher; or - meets the requirements identified in CEN Workshop Agreement 14167-2 [4], or - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [3], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures. b) [CHOICE]: [LCP] When outside the signature-creation product, application or device, the secrecy of the CA's private key shall be ensured. NOTE: This may be achieved using physical security or encryption. [NCP] When outside the signature-creation device (see a) above) the CA private signing key shall be encrypted with an algorithm and key-length that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key part. c) The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 7.4.4). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices. d) Backup copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use. e) Where the keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module."							
	Original resolution proposal	New text: "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 FIPS PUB 140-2 [6] level 3 o higher; "							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-008	1.1.1	7.2.9	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "d) Where the secure user device has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the signature-creation module. NOTE: Separation may be achieved by ensuring distribution and delivery at different times, or via a different route."							
	Original resolution proposal	New text: 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…"							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-009	1.1.1	7.3.1	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "b) [CONDITIONAL]: If the subject is a person and not the same as the subscriber, the subject shall be informed of his/her obligations. c) The CA shall communicate this information through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language. NOTE 1: A model PKI disclosure statement which may be used as the basis of such a communication is given in annex B. d) The service provider shall collect either direct evidence, or an attestation from an appropriate and authorized source, of the identity (e.g. name) and, if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the subject's identity shall be by appropriate means and in accordance with national law. e) [CHOICE]: [LCP] No requirement. [NCP] If the subject is a physical person evidence of the subject's identity (e.g. name) shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 2). Evidence for verifying other entities shall involve procedures which provide the same degree of assurance. NOTE 2: An example of evidence checked indirectly against a physical person is documentation presented for registration which was acquired as the result of an application requiring physical presence. f) [CONDITIONAL] If the subject is a physical person, evidence shall be provided of: - full name (including surname and given names); - date and place of birth, reference to a nationally recognized identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name. NOTE 3: It is recommended that the place be given in accordance to national conventions for registering births. g) [CONDITIONAL] If the subject is a physical person who is identified in association with a legal person, or organizational entity (e.g. the subscriber), evidence shall be provided of: - full name (including surname and given names) of the subject; - date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name; - full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber); - any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity; - evidence that the subject is associated with the legal person or other organizational entity. h) [CONDITIONAL] If the subject is an organizational entity, evidence shall be provided of: - full name of the organizational entity; - reference to a nationally recognized registration, or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name. i) [CONDITIONAL] If the subject is a device or system operated by or on behalf of an organizational entity, evidence shall be provided of: - identifier of the device by which it may be referenced (e.g. Internet domain name); - full name of the organizational entity; - a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name. j) The subscriber shall provide a physical address, or other attributes, which describe how the subscriber may be contacted. k) The CA shall record all the information necessary to verify the subject's identity, including any reference number on the documentation used for verification, and any limitations on its validity.							

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
		l) The CA shall record the signed agreement with the subscriber including: - agreement to the subscriber's obligations (see clause 6.2); - if required by the CA, agreement by the subscriber to user secure user device; - consent to the keeping of a record by the CA of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clause 7.4.11), and passing of this information to third parties under the same conditions as required by this policy in the case of the CA terminating its services; - whether, and under what conditions, the subscriber requires and the subject consents to the publication of the certificate; - confirmation that the information held in the certificate as being correct. NOTE 4: The subscriber may agree to different aspects of this agreement during different stages of registration. For example, agreement that the information held in the certificate is correct may be carried out subsequent to other aspects of the agreement. NOTE 5: This agreement may be in electronic form. m) The records identified above shall be retained for the period of time as indicated to the subscriber (see c) above) and as necessary for the purposes for providing evidence of certification in legal proceedings."							
	Original resolution proposal	New text: "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 clause (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."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-010	1.1.1	7.2.8	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "e) [CONDITIONAL] If a copy of the subject's public key is not required to be kept by the CA (see clause 7.2.4), on delivery to the subject, only the subject (or, if the key is not for electronic signatures, the subscriber) shall have access to its private key. Any copies of the subject's private key held by the CA shall be destroyed."							
	Original resolution proposal	New text: "e) [CONDITIONAL] If a copy of the subject's private key is no required…"							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-011	1.1.1	3.1	UNSTT-002		technical			not yet processed	
	Comment text	Missing definition.							
	Original resolution proposal	New text: "Extended Normalized Certificate Policy: normalized certificate policy requiring use of a secure user device."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-012	1.1.1	7.4.4	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "Certificate generation, subject device provision and revocation management d) The facilities concerned with certificate generation, subject device provision and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data. e) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) 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. f) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CA's physical and environmental security policy for systems concerned with certificate generation, subject device provision and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc. g) Controls shall be implemented to protect against equipment, information, media and software relating to the CA services being taken off-site without authorization. NOTE 1: See ISO/IEC 17799 for guidance on physical and environmental security. NOTE 2: Other functions may be supported within the same secured area provided that the access is limited to authorized personnel."							
	Original resolution proposal	New text: "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: ..."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-013	1.1.1	7.4.5	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "c) Media used within the CA shall be securely handled to protect media from damage, theft and unauthorized access."							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-014	1.1.1	7.4.8	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "Revocation status c) In the case of compromise the CA shall as a minimum provide the following undertakings: - inform all subscribers, relying parties and other CAs with which it has agreements or other form of established relations of the compromise;"							
	Original resolution proposal	New text: "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…"							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-015	1.1.1	7.4.9	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "CA General a) Before the CA terminates its services the following procedures shall be executed as a minimum: - the CA shall inform all subscribers, relying parties and other CAs with which it has agreements or other form of established relations;"							
	Original resolution proposal	New text: "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."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-016	1.1.1	7.4.11	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "The CA shall ensure that all relevant information concerning a 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. NOTE 1: Records concerning certificates include registration information (see clause 7.3.1) and information concerning significant CA environmental, key management and certificate management events. In particular: General a) The confidentiality and integrity of current and archived records concerning certificates shall be maintained. b) Records concerning certificates shall be completely and confidentially archived in accordance with disclosed business practices. c) Records concerning certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. The subject, and within the constraints of data protection requirements (see clause 7.4.10) the subscriber, shall have access to registration and other information relating to the subject. NOTE 2: This may be used, for example, to support the link between the certificate and the subject. d) The precise time of significant CA environmental, key management and certificate management events shall be recorded. NOTE 3: It is recommended that the CA states in its practices the accuracy of the clock used in timing of events, and how this accuracy is ensured. e) Records concerning certificates shall be held for a period of time as indicated in the CA's terms and conditions (see clause 7.3.4). f) The events shall be logged in a way that they cannot be easily deleted or destroyed (except for transfer to long-term media) within the period of time that they are required to be held. NOTE 4: This may be achieved, for example, through the use of write only media, a record of each removable media used and the use of off site backup. g) The specific events and data to be logged shall be documented by the CA. Registration h) The CA shall ensure all events relating to registration including requests for certificate re-key or renewal, are logged. i) The CA shall ensure that all registration information including the following is recorded: - type of document(s) presented by the applicant to support registration; - record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents, if applicable; - storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.3.1 l); - any specific choices in the subscriber agreement (e.g. consent to publication of certificate); - identity of entity accepting the application; - method used to validate identification documents, if any; - name of receiving CA and/or submitting Registration Authority, if applicable. j) The CA shall ensure that privacy of subject information is maintained."							
	Original resolution proposal	New text: "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)."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-017	1.1.1	3.2	UNSTT-002		technical			not yet processed	
	Comment text	Modify the text: "NCP+ Normalized Certificate Policy requiring use of a secure user device"							
	Original resolution proposal	New text: "NCP+ Extended Normalized Certificate Policy."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-018	1.1.1		TC-ESI_3-002		technical			not yet processed	
	Comment text	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.							
	Original resolution proposal								
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-019	1.1.1	7.2.9	OTHER-005		technical			not yet processed	
	Comment text	I am wondering whether we omitted a clause in TS 101 456 [1] to state that the CA shall inform their subscribers about the kind of environment that he shall use for the SSCD, pointing to CWA 14170 [12]: Security requirements for Signature Creation Systems.							
	Original resolution proposal	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."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-020	1.1.1	7.2.5	OTHER-006		technical			not yet processed	
	Comment text	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 necessarily compromise security. Probably we could advice CSPs to use dedicated keys (use should instead of shall), but not make that as a requirement.							
	Original resolution proposal	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.							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-021	1.1.1	7.4.7	OTHER-007		technical			not yet processed	
	Comment text	Update clause 7.4.7, note 1 to explicitly reference CWA 14167-1 [11] 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)".							
	Original resolution proposal	Update clause 7.4.7, note 1 to explicitly reference CWA 14167-1 [11] and add the reference to the bibliography/references.							
	Resolution comment								
	Resolution text								
Comment ID	**Deliverable version**	**Deliverable clause**	**Original contribution reference**	**Comment date**	**Comment type**	**Resolution source**	**Resolution date**	**Resolution status**	**Deliverable target version**
TS102042-022	1.1.1	8	OTHER-008		technical			not yet processed	
	Comment text	It is currently not clear when a new certification policy is necessary.							
	Original resolution proposal	Add to clause 8: "No changes should be made to a certificate policy which could affect a relying party's consideration on the reliability of the certificate issued by the CA."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-023	1.1.1	7.2.2 - b) - NCP	TC-ESI_1-004	22/10/2003	technical			not yet processed	
	Comment text	CA private signing keys, when exported, can be protected not only by means of encryption, but also by means of other mechanisms, like Shamir's or Blakley's threshold secret sharing mechanism.							
	Original resolution proposal	Change clause 7.2.2 - item b), paragraph [NCP] into "When outside the signature-creation device (see a) above) the CA private signing key shall be protected using cryptographic systems that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key component."							
	Resolution comment								
	Resolution text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-024	1.1.1	Annex D	TC-ESI_1-007	26/10/2003	technical			not yet processed	
	Comment text	Correct the inconsistencies in annex D, the cross reference between RFC 2527 and TS 101 456.							
	Original resolution proposal	Amendment proposed: * 3.4: change "7.3.5" into "7.3.6" * 4.4: change "7.3.5" into "7.3.6" * 5.2: change "7.4.5" into "7.4.3" (note 1) * 6.3: add "6.2, " before "7.2" * 6.4: add "7.2.7, " before "7.2.9" * 6.5: add "7.4.5, " before "7.4.6" * 6.6: change "7.3" into "7.4" (note 2) * 6.7: add "7.4.5, " before "7.4.6" NOTE 1: The procedural controls, as per RFC 2527, are: "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22). For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule). Identification and authentication requirements for each role may also be defined." NOTE2: The life cycle security controls, as per RFC 2527, are: "This subcomponent addresses system development controls and security management controls. System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design and implementation techniques (e.g., defensive programming) and development facility security. (<- this is not addressed by TS 101 456) Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation. (<- this is addressed in clause 7.4 of TS 101 456) This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM). (<- this is not addressed by TS 101 456)."							
	Resolution comment								
	Resolution text								

Annex A:
Comments in their original format

This annex collects the comments in their original format. To identify each contribution a unique identifier that includes a prefix is used (see clause 5 for an explanation of the identifier format). Hereafter the list of prefixes:

EESSI	EESSI Evaluation
JCPKI	Japan and China PKI Forums
MAINT	CEN/ISSS WS/E-Sign Area M and ETSI STF-210 maintenance groups
OTHER	Other: unknown originator
PR	PinkRoccade (Netherlands)
STF-220_2	ETSI STF-220 - Task 2
STF-220_4	ETSI STF-220 - Task 4
TC-ESI_1	TC-ESI member
TC-ESI_2	TC-ESI member
TC-ESI_3	TC-ESI member
UNSTT	Uninfo-STT (Italy)
XAdES-PT	XAdES-Plugtest

A.1 Comments from a TC-ESI member

A.1.1 TS 101 456 - Qualified certificate policy

A.1.1.1 Proposed amendments from CEN/ISSS area M on system backup and recovery

Contribution metadata	
ID contribution	TC-ESI_1-001
Source	TC-ESI member
Version of the deliverable	1.2.1
Date	14 February 2003

Contribution: comment

In clause 7.4.8 subsection CA General an additional sub-sub-section could be added, named "System backup and recovery", covering the need for these backups in order to resume functions upon disaster. This clause should specify that while the system data **backup** may be performed by one officer provided they have sufficient privileges, **restore** must be performed under at least dual control.

Contribution: proposed resolution

To add a sub-sub-section named "System backup and recovery" in clause 7.4.8 subsection CA General. To be further specified.

A.1.1.2 Auditor's view of system logs

Contribution metadata	
ID contribution	TC-ESI_1-002
Source	TC-ESI member
Version of the deliverable	1.2.1
Date	30 January 2003

Contribution: comment

Clause 7.4.3.g) last bullet reads:

"System Auditors: Authorized to view and maintain archives and audit logs of the CA trustworthy systems."

IMO auditors must just look at archives and log files "handcuffed". If they can play with them, then their audit function is devoid of trust. If I'm wrong please say it clear. If you, instead, agree, the sentence should read: "System Auditors: Authorized to view archives and audit logs of the CA trustworthy systems."

Contribution: proposed resolution

Clause 7.4.3.g) last bullet change the sentence "System Auditors: Authorized to view and maintain archives and audit logs of the CA trustworthy systems." to "System Auditors: Authorized to view archives and audit logs of the CA trustworthy systems."

A.1.1.3 Export of the CA private key

Contribution metadata	
ID contribution	TC-ESI_1-003
Source	TC-ESI member
Version of the deliverable	1.2.1
Date	22 October 2003

Contribution: comment

Clause 7.2.2 - item b):

CA private signing keys, when exported, can be protected not only by means of encryption, but also by means of other mechanisms, like Shamir's or Blakley's threshold secret sharing mechanism.

Contribution: proposed resolution

Change clause 7.2.2 - item b) into "When outside the signature-creation device (see a) above) the CA private signing key shall be protected using cryptographic systems that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key component."

A.1.1.4 Mapping with RFC 2527

Contribution metadata	
ID contribution	TC-ESI_1-006
Source	TC-ESI member
Version of the deliverable	1.2.1
Date	26 October 2003

Contribution

I noticed some possible inconsistencies in TS 101 456 annex D (X-ref between RFC 2527 and TS 101 456).

My suggested changes to the annex.

IETF RFC 2527 [2] policy reference	Qualified certificate
1 INTRODUCTION	
1.1 Overview	5.1
1.2 Identification	5.2
1.3 Community and Applicability	5.3
1.4 Contact Details	back of title page
2 GENERAL PROVISIONS	
2.1 Obligations	6.1, 6.2, 6.3
2.2 Liability	6.4
2.3 Financial Responsibility	7.5

IETF RFC 2527 [2] policy reference	Qualified certificate
2.4 Interpretation and Enforcement	5.4
2.5 Fees	N/A
2.6 Publication and Repositories	7.3.5, 7.3.6
2.7 Compliance Audit	N/A
2.8 Confidentiality Policy	7.3.1
2.9 Intellectual Property Rights	N/A
3 IDENTIFICATION AND AUTHENTICATION	
3.1 Initial Registration	7.3.1
3.2 Routine Rekey	7.3.2
3.3 Rekey After Revocation -- No Key Compromise	7.3.2
3.4 Revocation Request	7.3.~~5~~6
4 OPERATIONAL REQUIREMENTS	
4.1 Certificate Application	7.3.1
4.2 Certificate Issuance	7.3.3
4.3 Certificate Acceptance	7.3.1
4.4 Certificate Suspension and Revocation	7.3.~~5~~6
4.5 Security Audit Procedures	N/A
4.6 Records Archival	7.4.11
4.7 Key Changeover	7.3.2
4.8 Compromise and Disaster Recovery	7.4.8
4.9 CA Termination	7.4.9
5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	
5.1 Physical Security Controls	7.4.4
5.2 Procedural Controls	7.4.~~5~~3 (see note 1)
5.3 Personnel Security Controls	7.4.3
6 TECHNICAL SECURITY CONTROLS	
6.1 Key Pair Generation and Installation	7.2.8, 7.2.9
6.2 Private Key Protection	7.2.8
6.3 Other Aspects of Key Pair Management	7.2, 6.2
6.4 Activation Data	7.2.7, 7.2.9
6.5 Computer Security Controls	7.4.5, 7.4.6, 7.4.7
6.6 Life Cycle Security Controls	7.~~3~~4 (see note 2)
6.7 Network Security Controls	7.4.5, 7.4.6
6.8 Cryptographic Module Engineering Controls	7.2
7 CERTIFICATE AND CRL PROFILES	
7.1 Certificate Profile	7.3.3
7.2 CRL Profile	N/A
8 SPECIFICATION ADMINISTRATION	
8.1 Specification Change Procedures	7.1
8.2 Publication and Notification Procedures	7.1
8.3 Certification practice statement Approval Procedures	7.1

NOTE 1: he procedural controls, as per RFC 2527, are:
"In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).
For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."

NOTE2: The life cycle security controls, as per RFC 2527, are:
"This subcomponent addresses system development controls and security management controls.
System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design and implementation techniques (e.g. defensive programming) and development facility security (this is not addressed by TS 101 456).
Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation (this is addressed in clause 7.4 of TS 101 456).
This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM) (this is not addressed by TS 101 456).

A.1.2 TS 102 042 - Normalized certificate policy

A.1.2.1 Export of the CA private key

Contribution metadata	
ID contribution	TC-ESI_1-004
Source	TC-ESI member
Version of the deliverable	1.1.1
Date	22 October 2003

Contribution: comment

Clause 7.2.2 - item b), paragraph [NCP]:

CA private signing keys, when exported, can be protected not only by means of encryption, but also by means of other mechanisms, like Shamir's or Blakley's threshold secret sharing mechanism.

Contribution: proposed resolution

Change clause 7.2.2 - item b), paragraph [NCP] into "When outside the signature-creation device (see a) above) the CA private signing key shall be protected using cryptographic systems that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key component."

A.1.2.2 Mapping with RFC 2527

Contribution metadata	
ID contribution	TC-ESI_1-007
Source	TC-ESI member
Version of the deliverable	1.1.1
Date	27 October 2003

Contribution

I noticed some possible inconsistencies in TS 101 456 annex D (X-ref between RFC 2527 and TS 101 456).

My suggested changes to the annex.

IETF RFC 2527 [2] policy reference	Qualified certificate
1 INTRODUCTION	
1.1 Overview	5.1
1.2 Identification	5.2
1.3 Community and Applicability	5.3
1.4 Contact Details	back of title page
2 GENERAL PROVISIONS	
2.1 Obligations	6.1, 6.2, 6.3
2.2 Liability	6.4
2.3 Financial Responsibility	7.5
2.4 Interpretation and Enforcement	5.4
2.5 Fees	N/A
2.6 Publication and Repositories	7.3.5, 7.3.6
2.7 Compliance Audit	N/A
2.8 Confidentiality Policy	7.3.1
2.9 Intellectual Property Rights	N/A
3 IDENTIFICATION AND AUTHENTICATION	
3.1 Initial Registration	7.3.1
3.2 Routine Rekey	7.3.2
3.3 Rekey After Revocation -- No Key Compromise	7.3.2
3.4 Revocation Request	7.3.~~5~~6
4 OPERATIONAL REQUIREMENTS	
4.1 Certificate Application	7.3.1

IETF RFC 2527 [2] policy reference	Qualified certificate
4.2 Certificate Issuance	7.3.3
4.3 Certificate Acceptance	7.3.1
4.4 Certificate Suspension and Revocation	7.3.~~5~~6
4.5 Security Audit Procedures	N/A
4.6 Records Archival	7.4.11
4.7 Key Changeover	7.3.2
4.8 Compromise and Disaster Recovery	7.4.8
4.9 CA Termination	7.4.9
5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	
5.1 Physical Security Controls	7.4.4
5.2 Procedural Controls	7.4.~~5~~3 (see note 1)
5.3 Personnel Security Controls	7.4.3
6 TECHNICAL SECURITY CONTROLS	
6.1 Key Pair Generation and Installation	7.2.8, 7.2.9
6.2 Private Key Protection	7.2.8
6.3 Other Aspects of Key Pair Management	7.2, 6.2
6.4 Activation Data	7.2.7, 7.2.9
6.5 Computer Security Controls	7.4.5, 7.4.6, 7.4.7
6.6 Life Cycle Security Controls	7.~~3~~4 (see note 2)
6.7 Network Security Controls	7.4.5, 7.4.6
6.8 Cryptographic Module Engineering Controls	7.2
7 CERTIFICATE AND CRL PROFILES	
7.1 Certificate Profile	7.3.3
7.2 CRL Profile	N/A
8 SPECIFICATION ADMINISTRATION	
8.1 Specification Change Procedures	7.1
8.2 Publication and Notification Procedures	7.1
8.3 Certification practice statement Approval Procedures	7.1

NOTE 1: The procedural controls, as per RFC 2526, are:
"In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).
For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."

NOTE 2: The life cycle security controls, as per RFC 2527, are:
"This subcomponent addresses system development controls and security management controls.
System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design and implementation techniques (e.g., defensive programming) and development facility security (this is not addressed by TS 101 456).
Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation (this is addressed in clause 7.4 of TS 101 456).
This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM) (this is not addressed by TS 101 456).

A.1.3 TS 102 023 - Time-stamping policy

A.1.3.1 Export of the CA private key

Contribution metadata	
ID contribution	TC-ESI_1-005
Source	TC-ESI member
Version of the deliverable	1.2.1
Date	22 October 2003

Contribution: comment

Clause 7.2.2 - item b):

Nothing is said about how long should the exported key protection last.

Contribution: proposed resolution

Two possible amendments can apply:

1) Reword the paragraph with the same new text proposed for TS 101 456:

    - When outside the signature-creation device (see a) above) the CA private signing key shall be protected using systems that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key part.

2) Add the following sentence at the end of the paragraph: "The protection must be capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key part".

A.2 Comments and proposed amendments from UNINFO-STT (Italy)

A.2.1 Proposed amendments on TS 101 456

Contribution metadata	
ID contribution	UNSTT-001
Source	Uninfo-STT
Version of the deliverable	1.2.1
Date	

Contribution

Introduction

The present document means to give suggestions in order to modify TS 101 456 [2]: 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

Clause 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 clause 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 FIPS PUB 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 clause (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 **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 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).

A.2.2 Proposed amendments on TS 102 042

Contribution metadata	
ID contribution	UNSTT-002
Source	Uninfo-STT
Version of the deliverable	1.2.1
Date	

Contribution

Introduction

The present document means to give suggestions in order to modify TS 102 042: 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 includes much text that is in common with TS 101 456 the proposed amendments are roughly the same as those proposed to TS 101 456.

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**

Clause 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 clause 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 FIPS PUB **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 FIPS PUB **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 FIPS PUB **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 clause (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).

A.2.3 Early informal comments on TS 101 733 from STT-A2 WG (September 2002)

Contribution metadata	
ID contribution	UNSTT-003
Source	Uninfo-STT
Version of the deliverable	1.4.0
Date	September 2002

Contribution

- References to the various RFCs and Internet Drafts from PKIX (especially RFC 2459 and RFC 3280).
- 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 verification processes (initial and usual), even if it is a matter of CWA 14170.
- 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".

A.2.4 Stable informal comments on TS 101 733 from STT-A2 WG (February 2003)

Contribution metadata	
ID contribution	UNSTT-004
Source	Uninfo-STT
Version of the deliverable	1.4.0
Date	February 2003

Contribution

See the following clauses.

A.2.4.1 Proposals about the document contents

- Making the SignaturePolicyID signed attribute optional and without the NULL value.
- Making the SigningTime signed attribute optional.
- Generalization of the timemark concept (as an external trusted time indication, see ES-Cbis).
- ES as the minimum mandatory format.
- Signature policy: introducing the minimum mandatory format for a specific application as an additional rule.

A.2.4.2 Proposals about the document structure

- A better separation between the mandatory and optional formats; moving the optional formats from the body to an annex.
- Deleting all text and ASN.1 formal definition about Signature Policies from TS 101 733 and putting it into a specific document as for the XML version of formats and policies (UNINFO-STT, ETSI-STF).

A.2.4.3 Proposals for some additional explanatory documents

- Roadmap for the EESSI deliverables EESSI, from a functional perspective and from a new reader perspective: it could be a new version of EESSI DDD.
- A non-normative (Technical Report) document describing the whole model of the electronic signature generation and verification processes and formats: it could be a new detailed document based on the white papers "Validation of Electronic Signature" written by H.N. and D.P.
- A new document (Technical Report) about hand-written and electronic signatures interoperability, both from a legal perspective and from a technical perspective, including some case studies with and without signature policies and using different formats.

A.2.5 Proposed amendments to TS 101 862 from STT-A4 WG

Contribution metadata	
ID contribution	UNSTT-005
Source	Uninfo-STT
Version of the deliverable	1.2.1
Date	

Contribution

Introduction

TS 101 862, 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 is based upon RFC 3039, some comments to RFC 3039 are also made, which lead to some proposed TS 101 862 amendments.

A.2.5.1 References to be updated

Since TS 101 862 has been published, RFC 2459 has been replaced by RFC 3280. Thus it is suggested to accordingly modify TS 101 733 in the next TS version.

A.2.5.2 CSP identifier

a) Annex I of Directive 1999/93/EC [11], specifies: "Qualified certificates must contain:

….

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

TS 101 862 [7] 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."

A.2.5.3 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 clause 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 clauses 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."

A.2.5.4 Pseudonyms

A requirement is needed on how the pseudonym is to be "identified as such". RFC 3039 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 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."

A.2.5.5 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 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, clause 3.1.2. In addition to such identifier and where necessary to comply with RFC 3039 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], clause 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."

A.2.5.6 The key usage

There has been a long debate on RFC 3039 clause 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.

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 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."

A.2.6 Proposed amendments to TS 102 023 - Time-stamping policy

Contribution metadata	
ID contribution	UNSTT-006
Source	Uninfo-STT
Version of the deliverable	1.1.1
Date	

Contribution

Introduction

The present document means to give suggestions in order to modify TS 102 023: 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 PUB 140-1[4] or **FIPS PUB 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 PUB 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) Before the TSA terminates its time-stamping services the following procedures shall be executed as a minimum:

- 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;

✓ 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…"

A.3 Comments and proposed amendments from Japan and China PKI forums

A.3.1 Proposed amendments on TS 101 456

Contribution metadata	
ID contribution	JCPKI-001
Source	Japan and China PKI Forums
Version of the deliverable	1.2.1
Date	17 February 2003

Contribution

See the following clauses.

A.3.1.1 Comment #1, page 10

Comment

In "4.3 Certificate policy and certification practice statement", will it be better to add the specifications of the relations between them and the cross authentication?

A.3.1.2 Comment #2, page 18

Comment

"7.2.4 Key escrow", how to handle the problem of "legal monitor" in the wireless communications?

A.3.1.3 Comment #3, page 18

Comment

In "7.2 Public key infrastructure - Key management life cycle", why it doesn't mention the operation of "certification authority key update" like the protocols in PKIX?

A.3.2 Proposed amendments on TS 101 733

Contribution metadata	
ID contribution	JCPKI-002
Source	Japan and China PKI Forums
Version of the deliverable	1.3.1
Date	17 February 2003

Contribution

See the following clauses.

A.3.2.1 Rationale: Some comments regarding EESSI signature policy

Author: Japan Computer Research, 2003/02/17

Scope and Introduction

The purpose of the present document is to convey some comments upon the policy aspects of the electronic signature format as specified in [ESF] and [XAdES]. There are at least two obvious reasons to focus on this particular topic: the one is that one of the most distinct features of the specification seems to be incorporation of signature policy; the other is that the policy information issues in general can be regarded as one of the most important milestones in the future evolution of e-business.

It is now routine to standardize the encapsulation of signature data. And a number of these formats bind signature with corresponding public key, and often if not all the time, together with its certificate or certificate chain. That policy information can function as a means to validate status of accompanying object is well exemplified in the policy attributes of X.509 certificate profile. Nevertheless, it has to be said that attachment of policy to signature hasn't yet gained the rank of common acceptance. It has to be said, in this sense, that one of the most distinguishing characteristics of [ESF] lies in its introduction of signature policy.

However, we anticipate that the policy as proposed in [ESF] can have contextually entirely other use cases than those specific to that for public key certificates. To be more precise, due to more loose semantic constraints associated with digital signature, it is expected that application domain of the signature policy is far more broadly ranged compared to certificate policy. Accordingly, needs to address wider area of practical contexts are felt, and this naturally leads to the necessity of taking into account other policy related development efforts in the Internet community whose shared aim is to promote flexible online transactions (valued or otherwise) while approximating reliability of real world experience.

"Policy" has long been traditionally associated, one way or another, with the idea of authority, predominantly centrally and statically perceived at that. The underlying principle of certificate policy closely follows this, essentially due to the way it is bred. Against this, especially to the extent that each individual ought to possess his or her own policy, is a picture in which many policies dynamically interact to form the whole. And this may be thought of as what the "signature policy" might envisage, for signature marks each spatial and temporal lineament of some particular present event. In other words, it should suggest a way to collect disseminated policies in order to proffer a decision suitable to that point of time and space, a way to make feasible Policy Knowledge Interactivity. It is in this spirit that the following comments are delivered, although not always explicit.

Comments

1. On the mandated reference to policy. In the data structure, signature policy identifier is made mandatory [ESF; 8.9.1]. This can mean either that: (a) every signature MUST have a non-trivial signature policy available for retrieval in association with the identifier; or that (b) signature policy can have null (i.e. dummy and intentionally empty) signature policy in the case so desired:

   a) This case means that validation process refers to and explicitly made dependent on the signing process at each instant. I.e. the action of validation of a signature is determined by the signing of it at the time when the latter took place, so that the temporal medium between the two actions is made frozen. In particular, this allows the users to preserve unaltered the state and quality of signature relatively long time.

   b) In this case, the content of the policy can be determined at the time of the validation. Binding between the signature and validation is principally the responsibility of policy source (policy issuer or TSP), and the determination of actual policy content is left to the latter, and the issuance can be protracted to the time of the delivery.

   c) In practice, hybrid case is the most likely to be demanded. This is because:

      (i) Performance wise, a practical computing platform wants to avoid actual communication with the policy source to take place every each time of the signature generation. This is especially so in view that, for some algorithms, signing process is designed more costly in arithmetic operations than validation process. Also, applications serving as a service provider would surely have to process hundreds of requests in a second. All this would imply that signature policy may be cached until the time it is necessary to refresh, and would probably mean that policy content be left empty and signer decides its policy related action in terms of policy qualifiers only. Which in turn would mean that it is desired that policy qualifier carry validity dates or some sort of a "recommended best before."

      (i) Another reason why it is important to allow empty policy content at the time of signing is that, in encapsulating a transaction message in which signature data is to be attached, one might want to or have to place policy related information outside the signature data, for example using some other policy mechanisms (cf. item 2 below). Practically, this could perhaps mean often that two policy identifiers, that within the signature data and that outside it, are identical, but not necessarily.

2. On policy data or content. The design of [ESF] has that, according to the needs of the singing party and relying party, policy data or content can be obtained from the policy source the reference to which is embedded explicitly in the signature data in the form of mandatory policy identifier. [ESF] does not specify the policy content: "The precise content of a signature policy is not mandated by the present document." This could perhaps mean that not only its data structure but also the protocol through which it is obtained are left to the decision of policy source. Existing similar specification activities along these lines include [SAML], [XACML], and [WS-Policy]. We will examine briefly the possibility of applying these protocols to the purpose of obtaining policy content for the [ESF] signature data here:

   a) In General. These protocols are specified in terms of XML, while [ESF] data structure is defined in terms of ASN.1. So it would be natural to consider the use of [XAdES] instead of [ESF], to level the networking layer consistent. Similarly, in the following, the reference "[ESF]" is meant to be "[XAdES]", whenever the appropriateness of the context demands, without explicitly mentioned each time.

    b) SAML. By this, we mean to utilise SAML security assertions as policy content. Which would mean that policy source be SAML authority, messaging protocol be SAML request/response. [SAMLCore] states that SAML "is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subject, where a subject is an entity (either human or computer) that has an identity in some security domain." In order to fit exactly into this description, signature ought to represent the "entity" so intended, which is really the role of public key certificate as the common sense has it presently. However, the practical consideration ensues taking into account that promulgation of SAML is rapidly in place. Whereas, on the other hand, we believe that the signature policy of [ESF] type can act as an "external policy" for SAML, to the contrary.

    c) XACML. Although termed as "Access Control Markup Language," the motivation of XACML derives from "a pressing need for a common language for expressing security policy" ([XACML]). It is in this sense that XACML might just be suitable as the policy language for [ESF]. For this, however, we believe that one has to make a careful architectural consideration to cohere the two semantically (cf. item 5 for a brief remark on this).

    d) Web Services Policy Framework. Similar to applicability of XACML, but with a more restricted context of the web services interoperability. There are on-going investigations as to how [XACML] and [WS-Policy] can be made consistent in practice. Here we would rather insist on the synergy of [ESF] with [XACML] for the reason that semantics of XACML is more general in nature. To add, in conjunction with the overall web services security standards, one might think of applying secure SOAP messaging in the form of Web Services Security, for the signature policy queries (including referencing). We feel that this certainly is a potential.

3. On policy protection. The mechanism for policy protection is provided by the authentication of policy source ([ESF; 6.11]). The latter is rendered in terms of the hash calculation of the policy identifier. Also, binding of the policy source and actual policy seems to be rendered by the same mechanism (although only implicit, cf. [ESF; 11.1]). This may not offer enough level of protection, for a complex distributed policy environment in which, for example, policy source refers to another policy source and so on (which seems to be case with [SAML] in cooperation with [XACML]). Further, signature policy doesn't seem to carry its own signature explicitly, which means, if it is to be signed, the signature data are to be attached externally. We believe, to complement this, that signing of signature policy has to be described in detail, at least normatively (as XACML TC does). For especially, there may arise possible semantic ambiguities between "signature policy" and "policy signature." And it could well happen that the latter may be provided by some TSP other than policy issuer itself.

4. On signature policy data structure. Although not normative, we have a number of reasons that signature policy specified in [ESF] has to be examined closely. The primary one being its position with respect to other policy assertions mentioned above (cf. item 2), we feel that [ESF] signature policy format has to address either possible interoperability with or definitive differentiation from these other standards. Here are a couple of fragmental comments:

    a) On Rules. The terminology employed, "Common Rules" ([ESF; 11.3]) and "Commitment Rules" ([ESF; 11.4]), seems to be rather awkward especially when compared with other standards. It is suspected that this was intentionally chosen with some specific application in mind, but we could not have identified the relevant passages in the specification.

    b) On Extensions. In practice, we believe that heavy usage of SignPolExtensions ([ESF; 11.11]) are expected to be inevitable, for example in embedding signatures or other validation data for further protection depending on the circumstances (see item 3). We feel that it would be a good idea to specify what instances of extensions should be expected as rendered in RFC 3280.

5. On interoperability with XACML. It is often expected that XACML will fill in the gap where it is currently lacking the means to proffer semantic information for establishing secure transactions. It is to this extent that we feel policy framework of XACML should be taken into account in configuring the application domain of signature policy, regardless of whether transaction of the latter takes place through application layer protocols or not.

References

[ESF] ETSI TS 101 733: "Electronic Signature Formats".

[RFC3280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[SAMLCore]	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML).
[XACML]	OASIS extensible Access Control Markup Language (XACML).
[XAdES]	ETSI TS 101 903: "XML Advance Electronic Signatures (XAdES)".
[WS-Policy]	Web Services Policy Framework (WS-Policy).

A.3.2.2 Comment #1, pages 49, 67 and 76

Comment

"OPTIONAL" should be described after `[2] OtherRevVals` marked `****`.

```
RevocationValues ::= SEQUENCE {
crlVals         [0] SEQUENCE OF CertificateList OPTIONAL
ocspVals        [1] SEQUENCE OF BasicOCSPResponse OPTIONAL
otherRevVals    [2] OtherRevVals  ****
}
```

Resolution

This problem was fixed in the version 1.4.0.

A.3.2.3 Comment #2, pages 16 and 17

Comment

Timestamp seem unnecessary in ES-X Type1 and ES-X Type2, since ES-X-L is enough.

These two should be deleted to avoid being complicacy of specifications.

A.3.2.4 Comment #3, clause 8.9.1

Comment

Signature policy is made mandatory in the specification, while it is felt necessary to specify a mechanism that allows dynamic policy referencing, which is presently lacking.

At the same time, it is preferable that there is a method to link policy inside signature and that outside signature data.

A.3.2.5 Comment #4, clause 11.1

Comment

As a part of the policy source protection, we feel it is necessary to consider signature of the signature policy itself, not just its hash value.

A.3.2.6 Comment #5, clause 11.11

Comment

As the use case demand for the signature policy extension is deemed to increase, it would be nice to have a concrete specification of extension instances as has been done in X.509 certificate profile standard (RFC 3280).

A.3.2.7 Comment #6, clause 5.4.2

Comment

"**CRI Information**" may be a spelling mistake for "**CRL Information**".

Resolution

This problem was fixed in the version 1.4.0.

A.3.2.8 Comment #7, clauses 5.4.5 and 5.4.7

Comment

The same clause title "Timestamping for long life of signature" (This applies also to V1.4.0).

A.3.3 Proposed amendments on TS 101 903

Contribution metadata	
ID contribution	JCPKI-003
Source	Japan and China PKI Forums
Version of the deliverable	1.1.1
Date	17 February 2003

Contribution

See the following clauses.

A.3.3.1 Rationale: "Some comments regarding EESSI Signature Policy"

Same as clause A.3.2.1.

A.3.3.2 Comment #1, page 17

Comment

Timestamp seems unnecessary in XAdES-X, since XadES-X-L is enough.

This should be deleted to avoid being complicacy of specifications.

A.3.3.3 Comment #2

Comment

It makes sense that signature format, which is designed to incorporates signature policy, is defined in terms of XML, when considered that the worldly policy standards, like SAML, XACML, WS-Security, are specified at the same processing layer using XML.

In this sense, it would be preferable (if not normatively, but informatively) for the present standard to investigate its practicable interoperability with these policy related standards.

A.3.3.4 Comment #3

Comment

Relative to TS 101 733 ES Formats, a profile of XML long term signature format was introduced assuming a similar use of CMS SignedData last year.

Relative to Japan e-Government, Electronic applications are specified to be XML based documents and XML signature will be in use. In this case, XadES matches well than ASN.1 based TS 101 733 from the point of view of long term signature save.

To diffuse the use of XadES, test programs for interoperability should be implemented.

Some errors are pointed out in some parts of XadES schema so that bug information should be opened to public promptly.

The manual of XML time-stamping used in the present document should be described soon after OASIS standard formulation.

A.3.4 Proposed amendments on TS 101 861 - Time stamping profile

Contribution metadata	
ID contribution	JCPKI-004
Source	Japan and China PKI Forums
Version of the deliverable	1.2.1
Date	17 February 2003

Contribution

See the following clauses.

A.3.4.1 Comment #1, clause 5.1.2

Comment

Please add "One of " to the beginning of the sentence, because the sentence uses "must".

A.3.4.2 Comment #2, clause 5.2.3

Comment

Please add "One of " to the beginning of the sentence, because the sentence uses "must".

A.3.4.3 Comment #3

Comment

This profile is appropriate for common use of time stamp.

A.3.5 Comments and proposed amendments on TS 102 023

Contribution metadata	
ID contribution	JCPKI-005
Source	Japan and China PKI Forums
Version of the deliverable	
Date	17 February 2003

Contribution

See the following clauses.

A.3.5.1 Comment #1, clause 4.2

Comment

It should be clearly defined the TSA's key.

Because readers cannot distinguish if it is TSA's key or TSU's key.

A.3.5.2 Comment #2, clause 4.2

Comment

We propose to describe a restriction on key backup.

E.g. "TSA's key should not be cloned"

A.3.5.3 Comment #3, clause 7.1.2 d)

Comment

Readers easily understand "The expiration date of the time-stamp token, TSA assured,"

A.3.5.4 Comment #4, clause 7.1.2 j)

Comment

"See clause 7.4.10" is wrong. "See clause 7.4.11" is right.

A.3.5.5 Comment #5, clause 7.2.1 b)

Comment

FIPS PUB 140-2 is also required.

A.3.5.6 Comment #6, clause 7.2.2 a)

Comment

FIPS PUB 140-2 is also required.

A.3.5.7 Comment #7, clause 7.2.2 b)

Comment

Following note is needed.

NOTE: When the backup key is recovered, the TSA needs to assure that it does not use previously used serial numbers in the TSTs for new TSTs.

A.3.5.8 Comment #8, clause 7.2.4

Comment

NOTE 1: "See clause 7.4.10" is wrong. "See clause 7.4.11" is right.

A.3.5.9 Comment #9, clause 7.3.1 e)

Comment

Following measure is needed.

If the TSA's clock has been out of the stated accuracy and TSTs were issued before it was detected, the TSA shall revoke the TSTs.

A.3.5.10 Comment #10, clause 7.3.2 a)

Comment

The TSA also needs to show to users how it can prove its clock's correctness.

For instance, The TSA shall keep and show tractability and authenticity to UTC as its time source to users.

An investigation of guideline is required.

A.3.5.11 Comment #11, clause 7.3.2 d)

Comment

We believe that "the TSA should not issue time-stamps when it is processing for a leap second".

Some investigation of guideline is required.

A.3.5.12 Comment #12, clause 7.4.8

Comment

- It should be provided a way of how to deal with issued TSTs in the following cases.

    1. Compromise of the TSA's signing key.

    2. Detected loss of calibration.

A.3.5.13 Comment #13, clause 7.4.8 c)

Comment

There will be possibility that TST is issued after compromise occurred and it cannot be detected for a while.

So we believe that when such cases happened the TSA need to show information of it to relying parties and subscribers. (E.g. by time-stamps revocation list.)

Some investigation of guideline is required.

A.3.5.14 Comment #14

Comment

Referring to TS 102 023, as examples of a specific TSA policy, two operation regulations were created in FY2002 report, "Time-stamping usage guideline".

1. Example of time-stamping service operation regulation using simple protocol.

2. Example of time-stamping service operation regulation using linking protocol.

Also in "Time-stamping usage guideline", the important matters on use of time-stamping were summarized. Here we discussed about "Time Authentication" which is not specifically described in TS 102 023. A time-stamp token issued by TSA should have the correct time but the token does not have a mechanism to prove that the token itself uses a reliable time source to guarantee the time accuracy. The time included in time-stamp token that TSA insist the accuracy should link to the national standard time based UTC and there should be a mechanism to guarantee the accuracy.

A.3.6 Comments and proposed amendments on TR 102 038

Contribution metadata	
ID contribution	JCPKI-006
Source	Japan and China PKI Forums
Version of the deliverable	1.1.1
Date	17 February 2003

Contribution

See the following clauses.

A.3.6.1 Comment #1

Comment

To describe about OCSP trust condition, both in CommonRules and CommitmentRules element schema, add following element

```
<xsd:element name="OCSPTrustCondition"
 type="OCSPTrustConditionType" minOccurs="0"/>
```

This addition should apply on signature policy clause of TS 101 733 in same syntax.

A.3.7 Comments and proposed amendments on TR 102 041

Contribution metadata	
ID contribution	JCPKI-007
Source	Japan and China PKI Forums
Version of the deliverable	1.2.1
Date	17 February 2003

Contribution

See the following clauses.

A.3.7.1 Comment #1, clause 8.3.1 - Signature validation policy

Comment

In this clause, the Reports describe two types of commitments, which are Common Rules and Commitment Rules.

However, meaning difference between these rules are little bit understandable. It is helpful for us if you explain some example of these Rules, especially commitment rules.

Also in this clause, description "trust conditions for user certificate, timestamps and attributes" should be added OCSP responder's trust conditions. This addition should apply on signature policy clause of TS 101 733 in same syntax.

A.3.7.2 Comment #2, clause 8.3.2 - Signature validation information

Comment

Revocation Requirements.

Please add CRL Distribution points not only full CRLs.

A.4 Comments and proposed amendments from a TC-ESI member

A.4.1 Proposed amendments on TS 101 456 - Qualified certificate policy

Contribution metadata	
ID contribution	TC-ESI_3-001
Source	TC-ESI member
Version of the deliverable	1.2.1
Date	

Contribution

See the following clauses.

A.4.1.1 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 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 and TS 102 042 (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.

Proposed Resolution

To be resolved.

A.4.2 Proposed amendments on TS 102 042 - Normalized certificate policy

Contribution metadata	
ID contribution	TC-ESI_3-002
Source	TC-ESI member
Version of the deliverable	1.1.1
Date	

Contribution

See the following clauses.

A.4.2.1 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 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 and TS 102 042 (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.

Proposed Resolution

To be resolved.

A.5 Comments and proposed amendments from Pink Roccade (Netherlands)

A.5.1 Proposed amendments on TS 101 456 - Qualified certificate policy

Contribution metadata	
ID contribution	PR-001
Source	PinkRoccade (Netherlands)
Version of the deliverable	1.2.1
Date	

Contribution

I will give some comments on a high abstraction level:

- For a CSP issuing qualified certificates TS 101 456 is the leading document. It has become a part of our voluntary certification schema and it is more or less copied into or (draft-)law on electronic signatures. Now I know CEN is not responsible for the TS 101 456 document but still I will give you this comments:
  - TS 101 456 is a set of requirements used by CSP's (technicians, quality managers and internal auditors) to build the CSP-organization and it is used by auditors to audit the CSP-organization. For the purpose it is used for TS 101 456 is too much written by technicians and too less by quality managers and auditors. It is not an easy document to handle.
  - TS 101 456 contains a lot of redundancy.
- In your workshop agreements CEN has written: "This CEN Workshop Agreement can in no way be held as being an official standard as developed by CEN National Members". Nonetheless CWA 14169 Secure Signature Creation Devices has become a part of the Dutch (draft) law on electronic signatures. Can you give me some comments on this matter?
- In our guidance on TS 101 456 we refer on the document CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. The problem with CWA 14167-1 however is that it not only specifies requirements on a TWS but it specifies also a lot of requirements on a CSP. In this way CWA 14167-1 doubles with TS 101 456. The scope of CWA 14167-1 is too wide?

A.6 Comments and proposed amendments from EESSI evaluation

A.6.1 Suggested amendments on TS 101 456 - Qualified certificate policy (see EESSI #21(2002)04 - clause 6)

Contribution metadata	
ID contribution	EESSI-001
Source	EESSI Evaluation
Version of the deliverable	1.2.1
Date	

Contribution

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.

A.6.2 Suggested amendments on TS 101 862 - Qualified certificates profile (see EESSI #21(2002)04 - clause 6)

Contribution metadata	
ID contribution	EESSI-002
Source	EESSI Evaluation
Version of the deliverable	1.2.1
Date	

Contribution

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.

A.7 Comments and proposed amendments from CEN/ISSS WS/E-Sign Area M and ETSI STF-210 maintenance groups

A.7.1 Proposed amendments on TS 102 023 - Time-stamping policy

Contribution metadata	
ID contribution	MAINT-001
Source	CEN/ISSS WS/E-Sign Area M and ETSI STF-210 maintenance groups
Version of the deliverable	1.2.1
Date	

Contribution

See the following clauses.

Amendments related to the paper "Terminology for EESSI documents". TS 101 733 should be consistent with RFC 3161 and use the "time-stamp token" within a description and "TimeStampToken" for formal definitions (i.e. ASN.1 and XML). The TSA policy should also be consistent.

A.8 Other comments and proposed amendments

A.8.1 Proposed amendments on TS 101 456 - Qualified certificate policy

A.8.1.1 Advise on use of SSCD

Contribution metadata	
ID contribution	OTHER-001
Source	Other
Version of the deliverable	1.2.1
Date	

Contribution: comment

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

Contribution: 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."

A.8.1.2 Use of CA key for multiple policies

Contribution metadata	
ID contribution	OTHER-002
Source	Other
Version of the deliverable	1.2.1
Date	

Contribution: 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 necessarily compromise security. Probably we could advice CSPs to use dedicated keys (use should instead of shall), but not make that as a requirement.

Contribution: 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.

A.8.1.3 Reference to CWA 14167-1 in clause 7.4.7

Contribution metadata	
ID contribution	OTHER-003
Source	Other
Version of the deliverable	1.2.1
Date	

Contribution

Update clause 7.4.7, note 1 to explicitly reference CWA 14167-1 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)".

A.8.1.4 When a new policy OID is required

Contribution metadata	
ID contribution	OTHER-004
Source	Other
Version of the deliverable	1.2.1
Date	

Contribution: comment

It is currently not clear when a new certification policy is necessary.

Contribution: proposed resolution

Add to clause 8.

No changes should be made to a certificate policy which could affect a relying party's consideration on the reliability of the certificate issued by the CA.

A.8.2 Proposed amendments on TS 102 042 - Normalized certificate policy

A.8.2.1 Advise on use of SSCD

Contribution metadata	
ID contribution	OTHER-005
Source	Other
Version of the deliverable	1.1.1
Date	

Contribution: comment

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

Contribution: 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."

A.8.2.2 Use of CA key for multiple policies

Contribution metadata	
ID contribution	OTHER-006
Source	Other
Version of the deliverable	1.1.1
Date	

Contribution: 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 necessarily compromise security. Probably we could advice CSPs to use dedicated keys (use should instead of shall), but not make that as a requirement.

Contribution: 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.

A.8.2.3 Reference to CWA 14167-1 in clause 7.4.7

Contribution metadata	
ID contribution	OTHER-007
Source	Other
Version of the deliverable	1.1.1
Date	

Contribution

Update clause 7.4.7, note 1 to explicitly reference CWA 14167-1 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)".

A.8.2.4 When A new Policy OID is required

Contribution metadata	
ID contribution	OTHER-008
Source	Other
Version of the deliverable	1.1.1
Date	

Contribution: comment

It is currently not clear when a new certification policy is necessary.

Contribution: proposed resolution

Add to clause 8.

No changes should be made to a certificate policy which could affect a relying party's consideration on the reliability of the certificate issued by the CA.

A.8.3 Proposed amendments on TS 101 733 - Electronic signature formats

A.8.3.1 Archive timestamp

Contribution metadata	
ID contribution	OTHER-008
Source	Other
Version of the deliverable	1.4.1
Date	

Contribution

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.

A.8.4 Proposed amendments on TS 101 861 - Time stamping profile

A.8.4.1 Clause 5.2.1 - Accuracy and precision of time

Contribution metadata	
ID contribution	OTHER-010
Source	Other
Version of the deliverable	1.2.1
Date	

Contribution: comment

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 s is not allowed.

Contribution: proposed resolution

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."

A.8.4.2 Clause 5.2.1 - Ordering

Contribution metadata	
ID contribution	OTHER-011
Source	Other
Version of the deliverable	1.2.1
Date	

Contribution: comment

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.

Contribution: proposed resolution

Delete item.

A.8.4.3 Clause 6 mandate support for store and forward

Contribution metadata	
ID contribution	OTHER-012
Source	Other
Version of the deliverable	1.2.1
Date	

Contribution: comment

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.

Contribution: proposed resolution

Update as indicated:

One on-line protocol must be supported for every Time Stamping Authority (TSA).

A.8.4.4 Clause 7.1.1

Contribution metadata	
ID contribution	OTHER-013
Source	Other
Version of the deliverable	1.2.1
Date	

Contribution: comment

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.

Contribution: proposed resolution

Update as indicated:

"The AlgorithmIdentifier parameters field is optional.

Implementations should accept SHA-1 AlgorithmIdentifiers with absent parameters.

A.8.5 Proposed amendments on TS 101 862 - Qualified certificates profile

A.8.5.1 Country Name

Contribution metadata	
ID contribution	OTHER-014
Source	Other
Version of the deliverable	1.2.1
Date	

Contribution

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 [12]. (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.

A.9 Comments and proposed amendments from a TC-ESI member

A.9.1 Proposed amendments on TS 101 862 and related discussion threads

Contribution metadata	
ID contribution	TC-ESI_2-001
Source	TC-ESI member
Version of the deliverable	1.2.1
Date	11 June 2003

Contribution

To the maintenance team of TS 101 862.

TS 101 456 defines:

a) QCP public + SSCD: itu-t(0) identified-organization(4) etsi(0)
qualified-certificate-policies(1456)
policy-identifiers(1) qcp-public-with-sscd (1).

A certificate policy for qualified certificates issued to the public,
requiring use of secure signature-creation devices

b) QCP public: itu-t(0) identified-organization(4) etsi(0)
qualified-certificate-policies(1456)
policy-identifiers(1) qcp-public (2)

A certificate policy for qualified certificates issued to the public.

TS 101 862 defines id-etsi-qcs-QcCompliance:

An Identifier of the statement (represented by an OID), stating that the certificate is issued according to the EU-Directive [1], as implemented in the country under which law the issuer is operating.

```
esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED
BY id-etsi-qcs-QcCompliance }
--  This statement is a statement by the issuer that this
--  certificate is issued as a Qualified certificate according
--  Annex I and II of the Directive 1999/93/EC of the European Parliament
--  and of the Council of 13 December 1999 on a Community framework
--  for electronic signatures, as implemented in the law of the country
--  specified in the issuer field of this certificate.
```

```
id-etsi-qcs-QcCompliance      OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
```

TS 101 862 does not permit to make the same distinction as TS 101 456.
In particular if a verifier wants to make sure that the signature is a
Qualified Signature, it must be known that an SSCD has been be used.
This can currently only be checked when the following CP OID is being used:

itu-t(0) identified-organization(4) etsi(0)
qualified-certificate-policies(1456)
policy-identifiers(1) qcp-public-with-sscd (1)

but not when simply using a QCstatement extension.

It is thus requested to define an additional QCstatement equivalent to the "QCP public + SSCD" CP.

The big advantage would be that the CP under which the certificate is being issued may be kept, while simply adding a QCstatement to mean "QCP public + SSCD".

NOTE: The rest of the mail exchange have been removed for privacy.

A.9.2 Proposed amendments on TS 102 023 and related discussion threads

Contribution metadata	
ID contribution	TC-ESI_2-002
Source	TC-ESI member
Version of the deliverable	1.2.1
Date	13 June 2003

Contribution

To the maintenance team of TS 102 023.

In clause 7.2.3. we currently only have:

7.3.2 Clock Synchronization with UTC

b) The TSA clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration.

Let us consider two scenarios:

Scenario A.

The clock reference is outside the HSM. It is for example a PCI card placed in a PC with a crystal clock compensated in temperature and synchronized manually every week with UTC by an operator. The operator is able to set any time when performing the synchronization. Someone having an access to the room and knowing some ID and password could set any time.

This scenario relies on the security of the environment and on the respect of procedures.

Scenario B.

The clock reference is within a HSM (Tamper Resistant - Hardware Security Module), this means that both the clock and the TSU signing key are within the same HSM. The clock is based upon a crystal clock compensated in temperature and synchronized every week with UTC. Every week a compensation of only XX microseconds (e.g. 100 microseconds) is allowed. If more is being done, the private key will be zeroized and a new full installation must be done. Someone having an access to the room and knowing *everything* cannot do more that a clock drift of XX microseconds.

This scenario only relies on the security features of the HSM.

Conclusion

I see the need for two different qualities for the protection whether:

1) the security is achieved both by room access control and by procedures to be respected by human-beings, or

2) the security is achieved by security features built-in inside the HSM.

This should lead to define two different TSA policies, ... unless we mandate the later only.

NOTE: The rest of the mail exchange have been removed for privacy.

A.10 Comments and proposed amendments from ETSI STF-220 - Task 4

A.10.1 TS 101 456 - Qualified certificate policy

Contribution metadata	
ID contribution	STF220_4-001
Source	ETSI STF-220 - Task 4
Version of the deliverable	1.2.1
Date	8 September 2003

Contribution

See the following clauses.

A.10.1.1 Proposed amendments related to section "Introduction"

Please add the following text after the first paragraph.

Another important requirement of electronic commerce is the ability to identify, not only the originator of electronic information in the same way that documents are signed using a hand-written signature, but also their attribute(s), e.g. their role(s) in an organization.

This may be achieved using certification services in two ways:

- using attributes included in Public Key Certificates (PKCs);
- using attributes included in Attribute Certificates (ACs).

The former case is covered in the present document. See TS 102 158 for the latter case.

Please change the following paragraph as subsequently specified.

The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [1] (hereinafter referred to as "the Directive") identifies a special form of electronic signature which is based on a "qualified certificate". Annex I of this Directive 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).

The mentioned Directive also covers the use of attributes in public key certificates, since it mentions the possibility to include attributes in Public Key Certificates (PKCs) (see Annex I, clause d) which refers to the "provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended".

The present document specifies baseline policy requirements on the operation and management practices of certification authorities issuing qualified certificates in accordance with the Directive. The use of a secure-signature-creation device, as required through annex III of the Directive, is an optional element of the policy requirements specified in the present document."

A.10.1.2 Proposed amendments related to clause 2 "Reference"

Please add to the list:

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. ← a reference to this is asked to be added in clause 4.3.4

A.10.1.3 Proposed amendments related to clause 3.1 "Definitions"

Please add the following definitions.

attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity.

Attribute Granting Authority (AGA): authoritative source of an attribute

role: function, position or status that somebody has in an organization, in society or in a relationship.

A.10.1.4 Proposed amendments related to clause 4.1"Certification authority"

Typo ➔ Please change reference to clause 4.1 into reference to clause 4.2.

Please add the following paragraphs at the end.

When a signer signs a document it is of primary importance to be able to identify such signatory in the interest of accountability. This enables the transaction to be traceable. However, in many cases, in order to accept a signature, the acceptance criteria may not necessarily be based on the identity of the signer but instead, or additionally, on the qualification(s) of the signer. Qualifications in this context have the meaning of specific features or attributes that the signatory might possess in order to perform a certain act.

Such a qualification may be obtained using attributes within PKCs included or referenced in electronic signatures.

A.10.1.5 Proposed amendments related to clause 4.3.4 "Other CA Statements"

Please modify the first paragraph as follows.

In addition to the policy and practice statements a CA may issue terms and conditions of general commercial purpose. They must follow the requirements of general conditions and comply with the requirements set out in Directive 93/13/EEC 🡐 add reference ➔ as implemented in the national legislation of the member states. In specific, general conditions are non-negotiable and binding to a non-determined number of end users. They have, however, to be brought to the attention of contracting counter parties and especially to consumers. Terms and conditions will only be effective against relying parties, who have no other contractual arrangement with the CA if:

- they are easily accessible; and
- their existence together with information as to how they can be accessed is brought to their attention in a conspicuous manner; and
- they remain in line with the member state law regarding general conditions.

A.10.1.6 Proposed clause to be added: 4.5 "Certified attributes"

Before being granted, attributes shall be verified in a way that the certification authority is satisfied as to their authenticity. It shall be verified that, at the time of registration for an attribute, the individual was entitled to claim that attribute.

The Certification Authority is responsible for verifying the correct attribution of attributes to subjects (see also clause 6.4 Liability).

A.10.1.7 Proposed clause to be added: 4.6 "Attribute semantics"

The semantics of an attribute may be either defined in a standard (e.g. by ISO) or defined by any organization.

When the attribute is defined in a standard, it may be used in an open community.

NOTE: It may be specified using an OID that has a global international definition. This is in this way that X.509 has defined a set of standard attributes. When it is locally defined by any organization, two approaches are possible:

- use an OID located under the OID of the organization,
- define the OID of the "issuing authority" (e.g. as called in ISO/TS 17090-2, see Bibliography) and add a definition of the attribute in any syntax (e.g. character string, XML).

When the attribute is locally defined by an organization, its use may be restricted to a close community. The semantics of the attribute has then to be interpreted using the identifier of the attribute granting authority (also called sometimes "issuing authority") in combination with the definition of the attribute by that authority.

A.10.1.8 Proposed clause to be added: 6.3 "Subject obligations" (subsequent clauses must be renumbered accordingly)

The CA shall oblige, through agreement, the subscriber to agree with the subject that the subject is bound to:

- use the PKC solely for the usage specified in the CPS;
- notify the subscriber without any unreasonable delay, when there is an inaccuracy in the content of an PKC, whatever the reason may be, including a change in the ownership of an attribute.

A.10.1.9 Proposed amendments related to clause 7.3.1 "Subject initial registration"

Registration

In particular:

Please replace:

c) The service provider shall verify by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation.

with:

d) The service provider shall verify, at the time of registration, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation.

Please add:

l) The CA shall verify that, at the time of registration of an attribute to be included in a certificate, the individual was entitled to that attribute. That verification shall be done by appropriate means and in accordance with national law.

m) The CA shall record all information used to verify the attributes of the subject.

n) The CA shall ensure that the subject consents to include attributes in the PKC.

o) The CA shall record the information demonstrating that a subject has accepted to have attributes within PKCs.

A.10.1.10 Proposed amendments related to clause 7.3.2 "Certificate renewal, rekey and update"

Please add the following clause

Attribute Registration:

a) The CA shall check by appropriate means that the subject is entitled to the attributes requested to be certified.

b) The CA shall record all information used to verify the subjects' rights to exert the attributes to be registered (see item c), including any reference number on the documentation used for verification, and any limitations on its validity.

c) The CA shall verify by appropriate means in accordance with national law, the attributes of the person.

d) The CA shall record the signed agreement with the subscriber including:

- whether, and under what conditions, the subscriber requires the subject's consents to the inclusion in PKCs of the attributes that have been registered;
- confirmation that the information registered is correct.

NOTE 1: Other parties (e.g. the associated person or legal entity) may be involved in establishing this agreement.

NOTE 2: This agreement may be in electronic form, providing all involved parties consent.

A.10.1.11 Proposed amendments related to clause 7.3.4 "Dissemination of Terms and Conditions"

Please add the following requirements to item a)

- a clear description of the meaning of each type of attribute that is supported. That description shall be given in readily-understandable terms, and, if appropriate, the law or regulation that defines or assigns the attribute shall be indicated;
- the list of documents the subject must exhibit to prove his/her right to register an attribute and the procedures used by the CA for the verification of such right;
- how each attribute will be represented in the PKC (e.g. a character string and/or an OID);
- any limitations on their use;
- the subscriber's and subject's obligations as defined in clauses 6.2 and 6.3.

A.10.1.12 Proposed amendments related to "Annex E (informative): Bibliography"

Please add the following references:

ISO/TS 17090-1: "Health informatics - Public Key infrastructure. Part 1: Framework and overview".

ISO/TS 17090-2: "Health informatics - Public Key infrastructure. Part 2: Certificate profile".

ISO/TS 17090-3: "Health informatics - Public Key infrastructure. Part3: Policy Management of certification authority".

A.11 Proposed amendments from ETSI STF-220 Task 2

A.11.1 TS 101 456 - Qualified certificate policy

Contribution metadata	
ID contribution	STF220_2-001
Source	ETSI STF-220 –Task 2
Version of the deliverable	1.2.1
Date	15 May 2003

Contribution

A comparison has been carried between the Federal PKI and the ETSI Qualified Certificate Policy (TS 101 456 - QCP), initially put together by a US contractor directed by Federal PKI with subsequent input from members of the ETSI ESI TC.

Whilst the resulting conclusion is that the policies are broadly in line, the document identifies a number of areas as "missing" in the ETSI QCP. A significant number of these are issues relating to auditing the conformance of the CA to the policy and practices. It is suggested that this can be covered by reference to the CWA 14167-2 or a comparable national "voluntary accreditation" scheme. There are also other areas which are covered by other EESSI specifications (TS 101 862 and CWA 14168 / 14169).

A number of other missing items have been found to be comparable in the view of an ETSI expert.

There remain the following requirements from FPKI which have been identified as "missing" or partially covered in the QCP that are brought to the attention of the ETSI ESI TC for consideration in future updates to TS 101 456.

- Information about a revoked certificate shall remain in the status information until the certificate expires. (table 65)
- US feels all CA's should issue CRLs regardless of any other validation capability employed. (table 67)
- The issuance frequency for CRLs and CARLs shall be at least once each day; CRL and CARL issuance for reason of loss or compromise of private key shall take place within 18 hours of notification. (table 70)
- Audit logs shall be reviewed at least once every two months. A statistically significant set of security audit data generated by Agency CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity (table 78). Actions taken as a result of these reviews shall be documented. (table 79)
- Audit processes shall be invoked at system startup, and cease only at system shutdown. (table 88). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the Agency authority shall determine whether to suspend Agency CA operation until the problem is remedied. (table 89)
- Routine self-assessments of security controls shall be performed by the entity operating the CA. (table 90)
- Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS. (Table 121). Backups are to be performed and stored off-site not less than once per week. (Table 122). At least one full backup copy shall be stored at an offsite location (separate from the Agency CA equipment). (Table 123). The backup shall be stored at a site with physical and procedural controls commensurate to that of the Agency CA. (table 124)
- The Agency CA Policy Authority shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the Agency CA or its repository not authorized in this CP, the CPS, or other procedures published by the Agency Operational Authority. (table 133)

Documentation shall be maintained identifying all personnel who received training and the level of training completed. (table 136).

A.12 Proposed amendments from XadES-PLUGTESTS™

A.12.1 Proposed amendments on TS 101 903

Contribution metadata	
ID contribution	XAdES-PT-001
Source	XAdES-Plugtest
Version of the deliverable	1.1.1
Date	25 January 2004

Contribution

In the preparation of the XAdES-PLUGTESTS™ event some issues of the XAdES specification were brought up by different implementers. These issues were discussed during the interoperability event and have been incorporated into a document giving proposals for the maintenance process of the XAdES specification.

In the following sections the different issues are discussed in detail.

A.12.1.1 Issue #1 – <EncapsulatedOCSPValues>

Problem Description

In the clause 7.6.2 of the XAdES specification [1] it says:

> *OCSP Responses (`OCSPValues`) consist of a sequence of at least one OCSP Response. The* `<EncapsulatedOCSPValue>` *element contains the base64 encoding of a DER-encoded OCSP Response.* [1, clause 7.6.2]

During the XAdES-PLUGTESTST it turned out that this section has been interpreted differently by the participating implementers in terms of what the actual content of the `<EncapsulatedOCSPValue>` has to bee. Some implementers included the whole `OCSPResponse` others have just included the `BasicOCSPResponse` (contained in the `ResponseBytes` of the `OCSPResponse` as defined in RFC2560 [21]). Therefore, the specification should be more explicit about what to include into the `<EncapsulatedOCSPValue>` element.

Resolution Proposal

Since the additional information that is provided by the `OCSPResponse` is not needed to be archived, it was first suggested to include the `BasicOCSPResponse`. The different possibilities are:

- `OCSPResponse`: On the one hand, the additional information provided by the `OCSPResponse`—an integer value indicating if the request was successful—is not needed to be archived, however, this is how the actual version of the specification is to be interpreted most likely. On the other hand, the information provided by the `<OCSPReferences>` element reflects the content of the `BasicOCSPResponse`. Therefore, any other OCSP response type than the `BasicOCSPResponse` has to be referenced by a `<OtherRef>` element, most likely.Thus, an OCSP response containing a different response type will have to be included into a `<OtherValue>` element.

- `ResponseBytes`: The `ResponseBytes` are already in DER-encoded format. They include an additional object identifier indicating the type of the included OCSP response. The Response Bytes may again contain OCSP responses of different types. Therefore, the same arguments apply, as for the `OCSPResponse` stated in the paragraph above.

- `BasicOCSPResponse`: The `BasicOCSPResponse` contains exactly the data that needs to be archived and corresponds to the information provided by the `<OCSPRef>` element.

At the interop the participants agrred to use `OCSPResponse`, since this is basically what the standards said, and furthermore the only deployed implementation in Estonia uses that interpretation.

A.12.1.2 Issue #2 – <TimeStampType> Data Type

This problem was identified by most implementers throughout the implementation process and already discussed in advance of the XAdES-PLUGTESTS™ event.

Problem Description

The specification of the <TimeStampType> data type is broken in two ways:

1. While it is easy to verify the time-stamp by processing all <HashDataInfo> elements and comparing the resulting hash value to the hash value stored in the time-stamp, it is difficult, time-consuming and possibly even infeasible in the general case to verify, if the time-stamp is applied exactly on the data that is claimed by the XAdES specification. That is, to verify if the time-stamp is applied on the elements that are claimed to be time-stamped.
2. For the <AllDataObjectsTimeStamp>, <IndividualDataObjectsTimeStamp> and the <ArchiveTimeStamp> <HashDataInfo> elements have to be composed that resolve to exactly the same data as the corresponding <ds:Reference>s in the <ds:SignedInfo> do. In the general case it is difficult or probably infeasible to compose such a reference, because the result of resolving depends on the context (e.g. the node it is contained in).

Remarks

The input for the different time-stamps used in the current XAdES version is formed by means of <HashDataInfo> elements. These <HashDataInfo> elements have to be processed according to the reference processing model specified in the XMLDSig specificaion [3]. This is, in short, resolving the provided URI in the URI-attribute of the <HashDataInfo> element, applying the transforms that are specified by the optional <Transforms> child element of the <HashDataInfo> element and finally canonicalizing the result, if the output of the last transform (or the result of resolving the URI, if there is no transform at all) is a node list. This means that the result of processing one <HashDataInfo> element is octet data in any case. The resulting octets of all the included <HashDataInfo> elements are then concatenated in the order the <HashDataInfos> appear in the document to form the input for the time-stamp. These resulting octets are in fact the information that is time-stamped.

The current version of XAdES specification therefore mandates what the result of processing an <HashDataInfo> elements has to be. In the definition of the <SignatureTimeStamp> property it says for instance:

> *The* <SignatureTimeStamp> *element contains a single* <HashDataInfo> *element that refers to the* <ds:SignatureValue> *element of the XMLDSig signature. That is, the input for the time-stamp hash computation is the* <ds:SignatureValue> *XML element. [1, clause 7.3.1]*

A verifying application has to make sure that the time-stamp has been applied on the proper input data. This is, to verify somehow that processing the <HashDataInfo> element results in the data that is claimed by the XAdES specification. In case of the <SignatureTimeStamp> for instance, this is the <ds:SignatureValue> element. Thus, the verifying application has to check that the octets that are being time-stamped are a valid representation of the <ds:SignatureValue> element.

As an URI and an arbitrary number of transforms can be used to compose such a <HashDataInfo> element, it is infeasible to deduce from the specified URI and the given transforms to the result, in the general case. Thus, the only way to verify what has been time-stamped is to process the <HashDataInfo> element and analyze the result.

As one XML structure can have any number of different octet data representations that bear the same information, canonicalization has been introduced. Thus, the only practical way to verify the timestamp input is to compare the canonicalized form of the data that has to be time-stamped according To the specification with the data that results from processing the corresponding <HashDataInfo> element. In this case it would be sufficient to simply create the required input for the time-stamp, compute the digest value and compare it with the digest value in the time-stamp. However, the <HashDataInfo> element was introduced to identify the input of a given time-stamp in cases where the input is ambiguous. But it does not serve this purpose anyway, as has been shown above

Therefore, a new solution has to be found to identify the input-data of a given time-stamp in cases were this input cannot be unambiguously defined by the XAdES specification.

Resolution Proposal

During the interoperability event the following resolution proposal was discussed and agreed on:

The `<TimeStampType>` data type should be redefined to use an ID-list to identify the elements that have been time-stamped. An optional `<ds:CanonicalizationMethod>` element should indicate which canonicalization method to use for canonicalizing XML elements. If no canonicalization method is specified the standard canonicalization method as specified by the actual XMLDSig specification MUST be used.

In the case of included `<ds:Reference>` elements an additional referencedData-attribute indicates if the `<ds:Reference>` element itself or the data resulting from processing the `<ds:Reference>` should be included. If the referencedData-attribute is omitted or the attribute value is false the element identified by the included URI is included. If the referencedDataattribute value is true the `<ds:Reference>` has to be processed according to the reference processing model of the XMLDSig specification. The result is then used as input for the time-stamp. The result of the processing must be exactly the same data as that was used in the computation of the `<ds:Reference>` digest value.

```
<xsd:element name="TimeStamp" type="TimeStampType"/>
<xsd:complexType name="TimeStampType">
    <xsd:sequence>
        <xsd:element name="Include" type="IncludeType" maxOccurs="unbounded"/>
        <xsd:element ref="ds:CanonicalizationMethod" minOccurs="0"/>
        <xsd:choice>
            <xsd:element name="EncapsulatedTimeStamp">
            type="EncapsulatedPKIDataType"/>
            <xsd:element name="XMLTimeStamp" type="AnyType"/>
        </xsd:choice>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="IncludeType">
    <xsd:attribute name="uri" type="xsd:anyURI" use="required"/>
    <xsd:attribute name="referencedData" type="xsd:boolean" use="optional"/>
</xsd:complexType>
```

A.12.1.3 Issue #3 – `<ArchiveTimeStamp>`

Problem Description

The `<ArchiveTimeStamp>` definition is broken in two ways:

1. The `<ArchiveTimeStamp>` includes the `<SignedPropertiesElement>` twice.

2. The references to the `<SignedSignatureProperties>` and the `<SignedDataObjectProperties>` cannot be composed using ID-references, because these elements do not have an xsd:ID-attribute.

In clause 7.7.1 of the XAdES specification [1] it says:

> *The XAdES `<ArchiveTimeStamp>` element contains the following sequence of Hash-DataInfo elements:*
>
> - *One `<HashDataInfo>` element for each data object signed by the XMLDSIG signature The result of application of the transforms specified each `<HashDataInfo>` must be exactly the same as the octet stream that was originally used for computing the digest value of the corresponding `<ds:Reference>`.*
> - *One `<HashDataInfo>` element for the `<ds:SignedInfo>` element. The result of application of the transforms specified in this `<HashDataInfo>` must be exactly the same as the octet stream that was originally used for computing the signature value of the XMLDSIG signature.*
> - *One `<HashDataInfo>` element for the `<SignedSignatureProperties>` element.*
> - *One `<HashDataInfo>` element for the `<SignedDataObjectProperties>` element.*
> - *…*

In the first paragraph it says to include a `<HashDataInfo>` element for each `<ds:Reference>` in the XMLDSig signature. This obviously includes the reference to the `<SignedProperties>`. In the third and the fourth paragraph it says to include a `<HashDataInfo>` element for the `<SignedSignatureProperties>` and the `<SignedDataObjectProperties>`. These elements are already included by the reference to the `<SignedProperties>`. Additionally these two elements have no xsd:ID-attribute specified, thus they cannot be referenced using ID-references.

Resolution Proposal

Omit the `<HashDataInfo>` elements for the `<SignedSignatureProperties>` and the `<SignedDataObjectProperties>`. Additionally,

- either add an `<HashDataInfo>` element for the `<SignedProperties>` and omit the `<ds:Reference>` to the `<SignedProperites>`,
- or simply leave the `<ds:Reference>` to the signed properties included.

Add xsd:ID-attributes to the `<SignedSignatureProperties>` and the `<SignedDataObjectProperties>` elements as well as to the `<UnsigendSignatureProperties>` and the `<UnsignedDataObjectProperties>` elements.

A.12.1.4 Issue #4 – Requirement Levels (RFC2119)

Within the current version of the XAdES specification, the word 'must' is used to indicate a requirement at several places and should therefore say 'MUST' according to RFC2119 [22]. The RFC2119 defines how the key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' are to be interpreted in the sense of requirement level. Therefore, the specification should use these key words wherever a requirement is stated.

XAdES specification [1], clause 5, first paragraph:

> *The XML namespace URI that **must** be used by implementations of the present document . . . [1, clause 5]*

XAdES specification [1], clause 6.2, second paragraph:

> *. . . The `<SignedProperties>` **must** be covered by a Reference element of the XML signature. Alignment with the present document mandates that one `<SignedProperties>` element MUST exist. [1, clause 6.2]*

XAdES specification [1], clause 6.3, second paragraph:

> *However, the following restrictions apply for using `<ds:Object>`, `<QualifyingProperties>` and `<QualifyingPropertiesReference>`:*
>
> • . . .
>
> *• All signed properties **must** occur within a single `<QualifyingProperties>` element. This element can either be a child of the `<ds:Object>` element (direct incorporation), or it can be referenced by a `<QualifyingPropertiesReference>` element. See clause 6.3.1 for information how to sign properties.*
>
> • . . .

XAdES specification [1], clause 7.2.5, last paragraph:

> *At least one element of `<Description>`, `<ObjectIdentifier>` and xmlMimeType **must** be present within the property. [1, clause 7.2.5]*

XAdES specification [1], clause 7.2.8, paragraph 8:

> *. . . At least one of the two elements `<ClaimedRoles>` or `<CertifiedRoles>` **must** be present. [1, clause 7.2.8]*

XAdES specification [1], clause 7.7.1, paragraph 10:

> *The* `<XAdESArchiveTimeStamp>` *element contains the following sequence of* `<HashDataInfo>` *elements:*
>
> *• One* `<HashDataInfo>` *element for each data object signed by the XMLDSig signature. The result of application of the transforms specified each* `<HashData Info>` ***must*** *be exactly the same as the octet stream that was originally used for computing the digest value of the corresponding* `<ds:Reference>`*.*
>
> • . . .

A.12.1.5 Issue #5 – <QualityingProperties>

Clause 6.2 of the XAdES specification [1] says: 'The mandatory Target attribute refers to the XML signature.' This should be changed to: 'The mandatory Target-attribute MUST refer to the `<Id>`-attribute of the corresponding `<ds:Signature>`.'

A.12.1.6 Issue #6 – ASN.1 Encoding

For some ASN.1 PKI elements that are included into the XAdES signature the exact ASN.1 encoding mechanism is not specified (clauses 7.1 and 7.2.8 of the XAdES specification [1]). This should be changed to mandate the DER (Distinguished Encoding Rules [12]) encoding mechanism wherever an ASN.1 encoding is required.

A.12.1.7 Issue #7 – Trust Status Lists

The following proposal was made by members of the ETSI Technical Committee ESI (Electronic Signatures and Infrastructures):

> XAdES should probably be able to include Trust Status Lists (TSL [23]), beside certification and revocation information in future versions of the specification.

A.12.1.8 Issue #8 – `<SigningCertificate>`

In XAdES specification [1] clause 7.2.2, last but one paragraph it says:

> *If the signer uses an attribute certificate to associate a role with the electronic signature, such a certificate MUST be present in the* `<SignerRole>` *property. [1, clause 7.2.2]*

This sentence should be moved to clause 7.2.8 'The `<SignerRole>` element' of the XAdES specification.

A.12.1.9 Issue #9 – XAdES forms

The following proposal was made by members of the ETSI Technical Committee ESI (Electronic Signatures and Infrastructures):

> *In future versions of the XAdES it should be possible to have archival versions "references only", "values only" and "mixed".*

Currently, the XAdES specification mandates to include references to the certification and revocation information as well as the actual certification and revocation values in the XAdES-X-L and XAdES-A forms. For the purpose of archiving all information necessary to validate the signature at a later time it would however be sufficient to just include the actual certification and revocation values and omit the references. Therefore the standard should provide forms to include only the necessary information to avoid redundancies.

A.12.1.10 Issue #10 – archival forms

The following proposal was made by members of the ETSI Technical Committee ESI (Electronic Signatures and Infrastructures):

> *It should be possible in future versions of XAdES to have archival versions that build on XMLDSig signatures without the mandatory <*`SignedProperties`*>.*

With the current XAdES versions it is not possible to create valid XAdES-A archival versions out of a plain XMLDSig signature, because the mandatory `<SignedProperties>` cannot be added to the signature later. The XAdES specification should therefore provide forms that permit XAdES-A versions without the currently mandatory `<SigningTime>`, `<SigningCertificate>` and `<SignaturePolicyIdentifier>` properties.

A.12.1.11 Issue #11 – <AnyType> Data Type

In the actual version of the XAdES specification [1] the `<AnyType>` data type is defined as follows:

```
<xsd:complexType name="AnyType" mixed="true">
    <xsd:sequence>
        <xsd:any namespace="##any"/>
    </xsd:sequence>
    <xsd:anyAttribute namespace="##any"/>
</xsd:complexType>
```

This definition does not allow content that has no schema associated. Therefore the definition of the `<AnyType>` data type should read like the following:

```
<xsd:complexType name="AnyType" mixed="true">
    <xsd:sequence>
        <xsd:any namespace="##any" processContents="lax"/>
    </xsd:sequence>
    <xsd:anyAttribute namespace="##any"/>
</xsd:complexType>
```

A.12.1.12 Issue #12 – `<CertID>`

In the current version of the XAdES specification [1] the `<CertID>` element does not have an `URIattribute` for pointing to an archived version of the referenced certificate:

```
<xsd:complexType name="CertIDType">
<xsd:sequence>
<xsd:element name="CertDigest" type="DigestAlgAndValueType"/>
<xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"/>
</xsd:sequence>
</xsd:complexType>
```

Therefore the definition of the `<CertID>` element should read like the following to allow pointing to an archived version of the certificate:

```
<xsd:complexType name="CertIDType">
    <xsd:sequence>
        <xsd:element name="CertDigest" type="DigestAlgAndValueType"/>
        <xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"/>
    </xsd:sequence>
    <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>
```

A.12.1.13 Issue #13 – .NET validating parser

The Microsoft .NET validating XML parser fails to parse the current version of the XAdES schema, although the schema has been validated using the schema validating tools provided by the World Wide Web Consortium (W3C). In order to reach a larger community this issue should be fixed in future versions of the XAdES specification.

A.12.1.14 Issue #14 – XAdES schema

In the actual version of the XAdES schema which is part of the XAdES specification the import statement for the XMLDSig schema is missing. Since elements from the XMLDSig schema are referenced by the XAdES schema an import statement has to be present. Therefore the XAdES schema should read like the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://uri.etsi.org/01903/v1.1.1#"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns="http://uri.etsi.org/01903/v1.1.1#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    elementFormDefault="qualified">

<xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd"/>
```

A.12.1.15 Issue #15 – <QualifyingPropertiesReferenceType> data type

The `<QualifyingPropertiesReferenceType>` data type introduces a new `<Transforms>` element in the XAdES namespace for the `<ds:TransformsType>` rather than using a reference to the element type defined in the XMLDSig schema.

The current XAdES schema definition for the `<QualifyingPropertiesReferenceType>` data type is:

```
<xsd:complexType name="QualifyingPropertiesReferenceType">
    <xsd:sequence>
        <xsd:element name="Transforms" type="ds:TransformsType" minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="URI" type="xsd:anyURI" use="required"/>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

This should be changed to:

```
<xsd:complexType name="QualifyingPropertiesReferenceType">
    <xsd:sequence>
        <xsd:element ref="ds:Transforms" minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="URI" type="xsd:anyURI" use="required"/>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

A.12.1.16 Issue #16 – XAdES examples

The XAdES examples in the (non-normative) annex D of the current version of the XAdES specification [1] are not aligned with the specification. These examples should be fixed, or probably replaced by examples produced as test cases for the XAdES-PLUGTESTS™ event.

A.12.1.17 Issue #17 – `<DataObjectFormat>`

In the XAdES specification [1], clause 7.2.5, second paragraph it says:

> *. . . This (the `<DataObjectFormat>`) is a signed property that qualifies one specific signed data object. In consequence, an XML electronic signature aligned with the present document MAY contain more than one `<DataObjectFormat>` elements, each one qualifying one signed data object. [1, clause 7.2.5, second paragraph]*

However, later in the same clause the specification speaks about signed data object(s), suggesting that one `<DataObjectFormat>` applies for more than one signed data object, which it actually does not:

> *This element can convey:*
>
> - *Textual information related to the signed data object(s) in element `<Description>`;*

- *An identifier indicating the type of the signed data object(s) in element* `<ObjectIdentifier>`*;*
- *An indication of the MIME type of the signed data object(s), in element* `<MimeType>`*;*
- *An indication of the encoding format of the signed data object(s), in element* `<Encoding>`*.*

This should be changed to say 'object' wherever it says 'object(s)'.

Additionally, in XAdES specification [1], clause 7.2.4, fourth paragraph it says:

> *The mandatory ObjectReference attribute refers to the Reference element of the* `<ds:Signature>` *corresponding with the data object qualified by this property. [1, clause 7.2.5, fourth paragraph]*

This should be changed to say

> *The mandatory QbjectReference attribute MUST reference the* `<ds:Reference>` *element of the* `<ds:Signature>` *corresponding with the data object qualified by this property.*

in order to indicate that this is a requirement according to RFC2119 [22].

Additionally, the current version of the XAdES specification mandates the `<DataObjectFormat>` element to be present when the signed data objects have to be presented to the verifier. In the XAdES specification [1] it says:

> *. . . This element (the* `<DataObjectFormat>`*) MUST be present when it is mandatory to present the signed data object to human users on verification. . . .[1, clause 7.2.5, second paragraph]*

The first question is, does it make any sense to mandate the presentation of the signed data objects on verification, at all? Additionally, if it makes sense to mandate the presentation on verification, the data format may be defined implicitly by the application or desired use case, any way.

This issue needs further discussion.

A.12.1.18 Issue #18 – `<CertificateValues>`

Problem Description

On the one side the XAdES specification [1] says in clause 7.6.1, third paragraph:

> *In principle, the* `<CertificateValues>` *element contains the full set of certificates that have been used to validate the electronic signature, including the signer"s certificate. However, it is not necessary to include one of those certificates into this property, if the certificate is already present in the* `<ds:KeyInfo>` *element of the signature. [1, clause 7.6.1]*

On the other side the `<ds:KeyInfo>` element is not covered by the `<ArchiveTimeStamp>`(s). That is, certificates that are present in the `<ds:KeyInfo>` and are not included into the `<Certificatevalues>` are not time-stamped for archiving purposes.

Resolution Proposal

There are two possible solutions to this issue:

- Mandate the inclusion of all certificates in the certificate chain into the `<CertificateValues>` element.
- Mandate to include the `<ds:KeyInfo>` element into the `<ArchiveTimeStamp>`(s).

This issue needs further discussion.

A.12.1.19 Issue #19 – <CompleteCertificateRefs>

In the clause 7.4.1 of the XAdES specification it says:

> *The <`CertRefs`> element contains a sequence of <`Cert`> elements already defined in clause 7.2.2, incorporating the digest of each certificate and optionally the issuer and serial number identifier. [1, clause 7.4.1, last paragraph]*

However, the XAdES schema mandates the issuer and serial number identifier to be present in the `<Cert>` element. Therefore the word 'optionally' should be removed from the quoted sentence above.

History

Document history		
V1.1.1	February 2003	Publication
V1.2.1	June 2004	Publication