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

Technical Report

Electronic Signatures and Infrastructures (ESI); Maintenance report



Reference RTR/ESI-000020

2

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: <u>http://www.etsi.org</u>

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

Contents

Intell	ectual Property Rights	7
Forev	word	7
Introd	duction	7
1	Scope	8
2	References	8
3	Definitions and abbreviations	9
4	Role and structure of the present document	9
4.1	Role of the present document in the maintenance process	9
4.2	Structure of the present document	10
4.2.1	Clause 5: fields and structure	10
4.2.2	Annex A: Fields and structure	11
5	Comments	12
5 5.1	TS 101 456 - Qualified certificate policy	
5.2	TS 101 430 - Quanted certificate policy	
5.3	TS 101 755 - ES electronic signature formats	
5.4	TS 101 862 - Qualified certificate profile	
5.5	TS 101 903 - XML advanced electronic signatures (XAdES)	
5.6	TS 102 023 - Time stamping policy	
5.7	TR 102 038 - XML format for signature policies	
5.8	TR 102 041 - Signature policies report	
5.9	TS 102 042 - PKC certificate policy	
Anne	ex A: Comments in their original format	111
A.1	Comments from a TC-ESI member	111
A.1.1		
A.1.1.		
A.1.2	··· ·	
A.1.2.	1 2	
A.1.2.		
A.1.3	TS 102 023 - Time-stamping policy	115
A.1.3	.1 Export of the CA private key	115
۸ D	Comments and proposed amondments from LININEO STT (Italy)	116
A.2	Comments and proposed amendments from UNINFO-STT (Italy)	
A.2.1 A.2.2	Proposed amendments on TS 101 456	
A.2.2 A.2.3	1	
A.2.3 A.2.4	•	
A.2.4		
A.2.4	1	
A.2.4.		
A.2.5		
A.2.5.		
A.2.5.	1	
A.2.5.		
A.2.6		
A.3	Comments and proposed amendments from Japan and China PKI forums	128

A.3.1	Proposed amendments on TS 101 456	
A.3.1.1	Comment #1, page 10	
A.3.1.2	Comment #2, page 18	
A.3.1.3	Comment #3, page 18	129
A.3.2	Proposed amendments on TS 101 733	129
A.3.2.1	Rationale: Some comments regarding EESSI signature policy	129
A.3.2.2	Comment #1, pages 49, 67 and 76	
A.3.2.3	Comment #2, pages 16 and 17	
A.3.2.4	Comment #3, clause 8.9.1	
A.3.2.5	Comment #4, clause 11.1	132
A.3.2.6	Comment #5, clause 11.11	132
A.3.2.7	Comment #6, clause 5.4.2	
A.3.2.8	Comment #7, clauses 5.4.5 and 5.4.7	
A.3.3	Proposed amendments on TS 101 903	
A.3.3.1	Rationale: "Some comments regarding EESSI Signature Policy"	
A.3.3.2	Comment #1, page 17	
A.3.3.3	Comment #2	
A.3.3.4	Comment #3	
A.3.4	Proposed amendments on TS 101 861 - Time stamping profile	
A.3.4.1	Comment #1, clause 5.1.2.	
A.3.4.2	Comment #2, clause 5.2.3	
A.3.4.3	Comment #3.	
A.3.5	Comments and proposed amendments on TS 102 023	
A.3.5.1	Comment #1, clause 4.2	
A.3.5.2	Comment #2, clause 4.2	
A.3.5.3	Comment #3, clause 7.1.2 d)	
A.3.5.4	Comment #4, clause 7.1.2 j)	
A.3.5.5	Comment #4, clause 7.1.2 J)	
A.3.5.6	Comment #6, clause 7.2.2 a)	
A.3.5.7	Comment #7, clause 7.2.2 d)	
A.3.5.8	Comment #8, clause 7.2.2 0)	
A.3.5.9	Comment #9, clause 7.3.1 e)	
A.3.5.10		
A.3.5.11		
A.3.5.12		
A.3.5.12		
A.3.5.13		
A.3.6	Comments and proposed amendments on TR 102 038	
A.3.6.1	Comment #1	
A.3.7	Comments and proposed amendments on TR 102 041	
A.3.7.1	Comment #1, clause 8.3.1 - Signature validation policy	
A.3.7.2	Comment #2, clause 8.3.2 - Signature validation poncy	
A.3.1.2	Comment #2, clause 8.5.2 - Signature validation miormation	137
A.4 C	Comments and proposed amendments from a TC-ESI member	138
A.4.1	Proposed amendments on TS 101 456 - Qualified certificate policy	
A.4.1.1	Keys certified under multiple policies	
A.4.2	Proposed amendments on TS 102 042 - Normalized certificate policy	
A.4.2.1	Keys certified under multiple policies	
	Comments and proposed amendments from Pink Roccade (Netherlands)	
A.5.1	Proposed amendments on TS 101 456 - Qualified certificate policy	142
A.6 C	Comments and proposed amendments from EESSI evaluation	1/13
A.6.1	Suggested amendments on TS 101 456 - Qualified certificate policy (see EESSI #21(2002)04 - clause 6)	
A.6.2	Suggested amendments on TS 101 450 - Qualified certificates profile (see EESSI #21(2002)04 - clause 0) Suggested amendments on TS 101 862 - Qualified certificates profile (see EESSI #21(2002)04 - clause 0)	145
A.0.2		142
	6)	143
A.7 C	Comments and proposed amendments from CEN/ISSS WS/E-Sign Area M and ETSI STF-210	
	naintenance groups	144
A.7.1	Proposed amendments on TS 102 023 - Time-stamping policy	
	Other comments and proposed amendments	
A.8.1	Proposed amendments on TS 101 456 - Qualified certificate policy	144

A.8.1.1 Advise on use of SSCD	
A.8.1.2 Use of CA key for multiple policies	
A.8.1.3 Reference to CWA 14167-1 in clause 7.4.7	
A.8.1.4 When a new policy OID is required	
A.8.2 Proposed amendments on TS 102 042 - Normalized certificate policy	
A.8.2.1 Advise on use of SSCD	
A.8.2.2 Use of CA key for multiple policies	
A.8.2.3 Reference to CWA 14167-1 in clause 7.4.7	
A.8.2.4 When A new Policy OID is required	
A.8.3 Proposed amendments on TS 101 733 - Electronic signature formats	
A.8.3.1 Archive timestamp	
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	
A.8.4.2 Clause 5.2.1 - Ordering	
A.8.4.3 Clause 6 mandate support for store and forward	
A.8.4.4 Clause 7.1.1	
A.8.5 Proposed amendments on TS 101 862 - Qualified certificates profile	
A.8.5.1 Country Name	
A.9 Comments and proposed amendments from a TC-ESI member	150
A.9.1 Proposed amendments on TS 101 862 and related discussion threads	
A.9.1 Proposed amendments on TS 101 002 and related discussion threads	
-	
A.10 Comments and proposed amendments from ETSI STF-220 - Task 4	
A.10.1 TS 101 456 - Qualified certificate policy	
A.10.1.1 Proposed amendments related to section "Introduction"	
A.10.1.2 Proposed amendments related to clause 2 "Reference"	
A.10.1.3 Proposed amendments related to clause 3.1 "Definitions"	
A.10.1.4 Proposed amendments related to clause 4.1"Certification authority"	
A.10.1.5 Proposed amendments related to clause 4.3.4 "Other CA Statements"	
A.10.1.6 Proposed clause to be added: 4.5 "Certified attributes"	
A.10.1.7 Proposed clause to be added: 4.6 "Attribute semantics"	
A.10.1.8 Proposed clause to be added: 6.3 "Subject obligations" (subsequent clause	ses must be renumbered
accordingly)	
A.10.1.9 Proposed amendments related to clause 7.3.1 "Subject initial registration	
A.10.1.10 Proposed amendments related to clause 7.3.2 "Certificate renewal, rekey	
A.10.1.11 Proposed amendments related to clause 7.3.4 "Dissemination of Terms a	
A.10.1.12 Proposed amendments related to "Annex E (informative): Bibliography"	
A.11 Proposed amendments from ETSI STF-220 Task 2	
A.11.1 TS 101 456 - Qualified certificate policy	
TM	
A.12 Proposed amendments from XadES-PLUGTESTS TM	
A.12.1 Proposed amendments on TS 101 903	
A.12.1.1 Issue #1 – <encapsulatedocspvalues></encapsulatedocspvalues>	
A.12.1.2 Issue #2 - <timestamptype> Data Type</timestamptype>	
A.12.1.3 Issue #3 - <archivetimestamp></archivetimestamp>	
A.12.1.4 Issue #4 – Requirement Levels (RFC2119)	
A.12.1.5 Issue #5 – <qualityingproperties></qualityingproperties>	
A.12.1.6 Issue #6 – ASN.1 Encoding	
A.12.1.7 Issue #7 – Trust Status Lists	
A.12.1.8 Issue #8 - <signingcertificate></signingcertificate>	
A.12.1.9 Issue #9 – XAdES forms	
A.12.1.10 Issue #10 – archival forms	
A.12.1.11 Issue #11 – <anytype> Data Type</anytype>	
A.12.1.12 Issue #12 - <certid></certid>	
A.12.1.13 Issue #12NET validating parser	
A.12.1.14 Issue #14 – XAdES schema	
A.12.1.15 Issue #15 – <qualifyingpropertiesreferencetype> data type</qualifyingpropertiesreferencetype>	
A.12.1.16 Issue #16 – XAdES examples	
A.12.1.17 Issue #17 - <dataobjectformat></dataobjectformat>	
A.12.1.18 Issue #18 - <certificatevalues></certificatevalues>	

A.12.1.19	Issue #19 – <completecertificaterefs></completecertificaterefs>	166
History		67

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. 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);

11

- *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 Resolution comment	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 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		last bullet change the stem Auditors: Autho					chives and audit logs of ns".	the CA trustworthy		
	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		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 us	sed to generate	the certificates	"						
	Original resolution proposal	New text: "How	ever, the private key	used to sign the	e certificates,	1						
	Resolution comment											
	Resolution											

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	disseminates th	e CA's terms and con	ditions, and an	y published pol	icy and practice in	formation, to sub	nts, to relying parties. T scribers and relying par	ties".				
	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 conditionsto subscribers ad relying parties".											
	Resolution comment	on nt											
	Resolution text				-			1					
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		UNSTT-001		technical			not yet processed					
	text	 [6.2 [UNS11-001] [technical] [not yet processed] 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 registratio 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; not the currently proposed that the recognition of algorithms, with associated key length, being fit for the purposes of qualified certificates 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 su 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. f) if the certificate 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, due compromised; or control over the subjects private key has been lost due compromised; or 											

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 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 the 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 7.3.1 k); 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;											
	Resolution comment Resolution											
Comment ID	text 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	Modify the text: "b) CA key generation shall be carried out within a device which either:										
	text	- 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		"a) The CA private si	aning key shall		ed within a secure	e cryptographic d		1			
	text		quirements identified									
	Original resolution proposal	New text: "a) "T				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				
TS101456-010	1.2.1	7.2.9	UNSTT-001		technical			not yet processed					
	Comment text	Modify the 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: "NOT	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	"f) The subscril NOTE 7: The a i) The records	 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	provided at t NOTE 7: The i 											
	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	Modify the text:	Modify the text: "c) if the CA generated the subjects key:										
	text	- the procedu	the procedure of issuing the certificate is securely linked to the generation of the key pair by the CA;										
		 the private k 	the private key (or SSCD - see clause 7.2.9) is securely passed to the registered subscriber or subject."										
	Original	New text: "c) "i	New text: "c) "if the CA generated the subject's key:										
	resolution		re of issuing										
	proposal	 the private k 	ey is securely passed	d to the register	red subject"								
	Resolution												
	comment												
	Resolution												
	text												
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution reference	date	type	source	date		version				
TS101456-013	1.2.1	7.3.6	UNSTT-001		technical			not yet processed					
	Comment	Modify the text:											
	text		rtificate Revocation Li CRL shall state a time			nts (e.g. Delta CR	Ls) are used, the	ese shall be published a	t least daily and:				
			CRL may be publishe			next CRL issue."							
	Original	New text:				TICKE OTCE 1000C,							
	resolution		rtificate Revocation Li	ists (CRLs) incl	uding any varia	nts (e.g. Delta CR	(I s) are used the	ese shall be published a	t least daily and				
	proposal	- everv (CRL shall state a time	for next CRL i	ssue: and		(_ 0) are acea, are						
	P P		CRL may be publishe			next CRL issue:							
			L shall be signed by t				ted by the CA."						
	Resolution		č ,			, 0							
	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	generation, outside this f) Physical and themselves, certificate ge protection, fi against theff g) Controls sha without auth NOTE 1: See	 "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. 										
	Original resolution proposal Resolution	 device provision and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimet 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 2: NOTE 3:" 											
	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 b	e securely hand		nedia from damag	je, theft and unau						
	Original resolution proposal		within the CA shall b h to proactively preve			nedia from damag	je, theft, and unau	thorized access. Media	a life cycle management				
	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	Modify the text: "Revocation status										
	text	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	New text:										
	resolution		of compromise									
	proposal					ubjects) and any	entity with which	it has agreements or ot	her form of established			
		relations	, among which relying	g parties and C	As"							
	Resolution											
	comment											
	Resolution											
Comment ID	text Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable terret			
Comment ID	version	clause	Original contribution	date	type	source	date	Resolution status	Deliverable target version			
	Version	clause	reference	uate	type	Source	uate		Version			
TS101456-017	1.2.1	7.4.9	UNSTT-001		technical			not yet processed				
	Comment	Modify the text:			toonnoai			not yot proceeded				
	text		A terminates its servi	ices the followi	na procedures s	shall be executed	as a minimum:					
								or other form of establis	shed relations."			
	Original	New text: "CA g					0					
	resolution		A terminatesthe CA	shall								
	proposal	- inform al	I subscribers (and the	ese one in turn	will inform the s	ubjects) and any	entity with which i	it has agreements or ot	her form of established			
		relations	, among which relying	parties and C	As."							
	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	 record of applicab storage I 	ocument(s) presente unique identification e;	ed by the applica n data, numbers applications and	ant to support r , or a combinat d identification of	egistration; ion thereof (e.g. a documents, includ	ling the signed su	corded: license number) of ider bscriber agreement (se	
	Original resolution proposal	particular for the where the Certin Registration	e purpose of providin ication Service Prov	ng evidence of c rider is establish	ertification for t ed."	he purposes of le	gal proceedings a	ed for an appropriate pe according to the national ement (e.g. subjects' cor	law of the country
	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
FS101456-019	1.2.1	4.3	JCPKI-001	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text Original resolution proposal Resolution comment Resolution text	cross authentica	ation?	dressed by curr	ent TS 101 456)		cations of the relations b	
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
S101456-020	1.2.1	7.2.4	JCPKI-001	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text Original resolution proposal		ow", how to handle th						
	Resolution comment Resolution text	The present do	cument only applies	to signing keys	(not data encry	ption keys) for wh	nich data monitori	ng and Escrow is not ap	plicable.

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 F the protocols in		ure - Key manag	gement life cycl	e", why it doesn"t	mention the oper	ation of "certification aut	hority key update" like
	Original resolution proposal								
	Resolution comment	Issues relating	to handling (including	g changing) CA	keys is covered	d in clause 7.2.1 (generation) and c	lause 7.2.2 (storage bad	ckup 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	
	text	on a card. Thes I have, so far, ic signatures only clue about. With We should cons a) whether the b) how to addr Maintenance of Discussion: Key multiple us Providing a frar consumers rely It is technically key pair is gene this, but for son Issue revolves a) the quality of b) the creation Qualified certific not prohibit sub currently part of Qualified certific Article 5.1 signa	se certificates may be dentified one potentia r, the other for encryp hout a flag in the CP sider to look at: are are other potentia ress them. If the policies is proba- age: mework to support the ring on e-signatures; possible that the sar erated by the subscri- ne applications, this around: of the key pair genera- to of a close association cates are designed to pscriber generation o f Electronic Signatur- cates may be used to atures must be recog- such, although proba	e issued by diffe al conflict. Assu- btion. The two C the situation is I conflicts for the ably the right plate e use of e-signa- is an objective ne public key m ber, which he s- may be undesire ated; and on between the o offer a high le f keys. It should es Directive, no o support an art gnized in legal p ibly only if they	rent CAs, unde me that two CA As don't know a not transparent e configuration ace to deal with atures and crea under EESSI ar ay be included ends to more th able, particularly key pair and an vel of assurance be preferred th r conformance g icle 5.1 e-signa roceedings as t satisfy at least t	r different CPs. s issue two different about each other, to auditors either described above, this. ting an environment of the Directive. in more than one an one certification y where higher lev application for w e which needs to at the certificatior guidance. ture; they may als he equivalent of h	ent certificates to users can hardly and ent which will pron certificate. (This of on authority.) In ge vels of assurance hich it is to be use be maintained in a n authority takes r so be used for aut nand written signa	the same key, one spec made responsible for the note trust, and protecting could well be the case, fr eneral, there may be not are required.	ings they don't have a g the interests of or example, where the hing objectionable in e. TS 101 456 [2] does ing the keys. This is not se. signatures may be icle 2.2.

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
		 they indicate reference to a signature Therefore, there a) the intention b) the intention 	the document to whith is evidence of itself, i. e are two elements whith to express a commit to create the signatu	the signer to ta ch it is applied, e. of the act of hich electronic s ment; and ire.	ake on a commi or to some othe signing. signatures canr	er evidence); and not prove:		nmitment may be ambig	guous except by
		of demonstratin incorporating th One factor whic This could be a usage. The relying part intention to mal	g the signer's intentio is factor into an election chould provide evide chieved by restricting ty needs to know (in c ke the signature as a	ons. However, ir ronic signature, ence of the inter the use of a ke order to rely on handwritten one	ntent is an esse which is intend ntion to create a ey to a "signing" a "e-signature o e. This requires	ntial element of s led as a handwritt a signature equiva application, i.e. b equivalent to hanc two steps:	gning and there is en signature. Ilent to a h/w one, y including it in a Iwritten signature	is to "bind" the signing certificate (qualified) wi that the signer will no forcing that obligation e	a means of key to the application. hich specifies a key t be able to deny his
		(second bes - ensuring a r the use of h As a preference reason is that w The fact that:	st) by legal means; neans of signature cro is key pair for any oth e, the sscd on which t	eation which ma er purpose. he keys are sto	akes it clear to red should also	the signer that he be dedicated to a	is creating is equ a hw sign, but this	al to a h/w one; preven may carry unrealistic c	ting (as far as possible)
		 the signer p will provide prin by law was bein Enforcement: 	robably knew that key na facie evidence that ng undertaken as a re	t the signer kne sult.	w what kind of			i, i.e. that a commitmen	t that may be enforced
		may be many re - the certificat - the certificat guidance;	easons for NOT taking tion authority does no tion authority itself has	g any enforcem t regard the bre s not suffered a	ent action: each as being s iny loss, neithei	gnificant; will its inaction is	not (currently) in	contravention of any a	uditing criteria, or
		and - cost of legal The reliability of just be left to th competence an requirements in In due course, i	proceedings. f signatures = to h/w s e discretion of a certif d power to ensure a s TS 101 456 [2] and t is to be hoped (and	signatures is a r fication authorit single use of ke FS 102 042 [3] expected) that	matter of public y. The role of th ys used to crea (or for the time national laws w	interest, therefore e certification aut te such signature being, in any app ill impose the san	e, the responsibilit hority should be t s. This could be p ropriate maintena ne level of respon	o bring legal proceedin by for ensuring their effe take such steps as ar provided for by including nce document). sibility of a signer as cu the electronic signature	ectiveness should not e reasonably within its g appropriate urrently exist in relation

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		comments on a high					of our voluntary certifica	
		is used b quality m • TS 101 4 - In your work developed b	by auditors to audit the nanagers and auditors 456 contains a lot of r shop agreements CE by CEN National Merr	e CSP-organiza s. It is not an ea edundancy. N has written: ' bers". Nonethe	ation. For the pu sy document to 'This CEN Worl less CWA 1416	urpose it is used fo handle. kshop Agreement	or TS 101 456 is the can in no way be	auditors) to build the C coo much written by tech held as being an officia ces has become a part of	nnicians and too less by al standard as
		 In our guida for Electroni requirement 	c Signatures - Part 1:	e refer on the d	ocument CWA ty Requirement	14167-1 Security s. The problem w	ith CWA 14167-1	r Trustworthy Systems however is that it not o 7-1 doubles with ETSI	Managing Certificates
	Original	 In our guida for Electroni requirement 	nce on TS 101 456 w c Signatures - Part 1 s on a TWS but it spe	e refer on the d	ocument CWA ty Requirement	14167-1 Security s. The problem w	ith CWA 14167-1	however is that it not o	Managing Certificates nly specifies
	resolution	 In our guida for Electroni requirement 	nce on TS 101 456 w c Signatures - Part 1 s on a TWS but it spe	e refer on the d	ocument CWA ty Requirement	14167-1 Security s. The problem w	ith CWA 14167-1	however is that it not o	Managing Certificates nly specifies
	resolution proposal	 In our guida for Electroni requirement 	nce on TS 101 456 w c Signatures - Part 1 s on a TWS but it spe	e refer on the d	ocument CWA ty Requirement	14167-1 Security s. The problem w	ith CWA 14167-1	however is that it not o	Managing Certificates nly specifies
	resolution proposal Resolution	 In our guida for Electroni requirement 	nce on TS 101 456 w c Signatures - Part 1 s on a TWS but it spe	e refer on the d	ocument CWA ty Requirement	14167-1 Security s. The problem w	ith CWA 14167-1	however is that it not o	Managing Certificates nly specifies
	resolution proposal	 In our guida for Electroni requirement 	nce on TS 101 456 w c Signatures - Part 1 s on a TWS but it spe	e refer on the d	ocument CWA ty Requirement	14167-1 Security s. The problem w	ith CWA 14167-1	however is that it not o	Managing Certificates nly specifies

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 Original				aim supported b	y an audit is requ	ired before a CS	P is allowed (by the rele	vant Supervisory			
	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	I am wondering	whether we omitted	a clause in TS	101 456 [2] to s	ate that the CA s	hall inform their s	ubscribers about the kir	d of environment that			
	text											
	Original		ne shall use for the SSCD, pointing to CWA 14170 [13]: Security requirements for Signature Creation Systems. Add to clause 7.2.9:									
	resolution			e CA advises si	ibscribers as to	the environments	in which the SS	CD should be used. This	s includes the			
	proposal		acteristics of the devi									
	Resolution	Chara		ces and applica				or signing.				
	Resolution											
	comment											
	Resolution											
	Resolution text							1				
Comment ID	Resolution	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
	Resolution text Deliverable version	clause	contribution reference		type							
	Resolution text Deliverable	clause 7.2.5 I think it is not v	contribution reference OTHER-002 rery feasible to requir	date e CSPs not to u	type technical ise same signin	source	date	Resolution status not yet processed because I cannot see w instead of shall), but not	version			
	Resolution text Deliverable version 1.2.1 Comment text	7.2.5 I think it is not v necessarily con requirement.	contribution reference OTHER-002 rery feasible to requir npromise security. Pr	date e CSPs not to u robably we could	type technical ise same signin	source	date	not yet processed because I cannot see w	version			
	Resolution text Deliverable version 1.2.1 Comment	clause7.2.5I think it is not vnecessarily conrequirement.a) Replace texThe signing key	contribution reference OTHER-002 very feasible to requir npromise security. Pr tt in clause 7.2.5 with ys(s) used for genera	date re CSPs not to u robably we could : ting certificates,	type technical ise same signin d advice CSPs t as defined in c	source g key for QCPs at o use dedicated k lause 7.3.3, and/c	date nd NCPs. That's eys (use should or issuing revocat	not yet processed because I cannot see w	version hy that would t make that as a hall not be used for any			
Comment ID	Resolution text Deliverable version 1.2.1 Comment text Original resolution	clause7.2.5I think it is not v necessarily con requirement.a) Replace tex The signing key other purposes policy.NOTE:It is r b) An alternativ	contribution reference OTHER-002 very feasible to requir npromise security. Pr tt in clause 7.2.5 with (s(s) used for genera if this results in the v recommended that dir ve resolution is to del	date e CSPs not to u robably we could : ting certificates, riolation of THE fferent CA keys lete this clause.	type technical use same signin d advice CSPs t as defined in c SECURITY ME are used to issu	source g key for QCPs at o use dedicated k lause 7.3.3, and/c ASURES OR AN	date nd NCPs. That's eys (use should or issuing revocat Y OTHER SPEC	not yet processed because I cannot see w instead of shall), but not ion status information, s IFIC LIMITATIONS PRO	version hy that would t make that as a hall not be used for any VIDED FOR in this			
	Resolution text Deliverable version 1.2.1 Comment text Original resolution	clause7.2.5I think it is not vnecessarily conrequirement.a) Replace texThe signing keyother purposespolicy.NOTE:It is rb) An alternationJan Sauer comwould result in v	contribution reference OTHER-002 very feasible to requir npromise security. Pr tt in clause 7.2.5 with vs(s) used for genera if this results in the v recommended that dir ve resolution is to del ment: With the propo violation of the QCP.	date e CSPs not to u robably we could ting certificates, riolation of THE fferent CA keys lete this clause. used new wordin Same for NCP.	type technical use same signin d advice CSPs t as defined in c SECURITY ME are used to issu- ng of clause 7.2.	source g key for QCPs at o use dedicated k lause 7.3.3, and/c ASURES OR AN ue certificates unc 5 a), the QCP wil	date ad NCPs. That's aeys (use should ar issuing revocat Y OTHER SPECI ler different policities contain a require	not yet processed because I cannot see wi instead of shall), but not ion status information, s IFIC LIMITATIONS PRC ies. ement that something sh	version hy that would t make that as a hall not be used for any VIDED FOR in this			
	Resolution text Deliverable version 1.2.1 Comment text Original resolution proposal	clause7.2.5I think it is not vnecessarily conrequirement.a) Replace texThe signing keyother purposespolicy.NOTE:It is rb) An alternationJan Sauer comwould result in v	contribution reference OTHER-002 very feasible to requir npromise security. Pr tt in clause 7.2.5 with (s(s) used for genera if this results in the v recommended that dir ve resolution is to del ment: With the propo	date e CSPs not to u robably we could ting certificates, riolation of THE fferent CA keys lete this clause. used new wordin Same for NCP.	type technical use same signin d advice CSPs t as defined in c SECURITY ME are used to issu g of clause 7.2.	source g key for QCPs at o use dedicated k lause 7.3.3, and/c ASURES OR AN ue certificates unc 5 a), the QCP wil	date ad NCPs. That's aeys (use should ar issuing revocat Y OTHER SPECI ler different policities contain a require	not yet processed because I cannot see wi instead of shall), but not ion status information, s IFIC LIMITATIONS PRC ies. ement that something sh	version hy that would t make that as a hall not be used for any VIDED FOR in this			
	Resolution text Deliverable version 1.2.1 Comment text Original resolution proposal Resolution	clause7.2.5I think it is not vnecessarily conrequirement.a) Replace texThe signing keyother purposespolicy.NOTE:It is rb) An alternationJan Sauer comwould result in v	contribution reference OTHER-002 very feasible to requir npromise security. Pr tt in clause 7.2.5 with vs(s) used for genera if this results in the v recommended that dir ve resolution is to del ment: With the propo violation of the QCP.	date e CSPs not to u robably we could ting certificates, riolation of THE fferent CA keys lete this clause. used new wordin Same for NCP.	type technical use same signin d advice CSPs t as defined in c SECURITY ME are used to issu g of clause 7.2.	source g key for QCPs at o use dedicated k lause 7.3.3, and/c ASURES OR AN ue certificates unc 5 a), the QCP wil	date ad NCPs. That's aeys (use should ar issuing revocat Y OTHER SPECI ler different policities contain a require	not yet processed because I cannot see wi instead of shall), but not ion status information, s IFIC LIMITATIONS PRC ies. ement that something sh	version hy that would t make that as a hall not be used for any VIDED FOR in this			
	Resolution text Deliverable version 1.2.1 Comment text Original resolution proposal Resolution comment	clause7.2.5I think it is not vnecessarily conrequirement.a) Replace texThe signing keyother purposespolicy.NOTE:It is rb) An alternationJan Sauer comwould result in v	contribution reference OTHER-002 very feasible to requir npromise security. Pr tt in clause 7.2.5 with vs(s) used for genera if this results in the v recommended that dir ve resolution is to del ment: With the propo violation of the QCP.	date e CSPs not to u robably we could ting certificates, riolation of THE fferent CA keys lete this clause. used new wordin Same for NCP.	type technical use same signin d advice CSPs t as defined in c SECURITY ME are used to issu g of clause 7.2.	source g key for QCPs at o use dedicated k lause 7.3.3, and/c ASURES OR AN ue certificates unc 5 a), the QCP wil	date ad NCPs. That's aeys (use should ar issuing revocat Y OTHER SPECI ler different policities contain a require	not yet processed because I cannot see wi instead of shall), but not ion status information, s IFIC LIMITATIONS PRC ies. ement that something sh	version hy that would t make that as a hall not be used for any VIDED FOR in this			
	Resolution text Deliverable version 1.2.1 Comment text Original resolution proposal Resolution	clause7.2.5I think it is not vnecessarily conrequirement.a) Replace texThe signing keyother purposespolicy.NOTE:It is rb) An alternationJan Sauer comwould result in v	contribution reference OTHER-002 very feasible to requir npromise security. Pr tt in clause 7.2.5 with vs(s) used for genera if this results in the v recommended that dir ve resolution is to del ment: With the propo violation of the QCP.	date e CSPs not to u robably we could ting certificates, riolation of THE fferent CA keys lete this clause. used new wordin Same for NCP.	type technical use same signin d advice CSPs t as defined in c SECURITY ME are used to issu g of clause 7.2.	source g key for QCPs at o use dedicated k lause 7.3.3, and/c ASURES OR AN ue certificates unc 5 a), the QCP wil	date ad NCPs. That's aeys (use should ar issuing revocat Y OTHER SPECI ler different policities contain a require	not yet processed because I cannot see wi instead of shall), but not ion status information, s IFIC LIMITATIONS PRC ies. ement that something sh	version hy that would t make that as a hall not be used for any VIDED FOR in this			

Comment ID	Deliverable	Deliverable	Original contribution	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	reference	date	type	source	date		version
TS101456-027	1.2.1	7.4.7	OTHER-003		technical			not yet processed	
	Comment	Update clause 7		itly reference C	WA 14167-1 [1	2] and add the rei	ference to the bib	liography/references.	I
	text							dequately satisfying the	requirements of
			93/EC Annex II (f)".						·
	Original	Update clause	7.4.7, note 1 to explicit	itly reference C	WA 14167-1 [1	2] and add the ret	ference to the bib	liography/references.	
	resolution								
	proposal								
	Resolution								
	comment								
	Resolution								
	text								
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution reference	date	type	source	date		version
TS101456-028	1.2.1	8	OTHER-004		technical			not yet processed	
	Comment text	It is currently no	t clear when a new c	ertification polic	cy is necessary				
	Original	Add to clause 8	:						
	resolution		ould be made to a ce	ertificate policy v	which could affe	ect a relying party	s consideration c	on the reliability of the ce	ertificate issued by the
	proposal	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	Please add the	following text after th	e first paragrap	h.				
	text	documents are This may be ac - using attribu - using attribu	ant requirement of ele signed using a hand- hieved using certifica utes included in Public utes included in Attrib e is covered in the pr	written signatur tion services in c Key Certificate ute Certificates	re, but also thei two ways: es (PKCs); (ACs).	r attribute(s), e.g.	their role(s) in an	of electronic information organization.	in the same way that
	Original		following text after th						
	resolution					to identify not or	ly the originator	of electronic information	in the same way that
	proposal	documents are This may be ac - using attribu - using attribu	signed using a hand- hieved using certifica ites included in Public ites included in Attrib e is covered in the pr	written signatur tion services in c Key Certificate ute Certificates	re, but also thei two ways: es (PKCs); (ACs).	r attribute(s), e.g.	their role(s) in an		
	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				
	1.2.1 Introduction STF220_4-001 [08/09/2003] [technical] Introduction Introduction Introduction STF220_4-001 [08/09/2003] [technical] Introduction Introduction Introduction Stressed Intresech Stressed <t< td=""></t<>											
	resolution	The Directive 19 referred to as "t specifies require Directive specific certificates). The mentioned Certificates (PK on the purpose The present doo certificates in ad	he Directive") identifie ements for qualified c es requirements on c Directive also covers Cs) (see annex I, cla for which the certifica cument specifies base coordance with the Di	opean Parliame es a special forr ertificates. Anne ertification-serv the use of attril use d) which re the is intended". eline policy requirective. The use	ent and of the C m of electronic s ex II of the vice-providers is putes in public k fers to the "prov uirements on the e of a secure-si	signature which is suing qualified ce key certificates, sin vision for a specifi e operation and m gnature-creation of	based on a "qua ertificates (i.e. cert nce it mentions th c attribute of the s nanagement pract	signatory to be included	I of this Directive uing qualified attributes in Public Key I if relevant, depending horities issuing qualified			
	Resolution comment		t of the policy require	anenis speciliei								
	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		08/09/2003	technical			not yet processed	
	Comment text Original resolution proposal	Please add to th	e 93/13/EEC of 5 Apr ne list:					is is asked to be added	
	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	attribute: inform associated with Attribute Grantin	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	Please add the When a signer s transaction to b identity of the si features or attril	e traceable. However gner but instead, or a butes that the signato	at the end. of primary imp , in many case additionally, on ry might posse	ortance to be a s, in order to ac the qualification ss in order to pe	ble to identify suc cept a signature, (s) of the signer. (erform a certain a	the acceptance of Qualifications in the ct.	e interest of accountabili criteria may not necessa this context have the me c signatures.	rily be based on the					
	Original resolution proposal	Typo -> Please Please add the When a signer s transaction to b identity of the si features or attril	Such a qualification may be obtained using attributes within PKCs included or referenced in electronic signatures. Fypo -> 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 ransaction to be traceable. However, in many cases, in order to accept a signature, the acceptance criteria may not necessarily be based on the dentity of the signer but instead, or additionally, on the qualification(s) of the signer. Qualifications in this context have the meaning of specific eatures 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	In addition to th requirements of national legislat They have, how effective agains - they are eas - their existen	general conditions a ion of the member st vever, to be brought t trelying parties, who sily accessible; and	statements a C and comply with ates. In specific to the attention o have no other rmation as to ho	the requirement of contracting contracting contractual arra	its set out in Direct tions are non-neg punter parties and ingement with the accessed is broug	ctive 93/13/EEC -> otiable and bindin I especially to con CA if:	mercial purpose. They r > add reference è as im g to a non-determined sumers. Terms and col on in a conspicuous ma	plemented in the number of end users. nditions will only be			
	Original resolution proposal	In addition to th requirements of national legislat They have, how effective agains - they are eas - their existen	general conditions a ion of the member st vever, to be brought t trelying parties, who sily accessible; and	statements a C and comply with ates. In specific to the attention o have no other rmation as to ho	the requirement of contracting contracting contractual array contractual array	its set out in Direct tions are non-negounter parties and ingement with the accessed is broug	ctive 93/13/EEC -> otiable and bindin I especially to con CA if:	mercial purpose. They r > add reference è as im g to a non-determined sumers. Terms and col on in a conspicuous ma	plemented in the number of end users. nditions will only be			
	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	"Before being g the time of regis The Certification	stration for an attribut n Authority is respons	ed attributes": all be verified in ae, the individua sible for verifyin	I was entitled to	claim that attribu	te.	-	hall be verified that, at			
	Original	The Certification Authority is responsible for verifying the correct attribution of attributes to subjects (see also clause 6.4 Liability)." Add this new clause with title "Certified attributes":										
	resolution proposal	the time of regis	stration for an attribut	e, the individua	I was entitled to	claim that attribu	te.	to their authenticity. It see also clause 6.4 Liabi	shall be verified that, at ity)."			
	Resolution comment			,			,		<i></i>			
	Resolution text											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution reference	date	type	source	date		version
TS101456-036	1.2.1	4.6	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment		ause with title "Attribu						
	text		of an attribute may be				fined by any orga	anization.	
			ute is defined in a star						
								that X.509 has defined	d a set of standard
			utes. When it is locally				are possible:		
			se an OID located une						
					y" (e.g. as called	d in ISO/TS 17090	0-2, see Bibliogra	phy) and add a definition	on of the attribute in any
			yntax (e.g. character s					The compation of the	attribute has then to be
								ity") in combination with	attribute has then to be
		attribute by that		attribute grantin	ig authority (als		s issuing aution	ity) in combination with	
	Original		ause with title "Attribu	to somantics":					
	resolution		of an attribute may be		l in a standard (e a by ISO) or de	fined by any ora	nization	
	proposal		ute is defined in a star				anied by any orga		
	proposal						This is in this way	that X.509 has defined	a set of standard
			utes. When it is locally						
			se an OID located und				•		
)-2, see Bibliogra	phy) and add a definition	on of the attribute in any
		S	yntax (e.g. character s	string, XML).					
									attribute has then to be
				attribute grantir	ng authority (als	o called sometime	es "issuing author	ity") in combination with	h 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	"The CA shall o - use the PKC - notify the su including a c	 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											
Comment ID	text 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 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 of either paper or electronic documentation. 										
	Resolution comment		entier paper of electro	onic documenta	uUII.							
	Resolution											

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment	Resolution	Resolution date	Resolution status	Deliverable target version			
	Version	Clause	reference	uale	type	source	uale		version			
TS101456-039	1.2.1	7.3.1	STF220_4-001	08/09/2003	technical			not yet processed				
	Comment	In "Registration" please add:										
	text	 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 sha	Il record all information	on used to verify	y the attributes of	of the subject.						
		n) The CA sha										
			Il record the informat				have attributes v	vithin PKCs.				
	Original	In "Registration" please add:										
	resolution	I) 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										
	proposal	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				<u> </u>	•						
	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 Original resolution proposal	Please add the Attribute Regist a) The CA shal b) The CA shal number on t c) The CA shal d) The CA shal - whether, registere - confirma NOTE 1: Othe NOTE 2: This Please add the Attribute Regist a) The CA shal number on t c) The CA shal c) The CA shal number on t c) The CA shal c) The CA shal c) The CA	following clause ration: Il check by appropriat Il record all informatio he documentation use Il verify by appropriate Il record the signed ag and under what cond d; tion that the informati r parties (e.g. the ass agreement may be in following clause ration: Il check by appropriate Il record all informatio he documentation use Il verify by appropriate Il record the signed ag er, and under what coo	e means that the on used to verify ed for verification e means in accor- greement with the ditions, the substration on registered is occiated person electronic form e means that the on used to verify ed for verification greement with the nditions, the sub- ation registered occiated person	ne subject is en the subjects' ri on, and any limi- ordance with na the subscriber in scriber requires s correct. or legal entity) n, providing all in the subject is en- the subject is en- or legal entity)	ghts to exert the a tations on its valid titional law, the att ncluding: the subject's cons may be involved involved parties const titled to the attribut ghts to exert the a tations on its valid titional law, the att ncluding: es the subject's const may be involved i	attributes to be re dity. ributes of the per sents to the inclu- in establishing thi onsent. htes requested to attributes to be re dity. ributes of the per onsents to the inc	be certified. gistered (see item c), ir son. sion in PKCs of the attri s agreement. be certified. gistered (see item c), ir son. lusion in PKCs of the at	butes that have been		
	Resolution				., p. o Haing an n						
	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			
TS101456-041	1.2.1	7.3.4	STF220_4-001	08/09/2003	technical			not yet processed				
			following requiremen									
	text	 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. 										
	Original	- the subscriber's and subject's obligations as defined in clauses 6.2 and 6.3. Please add the following requirements to item a):										
	resolution				of attribute that	is supported. Tha	t description shall	l be given in readily-und	erstandable terms, and,			
	proposal	 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. 										
	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			
TS101456-042	1.2.1	Annex E	STF220_4-001	08/09/2003	technical			not yet processed				
	text	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".										
	Original resolution proposal	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".										
	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					
TS101456-043	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 Original resolution proposal	FPKI requireme Information abo	nt identified as "missi ut a revoked certifica	ng" or partially te shall remain	covered in the in the status inf	QCP: ormation until the	certificate expires	s (table 65).						
	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	The issuance fr	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	Audit logs shall last review shal the category an	I be examined (where	once every two the confidence ools to perform s	months. A state intervals for essuch a review),	istically significan ach category of se as well as a rease	ecurity audit data	udit data generated by are determined by the sany evidence of malicion	security ramifications of					
	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	Audit processes audit system ha		system startup, grity of the system	and cease only em or confident	at system shutdo iality of the inform	ation protected b	nould it become apparer y the system is at risk, t						
	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		ent identified as "miss										
	text	Routine self-ass	sessments of securit	y controls shall	be performed by	the entity operat	ing the CA (table	90).					
	Original												
	resolution												
	proposal												
	Resolution												
	comment												
	Resolution												
	text												
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
FS101456-050	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed					
	Comment	FPKI requireme	nt identified as "miss	sing" or partially	covered in the	QCP:			•				
	text	Full system bac	PKI 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).											
						per week (table 1	22).						
		Backups are to	be performed and st	ored off-site not	t less than once			oment) (table 123)					
		Backups are to At least one full	be performed and st backup copy shall b	ored off-site not e stored at an c	t less than once offsite location (s	eparate from the	Agency CA equip)				
	Original	Backups are to At least one full	be performed and st backup copy shall b	ored off-site not e stored at an c	t less than once offsite location (s	eparate from the	Agency CA equip	oment) (table 123). e Agency CA (table 124)).				
	Original	Backups are to At least one full	be performed and st backup copy shall b	ored off-site not e stored at an c	t less than once offsite location (s	eparate from the	Agency CA equip).				
	resolution	Backups are to At least one full	be performed and st backup copy shall b	ored off-site not e stored at an c	t less than once offsite location (s	eparate from the	Agency CA equip).				
	resolution proposal	Backups are to At least one full	be performed and st backup copy shall b	ored off-site not e stored at an c	t less than once offsite location (s	eparate from the	Agency CA equip).				
	resolution proposal Resolution	Backups are to At least one full	be performed and st backup copy shall b	ored off-site not e stored at an c	t less than once offsite location (s	eparate from the	Agency CA equip).				
	resolution proposal Resolution comment	Backups are to At least one full	be performed and st backup copy shall b	ored off-site not e stored at an c	t less than once offsite location (s	eparate from the	Agency CA equip).				
	resolution proposal Resolution comment Resolution	Backups are to At least one full	be performed and st backup copy shall b	ored off-site not e stored at an c	t less than once offsite location (s	eparate from the	Agency CA equip).				
Commont ID	resolution proposal Resolution comment Resolution text	Backups are to At least one full The backup sha	be performed and st backup copy shall b all be stored at a site	ored off-site no e stored at an o with physical a	t less than once offsite location (s nd procedural co	eparate from the	Agency CA equipurate to that of the	e Agency CA (table 124)					
Comment ID	resolution proposal Resolution comment Resolution text Deliverable	Backups are to At least one full The backup sha	be performed and st backup copy shall b all be stored at a site Original	ored off-site no e stored at an o with physical a	t less than once offsite location (s nd procedural co Comment	Resolution	Agency CA equipurate to that of the Resolution		Deliverable target				
Comment ID	resolution proposal Resolution comment Resolution text	Backups are to At least one full The backup sha	be performed and st backup copy shall b all be stored at a site Original contribution	ored off-site no e stored at an o with physical a	t less than once offsite location (s nd procedural co	eparate from the	Agency CA equipurate to that of the	e Agency CA (table 124)					
	resolution proposal Resolution comment Resolution text Deliverable version	Backups are to At least one full The backup sha	be performed and st backup copy shall b all be stored at a site Original contribution reference	Comment date	t less than once offsite location (s nd procedural co Comment type	Resolution	Agency CA equipurate to that of the Resolution	e Agency CA (table 124)	Deliverable target				
	resolution proposal Resolution comment Resolution text Deliverable version	Backups are to At least one full The backup sha Deliverable clause	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001	Comment date 15/05/2003	t less than once offsite location (s nd procedural co Comment type technical	Resolution source	Agency CA equipurate to that of the Resolution	e Agency CA (table 124)	Deliverable target				
	resolution proposal Resolution comment Resolution text Deliverable version	Backups are to At least one full The backup sha Deliverable clause	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the	Resolution source	Agency CA equipurate to that of the arrange of the second	Resolution status	Deliverable target version				
	resolution proposal Resolution comment Resolution text Deliverable version	Backups are to At least one full The backup sha Deliverable clause FPKI requireme The Agency CA	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss Policy Authority sha	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the ate administrativ	Resolution source	Agency CA equipurate to that of the solution date	Resolution status	Deliverable target version				
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment	Backups are to At least one full The backup sha Deliverable clause FPKI requirement The Agency CA involving the Agency CA	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss Policy Authority sha	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the ate administrativ	Resolution source	Agency CA equipurate to that of the solution date	Resolution status	Deliverable target version				
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment	Backups are to At least one full The backup sha Deliverable clause FPKI requireme The Agency CA	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss Policy Authority sha	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the ate administrativ	Resolution source	Agency CA equipurate to that of the solution date	Resolution status	Deliverable target version				
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment	Backups are to At least one full The backup sha Deliverable clause FPKI requirement The Agency CA involving the Agency CA	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss Policy Authority sha	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the ate administrativ	Resolution source	Agency CA equipurate to that of the solution date	Resolution status	Deliverable target version				
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment text	Backups are to At least one full The backup sha Deliverable clause FPKI requirement The Agency CA involving the Agency CA	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss Policy Authority sha	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the ate administrativ	Resolution source	Agency CA equipurate to that of the solution date	Resolution status	Deliverable target version				
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment text Original resolution	Backups are to At least one full The backup sha Deliverable clause FPKI requirement The Agency CA involving the Agency CA	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss Policy Authority sha	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the ate administrativ	Resolution source	Agency CA equipurate to that of the solution date	Resolution status	Deliverable target version				
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment text Original resolution proposal	Backups are to At least one full The backup sha Deliverable clause FPKI requirement The Agency CA involving the Agency CA	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss Policy Authority sha	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the ate administrativ	Resolution source	Agency CA equipurate to that of the solution date	Resolution status	Deliverable target version				
Comment ID <u> IS101456-051</u>	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment text Original resolution	Backups are to At least one full The backup sha Deliverable clause FPKI requirement The Agency CA involving the Agency CA	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss Policy Authority sha	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the ate administrativ	Resolution source	Agency CA equipurate to that of the solution date	Resolution status	Deliverable target version				
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment text Original resolution proposal Resolution	Backups are to At least one full The backup sha Deliverable clause FPKI requirement The Agency CA involving the Agency CA	be performed and st backup copy shall b all be stored at a site Original contribution reference STF220_2-001 ent identified as "miss Policy Authority sha	Comment date 15/05/2003 sing" or partially	t less than once offsite location (s nd procedural co Comment type technical covered in the ate administrativ	Resolution source	Agency CA equipurate to that of the solution date	Resolution status	Deliverable target version				

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 requireme	nt identified as "missi	ing" or partially	covered in the		d the level of trai	ning completed (table 1	36).
	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		ng keys, when export old secret sharing me		tected not only	by means of encry	yption, but also b	y means of other mecha	anisms, like Shamir's or
		•	stems that, according		•		, ,	private signing key sha acks for the residual life	Il be protected using of the encrypted key 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
TS101456-054	1.2.1	Annex D	TC-ESI_1-006	26/10/2003	technical			not yet processed	
	Comment text	Correct the inco	onsistencies in annex	CD, the cross re	ference betwee	n RFC 2527 and	TS 101 456.	· · ·	•
	Original resolution proposal	* 4.4: change * 5.2: change * 6.3: add "6 * 6.4: add "7 * 6.5: add "7 * 6.6: change * 6.7: add "7 NOTE 1: The - " NOTE 2: The - " - S fa a - S to e - T	7.3.5" into "7.3.6" "7.3.5" into "7.3.6" "7.4.5" into "7.4.3" (2, " before "7.2" 2.7, " before "7.2.9" 4.5, " before "7.4.6" "7.3" into "7.4" (note 4.5, " before "7.4.6" procedural controls, n this subcomponent for each task identifie dentification and aut life cycle security con This subcomponent a system development ecurity during produc ailsafe design and im ddressed by TS 101 eccurity management o configured security nsure their correct of his subcomponent c fethodology (TSDM)	as per RFC 252 t, requirements ed for each role, hentication requ htrols, as per RF addresses syste controls include t maintenance, plementation te 456). t controls includ . These tools ar peration. (<- this an also address level IV and V,	for recognizing it should also b uirements for ea FC 2527, are: m development e software engine chniques (e.g. c e execution of to d procedures in s is addressed in life-cycle secur independent life	e stated how man ch role may also b controls and secu- nvironment securi eering practices, s defensive program pols and procedur include checking th n clause 7.4 of TS ity ratings based, e-cycle security co	ay individuals are be defined" urity management software development aming) and devel res to ensure that he integrity of the 101 456). for example, on	personnel security, con	task (n out m rule) figuration management lularity, layering, use of (<- this is not s and networks adhere vare, and hardware to evelopment
	Resolution comment	I N	laturity Model (SEI-C	Jiviivi) (<- this is	not addressed t	<u>y 13 101 430).</u>			
	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 t	References to the various RFCs and Internet Drafts from PKIX (especially RFC 2459 / RFC 3280).											
	Original resolution proposal													
	Resolution comment Resolution	This suggestion	has been already a	pplied in the ne	w version 1.5.1									
	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 op	otional?	-	·									
	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	k may solve the	problems relate	ed to the compror	nission of TSA pr	ivate key.						
	Original resolution proposal													
	Resolution comment	on usage of time technologies that used there). In any case the	e-stamps for archiva at do not fall within th	l electronic form ne scope of sigr s options deper	ns. Usage of tir nature formats (ne-mark for achie although certain c	eving long term sig data structures sp	gnatures would rely on s	1 733 could certainly be					
	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 "	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 add	dressed by ETSI TC-	ESI activity on	CRL and OCS	P 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 nee	ed for a better specifi	cation of the ve	rification proce	sses (initial and u	sual), 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.	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 nee electronic signa		ices while using	the different fo	ormats, in order to	give a reader a d	comprehensive and over	all picture of the				
	Original resolution proposal												
	Resolution comment		of such a set of docu			h. This comment	could be raised to	o the ESI group.					
	Resolution text	No change. This	s comment could be	raised to the ES	SI 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		ed to introduce some y and the ones incluc					ing and path constraints cy Report".	s) included in the
	Original resolution proposal								
	Resolution	This is a topic th	nat falls out of the sco	pe of TS 101 7	'33, whose pur	oose is to specify	formats for advar	nced electronic signature	es. Relationship
	comment							tails within the Signatur	e Policy Report or other atures.
	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 Sigr	naturePolicyID signed	attribute option	nal and without	the NULL value.			
	Original resolution proposal								
	Resolution comment	This suggestion	has been already ap	plied in the nev	w 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 Sigr	hingTime signed attrib	oute optional.			·	· · · · ·	·
	Original resolution								
	proposal								
	Resolution comment	This suggestion	has been already ap	plied in the nev	w 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 con	cept (as an exte	rnal trusted tim	e indication, see I	ES-Cbis).						
	Original resolution proposal												
	Resolution comment	on usage of tim	e-stamps for archiva	al electronic forn	ns. Usage of tin	ne-mark for achie	ving long term sig	natures would rely on s	ver the current TS focus ecure archival 1 733 could certainly be				
	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				
FS101733-011	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	already applied	1.5.1				
	Comment text Original resolution	ES as the minir	num mandatory forn	nat.									
	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.	No change.										
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
S101733-012	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change					
	Comment text	Signature polic	y: introducing the mi	nimum mandato	bry format for a	specific application	n as an additiona	l rule.					
	Original resolution proposal												
	Resolution comment	include means identifying attrib defined. This is Committee of C	for specifying the "m outes required within a topic that next ver DASIS is currently de tocol will likely include	ninimum" ES form the signature, a rsions of signatu ealing with the p	mat that an app although it woul ire policy report roduction of a p	lication should ac d be worth to spe s should deal with protocol for reques	cept as valid? If s cify shorter mech n. As a quotation: sting generation a	w part of a signature pol o, the Signature Policy anisms to mandate spec the Digital Signature Se nd validation to a server ms that are the XML co	includes means for cific ES forms already ervices Technical of different XAdES				
	Resolution text	To be managed	d 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 d annex.	ocument structure: a	better separati	on between the	mandatory and c	ptional formats; r		hats from the body to an
	Original resolution proposal								
	Resolution comment	This suggestion	has been already ap	plied in the nev	w 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		ocument structure: de r the XML version of f			al definition about	t Signature Polici	es from TS 101 733 and	I putting it into a specific
	Original resolution proposal								
	Resolution comment	This suggestion	has been already ap	plied in the nev	w 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		dditional explanatory of ould be a new version			ESSI deliverables	s EESSI, from a f	unctional perspective ar	nd from a new reader
	Original resolution proposal								
	Resolution comment	·	of such a set of docu		-	n. This comment of	could be raised to	o the ESI group.	
	Resolution text	No change. Thi	s comment could be r	aised to the ES	SI 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	TS 101 733 wo	uld be a valuable outo	ome. This com	ment could be			processes for ES forms	s specified in				
	Resolution text	No change. This	s comment could be r	aised to the ES	SI 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 Original							en and electronic signa without signature policie					
	resolution proposal												
	Resolution comment	one environmer does it deal with signatures? As a quotation, traditionally han	t 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	Rationale: Som	e comments regardin	g EESSI Signa	ture Policy				•
	text	Author: Japan (Computer Research, 2	2003/02/17	-				
		Scope and Intro	oduction						
								ctronic signature forma	
								ne of the most distinct f	
						er is that the policy	information issue	es in general can be reg	garded as one of the
			milestones in the futu						
									ponding public key, and
								tion as a means to valid	
									attachment of policy to
					eptance. It has	to be said, in this	sense, that one c	of the most distinguishin	ig characteristics of
			introduction of signat					ana than these ana ifi	
								ases than those specifi ure, it is expected that a	
									actical contexts are felt,
									nity whose shared aim is
			ble online transaction						ity whose shared aim is
									tically perceived at that.
								gainst this, especially to	
									nd this may be thought
								nent of some particular	
								that point of time and	
								hough not always explic	
		Comments	J	· · · · · · · · · · · · · · · · · · ·		5	····, ···,		
			dated reference to po	licv. In the data	a structure, sian	ature policy identi	fier is made mand	datory [ESF; 8.9.1]. This	s can mean either that:
									(b) signature policy can
			e. dummy and intentic						
								process at each instar	nt. I.e. the action of
		validatio	n of a signature is det	ermined by the	signing of it at	the time when the	alatter took place	, so that the temporal m	edium between the two
		actions is	s made frozen. In par	ticular, this allo	ws the users to	preserve unaltere	ed the state and q	uality of signature relat	ively long time.
		(b) In this ca	ase, the content of the	policy can be	determined at t	he time of the vali	dation. Binding be	etween the signature ar	nd validation is
		principal	ly the responsibility of	policy source	(policy issuer o	r TSP), and the de	etermination of ac	tual policy content is lef	ft to the latter, and the
		issuance	e can be protracted to	the time of the	delivery.				
			ce, hybrid case is the						
								n the policy source to ta	
								ning process is designed	
								er would surely have to	
									sh, and would probably
								of policy qualifiers only.	Which in turn would
		mear	n that it is desired that	policy qualifie	r carry validity o	lates or some sort	of a recommend	ed best before.	

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
		 which exam within 2. On policy da be obtained [ESF] does r perhaps mea similar speci these protoc a) In Gener consider meant to b) SAML. B messagir informatic computer intended taking int type can c) XACML. language this, how remark o d) Web Ser There are synergy of services policy qu 3. On policy proterms of the mechanism which, for ex Further, sign attached ext TC does). For the service of t	her reason why it is im a signature data is to here of the signature data at the intersection of the signature data at the or content. The dest from the policy source hot specify the policy source hot specify the policy source han that not only its dat fication activities alon hols to the purpose of al. These protocols at the use of [XAdES] in be "[XAdES]", when ey this, we mean to ut ing protocol be SAML on. This security infor r) that has an identity which is really the ro- to account that promu- act as an "external po- Although termed as " e for expressing secur- ever, we believe that n this.) vices Policy Framewore otection. The mechan hash calculation of th (although only implicity cample, policy source nature policy doesn"t serially. We believe, to	be attached, or policy mechan nd that outside sign of [ESF] h e the reference content: "The p ta structure but g these lines in obtaining policy re specified in t instead of [ESF] ever the approp lise SAML sect request/respor mation is expre- in some securi- de of public key lgation of SAML Access Contro- ity policy' ([XAG one has to mal ork. Similar to a ons as to how [] for the reason he might think of encing). We fee ism for policy p e policy identifit t, cf. [ESF; 11.1 refers to anoth seem to carry it o complement ay arise possib	he might want to hisms (cf. item 2 it, are identical as that, accordi- to which is emi- precise content of also the protoc- nclude [SAML], y content for the erms of XML, w , to level the ne- priateness of the urity assertions ase. [SAMLCore essed in the forr ty domain". In co- v certificate as ti L is rapidly in p , to the contrary I Markup Langu CML]). It is in the ke a careful arc policability of X (XACML] and [In that semantics of applying secu- el that this certai protection is pro- tier. Also, bindin I]). This may no- er policy sources sown signature this, that signing le semantic am	or have to place below). Practicall but not necessar ing to the needs of bedded explicitly in of a signature polition of through which in [XACML], and [WS E[ESF] signature of thile [ESF] data st tworking layer correct explicitly content. I states that SAM in of assertions ab order to fit exactly the common sense lace. Whereas, or the common sense lace of the policy south the sof XACML is mo or SOAP messag inly is a potential. vided by the author of the policy south to offer enough level e explicitly, which is of signature policio biguities between	policy related info y, this could perh ily. the singing party n the signature da cy is not mandate t is obtained are I S-Policy]. We will data here: ructure is defined isistent. Similarly, s, without explicitly Which would me L "is an XML-base out subject, wher into this description has it presently. the other hand, we on of XACML der ML might just be ration to cohere the more restricted can regeneral in nature ing in the form of entication of policy ince and actual policy in seems to be case means, if it is to b cy has to be desc "signature policy"	and relying party, policities at a in the form of mand of by the present docur eft to the decision of po- examine briefly the po- in terms of ASN.1. So in the following, the re- y mentioned each time an that policy source b- ed framework for excha- e a subject is an entity on, signature ought to r However, the practical we believe that the sign ives from 'a pressing n suitable as the policy is the two semantically. (S ontext of the web services in practice. Here we we re. To add, in conjunct Web Services Security y source ([ESF; 6.11]). blicy seems to be render a complex distributed a with [SAML] in coop e signed, the signature	gnature data, for ro policy identifiers, that cy data or content can latory policy identifier. ment". This could olicy source. Existing ssibility of applying it would be natural to efference "[ESF]" is e SAML authority, anging security (either human or represent the "entity" so consideration ensues nature policy of [ESF] eed for a common anguage for [ESF]. For ee item 5 for a brief ces interoperability. yould rather insist on the ion with the overall web y, for the signature The latter is rendered in ered by the same d policy environment in eration with [XACML]). e data are to be normatively (as XACML

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	examined cl signature po couple of fra a) On Rules especial we could b) On Exter embeddi good ide 5. On interoper information f configuring t protocols or References [ESF] [RFC3280] [SAMLCore] [XACML] [XAdES]	e policy data structure osely. The primary on olicy format has to add agmental comments: s. The terminology em ly when compared with a not have identified the nsions. In practice, we ing signatures or other a to specify what insta- rability with XACML. It for establishing secure- the application domain	e being its pos ress either pos ployed, "Comm h other standar e relevant pase believe that he validation data ances of extens is often expec e transactions. of signature p ectronic Signature Key Infrastruct col for the OAS cess Control M L Advance Ele	ition with respect sible interopera- non Rules" ([ES rds. It is suspect sages in the spect a for further pro- sions should be ted that XACMI It is to this exter- olicy, regardles ure Formats". rure Certificate a SIS Security Ass arkup Languag ectronic Signatu	ct to other policy a ability with or defin SF; 11.3]) and "Co ted that this was in ecification. SignPolExtensions tection depending expected as rend will fill in the gap nt that we feel polis of whether trans	ssertions mention itive differentiation mmitment Rules" intentionally chose ([ESF; 11.11]) ar on the circumsta ered in RFC 3280 where it is curren icy framework of 2 action of the latte	ntly lacking the means XACML should be take or takes place through a	, we feel that [ESF] ndards. Here are a o be rather awkward pplication in mind, but table, for example in feel that it would be a to proffer semantic n into account in
	Resolution comment	the algorithm or stamping. What		he signature po ntifier does is t	blicy identifier de to fix rules that t	bes not protect the he verifier has to	e signature): this h follow to validate	has to be achieved by o	e relatively long time (if other means, like time-
	Resolution text	No change.			Cignaturer Olle				

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	RevocationValu crlVals ocspVals	nd 76: "OPTIONAL" s les ::= SEQUENCE { [0] SEQUENCE OF [1] SEQUENCE OF [2] OtherRevVals **	CertificateList C BasicOCSPRes) PTIONAL		ked ****.						
	Original resolution proposal	"OPTIONAL" sh	nould be described af	ter [2] OtherRe	vVals 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	some of the key		ert path can be	compromised.			fier has access to all the where verifier HAS NO					
	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	which is presen						sm that allows dynamic	policy referencing,				
	Original resolution proposal		•			· · · · · · · · · · · · · · · · · · ·							
	Resolution comment	 b) Further clari c) If there is an certainly not) Further clarification is requested regarding what is meant by "a mechanism that allows dynamic policy referencing";										
	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 Original	As a part of the	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.										
	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.											
Commont ID	Deliverable	Delbuereble		Commont	Comment	Decelution	Decelution	Resolution status	Doliverable terret				
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	type	Resolution source	Resolution date	Resolution status	Deliverable target version				
TS101733-023			contribution					no change	<u> </u>				
	version	clause 11.11 As the use case	contribution reference JCPKI-002	date 17/02/2003 ature policy ex	type technical tension is deem	source STF242 ned to increase, it	date 21/06/2003		version				
	version 1.3.1 Comment text Original resolution	clause 11.11 As the use case	contribution reference JCPKI-002 demand for the sign	date 17/02/2003 ature policy ex	type technical tension is deem	source STF242 ned to increase, it	date 21/06/2003	no change	version				
	version 1.3.1 Comment text Original	clause 11.11 As the use case instances as ha We share the a	contribution reference JCPKI-002 e demand for the sign is been done in X.509 uthor's view of that as	date 17/02/2003 ature policy ex certificate pro	type technical tension is deen file standard (R	source STF242 ned to increase, it FC 3280).	date 21/06/2003 would be nice to tensions will appe	no change have a concrete specific ear. Nevertheless, we ar	version				
	version 1.3.1 Comment text Original resolution proposal	clause 11.11 As the use case instances as ha We share the a	contribution reference JCPKI-002 e demand for the sign is been done in X.509	date 17/02/2003 ature policy ex certificate pro	type technical tension is deen file standard (R	source STF242 ned to increase, it FC 3280).	date 21/06/2003 would be nice to tensions will appe	no change have a concrete specific ear. Nevertheless, we ar	version				

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	n" may be a spelling r	mistake for "CR	L 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 claus	e title "Timestamping	for long life of	signature".	·	·		
	Original resolution proposal								
	comment	Will be correcte	d in next release.						
	Resolution text								

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution reference	date	type	source	date		version
TS101733-026	1.4.0	10.4	OTHER-009		technical	STF242	25/01/2004	already applied	1.5.1
	Comment text	attributes are no unsigned attribu The following ob id-aa-ets-archivu us(840) rsadsi(1 Archive timestan ArchiveTimeStan The value of me value) of the foll (a list of 11 diffe For further infor	ot present these attrib te. Several instances bject identifier identifie eTimestamp OBJECT 113549) pkcs(1) pkcs mp attribute values ha mpToken ::= TimeSta essageImprint field with lowing data objects as erent attributes follows mation and definition should be created usi	utes shall be a of this attribute s the Nested A DENTIFIER 9(9) smime(16 ave the ASN.1 ampToken thin TimeStamp of TimeStamp	dded to the ele e may occur wit Archive Timesta ::= { iso(1) mem 5) id-aa(2) 27} syntax Archive pToken shall be e electronic sign Token see clau	nd the entire elect ctronic signature p h an electronic signature p imp attribute: ber-body(2) TimeStampToken e a hash of the col ature: se 10.4.	prior to the timesta gnature both over	the Certificate values a imp. The Archive Time time and from different (without the type or le	TSAs.
	Original		•						
	resolution proposal								
	Resolution	This section has	s been re-written in th	e current versi	on.				
	comment								
	Resolution								
	text								

5.3 TS 101 861 - Time stamping profile

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
			reference						
TS101861-001	1.2.1	5.1.2	JCPKI-004	17/02/2003	editorial	STF242	21/06/2003	in process	
	Comment	Please add "On	e of" to the beginning	of the sentenc	e, because the	sentence uses "m	nust".		
	text								
	Original	Please add "On	e of" to the beginning	of the sentenc	e, because the	sentence uses "m	nust"		
	resolution								
	proposal								
	Resolution	Noted to be con	sidered for next revision	on.					
	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
TS101861-002	1.2.1	5.2.3	JCPKI-004	17/02/2003	editorial	STF242	21/06/2003	in process	
	Comment text		e of" to the beginning						
	Original resolution proposal	Please add "On	e of" to the beginning	g of the sentend	ce, because the	sentence uses "I	must".		
	Resolution comment	Noted to be cor	nsidered for next revis	sion.					
	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	
	text Original resolution proposal Resolution comment Resolution text		ppropriate for commo		· · · · · · · · · · · · · · · · · · ·				
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	 "a genTime a minimum 	rently includes the rec parameter limited to accuracy of one seco of the first requireme	represent time nd is required;'	I Contraction of the second	•	sentation of better	accuracy than 1 second	l is not allowed.
	Original resolution proposal		e parameter shall be Il be to the accuracy			l 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	What is the real provide ordering	parameter missing of son for not allowing c			vide this service.	Surely, all that th	e aim is to not make it n	nandatory for TSAs to					
	Original resolution proposal Resolution	Delete item.												
	comment Resolution	comment												
	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		t 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	It not explicit as	to which algorithm ic	dentifier this refe	ers to. Presume	ably, this is Hash	Algorithm in Mes	sageImprint.						
	text	It is not commo	n practice for "NULL"	' to be explicitly	included in the	algorithms param	eters. Why not a	llow the parameters to b	e non-present.					
	Original	Update as indic												
	resolution		dentifier parameters											
	proposal		s should accept SHA s should generate SH					parameters.						
	Resolution													
	1													
	comment Resolution													

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		UNSTT-005		editorial	STF242	09/01/2004	applied	1.3.1			
	Comment text	Since TS 101 8 TS version.	62 has been publishe	d, RFC 2459 h	as been replac	ed by RFC 3280.	Thus it is sugges	ted to accordingly modif	y reference in the next			
	Original resolution proposal	Modify the refer	ence to RFC 2459 int	to RFC 3280.								
	Resolution Done as per proposed resolution. comment											
	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				
	text	TS 101 862 spe said about the O b) Additionally, organization From the above "The name of th 1) a country na established; 2) the organiza If one CSP sets contains the ser organizationalU	CSP Identifier. It is the since one single CSF s or for issuing qualifi comments stems the e issuer contained in me stored in the cour tionName attribute sp up different CAs, eac ialNumber attribute w	of the issuer (cl erefore herewith P may set up di ed certificates e following prop the issuer field htryName attrib pecifying the re ch one specific vith a value whi specify further of	ause 4.1): "MU h proposed the ifferent Certifica with some diffe bosed amendme d (as defined in bute. The specif levant CSP ide to issue a diffe ich SHALL be u details of the sp	ST contain a cour organizationNam ation Authorities (e rent extensions) i ent to clause 4.1 t clause 3.1.1 in RI ied country SHAL ntifier. rent qualified certi nique for each C/ ecific CA."	ntry name stored e attribute to be a e.g. for issuing qu it is proposed that text: FC 3039) MUST o L be the country ificate type, it is a A within the same	alified certificates on be an attribute is used to in contain: in which the issuer of the Iso RECOMMENDED th CSP. Optionally, the CS	half of different client dentify the single CA. e certificate is nat the issuer field			
	Original resolution proposal	 a country na established; the organiza If one CSP sets contains the ser 	tionName attribute sp up different CAs, ead	ntryName attrib becifying the re ch one specific <i>i</i> ith a value whi	bute. The specil levant CSP ide to issue a diffe ich SHALL be u	ied country SHAL ntifier. rent qualified certi nique for each C/	L be the country ificate type, it is a	contain: in which the issuer of the Iso RECOMMENDED th CSP. Optionally, the CS	nat the issuer field			
	Resolution comment				02 280, X.509 \	7.3 Certificate Pro	file for Certificates	s Issued to Natural Pers	ons.			
	Resolution text	No change to 1	S 101 862, see TS 10	12 280.								

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		UNSTT-005		technical	STF242	09/01/2004	no change				
	Comment text	the identity of th - Date of birth - Place of Birth - Gender - Country of C For this reason	nat person". In order t h Citizenship it is suggested that ir ENDED in TS 101 86	o "confirm the i sertion in subje	dentity" of the sectDirectoryAttr	igner the followin butes of the corre	g data are comm	ature verification data to only deemed necessary es, as listed in RFC 303 " (Directive Annex I, ite	and used: 9 clause 3.2.1, is at			
	Original resolution proposal	4.2.1 Identity r (NOTE: Renu In order to provi not sufficient. A It is therefore R - dateOfBirth; - placeOfBirth - gender; - countryOfCi Where necessa	umbering of the subsected ide reliable information ctually the following of ECOMMENDED that n;	equent clauses on on the qualifi lata are commo a subject's cer idence field MA	is required.) ed certificate su only deemed ne tificate bears at tificate bears at	cessary: date of k least the followin	birth, place of birth g fields in the sub	irective [1] definition of a n, gender, country of citi ojectDirectoryAttributes a	zenship.			
	Resolution comment	Specific naming requirements incorporated in TS 102 280 - X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons No change to TS 101 862, see TS 102 280.										
	Resolution text											
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	carry the pseud defined. In fact could be misinte MUST be insert	onym. This could lead a fictitious name like erpreted as being a "r red in the "pseudonym	d to misunders "John Doe" rec real" name. To	tandings, even orded in the "co	malicious ones, if ommonName" and	a commonly agred	commonName" or "pset eed manner to identify p ate and place of birth, g ement in TS 101 862 [6]	seudonyms is not ender and citizenship,			
	Original resolution proposal	4.3.1 Pseudor In order to avoid is to hold the su		he pseudonym	NOT b	e held in the "con	nmonName" attrib	attribute SHALL be used bute.	I when the subject field			
	Resolution comment	Specific naming	requirements incorp	orated in TS 10				es Issued to Natural Pers	sons.			
	Resolution text	No change to T	S 101 862, see TS 10	02 280.								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
FS101862-005	1.2.1	4.3.2	UNSTT-005		technical	STF242	09/01/2004	no change					
	Comment text	happen to share born in the sam subject field. Th such identifier a sufficient to res subject. A printa When the "pseu	e the same surname a e place on the same his field, SHALL hold a and where necessary olve any subject name ableString character s udonym" attribute is us	and quite a few day. Therefore at least "an ider to comply with e collisions", ea separator (e.g. ' sed, a fictitious	v of them have f it is suggested ntifier assigned RFC 3039 follo ach CA SHALL "/") could be us	he same given na that TS 101 862 a by a government wing sentence: "If add a code it assi ed between the tw	me too, so it is po at least MANDAT or civil authority", is the CA's respo gns itself, which s o data. As an exa	ES usage of the serialN as per RFC 3039, clau onsibility to ensure that SHALL be unique for ea ample: "RGGFNC42H30	ns with the same name umber attribute in the se 3.1.2. In addition to the serialNumber is ch certificate of that DA952P/0001".				
	Original resolution proposal												
	Resolution comment		Specific naming requirements incorporated in TS 102 280 - X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons. No change to TS 101 862, see TS 102 280.										
	Resolution text	No change to T											
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
FS101862-006	1.2.1	4.4	UNSTT-005		technical	STF242	09/01/2004	no change					
	Comment text	combined with a In order to settle Additionally, sin digitalSignature It is also sugges repudiation and	here 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 ombined with any other key usage, i.e. if set, the key usage non-repudiation SHOULD be set exclusively." order to settle it, it is suggested to mandate the unique use of the non-repudiation bit into TS 101 862. dditionally, since also authentication certificates can be "qualified certificates", it is suggested to add the following statement: "Should the key usage gitalSignature bit be asserted, the RFC 3280 provisions SHALL be complied with." is also suggested that TS 101 862 mandates the keyUsage extension to be marked critical, to avoid any possible malicious misuse of the non- pudiation and of the authentication certificates.										
	Original resolution proposal	If the key usage SHALL be set e Should, instead The keyUsage		s asserted ther ISignature bit t marked critical	be asserted, the to avoid possib	RFC 3280 provis le malicious misus	ions SHALL be c se of different cer		usage non-repudiation				
	Resolution comment	Specific key us	age requirements inco	orporated in TS				ates Issued to Natural F	Persons.				
	Resolution text	No change to T	S 101 862, see TS 10	02 280.									

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	TS 101 862, we	do not have a CRL p	orofile in any of	the deliverable			a qualified certificate p at could impede interwo					
	Original resolution proposal		dressed by CEN ISSS	-	•								
	Resolution comment		nis 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 usa	age requirements inco	prporated in TS	5 102 280 - X.50	9 V.3 Certificate	Profile for Certific	ates Issued to Natural F	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
<u>TS101862-009</u>	1.2.1 Comment text	TS 101 456 def a) QCP public A certific b) QCP public: A certific TS 101 862 def An Identifier of 1 country under w esi4-qcStatem BY id-etsi-qcs This statem certificate i Annex I an and of the for electror specified ir id-etsi-qcs-QcC TS 101 862 doe Signature, it mu itu-t(0) identified but not when sin It is thus reques	ance team of TS 101 ines: + SSCD: itu-t(0) iden rate policy for qualified itu-t(0) identified-org cate policy for qualified ines id-etsi-qcs-QcCc the statement (repres which law the issuer is nent-1 QC-STATEME s-QcCompliance } nent is a statement by s issued as a Qualified d II of the Directive 19 Council of 13 Deceminant is signatures, as imported in the issuer field of this compliance OBJEC es not permit to make ust be known that an s d-organization(4) etsited age would be that the	862. tified-organizat d certificates is: anization(4) ets ed certificates is: anization(4) ets ed certificates is popliance: ented by an OI s operating. TI IDENTI the issuer that ed certificate ac 999/93/EC of the ber 1999 on a OI lemented in the s certificate. CT IDENTIFIER the same disting SSCD has been (0)qualified-cer ement extension tional QCstater	ion(4) etsi(0) qu sued to the pub si(0)qualified-ce ssued to the pub D), stating that TIFIED t this cording te European Pa Community fran a law of the cou the ise of the cou the sed. This tificate-policies(n. nent equivalent	alified-certificate lic, requiring use rtificate-policies(blic. the certificate is i rliament nework ntry s 1 } 1 456. In particul can currently onl 1456)policy-iden to the "QCP pub	-policies(1456) po of secure signatu 1456)policy-identi issued according ar if a verifier war by be checked whe tifiers(1) qcp-publ	blicy-identifiers(1) qcp-p ire-creation devices. fiers(1) qcp-public (2) to the EU-Directive [1], a to the EU-Directive [1], a to the following CP OID	ublic-with-sscd (1). as implemented in the e signature is a Qualified t is being used:
		NOTE: The r	rest of the mail excha	nge has been r	emoved for priv	/acy.			
	Original resolution proposal								
	Resolution comment		nent for SSCD added	to TS 101 862.					
	Resolution text	See TS 101 862	2 V1.3.1.						

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

	liverable /ersion	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
101903-001 1.1.1	.1		JCPKI-003	17/02/2003	Technical	STF242	25/01/2004	no change	
Cor	omment text	Author: Japan O Scope and Intro The purpose of and [XAdES]. T specification se most important It is now routine often if not all th accompanying of signature hasn't [ESF] lies in its However, we ar certificates. To the signature point and this natural to promote flexi "Policy" has lon The underlying individual ought of as what the " words, it should feasible Policy F Comments 1. On the many (a) every signature null (i.e. (a) This cas	JCPKI-003 e comments regardin. Computer Research, 2 oduction the present document here are at least two ems to be incorporation milestones in the future to standardize the emperiment object is well exemplified ty et gained the rank of introduction of signature the time, together with object is well exemplified ty et gained the rank of introduction of signature the time that the polic be more precise, due oblicy is far more broad ly leads to the necess ble online transaction g been traditionally as principle of certificate to possess his or here signature policy" might suggest a way to col Knowledge Interactivity dated reference to po gnature MUST have a e. dummy and intention e means that validation	g EESSI Signa 2003/02/17 It is to convey s obvious reasor on of signature re evolution of ncapsulation of its certificate o ried in the polic of common acc ure policy. y as proposed to more loose lly ranged com sity of taking int s (valued or oth sociated, one policy closely r own policy, is nt envisage, for lect disseminat ty. It is in this sp non-trivial sign ponally empty) sion process refe	ture Policy ture Policy some comment is to focus on t policy; the oth- e-business. signature data r certificate cha y attributes of eptance. It has in [ESF] can ha semantic const pared to certific o account othe nerwise) while a way or another follows this, ess a picture in wh signature mar ed policies in c pirit that the fol a structure, sign tature policy av gnature policy av gnature policy av	s upon the policy his particular topic er is that the polic and a number o an. That policy inf (.509 certificate p to be said, in this ave contextually e traints associated cate policy. Accord r policy related de approximating reli c, with the idea of sentially due to th ich many policies ks each spatial ar order to proffer a c lowing comments nature policy ident railable for retrieva in the case so de citly made depend	aspects of the ele c: the one is that of cy information issue of these formats bi- formation can func- profile. Nevertheles s sense, that one of with digital signal dingly, needs to a evelopment efforts iability of real work authority, predom te way it is bred. A dynamically inter ad temporal linear decision suitable to a re delivered, alt tifier is made man al in association w sired: dent on the signing	ectronic signature formation one of the most distinct in the sin general can be re- nd signature with correst ction as a means to value ss, it has to be said that of the most distinguishin cases than those specific ture, it is expected that a ddress wider area of pro- s in the Internet communi- d experience. inantly centrally and stat gainst this, especially to act to form the whole. A nent of some particular to that point of time and hough not always explice datory [ESF; 8.9.1]. Thi	teatures of the garded as one of the sponding public key, and date status of attachment of policy to ing characteristics of it to that for public key application domain of actical contexts are felt, nity whose shared aim is actically perceived at that. To the extent that each and this may be thought present event. In other space, a way to make sit. s can mean either that: (b) signature policy can int. I.e. the action of

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
		 (i) Performer (ii) Performer (iii) Another (iiii) Another (iii) Another (iii)	ce, hybrid case is the primance wise, a pract of the signature gene metic operations than ests in a second. All the in that policy content be in that it is desired that her reason why it is ir in high signature data is to inple using some othe in the signature data is to inple using some othe in the signature data is to inple using some othe in the signature data as at or content. The de from the policy source not specify the policy an that not only its da ification activities alor cols to the purpose of ral. These protocols a the use of [XAdES] i obe "[XAdES]", when By this, we mean to ut ing protocol be SAML ion. This security info er) that has an identity i, which is really the re to account that promu- act as an "external p Although termed as e for expressing secu- vever, we believe that on this.) rvices Policy Framew e on-going investigat of [ESF] with [XACMI security standards, cu- ueries (including refer- rotection. The mechar hash calculation of th (although only implici- xample, policy source- nature policy doesn"t ternally. We believe, f	tical computing eration. This is e validation proc his would imply be left empty an t policy qualifier mportant to allow be attached, or r policy mechar and that outside esign of [ESF] h the the reference content: "The p ata structure but ng these lines in obtaining policy are specified in t instead of [ESF] ever the approp- tilise SAML secu- request/respor rmation is expre- vin some securi- ole of public key ulgation of SAML bolicy" for SAML "Access Contro rity policy ([XAG to one has to mal- ork. Similar to a ions as to how [L] for the reason one might think of encing). We fee hism for policy p the policy identifi- it, cf. [ESF; 11.1 erefers to anoth seem to carry it to complement hay arise possib	platform wants specially so in ess. Also, appli that signature d signer decide carry validity of wempty policy he might want to isms (cf. item 2 it, are identical as that, according to which is em- precise content also the protoco- nclude [SAML], y content for the erms of XML, we have a content for the erms of XML, we cartificate as the protocoment. In of content for the content for the content for the pristeness of the unity assertions ase. [SAMLCord essed in the for ty domain". In of content for the content for the content for the content of applying sector of applying sector of applying sector of that this certa protection is pro- ter. Also, bindin []). This may no er policy sources own signature this, that signin le semantic am	to avoid actual co view that, for some cations serving as policy may be cac is its policy related lates or some sort content at the time or have to place below). Practical , but not necessar ing to the needs or bedded explicitly i of a signature polic col through which [XACML], and [W e [ESF] signature while [ESF] data st etworking layer con e context demands as policy content. e) states that SAM m of assertions ab order to fit exactly he common sense lace. Whereas, or y. age", the motivati is sense that XAC hitectural conside "ACML, but with a WS-Policy] can be s of XACML is mo ure SOAP message inly is a potential. wided by the author g of the policy sou of the policy sou of the policy sou of signature poli biguities between	e algorithms, sign s a service provide hed until the time action in terms of of a recommende e of signing is that policy related info ly, this could perh rily. f the singing party n the signature da cy is not mandate it is obtained are S-Policy]. We will data here: rructure is defined insistent. Similarly s, without explicit Which would me L "is an XML-bas pout subject, when into this description has it presently. In the other hand, on of XACML der CML might just be ration to cohere the more restricted c e made consistent re general in nature ging in the form of entication of polic urce and actual polic of protection, for n seems to be desc "signature policy"	of policy qualifiers only. ed best before. t, in encapsulating a tra- brmation outside the sig- aps mean often that two y and relying party, poli- ata in the form of mand- ed by the present docur- left to the decision of pr- examine briefly the po- the terms of ASN.1. So , in the following, the re- y mentioned each time an that policy source b- ed framework for excha- re a subject is an entity on, signature ought to r However, the practical we believe that the sign tives from 'a pressing n suitable as the policy I he two semantically. (S ontext of the web servi- t in practice. Here we w ure. To add, in conjunct Web Services Security y source ([ESF; 6.11]). blicy seems to be rende- or a complex distributed se with [SAML] in coop- pe signed, the signature	d more costly in process hundreds of sh, and would probably Which in turn would ansaction message in gnature data, for to policy identifiers, that cy data or content can latory policy identifier. ment". This could olicy source. Existing ssibility of applying it would be natural to afference "[ESF]" is e SAML authority, anging security (either human or represent the "entity" so consideration ensues nature policy of [ESF] eed for a common anguage for [ESF]. For ee item 5 for a brief ces interoperability. yould rather insist on the ion with the overall web y, for the signature The latter is rendered in ered by the same d policy environment in eration with [XACML]). e data are to be normatively (as XACML

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	examined cl signature po couple of fra a) On Rules especiall we could b) On Exter embeddi good ide 5. On interoper information f	osely. The primary on licy format has to add gmental comments: s. The terminology em y when compared wit not have identified th sions. In practice, we ng signatures or othe a to specify what insta- rability with XACML. If for establishing secure he application domain	e being its pos lress either pos hployed, "Comr h other standau e relevant pass believe that he r validation data ances of extens t is often expect e transactions. n of signature p Electronic Signature cocl for the OA ccess Control I (ML Advance E	ition with respensible interopera- spible interopera- non Rules" ([ES rds. It is suspect sages in the spice eavy usage of S a for further pro- sions should be ted that XACMI It is to this exter- bolicy, regardles ature Formats". cture Certificate SIS Security As Markup Langua	ct to other policy a ability with or defin (F; 11.3]) and "Co ted that this was in ecification. SignPolExtensions tection depending expected as rend will fill in the gap not that we feel pol s of whether trans and Certificate R sertion Markup Li ge (XACML).	evocation List (CI	e expected to be inevi nces (see item 3). We). htly lacking the means XACML should be take tr takes place through a RL) Profile.	, we feel that [ESF] ndards. Here are a o be rather awkward pplication in mind, but table, for example in feel that it would be a to proffer semantic on into account in
	Resolution comment	the algorithm or stamping. What		he signature po entifier does is t	blicy identifier de to fix rules that t	bes not protect the he verifier has to	e signature): this I follow to validate	has to be achieved by o	e relatively long time (if other means, like time-
	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		tamp seems unneces deleted to avoid being			S-X-L is enough.			
	Original resolution proposal								
	Resolution comment	AND some of th		the cert path ca	an be comprom			verifier has access to a ronments where verifier	
	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	worldly policy st	andards, like SAML, 2 would be preferable (XACML, WS-S	ecurity, are spe	cified at the same	processing layer	erms of XML, when con using XML. vestigate its practicable	
	Original resolution proposal								
	Resolution comment	the developmen		0			atives on the field	s where it develops its o	documents. And indeed
	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	year. Relative to Japa XadES matches To diffuse the u Some errors are	an e-Government, Ele s well than ASN.1 bas se of XadES, test pro e pointed out in some	ectronic applica sed TS 101 733 ograms for inter parts of XadE	tions are speci from the point operability sho S schema so th	fied to be XML ba of view of long te uld be implemente at bug information	sed documents a erm signature save ed. n should be opene	ming a similar use of CN nd XML signature will b e. ed to public promptly. SIS standard formulatior	e in use. In this case,
	Original resolution proposal								
	Resolution comment	Dealing where on number of tests	for facilitating develo	ons are being opments of such orking on main	developed and n tools.	interoperability ar	-	ng assessed. The group e a report on all outstan	
	Resolution text								

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
			reference						
TS101903-005	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment		6.2 of the XAdES sp						
	text						onse. The <enca< td=""><td>psulatedOCSPValue> e</td><td>element contains the</td></enca<>	psulatedOCSPValue> e	element contains the
		base64 encodir	ng of a DER-encoded	OCSP Respor	se. [1, clause 7	.6.2]			
									ters in terms of what the
	1								s have just included the
							efined in RFC 25	60 [21]). Therefore, the	specification should be
	Original		out what to include i					· · · · · · ·	
	Original					onse is not neede	d to be archived,	it was first suggested to	o include the
	-		sponse. The different			ovided by the OC		n integer volue indicatio	a if the request was
	proposal							n integer value indicatir	nost likely. On the other
									refore, any other OCSP
									response containing a
			ponse type will have						response containing a
							nclude an additio	nal object identifier indi	cating the type of the
									ne arguments apply, as
		for the OCS	PResponse stated in	the paragraph	above.		-	•	
		- BasicOCSP	Response: The Basi	cOCSPRespons	se contains exac	ctly the data that i	needs to be archi	ved and corresponds to	the information
			the <ocspref> ele</ocspref>						
					lesponse, since	this is basically v	what the standard	s said, and furthermore	the only deployed
		implementation	in Estonia uses that	interpretation.					
	Resolution								
	comment								
	Resolution								
	text								

	version	clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
S101903-006 1.	.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	 While it is eastored in the exactly on the time-star For the <aiii composed="" difficult="" li="" or="" prin).<="" the=""> Remarks The input for the elements have provided URI in element of the element of the element of the element of the signature. That he input for the current ver definition of the The <signature <hashdatal="" a="" application="" he="" of="" signature="" signature.="" td="" that="" the="" the<="" uri="" verified="" verifying=""><td>ption on of the <timestam asy to verify the time e time-stamp, it is diff- ne data that is claimed nped. DataObjectsTimeSta hat resolve to exactly robably infeasible to e different time-stam to be processed acc the URI-attribute of <hashdatainfo> eler sform at all) is a nod of all the included < or the time-stamp. Th sion of XAdES speci <signaturetimestan TimeStamp> element is, the input for the t itication has to make Info> element results ureValue> element. Th atureValue> element an arbitrary number nd the given transfor > element and analy ructure can have any us, the only practical the specification with the ply create the requir HashDataInfo> element urpose anyway, as h</signaturetimestan </hashdatainfo></timestam </td><td>pType> data typ -stamp by proce ficult, time-consi ed by the XAdES amp>, <individua y the same data compose such a ps used in the co ording to the ref the <hashdatal nent and finally e list. This mear HashDataInfo> hese resulting o fication therefor mp> property it at contains a sin ime-stamp hash sure that the tim is in the data that fhus, the verifyint. of transforms ca ms to the result ze the result. I number of diffe way to verify the he data that res ed input for the tent was introdu has been shown</hashdatal </individua </td><td>be is broken in tressing all <hash uming and poss S specification. alDataObjectsTi as the correspont a reference, bed current XAdES version is that the correspont a reference, bed current XAdES version is concelled by the stat the result elements are the ctets are in fact the mandates which says for instance igle <hashdatai is computation is ne-stamp has be the co</hashdatai </hash </td><th>DataInfo> element ibly even infeasib That is, to verify if meStamp> and the proding <ds:reference trause the result of the result of the result of the result, if the out the result, if the out the result, if the out the information the the result of pro- ter concatenated in the result of pro- ter applied on the the <ds:signature the <ds:signature the <ds:signature the <ds:signature the sto check that the the sto check that the the sto compare the sting the correspon- tion the digest version of a giver</ds:signature </ds:signature </ds:signature </ds:signature </ds:reference </th><td>le in the general of the time-stamp is and experiences in the eds for resolving depend by means of edg forms that are spec- top the last tra- forms that are spec- top edge edge edge forms that are spec- top the last tra- forms that are spec- top the last tra- form the spec- top the last the same the canonicalized proteing edg thashData ralue and compar- top time-stamp in ca</td><td>g the resulting hash valu- case to verify, if the times applied on the elemen stamp> <hashdatainfo> :SignedInfo> do. In the ds on the context (e.g. t shDataInfo> elements. g specificaion [3]. This i ecified by the optional < ansform (or the result of > element is octet data :HashDataInfo> elements ha :SignatureValue> element ment. [1, clause 7.3.1] a. This is, to verify some</hashdatainfo></td><th>e-stamp is applied ts that are claimed to elements have to be general case it is he node it is contained These <hashdatainfo> s, in short, resolving the Transforms> child resolving the URI, if in any case. The r in the document to as to be. In the ent of the XMLDSig ehow that processing mp> for instance, this is a valid representation deduce from the nped is to process the zation has been s to be time-stamped case it would be e in the time-stamp. ambiguous. But it does</hashdatainfo></th></signature></aiii>	ption on of the <timestam asy to verify the time e time-stamp, it is diff- ne data that is claimed nped. DataObjectsTimeSta hat resolve to exactly robably infeasible to e different time-stam to be processed acc the URI-attribute of <hashdatainfo> eler sform at all) is a nod of all the included < or the time-stamp. Th sion of XAdES speci <signaturetimestan TimeStamp> element is, the input for the t itication has to make Info> element results ureValue> element. Th atureValue> element an arbitrary number nd the given transfor > element and analy ructure can have any us, the only practical the specification with the ply create the requir HashDataInfo> element urpose anyway, as h</signaturetimestan </hashdatainfo></timestam 	pType> data typ -stamp by proce ficult, time-consi ed by the XAdES amp>, <individua y the same data compose such a ps used in the co ording to the ref the <hashdatal nent and finally e list. This mear HashDataInfo> hese resulting o fication therefor mp> property it at contains a sin ime-stamp hash sure that the tim is in the data that fhus, the verifyint. of transforms ca ms to the result ze the result. I number of diffe way to verify the he data that res ed input for the tent was introdu has been shown</hashdatal </individua 	be is broken in tressing all <hash uming and poss S specification. alDataObjectsTi as the correspont a reference, bed current XAdES version is that the correspont a reference, bed current XAdES version is concelled by the stat the result elements are the ctets are in fact the mandates which says for instance igle <hashdatai is computation is ne-stamp has be the co</hashdatai </hash 	DataInfo> element ibly even infeasib That is, to verify if meStamp> and the proding <ds:reference trause the result of the result of the result of the result, if the out the result, if the out the result, if the out the information the the result of pro- ter concatenated in the result of pro- ter applied on the the <ds:signature the <ds:signature the <ds:signature the <ds:signature the sto check that the the sto check that the the sto compare the sting the correspon- tion the digest version of a giver</ds:signature </ds:signature </ds:signature </ds:signature </ds:reference 	le in the general of the time-stamp is and experiences in the eds for resolving depend by means of edg forms that are spec- top the last tra- forms that are spec- top edge edge edge forms that are spec- top the last tra- forms that are spec- top the last tra- form the spec- top the last the same the canonicalized proteing edg thashData ralue and compar- top time-stamp in ca	g the resulting hash valu- case to verify, if the times applied on the elemen stamp> <hashdatainfo> :SignedInfo> do. In the ds on the context (e.g. t shDataInfo> elements. g specificaion [3]. This i ecified by the optional < ansform (or the result of > element is octet data :HashDataInfo> elements ha :SignatureValue> element ment. [1, clause 7.3.1] a. This is, to verify some</hashdatainfo>	e-stamp is applied ts that are claimed to elements have to be general case it is he node it is contained These <hashdatainfo> s, in short, resolving the Transforms> child resolving the URI, if in any case. The r in the document to as to be. In the ent of the XMLDSig ehow that processing mp> for instance, this is a valid representation deduce from the nped is to process the zation has been s to be time-stamped case it would be e in the time-stamp. ambiguous. But it does</hashdatainfo>

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	The <timestam <ds:canonicaliz method is speci In the case of in resulting from p identified by the reference proce exactly the sam <xsd:clearent na<br=""><xsd:complexty <xsd:sequences <xsd:element na<br=""><xsd:choice> <xsd:element na<br=""> </xsd:element></xsd:choice></xsd:element></xsd:sequences </xsd:complexty </xsd:clearent></ds:canonicaliz </timestam 	poperability event the approperability event the ationMethod> eleme fied the standard car cluded <ds:reference rocessing the <ds:ref included URI is inclu- ssing model of the X e data as that was us ame="TimeStamp" ty /pe name="TimeStamp" ty /pe name="TimeStamp" ty ef="ds:Canonicalization" ame="EncapsulatedTatedPKIDataType"/> ame="XMLTimeStam" > ype> /pe name="IncludeTy ame="uri" type="xsd: ame="referencedDatatedPatedPatedPatedPatedPatedPatedPate</ds:ref </ds:reference 	ould be redefine nt should indication mices ionicalization mices elements an eferences should ided. If the referent MLDSig specific sed in the comp "pe="TimeStamp npType"> "IncludeType" non Method" min TimeStamp"> np" type="AnyTy /pe"> anyURI" use="r	ed to use an ID the which canor ethod as specif a additional refe d be included. I rencedDataattri cation. The resu utation of the < oType"/> haxOccurs="un Dccurs="0"/>	-list to identify the icalization method ied by the actual > rencedData-attrib f the referencedD bute value is true ilt is then used as ds:Reference> dig	elements that ha d to use for canor KMLDSig specific ute indicates if the ata-attribute is on the <ds:reference input for the time</ds:reference 	ation MUST be used. e <ds:reference> elem</ds:reference>	s. If no canonicalization ent itself or the data alue is false the element d according to the
	Resolution comment		, por						
	Resolution text								

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
T0404000 007				05/04/0004	ta abusia al				
TS101903-007	1.1.1		XAdES-PT-001		technical			not yet processed	
	Comment		meStamp> definition						
	text		eTimeStamp> incluc						
					es> and the <s< th=""><th>ignedDataObjectF</th><th>roperties> canno</th><th>t be composed using II</th><th>D-references, because</th></s<>	ignedDataObjectF	roperties> canno	t be composed using II	D-references, because
			nts do not have an x						
			of the XAdES specifi						
			rchiveTimeStamp> e						
								application of the trans	
		<ds:referen< th=""><th></th><th>y the same as the</th><th>e octet stream i</th><th>nat was originally</th><th>used for comput</th><th>ng the digest value of t</th><th>ne corresponding</th></ds:referen<>		y the same as the	e octet stream i	nat was originally	used for comput	ng the digest value of t	ne corresponding
				or the ads. Signer	linfo> element	The result of appl	ication of the tran	seforme energified in this	HashDataInfo> must
								of the XMLDSIG signat	
			DataInfo> element fo				e signature value		luie.
			DataInfo> element fo						
		-							
		In the first parac	praph it says to inclu	de a <hashdata< th=""><th>Info> element f</th><th>or each <ds:refe< th=""><th>ence> in the XM</th><th>LDSig signature. This o</th><th>bviously includes the</th></ds:refe<></th></hashdata<>	Info> element f	or each <ds:refe< th=""><th>ence> in the XM</th><th>LDSig signature. This o</th><th>bviously includes the</th></ds:refe<>	ence> in the XM	LDSig signature. This o	bviously includes the
								ataInfo> element for the	
								cluded by the reference	
								not be referenced using	
	Original							Properties>. Additionally	
	resolution							the <signedproperites< th=""><th></th></signedproperites<>	
	proposal		ave the <ds:reference< th=""><th></th><th></th><th></th><th></th><th>0</th><th></th></ds:reference<>					0	
							ctProperties> elei	ments as well as to the	
			atureProperties> and						
	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
TS101903-008	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	"MUST" accordi "SHOULD", "SH specification sho XAdES specification sho XAdES specification sho XAdES specification - The <signed - SignedPropert XAdES specification - All signed pro- (direct incorp properties. - All signed pro- (direct incorp pro- (direct incorp pro- (direct incorp) pro- (direct incorp) pro- (direct</signed 	ing to RFC 2119 [22]. HOULD NOT", "RECC ould use these key we ation [1], clause 5, firs space URI that must l ation [1], clause 6.2, s Properties> must be of ties> element MUST of ation [1], clause 6.3, s Howing restrictions ap roperties must occur v poration), or it can be ation [1], clause 7.2.5 ment of <descriptions ation [1], clause 7.2.8 of the two elements < ation [1], clause 7.7.1 chiveTimeStamp> ele DataInfo> element for Info> must be exactly</descriptions 	The RFC 2119 DMMENDED", " ords wherever a st paragraph: be used by impl second paragra covered by a Re exist. [1, secion second paragra poly for using <c within a single < referenced by a , last paragraph s, <objectidenti , paragraph 8: ClaimedRoles> , paragraph 10: ment contains each data obje</objectidenti </c 	defines how th MAY", and "OP a requirement is lementations of ph: eference element 6.2] ph: ds:Object>, <qu cualifyingPropt a <qualifyingpropt a <qualifyingpropt a <qualifyingpropt a cualifyingPropt a cualifyin</qualifyingpropt </qualifyingpropt </qualifyingpropt </qu 	e key words "MUS TIONAL" are to be stated. the present docum nt of the XML sign ualifyingProperties erties> element. T opertiesReference imeType must be ples> must be present quence of <hashle< td=""><td>ST", "MUST NOT e interpreted in th ment [1, clause ature. Alignment s> and <qualifyin This element can e> element. See of present within the sent. [1, clause 7 DataInfo> elemer ure. The result of</qualifyin </td><td>with the present docum gPropertiesReference> either be a child of the clause 6.3.1 for informa e property. [1, clause 7 .2.8]</td><td>LL", "SHALL NOT", t level. Therefore, the nent mandates that one .: <ds:object> element tion how to sign .2.5]</ds:object></td></hashle<>	ST", "MUST NOT e interpreted in th ment [1, clause ature. Alignment s> and <qualifyin This element can e> element. See of present within the sent. [1, clause 7 DataInfo> elemer ure. The result of</qualifyin 	with the present docum gPropertiesReference> either be a child of the clause 6.3.1 for informa e property. [1, clause 7 .2.8]	LL", "SHALL NOT", t level. Therefore, the nent mandates that one .: <ds:object> element tion how to sign .2.5]</ds:object>
	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
TS101903-009	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment	Clause 6.2 of th	e XAdES specification	on [1] says: "The	e mandatory Ta	rget attribute refe	rs to the XML sig	nature." This should be	changed to: "The
	text	mandatory Targ	get-attribute MUST re	fer to the <id>-</id>	attribute of the o	corresponding <d< td=""><td>s:Signature>."</td><td></td><td>C C</td></d<>	s:Signature>."		C C
	Original								
	resolution								
	proposal								
	Resolution								
	comment								
	Resolution								
	text							•	
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution reference	date	type	source	date		version
TS101903-010	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment	For some ASN.	1 PKI elements that a	are included inte	the XAdES sig	nature the exact	ASN.1 encoding	mechanism is not speci	fied (clauses 7.1 and
	text	7.2.8 of the XA	dES specification [1])	. This should be	e changed to ma	andate the DER (Distinguished End	coding Rules [12]) enco	ding mechanism
	text 7.								
		wherever an AS	SN.1 encoding is requ	uired.					
		wherever an AS	SN.1 encoding is requ	uired.					
	Original resolution	wherever an AS	SN.1 encoding is requ	uired.					
		wherever an AS	SN.1 encoding is requ	uired.					
	resolution	wherever an AS	SN.1 encoding is requ	uired.					
	resolution proposal Resolution comment	wherever an AS	SN.1 encoding is requ	uired.					
	resolution proposal Resolution comment Resolution	wherever an AS	SN.1 encoding is requ	uired.					
	resolution proposal Resolution comment Resolution text		¥1	uired.					
Comment ID	resolution proposal Resolution comment Resolution text Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
Comment ID	resolution proposal Resolution comment Resolution text		¥1		Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
	resolution proposal Resolution comment Resolution text Deliverable	Deliverable	Original contribution	Comment				Resolution status	•
	resolution proposal Resolution comment Resolution text Deliverable version	Deliverable clause	Original contribution reference XAdES-PT-001	Comment date 25/01/2004	type technical	source	date	not yet processed	version
	resolution proposal Resolution comment Resolution text Deliverable version	Deliverable clause The following pl	Original contribution reference XAdES-PT-001 roposal was made by	Comment date 25/01/2004 members of th	type technical e ETSI Technic	source al Committee ES	date (Electronic Sign		version es):
	resolution proposal Resolution comment Resolution text Deliverable version 1.1.1 Comment text	Deliverable clause The following pr XAdES should	Original contribution reference XAdES-PT-001 roposal was made by	Comment date 25/01/2004 members of th	type technical e ETSI Technic	source al Committee ES	date (Electronic Sign	not yet processed atures and Infrastructure	version es):
Comment ID TS101903-011	resolution proposal Resolution comment Resolution text Deliverable version 1.1.1 Comment	Deliverable clause The following pr XAdES should	Original contribution reference XAdES-PT-001 roposal was made by	Comment date 25/01/2004 members of th	type technical e ETSI Technic	source al Committee ES	date (Electronic Sign	not yet processed atures and Infrastructure	version es):
	resolution proposal Resolution comment Resolution text Deliverable version 1.1.1 Comment text Original	Deliverable clause The following pr XAdES should	Original contribution reference XAdES-PT-001 roposal was made by	Comment date 25/01/2004 members of th	type technical e ETSI Technic	source al Committee ES	date (Electronic Sign	not yet processed atures and Infrastructure	version es):
	resolution proposal Resolution comment Resolution text Deliverable version 1.1.1 Comment text Original resolution	Deliverable clause The following pr XAdES should	Original contribution reference XAdES-PT-001 roposal was made by	Comment date 25/01/2004 members of th	type technical e ETSI Technic	source al Committee ES	date (Electronic Sign	not yet processed atures and Infrastructure	version es):
	resolution proposal Resolution comment Resolution text Deliverable version 1.1.1 Comment text Original resolution proposal	Deliverable clause The following pr XAdES should	Original contribution reference XAdES-PT-001 roposal was made by	Comment date 25/01/2004 members of th	type technical e ETSI Technic	source al Committee ES	date (Electronic Sign	not yet processed atures and Infrastructure	version es):
	resolution proposal Resolution comment Resolution text Deliverable version 1.1.1 Comment text Original resolution proposal Resolution	Deliverable clause The following pr XAdES should	Original contribution reference XAdES-PT-001 roposal was made by	Comment date 25/01/2004 members of th	type technical e ETSI Technic	source al Committee ES	date (Electronic Sign	not yet processed atures and Infrastructure	version es):

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	In XAdES specification [1] clause 7.2.2, last but one paragraph it says:									
	text	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]</signerrole>									
		This sentence should be moved to clause 7.2.8 'The <signerrole> element' of the XAdES specification</signerrole>									
	Original resolution				~		·				
	proposal										
	Resolution comment										
	Resolution										
	text	Deliverable	Original	Commont	Commont	Decelution	Decolution	Decelution status	Deliverable terret		
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	It should be pos <signedpropert With the current mandatory <sig< td=""><td>ssible in future version ties>. t XAdES versions it is</td><td>ns of XAdES to s not possible to not be added to</td><td>have archival v create valid XA the signature la</td><td>ersions that build AdES-A archival v tter. The XAdES s</td><td>on XMLDSig sign ersions out of a p pecification shoul</td><td>atures and Infrastructure atures without the mar lain XMLDSig signature d therefore provide for entifier> properties.</td><td>datory</td></sig<></signedpropert 	ssible in future version ties>. t XAdES versions it is	ns of XAdES to s not possible to not be added to	have archival v create valid XA the signature la	ersions that build AdES-A archival v tter. The XAdES s	on XMLDSig sign ersions out of a p pecification shoul	atures and Infrastructure atures without the mar lain XMLDSig signature d therefore provide for entifier> properties.	datory		
	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	<xsd:complexty <xsd:sequer <xsd:any </xsd:any </xsd:sequer This definition d following: <xsd:complexty <xsd:sequer< td=""><td>y namespace="##any ence> loes not allow conten ype name="AnyType" nce> y namespace="##any</td><td>" mixed="true"> "/> t that has no sc " mixed="true"></td><td>hema associate</td><td></td><td></td><td>AnyType> data type sh</td><td>ould read like the</td></xsd:sequer<></xsd:complexty </xsd:complexty 	y namespace="##any ence> loes not allow conten ype name="AnyType" nce> y namespace="##any	" mixed="true"> "/> t that has no sc " mixed="true">	hema associate			AnyType> data type sh	ould read like the		
	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					
<u>TS101903-016</u>	Comment text	referenced cert <xsd:complext <xsd:sequence <xsd:element n<br=""></xsd:element></xsd:sequence </xsd:complext Therefore the d <xsd:complext <xsd:seque <xsd:seque< td=""><td>ersion of the XAdES s ificate: ype name="CertIDTy ame="CertDigest" typ ame="IssuerSerial" ty ame="IssuerSerial" ty pe> ginition of the <certi ype name="CertIDTy nce> ment name="CertDig</certi </td><td>specification [1] pe"> pe="DigestAlgA /pe="ds:X509ls D> element sho pe"> est" type="Dige</td><td>the <certid> e ndValueType"/: suerSerialType buld read like th</certid></td><td>> "/> e following to allo Type"/></td><td></td><td>rchived version of the o</td><td></td></xsd:seque<></xsd:seque </xsd:complext 	ersion of the XAdES s ificate: ype name="CertIDTy ame="CertDigest" typ ame="IssuerSerial" ty ame="IssuerSerial" ty pe> ginition of the <certi ype name="CertIDTy nce> ment name="CertDig</certi 	specification [1] pe"> pe="DigestAlgA /pe="ds:X509ls D> element sho pe"> est" type="Dige	the <certid> e ndValueType"/: suerSerialType buld read like th</certid>	> "/> e following to allo Type"/>		rchived version of the o					
	<xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"></xsd:element>												
	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 schema val		by the World V				hough the schema has arger community this is:					
	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		
TS101903-018	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed			
	Comment text	ment In the actual version of the XAdES schema which is part of the XAdES specification the import statement for the XMLDSig sche									
	Original	Contennaized	ation="http://www.w3	5.61g, 11(2002,11		0 20020212, Xillia					
	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	
TS101903-019	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed		
<u>TS101903-019</u>	1.1.1 XAdES-PT-001 25/01/2004 technical not yet processed Comment text The <qualifyingpropertiesreferencetype> data type introduces a new <transforms> element in the XAdES namespace for th cds: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:attribute name="URI" type="rsd:anyURI" use="required"></xsd:attribute> <</xsd:sequence></xsd:complextype></qualifyingpropertiesreferencetype></transforms></qualifyingpropertiesreferencetype>									
	Resolution									
Comment ID	text Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version	
TS101903-020	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed		
	Comment text Original resolution proposal Resolution comment		amples in the (non-no	ormative) annex	D of the currer			AdES-PLUGTESTS TM		
	Resolution text									

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS101903-021	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed	
	Comment text	This (the <da aligned with the clause 7.2.5, se However, later than one signed This element ca - Textual info - An identifier - An indication This should be Additionally, in 2 The mandatory property. [1, cla This should be The mandatory qualified by this in order to indic Additionally, the have to be pres This element [1, clause 7.2 The first question sense to mandatory</da 	pecification [1], claus ataObjectFormat>) is present document M cond paragraph] in the same section th d data object, which it an convey: rmation related to the rindicating the type o n of the MIME type o n of the encoding forn changed to say "obje XAdES specification ObjectReference attu use 7.2.5, fourth para changed to say QbjectReference attu use 7.2.5, fourth para changed to say QbjectReference attu property. ate that this is a reque e current version of the mented to the verifier. (the <dataobjectfon 2.5, second paragrap on is, does it make ar</dataobjectfon 	e 7.2.5, second a signed prope IAY contain mo he specification actually does r signed data ob f the signed data f the si	paragraph it sa rty that qualifies re than one <d speaks about s ot: a object(s) in eleme a object(s) in el a object(s), in el d data object(s) d data object(s) says "object(s)" fourth paragra he Reference e erence the <ds fication mandat pecification [1] e present when indate the prese</ds </d 	s one specific sigr ataObjectFormats signed data object ent <descriptions; ement <objectide lement <mimetyp), in element <end aph it says: lement of the <ds :References elem 9 [22]. es the <dataobje t says: it is mandatory to ntation of the sign</dataobje </ds </end </mimetyp </objectide </descriptions; 	 elements, each suggesting th entifier>; coding>. Signature> correst ent of the <ds:si< li=""> ectFormat> element present the sign ed data objects of </ds:si<>	n consequence, an XML one qualifying one sign hat one <dataobjectfor esponding with the data gnature> corresponding ent to be present when t hed data object to huma on verification, at all? Ac plication or desired use</dataobjectfor 	ed data object. [1, mat> applies for more object qualified by this g with the data object he signed data objects n users on verification Iditionally, if it makes
	Original resolution								
	proposal								
	Resolution								
	comment								
l	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		the XAdES specifica				·		•					
	text								signature, including the					
						nose certificates ir	nto this property,	f the certificate is alread	dy present in the					
			ement of the signatu											
		On the other side the <ds:keyinfo> element is not covered by the <archivetimestamp>(s). That is, certificates that are present in the <ds:< td=""></ds:<></archivetimestamp></ds:keyinfo>												
	and are not included into the <certificatevalues> are not time-stamped for archiving purposes.</certificatevalues>													
	Original		There are two possible solutions to this issue: - Mandate the inclusion of all certificates in the certificate chain into the <certificatevalues> element.</certificatevalues>											
	resolution						eValues> elemen	t.						
	proposal		Mandate to include the <ds:keyinfo> element into the <archivetimestamp>(s).</archivetimestamp></ds:keyinfo>											
		This issue need	his issue needs further discussion.											
	Resolution													
	comment													
	Resolution text													
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target					
	version	clause	contribution reference	date	type	source	date		version					
TS101903-023	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed						
	Comment	In the clause 7.4	4.1 of the XAdES spe	cification it say	s:									
	text						clause 7.2.2, inc	orporating the digest of	each certificate and					
			suer and serial numb											
						per identifier to be	present in the <0	Cert> element. Therefore	e the word "optionally"					
		should be remo	ved from the quoted	sentence above	Э.									
	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	quality of the pa "Another one co the signature wa present docume	arametric data points posists to use a time- as generated before ent."	that anchor the stamp which all the date contair	m to the real wo ows to prove th ned in the time-	orld. In this instand at a datum existe stamp token. Polic	ce this being the d before a particu cy requirements t	a structure that represe time data and how it was llar time. This technique o cover that case is the	s applied." allows to prove that primary reason of the				
	Original resolution proposal Resolution	the parametric of	e quality of this evide data points In this i consists to usePo	nstance this is t	he time data ar	nd how".	inaging the data s	structure that represents	and on the quality of				
	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		Nodify 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										
	text	such an organization is expected to suitably inform its end users."											
	Original resolution proposal Resolution	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"											
	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	always defined	by the provider."	-	•			e TSA practice statemer	nt is				
	Original resolution proposal	New text: "A tim	ie-stamp policy may l	be defined by th	ne user of time-	stamp services	II						
	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	objectives wher	e considered necess	ary to provide th	he necessary co	onfidence that the	se objective will I	pecific requirements for be met."	controls to meet those				
	Original resolution proposal	New text: "The	requirements wher	e considered n	ecessary to pro	vide the necessa	y confidence that	t 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	······································											
	Original resolution proposal	New text: "Th	New text: "The current document addresses requirements for TSAs issuing time stamp tokens digitally signed by the TSA itself that is synchronized vith 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 refe	rence "FIPS PUB 14	0-1 (1994): "Se	curity Requirem	ents For Cryptog	raphic Modules".						
	Original resolution proposal	New reference:	FIPS PUB 140-2 (20	01): "Security F	Requirements F	or Cryptographic	Modules".						
	Resolution	ľ											
	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	reference."			-	Ū.		me-stamp either directly	or incorporated by			
	Original resolution proposal	New text: "The	e TSA shall also ens	ure adherence t	to any additiona	I obligations indic	ated in the time-s	stamp token"				
	Resolution											
Comment ID	Resolution											
	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	that t	dvisable that, when he private key used t					-stamp token has been	correctly signed and			
	Original resolution proposal Resolution	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."										
	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	the time of the ti	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;									
	Original resolution proposal	New text: "a) verify that th compromise	e time-stamp token's	s digital signatur	e is a valid one	, particularly that	the private key us	sed to sign the time-stan	np token has not been			
	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	being used a	d life-time of the sigr and the private key le of time during which 1	ength).	•		ds on the hashing	g algorithm being used,	the signature algorithm				
	Original resolution proposal Resolution		New text: d) The expected life-time of the signature associated to the time-stamp token) The period of time during which TSA event logs (see clause 7.4.11)										
	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 Original resolution	 b) The generat - meets th New text: "The " 	 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" 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: 										
	proposal Resolution comment Resolution	- meets the requirements identified in FIPS PUB 140-1[4] or FIPS PUB 140-2 [7] level 3 or higher; or"											
Comment ID	text Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
FS102023-012	1.1.1	7.2.2	UNSTT-006		technical			not yet processed					
-	Comment text	Modify the text: "a) The TSA pri			sed within a cry								
	Original resolution proposal		vate signing key shal e requirements ident					er; 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			
TS102023-013	1.1.1	7.2.4	UNSTT-006		technical			not yet processed				
	Comment text	- C	following additional c clause 7.4.10 require	s that records con of the validity	oncerning time- of the TSA's si	stamping services	s shall be held for nger the validity p	r a period of time as app period of the TSA certific	ropriate for at least 1 ate will be, the longer			
	Original resolution proposal	- C va	alidity of the TSA's s	s that records controls ignature verification	oncerning time- ition (public) key	stamping services / as appropriate fe	or providing nece	r a period of time after th ssary legal evidence an nger the size of the reco	d as notified in the TSA			
	Resolution comment Resolution											
Comment ID	text Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
S102023-014	1.1.1	7.2.5	UNSTT-006		technical			not yet processed				
	Comment text	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."										
	Original resolution proposal	 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)." 										
	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			
FS102023-015	1.1.1	7.2.6	UNSTT-006		technical			not yet processed				
	Comment text	Modify the title:	"Life cycle managen	nent of cryptogr	aphic module us	sed to sign time-s	tamps".					
	Original resolution proposal	New title: "Life o	cycle management o	f cryptographic	module used to	sign 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					
TS102023-016	1.1.1	7.3.1	UNSTT-006		technical			not yet processed						
	Comment text	h) The name o	otocol for a time-stam f the issuing TSA sha fier for the unit which	all be identified i	in the time-stam									
	Original resolution proposal	h) The name o	otocol for requests/res f the issuing TSA fier for the time-stam	-	-		3161 and							
	Resolution comment Resolution													
Comment ID	text 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	7.3.2 UNSTT-006 technical not yet processed											
	Comment text													
	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 obsolescend		vorthy systems	shall be secure	ly handled to prot	ect media from d	amage, theft, unauthoriz	red access and					
	Original resolution proposal		within the TSA trustw nagement shall be su				ect media from d	amage, theft and unauth	orized access. Media					
	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	Modify the text:			•			· · ·	
	text	"e) TSA person	nel shall be accounta	ble for their act	ivities, for exam	ple by retaining e	vent logs (see cla	ause 7.4.10)."	
	Original	New text:							
	resolution	"e) TSA person	nel shall be accounta	ble for their act	ivities, for exam	ple, by retaining e	event logs (see cl	ause 7.4.11)."	
	proposal								
	Resolution								
	comment								
	Resolution								
	text				-				
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
TS102023-020	1.1.1	7.4.8	reference UNSTT-006		tashaisal				
13102023-020	Comment	Modify the text:			technical			not yet processed	
	text			TSA's operatio			incontrad comprar	nice or loss of colibratio	n the TSA chall not
	text						ispected compror	nise or loss of calibration	n the TSA shall hot
	Original	New text:	tamp tokens until ste	ps are taken to	recover from th	e compromise.			
	resolution		of compromise to the	TSA's operatio		oto cianina kov o	ompromiso) "		
	proposal			ISAS Operatio	n (e.g. 13A ph	ale signing key c	ompromise)		
	Resolution								
	comment								
	Resolution								
Comment ID	Resolution text	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
Comment ID	Resolution text Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
Comment ID	Resolution text	Deliverable clause	contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
	Resolution text Deliverable version	clause	contribution reference		type				•
Comment ID TS102023-021	Resolution text Deliverable version	clause 7.4.9	contribution reference UNSTT-006					Resolution status	•
	Resolution text Deliverable version 1.1.1 Comment	clause 7.4.9 Modify the text:	contribution reference UNSTT-006	date	type technical	source	date	not yet processed	•
	Resolution text Deliverable version	clause 7.4.9 Modify the text: "a) Before the T	contribution reference UNSTT-006	date	type technical vices the follow	source	date	not yet processed	version
	Resolution text Deliverable version 1.1.1 Comment	clause 7.4.9 Modify the text: "a) Before the T - the TSA	contribution reference UNSTT-006 SA terminates its tim shall transfer obligati	date e-stamping ser	type technical vices the follow e party for main	source	date	not yet processed	•
	Resolution text Deliverable version 1.1.1 Comment text	clause7.4.9Modify the text:"a) Before the T- the TSAthe correct	contribution reference UNSTT-006	date e-stamping ser	type technical vices the follow e party for main	source	date	not yet processed	version
	Resolution text Deliverable version 1.1.1 Comment	clause7.4.9Modify the text:"a) Before the T- the TSAthe correstNew text:	contribution reference UNSTT-006 SA terminates its tim shall transfer obligati ect operation of the TS	date e-stamping ser ons to a reliabl SA for a reason	type technical vices the follow e party for main able period;"	source	date nall be executed a and audit archive	not yet processed as a minimum: s (see clause 7.4.10) ne	version
	Resolution text Deliverable version 1.1.1 Comment text Original resolution	clause 7.4.9 Modify the text: "a) Before the T - the TSA the corres New text: "a) Before the T	contribution reference UNSTT-006 SA terminates its tim shall transfer obligati ect operation of the TS	date e-stamping ser ons to a reliabl SA for a reason e-stamping ser	type technical vices the follow e party for main able period;" vices the follow	source	date nall be executed a and audit archive nall be executed a	not yet processed as a minimum: s (see clause 7.4.10) ne as a minimum:	version
	Resolution text Deliverable version 1.1.1 Comment text Original	clause 7.4.9 Modify the text: "a) Before the T - the TSA the corre New text: "a) Before the T - The TSA	contribution reference UNSTT-006 SA terminates its tim shall transfer obligati ect operation of the TS SA terminates its tim shall transfer obligati	date e-stamping ser ons to a reliable SA for a reason re-stamping ser tions to a reliab	type technical vices the follow e party for main able period;" vices the follow le party for main	source	date nall be executed a and audit archive nall be executed a	not yet processed as a minimum: s (see clause 7.4.10) ne	version
	Resolution text Deliverable version 1.1.1 Comment text Original resolution proposal	clause 7.4.9 Modify the text: "a) Before the T - the TSA the corre New text: "a) Before the T - The TSA	contribution reference UNSTT-006 SA terminates its tim shall transfer obligati ect operation of the TS	date e-stamping ser ons to a reliable SA for a reason re-stamping ser tions to a reliab	type technical vices the follow e party for main able period;" vices the follow le party for main	source	date nall be executed a and audit archive nall be executed a	not yet processed as a minimum: s (see clause 7.4.10) ne as a minimum:	version
	Resolution text Deliverable version 1.1.1 Comment text Original resolution	clause 7.4.9 Modify the text: "a) Before the T - the TSA the corre New text: "a) Before the T - The TSA	contribution reference UNSTT-006 SA terminates its tim shall transfer obligati ect operation of the TS SA terminates its tim shall transfer obligati	date e-stamping ser ons to a reliable SA for a reason re-stamping ser tions to a reliab	type technical vices the follow e party for main able period;" vices the follow le party for main	source	date nall be executed a and audit archive nall be executed a	not yet processed as a minimum: s (see clause 7.4.10) ne as a minimum:	version
	Resolution text Deliverable version 1.1.1 Comment text Original resolution proposal Resolution	clause 7.4.9 Modify the text: "a) Before the T - the TSA the corre New text: "a) Before the T - The TSA	contribution reference UNSTT-006 SA terminates its tim shall transfer obligati ect operation of the TS SA terminates its tim shall transfer obligati	date e-stamping ser ons to a reliable SA for a reason re-stamping ser tions to a reliab	type technical vices the follow e party for main able period;" vices the follow le party for main	source	date nall be executed a and audit archive nall be executed a	not yet processed as a minimum: s (see clause 7.4.10) ne as a minimum:	version

appropriate New text: f) "Records co Deliverable clause 4.2 t should be cle	ncerning time-stampi for providing necess	Comment date 17/02/2003 's key.	ce and as notif	ied in the TSA dis	closure statemen	not yet processed f the validity of the TSA' t (see clause 7.1.2)." ature verification (public Resolution status	
 f) Records cor appropriate New text: f) "Records cords Deliverable clause 4.2 t should be cle 	Original contribution reference JCPKI-005 arly defined the TSA	Comment date 17/02/2003 's key.	ce and as notif after the expira Comment type	tion of the validity Resolution source	of the TSA's sign Resolution date	t (see clause 7.1.2)." ature verification (public Resolution status	c) key as appropriate" Deliverable target
New text: f) "Records cc Deliverable clause 4.2 t should be cle	Original contribution reference JCPKI-005 arly defined the TSA	Comment date 17/02/2003 's key.	after the expira	tion of the validity Resolution source	of the TSA's sign Resolution date	ature verification (public	Deliverable target
 f) "Records control of the second seco	Original contribution reference JCPKI-005 arly defined the TSA	Comment date 17/02/2003 's key.	Comment type	Resolution	Resolution date	Resolution status	Deliverable target
clause 4.2 t should be clea	contribution reference JCPKI-005 arly defined the TSA	date 17/02/2003 's key.	type	source	date		
clause 4.2 t should be clea	contribution reference JCPKI-005 arly defined the TSA	date 17/02/2003 's key.	type	source	date		
clause 4.2 t should be clea	contribution reference JCPKI-005 arly defined the TSA	date 17/02/2003 's key.	type	source	date		
t should be cle	arly defined the TSA	's key.	technical	STF242	21/06/2003	na changa	1
		's key.		1		no change	
		II IL IS I SASKE	y or TSU's key.		-	· · · · · ·	
						key resides in a specific .2.1 should be changed	
					0		
Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
1.2	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
			•	•	·		
E.g. "TSA's key	should not be clone	d".					
t is not evently	alaar what "alaaad" r	maana Daguira	manta far agai	ity of any bookup	kovo oro oovoroo	1	
t is not exactly	clear what cloned r	neans. Require	ments for secu	пту ог апу раскир	keys are covered	1 UY 7.2.2 D & C.	
1.: //	Deliverable clause 2 /e propose to .g. "TSA's key	Deliverable clause Original contribution reference 2 JCPKI-005 /e propose to describe a restrictior .g. "TSA's key should not be clone	Deliverable clause Original contribution reference Comment date 2 JCPKI-005 17/02/2003 /e propose to describe a restriction on key backup .g. "TSA's key should not be cloned".	Deliverable clause Original contribution reference Comment date Comment type 2 JCPKI-005 17/02/2003 technical /e propose to describe a restriction on key backup. .g. "TSA's key should not be cloned".	Deliverable clause Original contribution reference Comment date Comment type Resolution source 2 JCPKI-005 17/02/2003 technical STF242 /e propose to describe a restriction on key backup. .g. "TSA's key should not be cloned". STF242	Deliverable clause Original contribution reference Comment date Resolution type Resolution source Resolution date 2 JCPKI-005 17/02/2003 technical STF242 21/06/2003 /e propose to describe a restriction on key backup. .g. "TSA's key should not be cloned".	Deliverable clause Original contribution reference Comment date Resolution type Resolution source Resolution date Resolution date 2 JCPKI-005 17/02/2003 technical STF242 21/06/2003 no change /e propose to describe a restriction on key backup.

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 exp	iration date of t	he time-stamp	token, TSA assur	ed,"		
	Original resolution proposal								
	Resolution comment	Time-stamps va using additiona		fter this period.	It is only nece	ssary to provide a	additional protection	on to maintain the integr	ty of the token (e.g.
	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 o	lause 7.4.11' is	right"				
	Original resolution proposal	"See clause 7.4	.10" is wrong. "See c	lause 7.4.11' is	right"				
	Resolution comment	Correction note	d.						
	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 PL	JB 140-2 to be consid	lered for next re	evision.				
	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	FIPS PUB 140-	2 is also required.						
	resolution proposal								
	Resolution	Use of FIPS PL	JB 140-2 to be consid	dered for next re	evision.				
	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
TS102023-029	1.2.1	7.2.2 b)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process	
	Comment text			ecovered, the T	SA needs to a	sure that it does	not use previously	y used serial numbers ir	the TSTs for new
		TSTs							
	Original resolution proposal	Following note i	is needed. n the backup key is r	ecovered, the T	SA needs to as	ssure that it does	not use previously	y used serial numbers ir	
		Following note i NOTE: When TSTs	is needed. n the backup key is r				-		
	resolution proposal Resolution	Following note i NOTE: When TSTs	is needed. n the backup key is r s.				-		
Comment ID	resolution proposal Resolution comment Resolution	Following note i NOTE: When TSTs To be considere Deliverable clause	is needed. n the backup key is r s. ed for next revision. Original contribution reference				-		
Comment ID	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1	Following note i NOTE: When TSTs To be considere Deliverable clause 7.2.4	is needed. n the backup key is r s. ed for next revision. Original contribution reference JCPKI-005	It is recommend Comment date 17/02/2003	ded that new ke	vs are generated Resolution source STF242	instead.	y used serial numbers ir	the TSTs for new
	resolution proposal Resolution comment Resolution text Deliverable version	Following note i NOTE: When TSTs To be considere Deliverable clause 7.2.4	is needed. n the backup key is r s. ed for next revision. Original contribution reference	It is recommend Comment date 17/02/2003	ded that new ke	vs are generated Resolution source STF242	instead. Resolution date	y used serial numbers ir	the TSTs for new
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment text Original	Following note i NOTE: When TSTs To be considere Deliverable clause 7.2.4 NOTE 1: "See	is needed. n the backup key is r s. ed for next revision. Original contribution reference JCPKI-005	It is recommend Comment date 17/02/2003 ong. "See claus	Comment type editorial e 7.4.11" is right	vs are generated Resolution source STF242	instead. Resolution date	y used serial numbers ir	the TSTs for new
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment text Original resolution	Following note i NOTE: When TSTs To be considere Deliverable clause 7.2.4 NOTE 1: "See	is needed. In the backup key is r S. ed for next revision. Original contribution reference JCPKI-005 clause 7.4.10" is wre	It is recommend Comment date 17/02/2003 ong. "See claus	Comment type editorial e 7.4.11" is right	vs are generated Resolution source STF242	instead. Resolution date	y used serial numbers ir	the TSTs for new
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment text Original	Following note i NOTE: When TSTs To be considere Deliverable clause 7.2.4 NOTE 1: "See	is needed. n the backup key is r s. ed for next revision. Original contribution reference JCPKI-005 clause 7.4.10" is wr e clause 7.4.10" is wr	It is recommend Comment date 17/02/2003 ong. "See claus	Comment type editorial e 7.4.11" is right	vs are generated Resolution source STF242	instead. Resolution date	y used serial numbers ir	the TSTs for new
	resolution proposal Resolution comment Resolution text Deliverable version 1.2.1 Comment text Original resolution proposal	Following note i NOTE: When TSTs To be considere Deliverable clause 7.2.4 NOTE 1: "See NOTE 1: "See	is needed. n the backup key is r s. ed for next revision. Original contribution reference JCPKI-005 clause 7.4.10" is wr e clause 7.4.10" is wr	It is recommend Comment date 17/02/2003 ong. "See claus	Comment type editorial e 7.4.11" is right	vs are generated Resolution source STF242	instead. Resolution date	y used serial numbers ir	the TSTs for new

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 meas If the TSA's cloc		e stated accura	cy and TSTs w	ere issued before	it was detected, t	the TSA shall revoke the	e TSTs.
	Original resolution proposal	Following meas If the TSA's cloc	ure is needed. ck has been out of the	e stated accura	cy and TSTs w	ere issued before	it was detected,	the TSA shall revoke the	e TSTs.
	Resolution comment Resolution		me-stamp tokens is n cepted accuracy.	ot practical. It i	s preferable to	ensure that the T	SA stops issuing	tokens well before there	is a risk that the clock
Comment ID	text 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	For instance, Th	eeds to show to users ne TSA shall keep an n of guideline is requir	d show tractabi			s time source to u	sers.	
	Original resolution proposal								
	Resolution comment	Noted to be con	sidered for next revis	ion. Synchroniz	zation 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		"the TSA should not tion of guideline is red		nps when it is p	processing for a le	eap second".		
	Original								
	resolution								
	proposal								
	Resolution	Issue noted. Ho	wever, the importanc	e of availability	of time-stampi	ng services needs	s to be taken into	account.	
	1	-	,		· •	.			
	comment								
	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
TS102023-034	1.2.1	7.4.8	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text		vided a way of how to of the TSA"s signing of calibration		ed TSTs in the	following cases.			
	Original resolution proposal								
	Resolution comment	Steps required a	already specified in cla	ause 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	So we believe the revocation list).	ssibility that TST is is nat when such cases ion of guideline is req	happened the				while. s and subscribers (e.g.	by time-stamps
	Original resolution proposal								
		Since the impac place to avoid s	•	se is difficult to	predict it is not	clear whether au	tomatic recovery	is practical. It is prefera	ble to measures in
	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	guideline". 1. Example of 2. Example of Also in "Time-st Authentication" token does not	time-stamping service time-stamping service amping usage guidel which is not specifica have a mechanism to	e operation regi e operation regi ine", the import ally described in prove that the	ulation using sir ulation using lin ant matters on the above ETS token itself use	nple protocol. king protocol. use of time-stamp SI TS. A time-stam s a reliable time s	bing were summa np token issued b source to guarante	d in FY2002 report, "Tin rized. Here we discusse y TSA should have the ee the time accuracy. Th d there should be a me	ed about "Time correct time but the he time included in
	Original resolution proposal								
	Resolution comment Resolution text	The requiremen used.	ts for synchronization	n with UTC are	specified in cla	use 7.3.2. It is left	open to the imple	ementation to decide wh	nich mechanism is to be
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				•	" within a descrip	tion and "TimeStampTo	oken" for formal
	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	In clause 7.2.3. 7.3.2 Clock Sy b) The TSA clo Let us consider Scenario A. The clock refere synchronized m having an acces This scenario re Scenario B. The clock refere within the same compensation co installation mus This scenario of Conclusion I see the need f 1) the security	ance team of TS 102 we currently only ha ynchronization with U ocks shall be protecte two scenarios: ence is outside the H hanually every week we ss to the room and kr elies on the security c ence is within a HSM e HSM. The clock is b of only XX microsecol	023. ve: TC ad against threa SM. It is for exa vith UTC by an nowing some IE of the environme (Tamper Resis ased upon a cr nds (e.g. 100 m having an acce rity features of ies for the prote oom access co	ts which could r ample a PCI car operator. The c and password ent and on the r tant - Hardware ystal clock com icroseconds) is ess to the room the HSM. ection whether: ntrol and by pro-	d placed in a PC perator is able to could set any tim espect of procedu Security Module pensated in temp allowed. If more and knowing *even	with a crystal cloc set any time whe e. ures.), this means that erature and syncl is being done, the erything* cannot d	he clock that takes it ou ek compensated in temp en performing the synch nronized every week wit private key will be zerc lo more that a clock drift	erature and ronization. Someone TSU signing key are h UTC. Every week a vized and a new full
		This should lead	d to define two differe	ent TSA policies	s, unless we r	nandate 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 shoul	d the exported	key protection I	ast.			
	Original resolution proposal	 Reword the When ou state of t Add the following the state of the stat	he art, are capable to	ame new text p reation device (withstand cryp	see a) above) t tanalytic attack	he CA private sig s for the residual	life of the encrypt		s that, according to the s for the residual life of
	Resolution comment								
	Resolution text								

5.7 TR 102 038 - XML format for signature policies

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
			reference						
TR102038-001	1.1.1		JCPKI-006	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment text	<xsd:element na<br="">type="OCSPTr</xsd:element>	out OCSP trust condit ame="OCSPTrustCor ustConditionType" mi oould apply on signatu	ndition" nOccurs="0"/>			les element scher	na, add following eleme	ent
	Original resolution proposal	To describe abo <xsd:element na<br="">type="OCSPTr</xsd:element>		ion, both in Condition" nOccurs="0"/>	mmonRules and	d CommitmentRul	les element scher	na, add following eleme	ent
	Resolution comment						see also response	e to "comments regardir	ng EESSI Signature
	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		ne Reports describe						
	text			en these rules a	are little bit und	erstandable. It is l	nelpful for us if you	ı explain some example	e of these Rules,
		especially comm							
		Also in this clau	se, description "trust	t conditions for u	user certificate,	timestamps and a	attributes" should b	be added OCSP respor	ider's trust conditions.
			ould apply on signat						
	Original		ne Reports describe						
				en these rules a	are little bit und	erstandable. It is i	nelptul for us if you	i explain some example	e of these Rules,
	proposal	especially com		conditions for u	ser certificate	timestamps and a	attributes" should b	be added OCSP respor	der's trust conditions
			ould apply on signat					le audeu OCOI Tespor	
	Resolution							e to "comments regardi	ng EESSI Signature
		Policy".				griatare perioree			ig EECCI olghataro
	Resolution								
	text								
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution reference	date	type	source	date		version
TR102041-002	1.2.1	8.3.2	JCPKI-007	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment	Revocation Rec	uirements				<u>.</u>		
	text		_ Distribution points	not only full CRL	_S.				
	Original	Revocation Rec							
	resolution	Please add CRI	Distribution points	not only full CRI	_S.				
	proposal								
	Resolution comment	This comment is Policy".	s to be fed into sepa	rate activities wi	thin ETSI on si	gnature policies -	see also response	e to "comments regardi	ng EESSI Signature
	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	•	rence "FIPS PUB 140	, , , , , , , , , , , , , , , , , , ,	, ,	<u>, , , , , , , , , , , , , , , , , , , </u>	•		
	Original resolution proposal	New reference:	FIPS PUB 140-2 (20	01): "Security R	Requirements Fo	or Cryptographic I	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		"The certification aut	hority has overa	all responsibility	for the provision	of the certification	n services identified in c	lause 4.1. The
	text	certification auth	nority's key is used to	sign the qualifi	ed certificates a	and it is identified	in the certificate a	as the issuer."	
	Original resolution proposal		Certification Authority tified in the certificate					s identified in clause 4.2 ites."	2. The certification
	Resolution comment								
	Resolution text		-	_	_	-		-	
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Delbueneble tennet
	version	clause	contribution reference	date	type	source	date		Deliverable target version
TS102042-003	version 1.1.1	clause 4.1 (2nd para)	reference	date	type editorial	source	date	not yet processed	•
TS102042-003		4.1 (2nd para)	reference		editorial		date	not yet processed	•
TS102042-003	1.1.1 Comment text Original resolution	4.1 (2nd para) Modify the text:	reference UNSTT-002	sed to generate	editorial the certificates	n 	date	not yet processed	•
TS102042-003	1.1.1 Comment text Original	4.1 (2nd para) Modify the text:	reference UNSTT-002 "However, the key us	sed to generate	editorial the certificates	n 	date	not yet processed	•

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							nts, to relying parties. T bscribers and relying pa	
	Original resolution proposal		emination service: dis ilable the CA's terms					es them available to relyi	ng parties. This service
	Resolution comment Resolution								
Comment ID	text 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	
	text	obligations: a) accurate and registration; b) the key pair c) reasonable of d) [CONDITIOI - subject k policy; - a key ler e) [CONDITIOI holds the pri f) [NCP+] only g) [NCP+] [CO device used	d complete information is only used in accord care is exercised to a NAL] if the subscriber acys are generated us ngth and algorithm is use NAL] if the subscriber ivate key once deliver use the subject's priv	on is submitted dance with any void unauthoriz or subject gen sing an algorith used which is ru or subject gen red to the subje vate key for sigu bject's keys are ting;	to the CA in acc limitations notif red use of the s erates the subje m recognized as be erates the subje act; ning or decrypti e generated unc	cordance with the ied to the subscril ubject's private ke ect's keys: y industry as bein eing fit for the use ect's keys and the ng with the secure der control of the s	requirements of ber (see clause 7 ey; ing fit for the uses es of the certified e private key is fo e user device; subscriber, gener	of the certified key as id key as identified in the o r creating electronic sigr rate the subject's keys w	vith regards to entified in the certificate certificate policy; natures only the subject rithin the secure user

Comment ID	Deliverable version	Deliverable clause	Original contribution reference CA shall oblige, throu	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version		
	Original resolution proposal	 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); 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 dem." 									
	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 Comment text	7.2.1 UNSTT-002 technical not yet processed 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:									
	Original resolution proposal	 meets the requirements identified in FIPS PUB 140-1 [2] or 140-2 [6] level 3 o higher;" 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 									
	Resolution comment Resolution text		equirements identified								

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		"a) [CHOICE]:				·		·				
	text		rivate signing key sha	all be held and	used in a produ	ct, application or	device which doe	s not compromise the s	ecurity of the private				
		key and which:											
			equirements identified										
								r equivalent security crit	teria.				
		 [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 											
							/IEC 15/08 [3] or	r equivalent security crit	toria. This shall he to a				
									ig into account physical				
			echnical security mea		requirements of				ig into account physical				
		b) [CHOICE]:		ouroo.									
			side the signature-cre	eation product.	application or d	evice, the secrec	y of the CA's priva	ate key shall be ensure	d.				
		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 hat, 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 phys 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.											
					all be subject to	the same or grea	ater level of secur	ity controls as keys cur	rently in use.				
			eys are stored in a de outside the hardware r		ocessing hardw	are module, acce	ss controls shall b	be in place to ensure th	at the keys are not				
	Original	New text: "a) [0	CHOICE]										
	resolution	[LCP] "The CA.	"										
	proposal		40-1 [2] or FIPS PUB										
			private signing key "										
		- meets the re	equirements identified	in FIPS PUB 1	40-1 [2] or FIP	S PUB 140-2 [6] le	evel 3 o higher; "						
	Resolution												
	comment												
	Resolution												
	text												

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS102042-008	1.1.1	7.2.9	UNSTT-002		technical			not yet processed					
	Comment	Modify the text:	"d) Where the secure	the activation data sha	II be securely prepared								
	text	and distributed	distributed separately from the signature-creation module.										
		NOTE: Sepa											
	Original	New text: d) V	ew text: d) Where the secure user device has associated user activation data separately from the secure user device.										
	resolution	NOTE: "Sep											
	proposal												
	Resolution												
	comment												
	Resolution												
	text												

Comment ID	Deliverable version	Deliverable clause	Original contribution reference I record the signed ag	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version		
	Original resolution proposal	n j) This comma should be cancelled from this clause (Subject registration) and inserted in "Subscriber's obligations" (this kind of information is									
	Resolution comment	m) "legal proc	ceedings according to	the national la	w of the country	y where the Certif	fication Service P	rovider is established."			
	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	subject (or, i		ectronic signatu				se 7.2.4), on delivery to e key. Any copies of the			
	Original resolution proposal	New text:	NAL] If a copy of the s		e key is no requ	ired"					
	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	on.			·	·						
	Original resolution proposal	New text: "Exte	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					
		 which physic Physical program generation, outside this Physical and themselves, certificate generation, fitheft, breakii Controls shawithout auth NOTE 1: See NOTE 2: Othe 	cally protects the serv stection shall be achie subject device provisi perimeter. d environmental secur and the facilities use eneration, subject dev ire safety factors, failung and entering, and all be implemented to orization. ISO/IEC 17799 for gur r functions may be su	vices from comp eved through the ion and revocation in the support the vice provision a ure of support in disaster recover protect against idance on physioported within	promise through e creation of cle tion manageme all be implemen eir operation. Th and revocation m g utilities (e.g. p ery, etc. t equipment, info sical and environ the same secur	a unauthorized ac arly defined secu ant services. Any p ted to protect the ac CA's physical a banagement servi bower, telecommu- bormation, media a anmental security. ed area provided	cess to systems rity perimeters (i. arts of the premi facility housing s and environmenta ces shall address inications), struct and software rela- that the access i	e. physical barriers) aro ses shared with other or ystem resources, the sy al security policy for syst s the physical access co	und the certificate rganizations shall be estem resources ems concerned with ontrol, natural disaster leaks, protection against being taken off-site				
	resolution proposal	e) Physical pro device provi NOTE 1: As de subje	sion and revocation n efined at the beginnin	eved through th nanagement se g of the docum CA gives Regis	e creation of cle ervices. Any par lent, a "subject o stration authoriti	arly defined secu ts of the premises device provision s es the responsibil	rity perimeters (. s shared with othe ervice prepares a) around the certificate er organizations shall be and provides a signature nature devices to subjec	e outside this perimeter. e-creation device to				
	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	Modify the text:											
	text	"c) Media used	within the CA shall b	e securely hand	dled to protect n	nedia from damag	ge, theft and unau	uthorized access."					
	Original	New text:											
	resolution	"c) Media used within the CA shall be securely handled to protect media from damage, theft, and unauthorized access. Media life cycle management											
	proposal	shall be such to proactively prevent obsolescence."											
	Resolution												
	comment Resolution												
	text												
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
Comment ID	version	clause	contribution	date	type	source	date	Resolution status	version				
TS102042-014	1.1.1	7.4.8											
	Comment		7.4.8 UNSTI-002 Itechnical Inot yet processed Modify the text: "Revocation status										
	text	c) In the case of compromise the CA shall as a minimum provide the following undertakings:											
								n of established relations	s of the compromise;"				
	Original	New text:	· · · · · · · · · · · · · · · · · · ·						•				
	resolution		of compromise										
	proposal					subjects) and any	y entity with whicl	h it has agreements or o	ther form of established				
		relations	, among which relyin	g parties and C	As"								
	Resolution												
	comment												
	Resolution text												
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
Comment iD	version	clause	contribution	date	type	source	date	Resolution status	version				
	Version	olause	reference	dute	type	300100	unic		Version				
TS102042-015	1.1.1	7.4.9	UNSTT-002		technical			not yet processed					
10102012 010	Comment	Modify the text:			toorninour			not yot proceedu					
	text		CA terminates its serv	vices the followi	na procedures s	shall be executed	as a minimum:						
								or other form of establis	shed relations;"				
	Original	New text: "CA g					0						
	resolution	a) before the C	A terminatesthe C										
	proposal	- inform a				subjects) and any	entity with which	it has agreements or oth	ner form of established				
	proposal	- 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."											
		relations	, among which relyin	g parties and C	As."								
	Resolution	relations	, among which relyin	g parties and C	As."								
	Resolution comment	relations	, among which relyin	g parties and C	As."								
	Resolution	relations	, among which relyin	g parties and C	As."								

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: for the purpose NOTE 1: Reco envir In particular: General a) The confide b) Records cor proceedings registration NOTE 2: This d) The precise NOTE 3: It is r e) Records cor f) The events time that the NOTE 4: This back g) The specific Registration h) The CA sha i) The CA sha i) The CA sha i) The CA sha c type of c c record o applicab c storage c identity c c method c name of	"The CA shall ensure of providing evidence ords concerning certifi- conmental, key manage ntiality and integrity of ncerning certificates s ncerning certificates s s. The subject, and wi and other information may be used, for exa- time of significant CA recommended that the ncerning certificates s shall be logged in a we ey are required to be I may be achieved, for up. c events and data to b Il ensure all events re- il ensure that all regis locument(s) presente f unique identification ile;	e of certification cates include re gement and cert f current and ar hall be complet hall be made a thin the constra relating to the mple, to suppor environmental e CA states in it hall be held for vay that they ca held. e logged shall the lating to registra tration informat d by the applications and poscriber agreen application docume submitting Regi	tinformation co for the purpose egistration inforn ifficate manager chived records ely and confide vailable if requir ints of data pro- subject. If the link betwe key managem s practices the a period of time nnot be easily co ogh the use of w be documented ation including the ation including the ation including the ation including the ation including the ation including the ation including the ation including the ation including the ation inc	es of legal proceed mation (see claus ment events. concerning certific ntially archived in red for the purpos tection requireme en the certificate accuracy of the cl e as indicated in the leleted or destroy rite only media, a by the CA. requests for certific e following is recor- egistration; on thereof (e.g. al ocuments, includie ent to publication of ty, if applicable.	dings. e 7.3.1) and infor cates shall be ma accordance with es of providing e nts (see clause 7 and the subject. e management ev ock used in timin ne CA's terms an ed (except for tra record of each re cate re-key or rea orded: oplicant's drivers ng the signed su	for an appropriate perio rmation concerning sign aintained. disclosed business pra vidence of certification f 7.4.10) the subscriber, si vents shall be recorded. In g of events, and how the d conditions (see clause insfer to long-term medi emovable media used a	ificant CA actices. or the purpose of legal hall have access to is accuracy is ensured. e 7.3.4). a) within the period of and the use of off site
	Original	New text: "The	CA shall ensure that	all relevant info	rmation concerr	ning a qualified ce		ed for an appropriate pe	
	resolution proposal	particular for the where the Certi Registration	e purpose of providing fication Service Provi Il ensure that all regis	g evidence of co der is establish	ertification for th ed."	e purposes of leg	al proceedings a	ement (e.g. subjects' cor	law of the country
	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		
TE100040 017	1 1 1	2.0			tachnical			not vot processed			
TS102042-017	1.1.1	3.2	UNSTT-002		technical			not yet processed			
	Comment	Modify the text:	"NCP+ Normalized C	ertificate Policy	requiring use a	of a secure user d	evice"				
	text			-							
	Original	New text: "NCP+ Extended Normalized Certificate Policy."									
	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
S102042-018	1.1.1		TC-ESI_3-002		technical			not yet processed	
5102042-018	Comment text	on a card. Thes I have, so far, is signatures only clue about. Witt We should cons a) whether the b) how to addr Maintenance of Discussion Key multiple us Providing a frar consumers rely It is technically key pair is gene this, but for son Issue revolves a) the quality of b) the creation Qualified certific not prohibit sub currently part o Qualified certific Article 5.1 signar recognized as s It is suggested, function of a ha In respect of bo should provide Signatures in th - they indicator reference to - a signature Therefore, ther a) the intentior b) the intentior	oked at possible con se certificates may be dentified one potentia , the other for encryp hout a flag in the CP sider to look at: are are other potentia ress them. If the policies is proba- arage: mework to support the ring on e-signatures; possible that the sar erated by the subscri- ne applications, this is around: of the key pair genera- to of a close association cates are designed to poscriber generation of f Electronic Signature, of Electronic Signature, such, although proba- therefore, that subscri- ne real world perform e a will or intention b the document to who is evidence of itself, e are two elements v in to express a comm in to create the signat 5.1 electronic signature	e issued by diffe al conflict. Assur- otion. The two C _i the situation is r I conflicts for the ably the right place e use of e-signa- is an objective u- ne public key may ber, which he se may be undesirated ated; and on between the k- poffer a high leve f keys. It should es Directive, nor o support an arti- gnized in legal pri- bly only if they signer to ta- i.e. one which is es AND any e-si- ance to any third two main functi- y the signer to ta- ich it is applied, i.e. of the act of which electronic itment; and ure.	v arise when the rent CAs, under me that two CAs As don't know a not transparent e configuration of ce to deal with t atures and creat under EESSI an ay be included i ands to more that able, particularly key pair and an vel of assurance be preferred that conformance g cle 5.1 e-signat roceedings as the satisfy at least the	different CPs. s issue two differe bout each other, to auditors either. lescribed above, a his. ing an environme d the Directive. n more than one of an one certification where higher lev application for wh which needs to k at the certification uidance. ure; they may also be definition of an urpose of creating as a handwritten s s intended to be a r reasonably rely of tment. (The exact ar evidence); and hot prove:	ent certificates to users can hardly and nt which will pron certificate. (This of n authority.) In ge rels of assurance nich it is to be use be maintained in authority takes r o be used for aut and written signa advanced electro g any type electro signature by a rel a handwritten sig on this.	ssued to a key pair, e.g the same key, one spec made responsible for th note trust, and protectin could well be the case, f eneral, there may be no are required. all aspects of the servic esponsibility for general hentication in general u- tures. Other electronic so poic signature under art nic signature which is ir	g the interests of for example, where the thing objectionable in e. TS 101 456 [1] does ting the keys. This is not se. signatures may be icle 2.2. htended to fulfil the stricted to that purpose. is a need that they guous except by

	Resolution	1									
	resolution proposal	"NOTE: It is r						CD should be used. Thi t of signing."	s includes the		
	Comment text Original		the SSCD, pointing t					subscribers about the kir Systems.	d of environment that		
S102042-019	1.1.1	7.2.9	OTHER-005		technical			not yet processed			
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version		
	comment Resolution text										
	Resolution										
	resolution proposal										
	Original		r olghataror nowovor				guily our our and ing				
		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.									
			proceedings.								
		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;									
		 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 									
		Enforcement: It has been argued that certification authorities should be free to decide for themselves whether to enforce obligations against a subscriber. There									
		 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. 									
		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:									
		the use of h	is key pair for any oth	ner purpose.		-		ual to a h/w one; prevent			
		 making it cle (second bes) 	ear to the signer that st) by legal means;	his key, certifica	ate, must only b	e used to create a	u	nforcing that obligation e	•		
		lintention to make	ke the signature as a	handwritten on	e. This reauires	two steps:					

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	a) Replace text in clause 7.2.5 with:								
	resolution proposal	 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	This is not a rec	quirement that can be	e understood ea	asily. Actually, I	think that the new	wording is mear	lingless.		
	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.							
		protected using	ange clause 7.2.2 - item b), paragraph [NCP] into "When outside the signature-creation device (see a) above) the CA private signing ke otected using cryptographic systems that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual crypted 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 inco	onsistencies in annex	D, the cross re	ference betwee	n RFC 2527 and	TS 101 456.		
		Amendment pro							
	resolution		"7.3.5" into "7.3.6"						
proposal * 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 "7.4.6" * 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					e.(22). rule). Identification and				
	Resolution comment Resolution	authentication r NOTE2: The I "This subcompo System develop during product r implementation Security manag security. These (<- this is addree This subcompo level IV and V, i	equirements for each life cycle security con onent addresses syst oment controls includ maintenance, softwar techniques (e.g., def gement controls includ tools and procedures assed in clause 7.4 of nent can also addres	n role may also htrols, as per RF tem development re engineering p fensive program de execution of s include check TS 101 456) is life-cycle secu	be defined." C 2527, are: nt controls and s environment se practices, softwa ming) and deve tools and proce ing the integrity urity ratings bas	security managem curity, developme are development r elopment facility s dures to ensure t of the security so ed, for example, o	nent controls. ent personnel sec methodology, mo ecurity. (<- this is hat the operation oftware, firmware, on the Trusted So	urity, configuration man dularity, layering, use of not addressed by TS 1 al systems and network	agement security f failsafe design and 01 456) s adhere to configured e their correct operation. ethodology (TSDM)
	text								
	lexi								

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:

111

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			
	rpretation and Enforcement	5.4			
2.5 Fee		N/A			
	lication and Repositories	7.3.5, 7.3.6			
	npliance Audit	N/A			
	fidentiality Policy	7.3.1			
	Ilectual Property Rights	N/A			
	TIFICATION AND AUTHENTICATION	7.0.1			
	al Registration	7.3.1			
	tine Rekey	7.3.2 7.3.2			
3.3 Rek	ey After Revocation No Key Compromise ocation Request	7.3. 5 6			
	RATIONAL REQUIREMENTS	7.3.90			
	tificate Application	7.3.1			
	lificate Issuance	7.3.3			
	lificate Acceptance	7.3.1			
	tificate Suspension and Revocation	7.3. 5 6			
	urity Audit Procedures	N/A			
	ords Archival	7.4.11			
	Changeover	7.3.2			
	npromise and Disaster Recovery	7.4.8			
	Termination	7.4.9			
5 PHYS	SICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS				
	sical Security Controls	7.4.4			
	cedural Controls	7.4. 5 3 (see note 1)			
	sonnel Security Controls	7.4.3			
	INICAL SECURITY CONTROLS				
	Pair Generation and Installation	7.2.8, 7.2.9			
	ate Key Protection	7.2.8			
6.3 Oth	er Aspects of Key Pair Management	7.2, 6.2			
	vation Data	7.2.7, 7.2.9			
	nputer Security Controls	7.4.5, 7.4.6, 7.4.7			
	Cycle Security Controls	7. 3 4 (see note 2)			
	work Security Controls	7.4.5, 7.4.6			
	otographic Module Engineering Controls	7.2			
	IFICATE AND CRL PROFILES				
	tificate Profile	7.3.3			
		N/A			
	CIFICATION ADMINISTRATION				
	cification Change Procedures	7.1			
	lication and Notification Procedures	7.1			
	tification 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	deperihed together			
	with the responsibilities for each role.(22).	e described, logether			
	For each task identified for each role, it should also be stated how ma	any individuals are			
	required to perform the task (n out m rule).Identification and authentic				
	each role may also be defined."				
NOTE2:	The life cycle security controls, as per RFC 2527, are:				
	"This subcomponent addresses system development controls and se	curity 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 I correct operation (this is addressed in clause 7.4 of TS 101.456)	naruware to ensure their			
	correct operation (this is addressed in clause 7.4 of TS 101 456).	t for example on the			
	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).				

113

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		

114

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 Certi	ficate Issuance	7.3.3
4.3 Certi	ficate Acceptance	7.3.1
4.4 Certi	ficate Suspension and Revocation	7.3. 5 6
4.5 Secu	urity Audit Procedures	N/A
4.6 Reco	ords Archival	7.4.11
4.7 Key (Changeover	7.3.2
	promise and Disaster Recovery	7.4.8
	Fermination	7.4.9
5 PHYSI	ICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTR	OLS
	sical Security Controls	7.4.4
	edural Controls	7.4. 5 3 (see note 1)
	onnel Security Controls	7.4.3
	NICAL SECURITY CONTROLS	
	Pair Generation and Installation	7.2.8, 7.2.9
	ate Key Protection	7.2.8
	r Aspects of Key Pair Management	7.2, 6.2
	vation Data	7.2.7, 7.2.9
	puter Security Controls	7.4.5, 7.4.6, 7.4.7
	Cycle Security Controls	7. 3 4 (see note 2)
	vork Security Controls	7.4.5, 7.4.6
	tographic Module Engineering Controls	7.2
	IFICATE AND CRL PROFILES	1.2
	ficate Profile	7.3.3
	Profile	N/A
	IFICATION ADMINISTRATION	
	cification Change Procedures	7.1
	ication and Notification Procedures	7.1
	fication practice statement Approval Procedures	7.1
	The procedural controls, as per RFC 2526, are:	1.1
	"In this subcomponent, requirements for recognizing trusted rol	os aro doscribod, togothor
	with the responsibilities for each role.(22).	es are described, logeriler
	For each task identified for each role, it should also be stated h	ow many individuals are
	required to perform the task (n out m rule). Identification and au	
	each role may also be defined."	
	The life cycle security controls, as per RFC 2527, are:	
	"This subcomponent addresses system development controls a	and security management
	controls.	
	System development controls include development environmer	nt security, development
	personnel security, configuration management security during p	
	engineering practices, software development methodology, mo	
	failsafe design and implementation techniques (e.g., defensive	
(development facility security (this is not addressed by TS 101 4	56).
Ś	Security management controls include execution of tools and p	rocedures to ensure that the
(operational systems and networks adhere to configured securit	y. These tools and procedures
i	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	S).
-	This subcomponent can also address life-cycle security ratings	based, for example, on the
	Trusted Software Development Methodology (TSDM) level IV a	
	security controls audit, and the Software Engineering Institute's	
:		Capability maturity mouor

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.

116

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).

118

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 dataseparately 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).
- 1) 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;

124

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.

125

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.

ETSI

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

[7]

"...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)"

 \checkmark 2 References

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

 \checkmark 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)...
- \checkmark 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?

129

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.

132

[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.

133

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

137

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

140

• *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	

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	

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	

148

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 - Accurac	y 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:

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 \rightarrow 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:

- 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 <OtherRalue> 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 agreed 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-PLUGTESTSTM event.

159

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> element 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 timestamped. 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">
    <rpre><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.
- 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.

161

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> <u>must</u> 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 <u>must</u> 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 <u>must</u> 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> <u>must</u> 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> <u>must</u> 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:

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

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:

This should be changed to:

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-PLUGTESTSTM 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]

166

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

167