# 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.

**DECT**<sup>TM</sup>, **PLUGTESTS**<sup>TM</sup> and **UMTS**<sup>TM</sup> are Trade Marks of ETSI registered for the benefit of its Members. **TIPHON**<sup>TM</sup> and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members. **3GPP**<sup>TM</sup> is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

# Contents

Intelle	ectual Property Rights	7
Forew	/ord	7
Introd	luction	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	Commente	12
51	TS 101 456 Ouglified contificate policy	12 12
5.1	TS 101 450 - Qualmed certificate policy	12 /11
5.2	TS 101 755 - ES electronic signature formats	
5.5	TS 101 862 - Qualified certificate profile	
5.5	TS 101 903 - XML advanced electronic signatures (XAdES)	
5.5	TS 107 903 - Time stamping policy	01 79
5.0	TR 102 038 - XML format for signature policies	
5.8	TR 102 050 - Aire formation signature policies	
5.9	TS 102 042 - PKC certificate policy	
Anne	x A: Comments in their original format	111
A 1	Comments from a TC-FSI member	111
A 1 1	TS 101 456 - Qualified certificate policy	
A 1 1	Proposed amendments from CEN/ISSS area M on system backup and recovery	
A.1.1.2	2 Auditor's view of system logs	
A.1.1.3	3 Export of the CA private key	
A.1.1.4	4 Mapping with RFC 2527	
A.1.2	TS 102 042 - Normalized certificate policy	
A.1.2.1	1 Export of the CA private key	114
A.1.2.2	2 Mapping with RFC 2527	114
A.1.3	TS 102 023 - Time-stamping policy	115
A.1.3.	1 Export of the CA private key	115
A 2	Comments and proposed amondments from LININEO STT (Italy)	116
A.2 1	Droposed amendments on TS 101 456	110 116
A.2.1	Proposed amendments on TS 101 450	110
A.2.2	Figure Formation Figure	119 122
A.2.3 $\Delta 2.4$	Stable informal comments on TS 101 733 from STT_A2 WG (September 2002)	122 122
A 2 4	Proposals about the document contents	122
A 2.4 2	<ul> <li>Proposals about the document structure</li> </ul>	123
A.2.4.3	3 Proposals for some additional explanatory documents	
A.2.5	Proposed amendments to TS 101 862 from STT-A4 WG.	
A.2.5.1	1 References to be updated	
A.2.5.2	2 CSP identifier	
A.2.5.3	3 Identity of the signer	
A.2.5.4	4 Pseudonyms	
A.2.5.5	5 SerialNumber attribute	
A.2.5.6	6 The key usage	
A.2.6	Proposed amendments to TS 102 023 - Time-stamping policy	126
A.3	Comments and proposed amendments from Japan and China PKI forums	128

A.3.1	Proposed amendments on TS 101 456	128
A.3.1.1	Comment #1, page 10	129
A.3.1.2	Comment #2, page 18	129
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	132
A.3.2.3	Comment #2, pages 16 and 17	132
A.3.2.4	Comment #3, clause 8.9.1	132
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	132
A.3.2.8	Comment #7, clauses 5.4.5 and 5.4.7	133
A.3.3	Proposed amendments on TS 101 903	133
A.3.3.1	Rationale: "Some comments regarding EESSI Signature Policy"	133
A.3.3.2	Comment #1, page 17	133
A.3.3.3	Comment #2	133
A.3.3.4	Comment #3	133
A.3.4	Proposed amendments on TS 101 861 - Time stamping profile	134
A.3.4.1	Comment #1. clause 5.1.2.	134
A.3.4.2	Comment $\#2$ , clause 5.2.3.	.134
A.3.4.3	Comment #3	134
A 3 5	Comments and proposed amendments on TS 102 023	134
A 3 5 1	Comment #1 clause 4.2	134
A 3 5 2	Comment #2 clause 4.2	135
A 3 5 3	Comment #3, clause $7.1.2$ d)	135
A 3 5 4	Comment #4 clause $7.1.2$ d)	135
A 3 5 5	Comment #5, clause 7.2.1 b)	135
A 3 5 6	Comment #6, clause $7.2.10$	135
Δ357	Comment #7, clause $7.2.2 \text{ a}$	135
A 3 5 8	Comment #8, clause $7.2.2$ b)	135
Δ359	Comment #0, clause 7.3.1 e)	135
Δ 3 5 10	Comment #10, clause $7.3.2$ a)	136
Δ 3 5 11	Comment #11, clause $7.3.2$ d)	136
A 3 5 12	Comment #12 clause 7.4.8	136
A 3 5 13	Comment #12, clause 7.4.8 c)	136
Δ 3 5 1/	Comment #14	136
A 3 6	Comments and proposed amendments on TP 102 038	137
A.3.61	Comment #1	137
Δ37	Comments and proposed amendments on TR $102.041$	137
A 3 7 1	Comment #1 clause 8.3.1 Signature validation policy	137
A.3.7.1	Commont #2, clause 8.3.2 - Signature validation information	127
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	138
A.4.1.1	Keys certified under multiple policies	138
A.4.2	Proposed amendments on TS 102 042 - Normalized certificate policy	140
A.4.2.1	Keys certified under multiple policies	140
A.5 C	Comments and proposed amendments from Pink Roccade (Netherlands)	.142
A.5.1	Proposed amendments on TS 101 456 - Qualified certificate policy	142
A 6 (	Comments and proposed amendments from FESSI evaluation	1/13
A.6 1	Suggested amondments on TS 101 456 Qualified certificate policy (see EESSI #21/2002)04 clause 6)	1/2
A.0.1	Suggested amendments on TS 101 450 - Qualified certificates profile (see EESSI #21(2002)04 - clause 0)	145
A.0.2	Suggested amendments on 15 101 802 - Quanned certificates prome (see EESS1 #21(2002)04 - clause	142
	UJ	143
A.7 C	Comments and proposed amendments from CEN/ISSS WS/E-Sign Area M and ETSI STF-210	
n	naintenance groups	144
A.7.1	Proposed amendments on TS 102 023 - Time-stamping policy	144
/ • 1		
A.8 C	Other comments and proposed amendments	.144
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	146
A.8.2.3 Reference to CWA 14167-1 in clause 7.4.7	147
A.8.2.4 When A new Policy OID is required	147
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-FSI member	150
A 9.1 Proposed amendments on TS 101.862 and related discussion threads	150
A.9.1 Proposed amendments on TS 102 022 and related discussion threads	
A.5.2 Proposed amendments on 15 102 025 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	1"
A.10.1.10 Proposed amendments related to clause 7.3.2 "Certificate renewal, rekey	and update"156
A.10.1.11 Proposed amendments related to clause 7.3.4 "Dissemination of Terms a	Ind Conditions"156
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	
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 #13 – .NET validating parser	
A.12.1.14 Issue #14 – XAdES schema	
A.12.1.15 Issue #15 – <qualifyingpropertiesreferencetvne> data type</qualifyingpropertiesreferencetvne>	
A.12.1.16 Issue $\#16 - XAdES$ examples	
A.12.1.17 Issue #17 - <dataobjectformat></dataobjectformat>	
A 12 1 18 Issue #18 - <certificatevalues></certificatevalues>	165

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	In clause 7.4.8	clause 7.4.8 subsection CA General an additional sub-sub-section could be added, named "System backup and recovery", covering the need for									
	text	these backups	in order to resume fur	nctions upon dis	saster. This cla	use should specify	that while the sy	stem data backup may	be performed by one			
	Original	riginal To add a sub-sub-section named "System backup and recovery" in clause 7.4.8 subsection CA General. To be further specified.										
	resolution											
	proposal											
	Resolution											
	Comment											
	text											
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS101456-002	1.2.1	7.4.3 g)	TC-ESI_1-002	30/01/2003	technical			not yet processed				
	Comment	Clause 7.4.3.g)	last bullet reads:									
	text	"System Audito	rs: Authorized to view	and maintain a	archives and au	dit logs of the CA	trustworthy syste	MS". 	l of truct If I are wrong			
		nease say it cle	as just look at archiv	uree the senter	nanuculieu . li nce should read	"System Auditor	s. Authorized to v	iew archives and audit	logs of the CA			
		trustworthy syst	tems" performed unde	er at least dual	control.	. Oystern / touttor						
	Original	Clause 7.4.3.g)	last bullet change the	e sentence "Sys	stem Auditors: A	Authorized to view	and maintain arc	hives and audit logs of	the CA trustworthy			
	resolution	systems" to "Sy	stem Auditors: Autho	rized to view ar	chives and aud	it logs of the CA to	rustworthy system	is".				
	proposal					-						
	Resolution											
	comment											
	Resolution											
	τεχτ	1										

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
		-	reference					· · · · ·					
TS101456-003	1.2.1	2	UNSTT-001		editorial			not yet processed					
	Comment text	Update the refe	rence FIPS PUB 140	-1 (1994): "Sec	urity Requireme	ents For Cryptogra	aphic Modules".						
	Original	New reference:	New reference: FIPS PUB 140-2 (2001): "Security Requirements For Cryptographic Modules".										
	resolution												
	proposal												
	Resolution												
	comment												
	Resolution												
	text								<b></b>				
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	туре	source	date		version				
TS101456 004	1 2 1	4.1 (1ct para)			oditorial			not vot processed					
13101430-004	Comment	4.1 (1St para)	Modify the text: "The certification authority has overall responsibility for the provision of the certification services identified in clause 4.1. The										
	toyt	certification authority's key is used to sign the gualified certificates and it is identified in the certificate as the issuer".											
	Original	New text: "The	Certification Authority	has overall res	sponsibility for t	he provision of ce	rtification service	s identified in clause 4.2	The certification				
	resolution	authority is identified in the certificate as the issuer and its private key is used to sign gualified certificates".											
	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										
TS101456-005	1.2.1	4.1 (2nd para)	UNSTT-001		editorial			not yet processed					
	Comment	Modify the text:	"However, the key us	sed to generate	the certificates	"							
	text												
	Original	New text: "How	ever, the private key	used to sign the	e certificates,	"							
	resolution												
	proposal												
	Resolution												
	comment												
	Resolution												
1	text	1											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS101456-006	1.2.1	4.2	UNSTT-001		technical			not yet processed					
	Comment	Modify the text:	"Dissemination servi	ce: disseminate	es certificates to	subjects, and if t	he subject conser	nts, to relying parties. T	his service also				
	text	disseminates the	e CA's terms and con	ditions, and an	y published poli	cy and practice in	formation, to sub	scribers and relying par	rties".				
	Original	New text: "Disse	ew text: "Dissemination service: disseminates certificates to subjects, and if subject consents, makes them available to relying parties. This service										
	resolution	also makes ava	o makes available the CA's terms and conditionsto subscribers ad relying parties".										
	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				
<b>TO</b> 404 450 007	1.0.1												
15101456-007	1.2.1	6.2		41	tecnnical			not yet processed	- the - fell - when				
	Comment	Modify the text:	The CA shall oblige	, through agree	ement (see claus	se 7.3.1 n)), the s	ubscriber to ensu	re that the subject fulfils	s the following				
	text	obligations:	rate and complete inf	rmation to the		as with the requir	amonto of this no	liou portioulorly with ro	aarda ta ragistratian.				
		a) Submit accur	kov poir for electronic		d in accordance	with only other line	enterns or this po	the subseriber (see a					
		c) evercise rea	sonable care to avoid	unauthorized	u in accordance	e with any other in	mitations notified i		lause 7.3.4),				
		d) if the subscr	iber or subject genera	tes the subject	's kove.	ci s private key,							
		- denerate	subject's kevs using	an algorithm re	cognized as he	ing fit for the purr	oses of qualified	electronic signatures.					
		- use a key	v length and algorithm	which is record	nized as being	fit for the purpose	es of qualified elec	ctronic signatures:					
		NOTE 1 It is c	urrently proposed that	t the recognitio	n of algorithms	with associated k	ev length being f	it for the purposes of a	ualified certificates is				
		throu	gh a cryptographic ac	lvisorv panel ur	nder the commit	tee identified in a	rticle 9 of the Dire	ctive [1].					
		- 01	nly the subject holds t	he private key	once delivered	to the subject.							
		e) if the certification	ate policy requires us	e of an SSCD (	i.e. QCP public	+ SSCD), only us	e the certificate w	ith electronic signature	es created using such a				
		device;											
		NOTE 2: The a	above item is NOT ap	plicable to qual	ified certificate	policy: QCP publi	C.						
		f) if the certification	ate is issued by the C	A under certific	ate policy QCP	public + SSCD a	nd the subject's ke	eys are generated unde	er control of the				
		subscriber, generate the subject's keys within the SSCD to be used for signing; NOTE 3: The above item is NOT applicable to qualified certificate policy: QCP public.											
		g) notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:											
		<ul> <li>the subject's private key has been lost, stolen, potentially compromised; or</li> <li>control over the subjects private key has been lost due compromise of activation data (e.g. PIN code) or other reasons; and/or</li> </ul>											
		- inaccurat	cy of changes to the (	the subject's pr	ivoto kovicimed to	o the subscriber.	nonontly discontiv	aucd "					
		(iii) ioliowing cor	npromise, the use of	ine subjects pr	ivate key is imn	reciately and peri	nanenuy discontir	iueu.					

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
			reference										
	Original	New text: "The	CA shall oblige, throu	gh agreement	(see clause 7.3	.1 h)), the subscri	ber:						
	resolution	1) to make the	i) 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										
	proposal	In clause 7.3	3.1.a); at the aubiest fulfile th	o following obl	inctional								
		2) to ensure that the subject fulling 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.											
		particula	<ul> <li>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);</li> <li>c) exercise reasonable care to avoid unauthorized use of the subject's private key;</li> <li>d) idem;</li> </ul>										
		b) only use											
		c) exercise											
		d) idem;											
		e) idem;											
		f) idem;		anabla dalay d	directly or through	ah tha auhaarihar	if any						
		b) idem "	e CA without any reas	ionable delay, d	directly of through	gn the subscriber.	, ii any,						
	Resolution												
	comment												
	Resolution												
0	text	Dellassakla	Oninin al	0	0	Deschution	Deschutien	Deschutien status	Della sechia (ense)				
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	Version	clause	reference	uate	type	Source	uale		Version				
TS101456-008	1.2.1	7.2.1	UNSTT-001		technical			not yet processed					
	Comment	Modify the text:	"b) CA key generatio	n shall be carri	ed out within a	device which eithe	er:	· · ·					
	text	- meets the requirements identified in FIPS PUB 140-1 [5] level 3 or higher"											
	Original	New text: "b) CA key generation shall be carried out											
	resolution	- meets the requirements identified in FIPS PUB 140-1 [5] or FIPS PUB 140-2 [9] level 3 or higher"											
	Proposal												
	comment												
	Resolution												
	text												
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
T0404450.000	1.0.1	700			technical								
15101456-009	1.2.1	1.2.2 Modify the text:	UNSTT-001 "a) The CA private ci	 gning kov chall	he held and us	l ad within a secur	 o cryptographic d	Inot yet processed					
	text	- meets the re	a) me CA private si equirements identified	Lin FIPS PUB 1	40-1 [5] level 3	or higher."	e cryptographic u						
	Original	New text: "a) "T	he CA"			or nighter,							
	resolution	FIPS PUE	3 140-1 [5] or FIPS PI	UB 140-2 [9]"									
	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									
TS101456-010	1.2.1	7.2.9	UNSTT-001		technical			not yet processed				
	Comment	Modify the text:	"NOTE 2: Separation	n may be achiev	ved by ensuring	distribution and o	delivery at differer	nt times, or via a differer	it route."			
	text	nal New text: "NOTE 2: Separation may be achieved by ensuring distribution of activation data and delivery of secure signature creation device"										
	Original											
	resolution proposal											
	Resolution	solution										
	comment											
	Resolution											
	text								<b></b>			
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
<b>TO</b> 404 450 044	4.0.4	7.0.4										
15101456-011	1.2.1	1 7.3.1 UNSTI-001 [tecnnical ] not yet processed										
	Comment	Modify the text:				4						
	text	f) The subscrit	per shall provide a ph	ysical address,	or other attribu	tes, which descrit	be now the subsc	nder may be contacted.				
			ahava itana ahava da.	a natannh far								
		NOTE 7. The	above item above doe	es not apply for	QCP Public.							
		i) The records	identified above abol	I ha ratainad fa	r at the pariod of	f time on indicate	d to the cube orib	or (and b) above)	and an pagagary for			
		the nurnose	s for providing eviden	ce of certificati	at the period t	podings "			and as necessary for			
	Original	New text:	s for providing eviden		on in legal proc	eeungs.						
	resolution	"f) This comma	should be cancelled	from this section	on (Subject regi	etration) and inco	rted in "Subscribe	r's obligations" (this kin	d of information is			
	nronosal	nrovided at	the moment of signing	the agreement	of hy the subscr	ihor)		a s obligations (this kin				
	proposal	provided at	the moment of signing	g the agreement		1001).						
		NOTE 7. The i	tem above									
		i) "legal proceedings according to the national law of the country where the Certification Service Provider is established "										
	Resolution											
	comment	nent										
	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 vet processed				
	Comment	Modify the text:	"c) if the CA genera	ted the subjec	ts key:	1						
	text	- the procedu	re of issuing the certif	icate is securel	ly linked to the g	generation of the k	key pair by the CA	λ;				
		<ul> <li>the private k</li> </ul>	ey (or SSCD - see cla	ause 7.2.9) is s	ecurely passed	to the registered	subscriber or sub	ject."				
	Original New text: "c) "if the CA generated the subject's key:											
	resolution	esolution - the procedure of issuing										
	proposal	<ul> <li>the private k</li> </ul>	ey is securely passec	I to the register	ed subject"							
	Resolution											
	comment											
	Resolution											
	text		<b>•</b> • • • •									
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	reference	date	туре	source	date		version			
TS101456-013	1.2.1	7.3.6	UNSTT-001		technical			not yet processed				
	Comment	Modify the text:										
	text	"g) Where Ce	rtificate Revocation Li	sts (CRLs) incl	uding any varia	nts (e.g. Delta CR	Ls) are used, the	se shall be published a	t least daily and:			
		- every (	CRL shall state a time	for next CRL is	ssue; and							
		- a new	CRL may be publishe	d before the st	ated time of the	next CRL issue;"						
	Original	New text:										
	resolution	"g) Where Cel	rtificate Revocation Li	sts (CRLs) incl	uding any varia	nts (e.g. Delta CR	Ls) are used, the	se shall be published a	t least daily and:			
	proposal	- every C	CRL shall state a time	IOF NEXT CRL IS	ssue; and	nove CDL incurse						
			CRL may be publishe	he certification	aled lime of the	authority designa	ted by the $CA$ "					
	Resolution				autionty of all	autionty designa						
	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									
TS101456-014	1.2.1	7.4.4	UNSTT-001		technical			not yet processed				
	Comment	Modify the text:										
	text	"e) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate										
		generation, subject device provision and revocation management services. Any parts of the premises shared with other organizations shall be										
		outside this perimeter.										
		f) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources										
		themselves, and the facilities used to support their operation. The CA's physical and environmental security policy for systems concerned with										
	certificate generation, subject device provision and revocation management services shall address the physical access control, natural protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection											
		against thef	, breaking and entering	ng, and disaste	r 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 output output of the case of th										
		without auth	orization.									
		NOTE 1: See	SO/IEC 17799 for gu	idance on phys	sical and enviror	imental security.	4	. Particular and a state state of a				
	NOTE 2: Other functions may be supported within the same secured area provided that the access is limited to authorized personnel."											
	Original	New text: "Certi	ficate generation, suc	ect device pro	vision and revo	cation manageme	ent ritu a crimo oto ro (	) and used the contificate	experience which			
	resolution	e) Physical pro	tection shall be achie	ved through the	e creation of cle	any defined secu	nty perimeters (	.) around the certificate	generation, subject			
	proposal	device provision and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.										
		INUTE I. AS de	subjects". In the case the CA gives Registration authorities the responsibility to provide signature devices to subjects comma e) is									
		annli	coble only to subject (	device preparat	tion (and NOT n	rovision)	ity to provide sign					
		a) idem				10131011).						
		NOTE 2										
		NOTE 3:"										
	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									
TS101456-015	1.2.1	7.4.5	UNSTT-001		technical			not yet processed	l			
	Comment	Modify the text:										
	text	"c) Media used	within the CA shall be	e securely hand	lled to protect m	nedia from damag	e, theft and unau	thorized access."				
	Original	New text:										
	resolution	"c) Media used	within the CA shall be	e securely hand	led to protect m	nedia from damag	je, theft, and unau	uthorized access. Media	life cycle management			
	proposal	shall be suc	h to proactively preve	nt obsolescenc	e."							
	Resolution											
	comment											
	Resolution											
	text	1										

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
			reference		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,							
TS101456-016	1.2.1	7.4.8	UNSTT-001		technical			not yet processed				
	Comment	Modify the text:	"Revocation status									
	text	<li>b) In the case of</li>	of compromise the CA	shall as a min	imum provide t	he following unde	rtakings:					
		- inform all subscribers, relying parties and other CAs with which it has agreements or other form of established relations of the comprom										
	Original	New text:										
	resolution	a) In the case	of compromise									
	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										
	Decelution	relations	, among which relying	parties and C	AS"							
	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									
TS101456-017	1.2.1	7.4.9	UNSTT-001		technical			not yet processed				
	Comment	Modify the text:	"CA General									
	text	a) Before the C	CA terminates its serv	ices the followi	ng procedures s	shall be executed	as a minimum:					
		- the CA s	hall inform all subscri	bers, relying pa	arties and other	CAs with which it	has agreements	or other form of establis	shed relations."			
	Original	New text: "CA g	jeneral									
	resolution	a) before the C	A terminatesthe CA	shall	will information a	uhianta) and any			an form of optical links of			
	proposal	- Inform a	subscribers (and the	se one in turn	will inform the s	subjects) and any	entity with which	it has agreements or oth	her form of established			
	Pesolution	Telations	, among which relying	parties and C	45.							
	comment											
	Resolution											
	text											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	Version	Clause	reference	uale	type	Source	uale		Version
TS101456-018	1.2.1	7.4.11	UNSTT-001		technical			not yet processed	
	Comment	Modify the text:	"i) The CA shall er	sure that all re	gistration inform	nation including th	e following is reco	orded:	
	text	<ul> <li>type of d</li> </ul>	ocument(s) presented	d by the applica	ant to support re	egistration;			
		- record of	unique identification	data, numbers	, or a combinat	ion thereof (e.g. a	pplicant's drivers	license number) of iden	tification documents, if
		applicab	le; acation of conios of a	polications and	Lidentification	locumente includ	ing the signed sub	scriber agreement (co	a a a a a a a a a a a a a a a a a a a
		- any spec	cific choices in the sub	scriber agreen	nent (e.g. conse	ent to publication	of certificate);"	Scriber agreement (See	clause 7.3.1 11)),
	Original	New text: "The	CA shall ensure that a	all relevant info	rmation concer	ning a qualified ce	ertificate is recorde	ed for an appropriate pe	riod of time, in
	resolution	particular for the	e purpose of providing	evidence of co	ertification for th	ne purposes of leg	al proceedings a	ccording to the national	law of the country
	proposal	where the Certi	fication Service Provid	der is establish	ed."				
		Registration	I oncure that all region	tration informat		vifia abaiaaa in tha		mont (o a oubicato' oor	cont to publication of
		certificate)."	ii ensure that all regist		ion any spec		subscriber agree	ment (e.g. subjects cor	Sent to publication of
	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
TS101/56-019	121	13		17/02/2003	technical	STE2/2	21/06/2003	no change	
10101430-013	Comment	In clause "4.3 C	ertificate policy and c	ertification prac	tice statement	will it be better to	add the specific	ations of the relations b	etween them and the
	text	cross authentica	ation?	ermennen prat		,			
	Original								
	resolution								
	proposal	One en entificatio	· · · · · · · · · · · · · · · · · · ·						
	comment	Cross certificate	es not specifically add	ressed by curre	ent 15 101 456				
	Resolution								
	text			-	-				
Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
T0404450.000	4.0.4	7.0.4	reference	17/00/0000			0.4/0.0/00.00		
15101456-020	1.2.1	7.2.4	JCPKI-001	17/02/2003	technical	SIF242	21/06/2003	no change	
	text	7.2.4 Key esch	ow, now to nancie the		egai monitor in	i the wireless com	munications?		
	Original								
	resolution								
	proposal				(not data anomu	ntine kovo) for vik	iah data manitarin	a and Faster is not an	liachta
	Resolution	I ne present do	cument only applies to	signing keys	(not data encry	ption keys) for wh	ich data monitorin	g and Escrow is not ap	
	Resolution								
	text								

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version		
TS101456-021	1.2.1	7.2	JCPKI-001	17/02/2003	technical	STF242	21/06/2003	no change			
	Comment	In clause "7.2 F	ublic key infrastructu	ure - Key manad	ement life cycl	e", why it doesn"t	mention the oper	ation of "certification aut	hority key update" like		
	text	the protocols in	PKIX?				•		, , ,		
	Original resolution										
	proposal										
	Resolution	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).		
	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		
TS101456-022	1.2.1		TC-ESI_3-001		technical			not yet processed			
	Comment	Comment:									
	text	We have not lo	oked at possible con	flicts, which mag	y arise when th	ere are more than	one certificates i	ssued to a key pair, e.g.	generated and residing		
		on a card. Thes	se certificates may be	e issued by diffe	erent CAs, unde	r different CPs.					
		I have, so far, i	dentified one potentia	al conflict. Assu	me that two CA	s issue two differe	ent certificates to	the same key, one spec	ifying 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 clue about. Without a flag in the CP the situation is not transparent to auditors either. We should consider to look at:									
		a) whether the	ere are other potentia	I conflicts for the	e configuration	described above,	and				
		b) how to addr	ess them.	مامنا مامار مامار		4h:a					
		Maintenance of	r the policies is proba	ibly the right pla	ice to deal with	tnis.					
		Liscussion.									
		Providing a fram	aye. nework to support th	e use of e-sign	atures and crea	ting an environme	nt which will prop	note truet and protecting	n the interests of		
		consumers rely	ing on e-signatures:	is an objective i	under EESSI ar	and the Directive		iote trust, and protecting			
		It is technically	nossible that the san	ne nublic kev m	av be included	in more than one	certificate (This o	could well be the case for	or example where the		
		key pair is dene	erated by the subscri	her which he se	ends to more th	an one certificatio	n authority) In de	peral there may be not	hing objectionable in		
		this, but for son	ne applications, this i	may be undesira	able, particularly	v where higher lev	els of assurance	are required.			
		Issue revolves	around:			,					
		a) the quality of	of the key pair genera	ated: and							
		b) the creation	of a close association	on between the	key pair and an	application for wl	hich it is to be use	ed.			
		Qualified certifi	cates are designed to	o offer a high le	vel of assuranc	e which needs to	be maintained in	all aspects of the service	e. TS 101 456 [2] does		
		not prohibit sub	scriber generation of	f keys. It should	be preferred th	at the certification	authority takes r	esponsibility for generat	ing the keys. This is not		
		currently part o	f Electronic Signature	es Directive, no	r conformance g	guidance.					
		Qualified certifi	cates may be used to	o support an art	icle 5.1 e-signa	ture; they may als	o be used for aut	hentication in general us	se.		
		Article 5.1 signa	atures must be recog	inized in legal p	roceedings as t	he equivalent of h	and written signa	tures. Other electronic s	signatures may be		
		recognized as a	such, although proba	bly only if they	satisfy at least t	he definition of an	advanced electro	onic signature under arti	cle 2.2.		
		It is suggested,	therefore, that subse	criber key pairs	issued for the p	ourpose of creating	g any type electro	nic signature which is in	tended to fulfil the		
		function of a ha	and written signature,	i.e. one which	is to be treated	as a handwritten	signature by a rel	ying party, should be rea	stricted to that purpose.		
		In respect of bo	oth qualified certificat	es AND any e-s	ignature which	is intended to be	a handwritten sig	nature equivalent, there	is a need that they		
		should provide	a high level of assura	ance to any thire	d party who ma	y reasonably rely	on this.				

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
		Signatures in th	e real world perform t	wo main function	ons:			-				
		- they indicate	a will or intention by	the signer to ta	ike on a commit	ment. (The exact	nature of the con	nmitment may be ambio	yuous except by			
		reference to	the document to which	ch it is applied,	or to some othe	er evidence); and		, , , , , , , , , , , , , , , , , , , ,				
		- a signature i	is evidence of itself. i.e	e. of the act of	sianina.	,,						
		Therefore, there	e are two elements wh	nich electronic	signatures cann	ot prove:						
		a) the intention	to express a commit	ment: and	5							
		b) the intention	to create the signatu	re.								
		Even an article	5.1 electronic signatu	re created usin	a public kev crv	ptography, i.e. die	pital signatures, a	re not (unless there is c	other evidence) capable			
		of demonstratin	a the signer's intentio	ns. However. ir	tent is an essei	ntial element of si	aning and there is	s an urgent need to find	a means of			
		incorporating th	is factor into an electr	onic signature	which is intend	ed as a handwritt	en signature					
		One factor whic	h could provide evide	nce of the inter	tion to create a	signature equiva	lent to a h/w one	is to "bind" the signing	key to the application			
		This could be a	chieved by restricting	the use of a ke	v to a "signing"	application i.e. b	v including it in a	certificate (qualified) wh	hich specifies a key			
		usage	onio vou by rootholing		y to a orgining		y morading it in a	(qualities) m				
		The relving part	he 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 mak	itention to make the signature as a handwritten one. This requires two steps:									
		- making it cle	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 bes	(second best) by legal means;									
		- ensuring a n	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 use of his key pair for any other purpose. As a preference, the section which the keys are stored should also be dedicated to a bwisign, but this may carry uprealistic costs implications. The									
		reason is that w	ill give an opportunity	to include som	ething on the c	asing of the sscd	which will alert th	e signer to its significan	ice as a signing device			
		The fact that:			ion ing on the o	aonig er are eeea						
		<ul> <li>key usage is</li> </ul>	s restricted, and									
		- the signer p	robably knew that key	usade was res	stricted							
		will provide prim	ha facie evidence that	the signer kne	w what kind of e	electronic signatu	re he was making	i.e. that a commitmen	t that may be enforced			
		by law was bein	ng undertaken as a res	sult			e ne nae manig	,				
		Enforcement										
		It has been arou	ed that certification a	uthorities shou	ld be free to dea	cide for themselve	es whether to enfo	orce obligations against	a subscriber. There			
		may be many re	easons for NOT taking	any enforcem	ent action:			stoo oxingullorio algullor				
		- the certificat	ion authority does not	regard the bre	ach as being si	onificant:						
		- the certificat	ion authority itself has	s not suffered a	ny loss, neither	will its inaction is	not (currently) in	contravention of any au	uditing criteria, or			
		quidance.							annig ernena, er			
		- the subscrib	er is a customer, there	e is a real confl	lict of interest - i	t is not a good ma	arketing practice t	o bring legal proceeding	as against customers:			
		and				e le liet a geoa lin		e anng legal precedani,	ge agamet eacternete,			
		- cost of legal	proceedings									
		The reliability of	signatures = to h/w s	ionatures is a r	matter of public	interest, therefore	e. the responsibilit	v for ensuring their effe	ctiveness should not			
		just be left to the	e discretion of a certifi	ication authority	. The role of the	e certification aut	nority should be to	take such steps as ar	e reasonably within its			
		competence an	d power to ensure a s	ingle use of ke	vs used to creat	te such signatures	s. This could be n	rovided for by including	appropriate			
		requirements in	TS 101 456 [2] and T	S 102 042 [3]	or for the time h	peing, in any appr	opriate maintena	nce document).				
		In due course i	t is to be hoped (and a	expected) that	national laws wi	Il impose the sam	e level of respon	sibility of a signer as cu	rrently exist in relation			
		to a handwritter	n signature. However	this cannot ha	open for so long	as there is ambi	auity surrounding	the electronic signature	e creation.			
L	1		i signataro: i lonever,				gaily barroanaing	and choose on the digitature				

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									
	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		
	Iter in the initial initinitial initinitial initiniti initial initial initial i									
	Original resolution proposal									
	Resolution comment									
	Resolution text									

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version	
TS101456-024	1.2.1		EESSI-001		technical			not yet processed		
	Comment text	<ul> <li>Mandate that Authority) to</li> </ul>	at either a formal asse issue its first qualifie	essment or a cland de certificate.	aim supported b	by an audit is requ	ired before a CS	P is allowed (by the rele	vant Supervisory	
	Original resolution proposal									
	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	
TS101456-025	1.2.1	7.2.9	OTHER-001		technical			not vet processed		
	Comment	I am wondering	whether we omitted	a clause in TS	101 456 [2] to s	tate that the CA s	hall inform their s	ubscribers about the kir	nd of environment that	
	text	he shall use for	the SSCD, pointing t	o CWA 14170	[13]: Security re	quirements for Si	gnature Creation	Systems.		
	Original	Add to clause 7	7.2.9:			•		•		
	resolution "NOTE: It is recommended that the CA advises subscribers as to the environments in which the SSCD should be used. This includes the									
	proposal	chara	acteristics of the devid	ces and applica	ations used, and	I the purpose or ir	tention of the act	of signing."		
	Resolution									
	comment									
	Resolution									
	text									
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version	
TS101456-026	1.2.1	7.2.5	OTHER-002		technical			not yet processed		
	Comment text	I think it is not v necessarily con requirement.	very feasible to require npromise security. Pro	e CSPs not to u obably we could	use same signin d advice CSPs t	g key for QCPs a to use dedicated l	nd NCPs. That's keys (use should	because I cannot see w instead of shall), but no	hy that would t make that as a	
	Original resolution proposal       a) Replace text in clause 7.2.5 with:         The signing keys(s) used for generating certificates, as defined in clause 7.3.3, and/or issuing revocation status information, shall not be under purposes if this results in the violation of THE SECURITY MEASURES OR ANY OTHER SPECIFIC LIMITATIONS PROVIDED FOR 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 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.									
	comment									
	Resolution									
	text									

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
TS101456-027	1.2.1	7.4.7	OTHER-003		technical			not yet processed					
	Comment text	Update clause RGW comment Directive 1999/9	7.4.7, note 1 to explici : "however, any such 93/EC Annex II (f)".	tly reference C reference shou	WA 14167-1 [1: Ild not be to the	2] and add the rel exclusion of any	erence to the bib other means of a	liography/references. dequately satisfying the	requirements of				
	Original resolution	Update clause	7.4.7, note 1 to explici	tly reference C	WA 14167-1 [1:	2] and add the rel	erence to the bib	liography/references.					
	proposal												
	Resolution comment												
	Resolution text												
Comment ID	Deliverable version	Deliverable clause	Deliverable clauseOriginal contribution referenceComment dateResolution sourceResolution dateResolution status versionDeliverable target version										
TS101456-028	1.2.1	8	OTHER-004		technical			not yet processed					
	Comment text	It is currently no	ot clear when a new co	ertification polic	cy is necessary								
	Original	Add to clause 8	:										
	resolution proposal	"No changes sh CA."	ould be made to a ce	rtificate policy v	which could affe	ect a relying party	s consideration o	n the reliability of the ce	rtificate issued by the				
	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											
TS101456-029	1.2.1	Introduction	STF220_4-001	08/09/2003	technical			not yet processed						
	Comment	Please add the	following text after the	e first paragrap	h.									
	text	Another importa	ant requirement of ele	ctronic comme	rce is the ability	to identify, not on	ly the originator o	f electronic information	in the same way that					
		documents are	signed using a hand-	written signatur	e, but also their	attribute(s), e.g. t	heir role(s) in an	organization.						
		This may be ac	hieved using certificat	ion services in	two ways:									
		<ul> <li>using attribut</li> </ul>	ites included in Public	Key Certificate	es (PKCs);									
		<ul> <li>using attribut</li> </ul>	ites included in Attribu	te Certificates	(ACs).									
		The former case	ormer case is covered in the present document. See TS 102 158 for the latter case.											
	Original	Please add the	ase add the following text after the first paragraph.											
	resolution	Another importa	ant requirement of ele	ctronic comme	rce is the ability	to identify, not on	ly the originator o	f electronic information	in the same way that					
	proposal	documents are	signed using a hand-	written signatur	e, but also their	attribute(s), e.g. t	heir role(s) in an	organization.						
		This may be ac	hieved using certificat	ion services in	two ways:									
		<ul> <li>using attribut</li> </ul>	ites included in Public	Key Certificate	es (PKCs);									
		<ul> <li>using attribut</li> </ul>	ites included in Attribu	te Certificates	(ACs).									
		The former case	e is covered in the pre	esent documen	t. See TS 102 1	58 for the latter ca	ase.							
	Resolution													
	comment													
	Resolution													
	text													

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version	
			reference							
TS101456-030	1.2.1	Introduction	STF220_4-001	08/09/2003	technical			not yet processed		
	Comment text	Please change The Directive 19 referred to as "t specifies requir. Directive specif certificates). The mentioned Certificates (PK on the purpose The present doo certificates in ac	the following paragra 999/93/EC of the Eur he Directive") identifi ements for qualified c ies requirements on c Directive also covers (Cs) (see annex I, cla for which the certifica cument specifies bas ccordance with the D	ph as subseque opean Parliame es a special forn certificates. Ann- certification-serv the use of attril use d) which re ate is intended". eline policy requirective. The use	ently specified. ent and of the Co m of electronic s ex II of the vice-providers is butes in public k fers to the "prov uirements on the e of a secure-sig	ouncil on a Comm signature which is suing qualified ce key certificates, sin vision for a specific e operation and m gnature-creation o	nunity framework based on a "qua ertificates (i.e. cer nce it mentions th c attribute of the s nanagement prac device, as require	for electronic signatures lified certificate". Annex tification authorities issu e possibility to include a signatory to be included tices of certification auth d through annex III of th	s [1] (hereinafter I of this Directive ing qualified attributes in Public Key if relevant, depending norities issuing qualified ne Directive, is an	
	optional element of the policy requirements specified in the present document.         Original resolution proposal       Please change the following paragraph as subsequently specified.         The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [1] (hereina referred to as "the Directive") identifies a special form of electronic signature which is based on a "qualified certificate". Annex I of this Dire 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 F Certificates (PKCs) (see annex I, clause d) which refers to the "provision for a specific attribute of the signatory to be included if relevant, c 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 issuir certificates in accordance with the Directive. The use of a secure-signature-creation device, as required through annex III of the Directive, or provision for a specifie direction device, as required through annex III of the Directive, or provision for a specific attribute of the signatory to be included if relevant, c on the purpose for which the certificate is intended".									
	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										
TS101456-031	1.2.1	2	STF220_4-001	08/09/2003	technical			not yet processed					
	Comment	Please add to the	ne list:										
	text	Council Directiv	e 93/13/EEC of 5 Apr	ril 1993 on unfa	ir terms in cons	umer contracts>	> a reference to the second	nis is asked to be added	d in clause 4.3.4				
	Original	Please add to the	lease add to the list:										
	resolution	Council Directiv	e 93/13/EEC of 5 Apr	ril 1993 on unfa	ir terms in cons	umer contracts>	> a reference to the	nis is asked to be added	d in clause 4.3.4				
	proposal												
	Resolution												
	comment												
	Resolution												
	text												

version         clause         contribution reference reference         date         type         source         date         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. associated with that entity. 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 proposal 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.         Society or in 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         Comment Resolution text         Deliverable clause         Original contribution reference         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 <tr< th=""><th></th><th>Deliverable</th><th>Deliverable</th><th>Original</th><th>Comment</th><th>Comment</th><th>Resolution</th><th>Resolution</th><th>Resolution status</th><th>Deliverable target</th></tr<>		Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
TS101456-032         1.2.1         3.1         STF220_4-001         08/09/2003         technical         not yet processed           TS101456-032         1.2.1         3.1         STF220_4-001         08/09/2003         technical         not yet processed           Comment text           Please add the following definitions. attribute information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.           Original resolution proposal         Please add the following definitions. 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 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 reference         Comment date         Resolution date         Resolution status         Deliverable target version           TS101456-033         1.2.1         4.1         STF220_4-001         08/09/2003         technical         not yet processed           TS101456-033         1.2.1         4.1         STF220_4-001         08/09/2003		version	clause	contribution	date	type	source	date		version				
TS101456-032       1.2.1       3.1       STF220_4-001       08/09/2003       technical       Inot yet processed         Comment text       Please add the following definitions. attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.         Original resolution proposal       Please add the following definitions. attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.         Resolution text       Resolution text       Comment         Deliverable version       Original contribution reference       Comment date       Resolution source         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       Inot yet processed         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       Inot yet processed				reference										
Comment text       Please add the following definitions. attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.         Original resolution proposal       Please add the following definitions. 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 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 text       Deliverable version       Original contribution reference       Comment date       Resolution source       Resolution date       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         Text       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       Into reference to clause 4.2.       Into reference to clause 4.2.	TS101456-032	1.2.1	3.1	STF220_4-001	08/09/2003	technical			not yet processed					
text       attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.         Original resolution proposal       Please add the following definitions. 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 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 text       Resolution text         Comment ID       Deliverable clause       Original contribution reference         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical         Version       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       Into the following paragraphs at the end.		Comment	Please add the	following definitions.										
Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.         Original resolution proposal       Please add the following definitions. attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in 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 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 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 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 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 the society or in a relationship.         Resolution text       Resolution text       Comment       Resolution text       Deliverable contribution reference       Resolution text       Deliverable version       Please change reference to clause 4.1 into reference to clause 4.2.         TS101456-033       1.2.1       4.1       STF220_4-001       08/09		text	attribute: inform	nation bounded to an e	entity that speci	ifies a character	istic of an entity, s	such as a group n	nembership or a role, or	r other information				
Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.         Original resolution proposal       Please add the following definitions. attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.         Resolution comment       Resolution comment         Resolution text       Original contribution or status         Comment ID       Deliverable clause       Original contribution attribution contribution reference       Comment date         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       not yet processed         Comment text       Typo -> Please add the following paragraphs at the end.       Attribute reference to clause 4.2.       Not yet processed			associated with	n that entity.										
Society or in a relationship.         Original resolution proposal       Please add the following definitions. attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.         Resolution comment       Resolution text       Comment clause       Comment contribution reference to clause       Comment date       Resolution source       Resolution date       Resolution source       Deliverable date       Deliverable target version         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       not yet processed         Typo -> Please add the following paragraphs at the end.       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       not yet processed			Attribute Granti	ing Authority (AGA): a	uthoritative sou	irce of an attribu	te role: function, p	position or status	that somebody has in a	an organization, in				
Original resolution proposal       Please add the following definitions. attribute: information bounded to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity. Attribute Granting Authority (AGA): authoritative source of an attribute role: function, position or status that somebody has in an organization, in society or in a relationship.         Resolution comment       Resolution text       Comment       Deliverable clause       Original contribution date       Comment type       Resolution source       Resolution date       Deliverable target version         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       Into reference to clause 4.2.         Please add the following paragraphs at the end.       Typo -> Please change reference to clause 4.1       Into reference to clause 4.2.			society or in a r	relationship.						-				
resolution proposal       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       Comment       Comment       Resolution date       Resolution type       Resolution source       Resolution date       Resolution status       Deliverable target version         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       Inot yet processed         Comment       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       Please add the following paragraphs at the end.		Original	Please add the	following definitions.										
proposal       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       Deliverable clause       Original contribution reference       Comment date       Resolution source       Resolution date       Resolution source       Resolution date       Resolution status       Deliverable target version         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       Into reference to clause 4.2.         Comment text       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       Into reference to clause 4.2.		resolution	attribute: inform	nation bounded to an e	entity that speci	ifies a character	istic of an entity, s	such as a group n	nembership or a role, or	r other information				
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       Original contribution reference       Comment date       Resolution source       Resolution date       Resolution source       Resolution date       Deliverable target version         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       Image: source of a status date       Imag		proposal	associated with	n that entity.										
society or in a relationship.         Resolution comment       Resolution text       Resolution text       Deliverable clause       Original contribution date       Comment type       Resolution source       Resolution date       Deliverable target version         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       not yet processed         Typo -> Please change reference to clause 4.1 into reference to clause 4.2.         Please add the following paragraphs at the end.			Attribute Granti	ing Authority (AGA): a	uthoritative sou	irce of an attribu	te role: function, p	position or status	that somebody has in a	n organization, in				
Resolution comment       Resolution text         Resolution text       Original contribution reference       Comment date       Resolution source       Resolution date       Resolution source       Deliverable date       Deliverable target version         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       not yet processed       Intervence of the second se			society or in a r	relationship.										
comment Resolution text       comment ID       Deliverable version       Original clause       Comment contribution reference       Comment date       Resolution source       Resolution date       Resolution status       Deliverable target version         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       not yet processed         Comment text       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       Typo -> Please add the following paragraphs at the end.		Resolution												
Resolution text       Resolution text         Comment ID       Deliverable version       Deliverable clause       Original contribution reference       Comment date       Resolution type       Resolution source       Resolution date       Resolution status       Deliverable target version         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       not yet processed         Comment text       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       Please add the following paragraphs at the end.		comment												
text       Comment ID       Deliverable version       Deliverable clause       Original contribution reference       Comment date       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       not yet processed         Version         text       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.         Please add the following paragraphs at the end.       Please add the following paragraphs at the end.		Resolution												
Comment ID       Deliverable version       Deliverable clause       Original contribution reference       Comment date       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       Interpretion         Comment text       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       Please add the following paragraphs at the end.       Interpretion		text		aliverable Original Commant Commant Desclution Desclution Desclution Status Deliverable torget										
version     clause     contribution reference     date     type     source     date     version       TS101456-033     1.2.1     4.1     STF220_4-001     08/09/2003     technical     not yet processed       Comment text       Please add the following paragraphs at the end.	Comment ID	Deliverable	Deliverable	eliverable Original Comment Comment Resolution Resolution Status Deliverable target										
reference       reference       not yet processed         TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       not yet processed         Comment text       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       Please add the following paragraphs at the end.		version	clause	clause contribution date type source date version										
TS101456-033       1.2.1       4.1       STF220_4-001       08/09/2003       technical       not yet processed         Comment text       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.       Please add the following paragraphs at the end.				reference										
Comment text       Typo -> Please change reference to clause 4.1 into reference to clause 4.2.         Please add the following paragraphs at the end.	TS101456-033	1.2.1	4.1	STF220_4-001	08/09/2003	technical			not yet processed					
text Please add the following paragraphs at the end.		Comment	Typo -> Please	change reference to	clause 4.1 into	reference to cla	use 4.2.							
· · · · · · · · · · · · · · · · · · ·		text	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			When a signer	signs a document it is	of primary imp	ortance to be at	ble to identify such	n signatory in the	interest of accountabilit	y. 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			transaction to b	be traceable. However	, in many cases	s, in order to acc	cept a signature, t	he acceptance cr	iteria may not necessar	rily 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			identity of the s	signer but instead, or a	dditionally, on t	the qualification	(s) of the signer. C	Jualifications in tr	is context have the me	aning of specific				
reatures or attributes that the signatory might possess in order to perform a certain act.			features or attri	ibutes that the signato	ry might posses	ss in order to pe	rform a certain ac	X.						
Such a qualification may be obtained using a 4 liste reference 4 a laws 4.2		Original		alion may be obtained	using attribute	S WILLIN PRUS II			signatures.					
Triginal Typo -> Please change reference to clause 4.1 into reference to clause 4.2.		Unginal	Typo -> Please	following percence to t	stause 4.1 into	reference to cla	use 4.2.							
<b>resolution</b> Please and the following paragraphs at the end.		proposal	Mease add the	aigna a document it is	at the end.	ortonoo to bo ob	ala ta idantifu ayak	a aignotory in the	interest of accountabilit	y This anables the				
proposal when a signer signs a document it is or primary importance to be able to identify such signatory in the interest of accountability. This enables the transaction to be transaction.		proposal	transaction to h	signs a document it is	in many case	in order to be at	pie to identify such	he accontance or	interest of accountabilit	ily be based on the				
identity of the signer but instead or additionally cases, in other to accept a signature, the acceptance chiefla may not necessarily be based of the			identity of the s	ignor but instead or a	ditionally cases	the qualification	(c) of the signer (	Ne acceptance cr	hie contaxt have the me	aning of specific				
features or attributes that the signatory might possess in order to perform a certain act			features or attri	ibutes that the signator	ry might posses	se in order to pe	(5) Of the signer. C	auainications in ti M	iis context have the me	aning of specific				
Such a qualification may be obtained using attributes within PKCs included or referenced in electronic signatures	1		features or attributes that the signatory might possess in order to perform a certain act.											
Resolution			Such a qualifier	ation may be obtained	using attribute	s within PKCs in	cluded or referen	ced in electronic	signatures					
comment		Resolution	Such a qualifica	ation may be obtained	using attribute	s within PKCs ir	ncluded or referen	ced in electronic	signatures.					
Resolution		Resolution	Such a qualifica	ation may be obtained	using attribute	s within PKCs ir	ncluded or referen	iced in electronic	signatures.					
text		Resolution comment Resolution	Such a qualifica	ation may be obtained	using attribute	s within PKCs ir	ncluded or referen	ced in electronic	signatures.					

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS101456-034	1.2.1	4.3.4	STF220_4-001	08/09/2003	technical			not yet processed					
	Comment	Please modify the	he first paragraph as f	follows.									
	text	In addition to the	e policy and practice	statements a C	A may issue ter	ms and conditions	s of general comn	nercial purpose. They n	nust follow the				
		requirements of	general conditions ar	nd comply with	the requirement	ts set out in Direc	tive 93/13/EEC ->	<ul> <li>add reference è as im</li> </ul>	plemented in the				
		national legislat	ion of the member sta	tes. In specific	, general conditi	ons are non-nego	otiable and binding	g to a non-determined r	number of end users.				
		They have, how	ever, to be brought to	the attention c	of contracting co	unter parties and	especially to con	sumers. Terms and cor	nditions will only be				
		effective agains	t relying parties, who	have no other o	contractual arra	ngement with the	CA if:						
		<ul> <li>they are easing</li> </ul>	sily accessible; and										
		<ul> <li>their existen</li> </ul>	ce together with infor	mation as to ho	w they can be a	accessed is broug	ht to their attentio	n in a conspicuous mai	nner; and				
		<ul> <li>they remain</li> </ul>	in line with the memb	er state law rec	garding general	conditions.							
	Original	Please modify the	he first paragraph as f	follows.	A				and fallen the				
	resolution	In addition to the	e policy and practice s	statements a C	A may issue ter	ms and conditions	s or general comm	nercial purpose. They n	nust follow the				
	proposal	national logislat	ion of the member sta	too In coorific	apporal conditi		tiphle and hinding	to a non determined r	plemented in the				
		They have how	ever to be brought to	the attention of	f contracting co	unter parties and		sumers Terms and cor	ditions will only be				
		effective agains	t relving parties who	have no other (	contractual arra	naement with the	CA if		lations will only be				
		<ul> <li>they are easily</li> </ul>	silv accessible: and			igomone with the	0/ ( 11.						
		<ul> <li>their existen</li> </ul>	ce together with infor	mation as to ho	w they can be a	accessed is broug	ht to their attentio	n in a conspicuous mai	nner: and				
		- they remain	they remain in line with the member state law regarding general conditions.										
	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										
TS101456-035	1.2.1	4.5	STF220_4-001	08/09/2003	technical			not yet processed					
	Comment	Add this new cla	ause with title "Certifie	ed attributes":									
	text	"Before being g	ranted, attributes shal	I be verified in	a way that the c	ertification author	ity is satisfied as	to their authenticity. It s	hall be verified that, at				
		the time of regis	stration for an attribute	e, the individual	was entitled to	claim that attribut	e.		4. A. II				
	Original	Add this name of	n Authority is response		g the correct att	ribution of attribute	es to subjects (se	e also clause 6.4 Liabil	ity).				
	Original	Add this new cla	ause with title Certifie	be verified in	a way that the	artification outbor	ity is potisfied as	to their outbooticity. It o	hall be verified that at				
	proposal	the time of region	tanted, attributes shall	the vermed in a	a way that the d	eluncation author	ity is satisfied as	to their authenticity. It s	nali de vermed triat, at				
	proposal	The Certification	a Authority is responsi	ible for verifying	was entitied to	ribution of attribut	e. As to subjects (se	a also clausa 6 / Liabil	ity) "				
	Resolution		T Autionity is respons		g the contest att				ity).				
	comment												
	Resolution	1											
	text												

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
<b>TO</b> 404 450 000	1.0.1	1.0	reference										
TS101456-036	1.2.1	4.6	STF220_4-001	08/09/2003	technical			not yet processed					
	Comment	Add this new cla	ause with title "Attribu	te semantics":			<i>c</i>						
	text	"The semantics	of an attribute may b	e either defined	l in a standard (	e.g. by ISO) or de	fined by any orga	anization.					
		When the attribu	ute is defined in a star	ndard, it may be	e used in an op	en community.							
		NOTE: It may	y be specified using a	In OID that has	a global interna	ational definition.	his is in this way	that X.509 has defined	a set of standard				
		attrib	utes. When it is locall	y defined by an	ly organization,	two approaches a	ire possible:						
		- Us	se an OID located un	der the OID of t	ne organization	;		nhu) and add a dafinitia	a of the ottaileute in easy				
		- 00			y (e.g. as called	111120/12 17090	J-2, see bibliogra	phy) and add a deimidd	on of the attribute in any				
		S) When the attribut	/max (e.g. character s	sung, AiviL).	ion ito uno mov	he restricted to a		. The compation of the	attribute has then to be				
		interpreted usin	preted using the identifier of the attribute granting authority (also called sometimes "issuing authority") in combination with the definition of the										
		attribute by that	ibute by that authority."										
	Original	Add this new cla	Induce by Inal authonity.										
	resolution	"The semantics	of an attribute may b	e either defined	l in a standard (	e a by ISO) or de	fined by any ora:	anization					
	proposal	When the attribution	ite is defined in a star	ndard it may be	e used in an on	e.g. by 100) of de	anned by any orga						
	propodu	NOTE: It ma	v be specified using a	n OID that has	a global interna	ational definition	This is in this way	that X 509 has defined	a set of standard				
		attrib	utes. When it is locall	v defined by an	v organization.	two approaches a	re possible:						
		- U	se an OID located un	der the OID of t	he organization	:							
		- de	efine the OID of the "i	ssuing authority	y" (e.g. as called	d in ISO/TS 17090	)-2, see Bibliogra	phy) and add a definitio	on of the attribute in any				
		S	/ntax (e.g. character s	string, XML).			U U		-				
		When the attribut	ute is locally defined t	y an organizat	ion, its use may	be restricted to a	close community	/. The semantics of the	attribute has then to be				
		interpreted usin	g the identifier of the	attribute grantir	ng authority (als	o called sometime	s "issuing authoi	rity") in combination with	n the definition of the				
		attribute by that authority."											
	Resolution	1											
	comment												
	Resolution												
	text												

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version		
			reference		-71						
TS101456-037	1.2.1	6.3	STF220_4-001	08/09/2003	technical			not yet processed			
	Comment text	Add this new clause with title "Subject obligations" (subsequent clauses must be renumbered accordingly): "The CA shall oblige, through agreement, the subscriber to agree with the subject that the subject is bound to: - use the PKC solely for the usage specified in the CPS; - notify the subscriber without any unreasonable delay, when there is an inaccuracy in the content of an PKC, whatever the reason may be, including a change in the ownership of an attribute."									
	Original resolution proposal	Add this new cla "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."								
	Resolution										
	comment Resolution text										
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version		
TS101456-038	1.2.1	7.3.1	STF220_4-001	08/09/2003	technical			not yet processed			
	Comment text	<ul> <li>In "Registration" please replace:</li> <li>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.</li> <li>with:</li> <li>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 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 or or electronic documentation.</li> </ul>									
<ul> <li>resolution proposal</li> <li>c) The service provider shall verify by appropriate means in accordance with national law, the identity and, if applicable, a person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person eit using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the electronic documentation.</li> <li>with:</li> <li>d) The service provider shall verify, at the time of registration, by appropriate means in accordance with national law, the any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked 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.</li> </ul>								and, if applicable, any physical person either vidence may be in the fo th national law, the ider ty shall be checked aga (see note 3). Submitted	specific attributes of the directly or indirectly orm of either paper or ntity and, if applicable, inst a physical person d evidence may be in		
	comment										
	Resolution text										

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version		
TS101456-039	1.2.1	7.3.1	STF220_4-001	08/09/2003	technical			not yet processed			
	Comment text	<ul> <li>In "Registration" please add:</li> <li>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 verification shall be done by appropriate means and in accordance with national law.</li> <li>m) The CA shall record all information used to verify the attributes of the subject.</li> <li>n) The CA shall ensure that the subject consents to include attributes in the PKC.</li> </ul>									
	Original resolution proposal	<ul> <li>In "Registration" please add:</li> <li>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. verification shall be done by appropriate means and in accordance with national law.</li> <li>m) The CA shall record all information used to verify the attributes of the subject.</li> <li>n) The CA shall ensure that the subject consents to include attributes in the PKC.</li> <li>o) The CA shall record the information demonstrating that a subject that accorded to have attributes within PKCs.</li> </ul>									
	Resolution comment Resolution text				× ,	<b>i</b>					

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	reference	date	туре	source	date		version
TS101456-040	1.2.1	7.3.2	STF220_4-001	08/09/2003	technical			not yet processed	
	Comment text	Please add the Attribute Regist a) The CA sha b) The CA sha number on t c) The CA sha d) The CA sha - whether registere - confirma	STF220_4-001 [08/09/2003 [technical] [Internation of the processed [Internation of the processed] [Internation of the processed [Internation of the processe						icluding any reference
		NOTE 1. Othe	agreement may be in	electronic form	or legal entity) providing all i	may be involved	in establishing th	is agreement.	
	Original resolution proposal	Please add the Attribute Regist a) The CA sha b) The CA sha number on t c) The CA sha d) The CA sha d) The CA sha - whethe registe - confirm NOTE 1: Othe NOTE 2: This	be certified. egistered (see item c), ir rson. Iusion in PKCs of the at	ncluding any reference tributes that have been					
	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									
TS101456-041	1.2.1	7.3.4	STF220_4-001	08/09/2003	technical			not yet processed				
	Comment	Please add the	following requirement	ts to item a):								
	text	- a clear desc	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 appropriat	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									
		- the list of do										
		of such right	of such right;									
		<ul> <li>how each at</li> </ul>	how each attribute will be represented in the PKC (e.g. a character string and/or an OID);									
		<ul> <li>any limitatio</li> </ul>	ns on their use;									
		<ul> <li>the subscrib</li> </ul>	er's and subject's obl	igations as def	ined in clauses (	6.2 and 6.3.						
	Original	Please add the	following requirement	ts to item a):								
	resolution	<ul> <li>a clear desc</li> </ul>	ription of the meaning	g of each type of	of attribute that i	s supported. That	description shall	be given in readily-und	erstandable terms, and,			
	proposal	if appropriat	e, the law or regulatio	n that defines	or assigns the a	ttribute shall be in	dicated;					
		<ul> <li>the list of do</li> </ul>	cuments the subject r	must exhibit to	prove his/her rig	tto register an a	attribute and the p	procedures used by the	CA for the verification			
		of such right	;		a. (							
		<ul> <li>how each at</li> </ul>	tribute will be represe	inted in the PK	C (e.g. a charac	ter string and/or a	an OID);					
		- any limitatio	ns on their use;									
		<ul> <li>the subscrib</li> </ul>	er's and subject's obl	igations as def	ined in clauses (	5.2 and 6.3.						
	Resolution											
	Comment											
	Resolution											
Commont ID	Deliverable	Deliverable	Original	Commont	Commont	Pasalution	Pecolution	Pecolution status	Deliverable target			
Comment ID	Deliverable	Deliverable	onginal	data	type	Resolution	data	Resolution status	Deliverable target			
	Version	clause	reference	uale	type	Source	uale		Version			
TS101456-042	121	Anney F	STF220 /-001	08/09/2003	technical			not vet processed				
10101400 042	Comment	Please add the	following references:	00/03/2000	teennieai			not yet processed	<u>L</u>			
	text	ISO/TS 17090-	1. "Health informatics	- Public key int	frastructure Par	t 1. Framework a	nd overview"					
	lont	ISO/TS 17090-2	2: "Health informatics	- Public key int	frastructure Par	t 2: Certificate pro	na overview . ofile"					
		ISO/TS 17090-3	3: "Health informatics	- Public key int	frastructure. Par	t 3: Policy Manag	ement of certifica	tion authority".				
	Original	Please add the	following references:									
	resolution	ISO/TS 17090-	1: "Health informatics	- Public key int	frastructure. Par	t 1: Framework a	nd overview".					
	proposal	ISO/TS 17090-2	2: "Health informatics	- Public key int	frastructure. Par	t 2: Certificate pro	ofile".					
		ISO/TS 17090-3	3: "Health informatics	- Public key in	frastructure. Par	t 3: Policy Manag	ement of certifica	tion authority".				
	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						
TS101456-043	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment	A comparison h	as been carried betw	een the Federa	I PKI and the E	TSI Qualified Cer	tificate Policy (TS	101 456 - QCP), initial	y put together by a US
	text	contractor direc	ted by Federal PKI w	ith subsequent	input from men	nbers of the ETSI	ESI TC.		
		Whilst the resul	ting conclusion is tha	t the policies ar	e broadly in line	e, the document ic	lentifies a number	r of areas as "missing" i	n the ETSI QCP. A
		significant num	per of these are issue	es relating to au	diting the confo	rmance of the CA	to the policy and	practices. It is suggeste	ed that this can be
		covered by refe	rence to the CWA 14	167-2 or a com	parable nationa	al "voluntary accre	ditation" scheme.	There are also other a	reas which are covered
		by other EESSI	specifications (TS 10	01 862 and CW	A 14168 / CWA	14169).			
	Original								
	resolution								
	proposal								
	Resolution								
	comment								
	Resolution								
0	text	Dellassable	Original	0	0	Deschutten	Deschutten	Deschutten status	Dellasseekle (enset
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	uate	туре	source	date		version
TS101456 044	1 2 1		STE220 2 001	15/05/2002	tochnical			not vot processed	
13101450-044	Commont	EDKI roquiromo	ont identified as "miss	ing" or partially	covorod in the			not yet processed	
	tovt	Information abo	ut a revoked certifica	te shall remain	in the status in	GOF.	cortificate expire	s (table 65)	
	Original	Information abo	ut a revokeu certinca				certificate expire.	5 (lable 05).	
	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						
TS101456-045	1.2.1		STF220_2-001	15/05/2003	technical	STF242		not yet processed	
	Comment	FPKI requireme	nt identified as "miss	ing" or partially	covered in the	QCP:		· · ·	
	text	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	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
--------------	-------------	-------------------	--------------------------	--------------------	--------------------	----------------------	---------------------	----------------------------	--------------------------
	version	clause	contribution	date	type	source	date		version
			reference						
TS101456-046	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment	FPKI requireme	ent identified as "missi	ng" or partially	covered in the	QCP:			
	text	The issuance fr	equency for CRLs and	d CARLs shall	be at least once	each day; CRL a	and CARL issuan	ce for reason of loss or	compromise of private
		key shall take p	lace within 18 hours of	of notification (t	able 70).				
	Original								
	resolution								
	proposal								
	Resolution								
	Baselution								
	test								
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
			reference		-71				
TS101456-047	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment	FPKI requireme	ent identified as "missi	ng" or partially	covered in the	QCP:	·		
	text	Audit logs shall	be reviewed at least of	once every two	months. A stati	stically significant	t set of security a	udit data generated by A	Agency CAs since the
		last review shal	I be examined (where	the confidence	e intervals for ea	ach category of se	ecurity audit data	are determined by the s	ecurity ramifications of
		the category an	d the availability of to	ols to perform s	such a review),	as well as a reaso	onable search for	any evidence of malicic	us activity (table 78).
		Actions taken a	s a result of these rev	iews shall be c	locumented (tab	le 79).			
	Original								
	resolution								
	Proposal								
	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						
TS101456-048	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment	FPKI requireme	ent identified as "missi	ng" or partially	covered in the	QCP:	·		
	text	Audit processes	s shall be invoked at s	system startup,	and cease only	at system shutdo	own (table 88). Sh	ould it become apparer	nt that an automated
		audit system ha	is failed, and the integ	rity of the syste	em or confidenti	ality of the inform	ation protected by	y the system is at risk, t	hen the Agency
		authority shall c	letermine whether to a	suspend Ageno	cy CA operation	until the problem	is remedied (tabl	e 89).	
	Original								
	resolution								
	proposal								
	Resolution								
	Bosolution								
	test								
1	IEXI								

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS101456-049	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed				
	Comment	FPKI requireme	ent identified as "missi	ng" or partially	covered in the	QCP:						
	text	Routine self-as	sessments of security	controls shall b	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									
TS101456-050	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed				
	Comment	FPKI requireme	ent identified as "missi	ng" or partially	covered in the	QCP:						
	text	Full system bac	kups, sufficient to rec	over from syste	em failure, shall	be made on a pe	riodic schedule, c	described in the respecti	ive CPS (table 121).			
		Backups are to	be performed and sto	ored off-site not	less than once	per week (table 1	22).					
		At least one full	backup copy shall be	stored at an o	ffsite location (s	eparate from the	Agency CA equip	oment) (table 123).				
		The backup sha	all be stored at a site v	with physical ar	nd procedural co	ontrols commensu	urate to that of the	e Agency CA (table 124)				
	Original											
	resolution											
	proposal											
	Resolution											
	comment											
	Resolution											
0	text	Dellasanahila	Original	0	0	Desclution	Desclution	Desclution status	Dellasseekle (enset			
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	uate	туре	source	uate		version			
TS101456 051	1 2 1			15/05/2002	toobnical			not vot processed				
13101450-051	Commont	EDKI roquiromo	STF220_2-001	15/05/2003	nechnical			not yet processed				
	toxt	The Ageney CA	Deliev Authority chol	ng or partially	covered in the	QCP. 10 and dissiplinar		norconnol who have no	formed extinne			
	lexi	involving the Ac	roncy Authonity Shar	tony pot outbori	ate auministrativ	the CDS or other	actions against	personner who have per				
		(table 133)	fivolving the Agency CA of its repository not autionized in this CF, the CFS, or other procedures published by the Agency Operational Autionity (rable 122)									
	Original											
	resolution											
	proposal											
	Resolution											
	comment											
	Resolution											
	text											
		I										

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	Version	Clause	reference	uale	type	300100	uale		Version
TS101456-052	1.2.1		STF220_2-001	15/05/2003	technical			not yet processed	
	Comment	FPKI requireme	ent identified as "miss	ing" or partially	covered in the	QCP:			
	text	Documentation	shall be maintained i	dentifying all pe	ersonnel who re	ceived training ar	d the level of trai	ning completed (table 1	36).
	Original								
	resolution								
	proposal								
	Resolution								
	comment								
	Resolution								
Commont ID	Deliverable	Deliverable	Original	Commont	Commont	Deselution	Decolution	Decelution status	Deliverable terret
Comment ID	Deliverable	Deliverable	Original	Comment	comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	reference	uale	туре	source	uale		version
TS101456-053	1.2.1	7.2.2 - b)	TC-ESI_1-003	22/10/2003	technical			not yet processed	
	Comment text	CA private sign Blakley's thresh	ing keys, when expor	ted, can be pro echanism.	tected not only	by means of encr	yption, but also b	y means of other mecha	anisms, like Shamir's or
	Original	Change clause	7.2.2 - item b) into "V	Vhen outside th	e signature-cre	ation device (see	a) above) the CA	private signing key sha	II be protected using
	resolution	cryptographic s	vstems that, accordin	a to the state o	f the art. are ca	pable to withstand	d cryptanalytic att	acks for the residual life	of the encrypted key or
	proposal	key component	".	.g					
	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									
TS101456-054	1.2.1	Annex D	TC-ESI_1-006	26/10/2003	technical			not yet processed				
	Comment	Correct the inco	onsistencies in annex	D, the cross re	ference betwee	n RFC 2527 and	TS 101 456.					
	text											
	Original	Amendment pro	oposed:									
	resolution	* 3.4: change										
	proposal	<ul> <li>* 4.4: change "7.3.5" into "7.3.6"</li> <li>* 5.2: change "7.4.5" into "7.4.3" (note 1)</li> <li>* 6.3: add "6.2, " before "7.2"</li> </ul>										
		* 6.4: add "7.	6.4: add "7.2.7, " before "7.2.9" 6.5: add "7.4.5, " before "7.4.6"									
		* 6.5: add "7.										
		* 6.6: change	- 7.3" Into "7.4" (note	2)								
		6.7. add 7.	4.5, Defore 7.4.6									
		NOTE 1: The - " NOTE 2: The - " - S - S fa - S ta - S ta - S ta - S ta - S - T M N	procedural controls, a In this subcomponent for each task identified Identification and auth life cycle security con This subcomponent a System development of ecurity during product ailsafe design and imp iddressed by TS 101 Security management to configured security. Insure their correct op This subcomponent ca Methodology (TSDM) I Maturity Model (SEI-CI	as per RFC 252 , requirements d for each role, hentication requ trols, as per RF ddresses syste controls include t maintenance, blementation te 456). controls includ These tools ar beration. (<- this in also address level IV and V, <u>MM) (&lt;- this is</u>	7, are: for recognizing it should also b irements for ea C 2527, are: m development e software engine chniques (e.g. o e execution of to d procedures in s is addressed in life-cycle secur independent life not addressed b	trusted roles are of e stated how man ch role may also b controls and secon nvironment secur being practices, s defensive program cols and procedur iclude checking the n clause 7.4 of TS ity ratings based, i-cycle security co by TS 101 456).	described, togeth ny individuals are be defined" urity management software development oftware developming) and developming) and developming) res to ensure that he integrity of the 5 101 456). for example, on to ontrols audit, and	er with the responsibiliti required to perform the t controls. personnel security, com nent methodology, mod opment facility security. the operational system security software, firmw the Trusted Software De the Software Engineerin	es for each role" (22). task (n out m rule) figuration management lularity, layering, use of (<- this is not s and networks adhere rare, and hardware to evelopment ng Institute's Capability			
	Resolution											
	Comment											
	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	he various RFCs and	Internet Drafts	from PKIX (es	pecially RFC 245	9 / RFC 3280).	· · · ·	
	Original resolution proposal								
	Resolution comment	This suggestior	has been already a	oplied in the ne	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
TS101733-002	1.4.0		UNSTT-003	01/09/2002	technical	STF242	02/09/2003	already applied	1.5.1
	Comment text	Signing Time o	ptional?						
	Original resolution proposal								
	Resolution comment	This suggestior	has been already a	oplied in the ne	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
TS101733-003	1.4.0		UNSTT-003	01/09/2002	technical	STF 242	23/01/2004	no change	
	Comment text	Time-mark: the	use of the time-mark	may solve the	problems relate	ed to the compror	nission of TSA pri	vate key.	
	Original resolution proposal								
	Resolution comment	The current ver on usage of tim technologies the used there). In any case the that outlines go	sion includes the tim e-stamps for archiva at do not fall within th choice of the various od practices and sce	e-mark concept l electronic form ne scope of sigr s options deper narios.	t and usage for ns. Usage of tin nature formats ( nds on the appli	producing the ES ne-mark for achie although certain o cations' scenarios	with Time Indicat ving long term sig data structures sp s. This issue falls i	ion (ES-T form). Howev gnatures would rely on s ecified within the TS 10 <sup>-</sup> into the one to produce a	er the current TS focus ecure archival 1 733 could certainly be a guidance document
	Resolution text	No change.							

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS101733-004	1.4.0		UNSTT-003	01/09/2002	technical	STF 242	23/01/2004	no change					
	Comment	The use of the	'Invalidity Date" exten	ision of a CRL	entry may inval	lidate all the forma	ats for long term s	ignatures.					
	text												
	Original												
	resolution												
	proposal Recolution	This is to be ad	dragged by FTOLTO			Darofiloo							
	Resolution	This is to be ad	aressed by ETSITC-I	EST activity on	CRL and OCS	promes.							
	Resolution	No change											
	text	No change.											
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
T0404700.005	4.4.0			04/00/0000	ta abada at		00/04/0004						
15101733-005	1.4.0	There is the second		01/09/2002		<u> 51F 242</u>	23/01/2004	Ino change					
	toxt	There is the nee											
	Original												
	resolution												
	proposal												
	Resolution	This is a topic the	hat falls out of the scc	pe of TS 101 7	33 . It's a matte	er of CWA 14171.							
	comment	•		•									
	Resolution	No change.											
	text					-	-	-					
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
T0101722 000	1.4.0			01/00/2002	taabaical	STE242	25/01/2004						
15101733-006	Commont	Thora is the par	UNSTI-003	01/09/2002	the different for	SIF242	25/01/2004	Ino change	all picture of the				
	text	electronic signa	ature model	ces write using			give a reader a c	omprehensive and over					
	Original												
	resolution												
	proposal												
	Resolution	The production	of such a set of docu	ments would ce	ertainly be wort	h. This comment	could be raised to	the ESI group.					
	comment				-			<b>.</b>					
	Resolution	No change. Thi	s comment could be r	aised to the ES	SI group.								
	text												

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
			reference						
TS101733-007	1.4.0		UNSTT-003	01/09/2002	technical	STF242	25/01/2004	no change	
	Comment	There is the nee	ed to introduce some	explanation ab	out the relation	ship between the	rules (some namir	ng and path constraints	) included in the
	text	Certificate Polic	y and the ones includ	led in the Signa	ature Policy eve	n if it is a matter o	of "Signature Polic	y Report".	
	Original								
	resolution								
	proposal							<u> </u>	
	Resolution	This is a topic th	hat falls out of the sco	pe of TS 101 7	33, whose purp	ose is to specify	formats for advance	ced electronic signature	es. Relationship
	comment	between rules in	n Certification Policy a	and Signature I	Policy would be	much better to be	e discussed in det	ails within the Signature	Policy Report or other
		document with I	proader scope than th	e current one,	which could co	ver the infrastruct	ure supporting adv	vanced electronic signa	atures.
	Resolution	No change.							
Commont ID		Deliverable	Original	Commont	Commont	Baselution	Pecolution	Possiution status	Dolivorable target
Comment ID	Version	clause	contribution	date	type	Resolution	date	Resolution status	version
	Version	clause	reference	uate	type	Source	uale		Version
TS101733-008	140		UNSTT-004	14/02/2003	technical	STF242	02/09/2003	already applied	151
10101700 000	Comment	Making the Sigr	naturePolicyID signed	attribute optio	nal and without	the NULL value	02/03/2000		1.0.1
	text	including the eligi	lataron oneyib eighea						
	Original								
	resolution								
	proposal								
	Resolution	This suggestion	has been already ap	plied in the nev	w version 1.5.1.				
	comment								
	Resolution								
	text				<u> </u>				
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
<b>TO</b> 404700.000	1.1.0			4.4/00/0000			00/00/0000		
15101733-009	1.4.0		<u>UNSTI-004</u>	14/02/2003	technical	STF242	02/09/2003	aiready applied	1.5.1
	text	Making the Sigr	ling lime signed attrib	ute optional.					
	Original								
	resolution								
	proposal								
	Resolution	This suggestion	has been already ap	plied in the nev	w version 1.5.1.				
	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										
TS101733-010	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change					
	Comment	Generalization	of the timemark conc	ept (as an exte	rnal trusted tim	e indication, see l	ES-Cbis).						
	text												
	Original												
	resolution												
	proposal						<u></u>						
	Resolution	The current ver	sion includes the tim	e-mark concept	t and usage for	producing the ES	with Time Indica	tion (ES-1 form). Howev	er the current TS focus				
	comment	on usage of tim	e-stamps for archiva	l electronic forn	ns. Usage of tin	ne-mark for achie	ving long term sig	natures would rely on s	ecure archival				
		technologies th	at do not fall within th	ne scope of sigr	nature formats (	although certain o	data structures sp	ecified within the TS 10	1 733 could certainly be				
	Deschutien	used there).											
	Resolution	No change.											
Commont ID	Deliverable	Deliverable	Original	Commont	Commont	Pacalution	Posolution	Possilution status	Doliverable target				
Comment ID	Version		onginal	data	type	Resolution	data	Resolution status	version				
	Version	clause	reference	uale	type	Source	uale		Version				
TS101733-011	140		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	already applied	151				
	Comment	ES as the minir	num mandatory form	at	toorninoar	011212	20/01/2001						
	text												
	Original												
	resolution												
	proposal												
	Resolution	In its current ve	n its current version, the only attribute that is mandatory to add to the CMS basic format is the SigningCertificate one.										
	comment		-		-			-					
	Resolution	No change.											
	text					-			-				
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS101733-012	1.4.0		UNS11-004	14/02/2003	technical	STF242	25/01/2004	no change					
	Comment	Signature policy	: introducing the mir	nimum mandato	bry format for a	specific application	on as an additiona	l rule.					
	text												
	Original												
	proposal												
	Proposal	Do not undorst	and vory wall the car	mont Doos it	maan that the s	ignaturo policy fo	rmat (which is no	w part of a signature pol	iou roport) should				
	comment	include means	for specifying the "mi	inimum" ES for	mean that an ann	lication should ac	cont as valid? If s	the Signature Policy	includes means for				
	comment	identifying attrik	ior specifying the mi	the signature	liat that an app	d be worth to spe	cify shorter mech	anisms to mandate spec	sific ES forms already				
		defined This is	a tonic that next ver	sions of signature, a	in lough it woul	s should deal with	Δs a quotation.	the Digital Signature Se	anvices Technical				
		Committee of C	ASIS is currently de	aling with the n	roduction of a n	rotocol for reques	ting generation a	nd validation to a server	of different XAdES				
		forms This pro	tocol will likely includ	e mechanisms	for identifying th	he different Electr	onic Signature for	ms that are the XMI co	ounterpart to the forms				
		defined in TS 1	01 733.				ee eignatare for						
	Resolution	To be managed	in future versions										
	text	l is inge											

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.	locument structure: a	better separation	on between the	mandatory and c	ptional formats; n	noving the optional form	ats from the body to an			
	Original resolution proposal											
	Resolution comment	This suggestior	n has been already ap	plied in the new	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	Improving the document as fo	nproving the document structure: deleting all text and ASN.1 formal definition about Signature Policies from TS 101 733 and putting it into a specific ocument as for the XML version of formats and policies.									
	Original resolution proposal											
	Resolution comment	This suggestior	This suggestion has been already applied in the new version 1.5.1.									
	Resolution text											
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
TS101733-015	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change				
	Comment text	Adding some a perspective: it c	dditional explanatory of could be a new version	documents: roa n of EESSI DD	admap for the E D.	ESSI deliverables	s EESSI, from a f	unctional perspective ar	d from a new reader			
	Original resolution proposal											
	Resolution comment	The production	of such a set of docu	ments would ce	ertainly be worth	n. This comment	could be raised to	the ESI group.				
	Resolution text	No change. Thi	s comment could be r	aised to the ES	SI group.							

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	reference	date	type	source	date		version			
TS101733-016	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change				
	Comment	Adding some ac	dditional explanatory	documents: a n	on-normative (	Technical Report)	document descri	bing the whole model of	the electronic			
	text	signature gener Signatures' writt	nature generation and verification processes and formats: it could be a new detailed document based on the white papers 'Validation of Electror natures' written by H.N. and D. P.									
	Original	5										
	resolution											
	proposal											
	Resolution	Certainly, such	a document giving ex uld be a valuable outo	planations on t come. This com	he model for si ment could be	gnature generatio raised to the ESI	n and verification aroup.	processes for ES forms	specified in			
	Resolution	No change. This	s comment could be r	aised to the ES	SI group.		<b>5</b> . • • • •					
Comment ID	Text	Deliverable	Original	Commont	Comment	Pesolution	Pesolution	Posolution status	Deliverable target			
Comment iD	version	clause	contribution	date	type	source	date	Resolution status	version			
			reference									
TS101733-017	1.4.0		UNSTT-004	14/02/2003	technical	STF242	25/01/2004	no change				
	Comment text	Adding some ac both from a lega formats.	dditional explanatory of a perspective and fro	documents: a n m a technical p	ew document ( erspective, inc	Technical Report, luding some case	) about hand-writt studies with and	en and electronic signat without signature policie	ures interoperability, s and using different			
	Original resolution proposal											
	Resolution comment	It is not clear the one environmer does it deal with signatures? As a quotation, traditionally han future. Please re	e precise meaning of at of both, electronic a a the production of a c a technical report has d-written signatures h efer to that ETSI TR.	"hand-written a ind hand-writte locument instru been produce have been used	nd electronic s n signatures ar icting on the wa d within ESI or I (even more th	ignatures interope Id how to manage ays electronic sign signature policies an one), where el	erability". Does thi both types? (the natures should be s which presents ectronic signature	s comment deal with the term interoperability cou managed for being equ different use cases in so es can play a relevant ro	e co-existence within uld indicate that) or ivalent to hand-written cenarios where ole in an immediate			
	Resolution text	No change.										

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS101733-018	1.3.1		JCPKI-002	17/02/2003	technical	STF242	25/01/2004	no change				
	Comment	Rationale: Som	e comments regarding	g EESSI Signat	ture Policy							
	text	Author: Japan C	Computer Research, 2	2003/02/17								
		Scope and Intro	oduction									
		The purpose of	the present documen	t is to convey s	ome comments	s upon the policy a	spects of the electron	ctronic signature format	t as specified in [ESF]			
		and [XAdES]. T	[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 se	cification 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	st important milestones in the future evolution of e-business.									
		It is now routine	to standardize the er	capsulation of	signature data.	And a number of	these formats bir	id signature with corres	ponding public key, and			
		often if not all th	time, together with	its certificate or	certificate chai	n. That policy info	rmation can funct	ion as a means to valic	late status of			
		accompanying	object is well exemplif	ied in the policy	/ attributes of X	.509 certificate pro	ofile. Nevertheles	s, it has to be said that	attachment of policy to			
		Signature nash i	t yet gained the rank t	or common acc	eptance. It has	to be said, in this	sense, that one o	r the most distinguishin	g characteristics of			
			ticipate that the police	i e policy.	in [ESE] can ba	vo contoxtually or	tiraly other use o	acas than those specifi	e to that for public kov			
		cortificatos. To l	ho moro prociso, duo	to moro looso (	n [EOF] can na	ve contextually en	with digital signat	ure it is expected that a	c to that for public key			
		the signature of	be more precise, due	ly ranged com	ared to certific	at a policy Accord	indly needs to ac	Idress wider area of ora	application domain of			
		and this natural	ly leads to the necess	ity of taking int	account other	nolicy related dev	elonment efforts	in the Internet commun	hity whose shared aim is			
		to promote flexi	ble online transaction	s (valued or oth	erwise) while a	poncy related de	bility of real work	l experience				
		"Policy" has lon	g been traditionally as	sociated, one	way or another.	with the idea of a	uthority, predomi	nantly centrally and stat	tically perceived at that.			
		The underlying	principle of certificate	policy closely f	ollows this, ess	entially due to the	wav it is bred. Ac	ainst this, especially to	the extent that each			
		individual ought	to possess his or her	own policy, is	a picture in whi	ch many policies of	dynamically intera	ict to form the whole. A	nd this may be thought			
		of as what the	signature policy" migh	t envisage, for	signature mark	s each spatial and	temporal lineam	ent of some particular	present event. In other			
		words, it should	suggest a way to coll	ect disseminat	ed policies in or	der to proffer a de	cision suitable to	that point of time and s	space, a way to make			
		feasible Policy I	Knowledge Interactivit	y. It is in this sp	pirit that the follo	owing comments a	are delivered, alth	ough not always explic	it.			
		Comments	-			-						
		1. On the man	dated reference to pol	icy. In the data	structure, signa	ature policy identif	ier is made mand	latory [ESF; 8.9.1]. This	s can mean either that:			
		(a) every sig	nature MUST have a	non-trivial sign	ature policy ava	ailable for retrieval	in association wi	th the identifier; or that	(b) signature policy can			
		have null (i.e	<ol> <li>dummy and intentio</li> </ol>	nally empty) si	gnature policy i	n the case so desi	ired:					
		(a) This cas	e means that validatio	n process refe	rs to and explicit	itly made depende	ent on the signing	process at each instan	t. I.e. the action of			
		validatio	n of a signature is det	ermined by the	signing of it at	the time when the	latter took place,	so that the temporal m	edium between the two			
		actions is	s made frozen. In part	icular, this allow	ws the users to	preserve unaltere	d the state and q	uality of signature relati	vely long time.			
		(b) In this ca	ase, the content of the	policy can be	determined at th	he time of the valid	dation. Binding be	tween the signature an	nd validation is			
		principal	ly the responsibility of	policy source (	policy issuer or	TSP), and the de	termination of act	tual policy content is lef	t to the latter, and the			
		issuance	e can be protracted to	the time of the	aelivery.	L						
		(c) in practic	ce, nybrid case is the	most likely to b	e demanded. I	nis is because:	mana un innationa uniti-	the policy course to to				
		(I) Perio	ormance wise, a pract	ical computing	platform wants	to avoid actual co		ine policy source to ta	ke place every each			
		time	or the signature gener	volidation need		view that, for some	e algorithms, sign	ing process is designed	n more costry in			
		anthr	neuc operations than	validation proc	that signature	cations serving as	bad until the time	it is necessary to refrac	process nunureus of			
		reque	that policy contant b	no would imply	d signer decide	s its policy related	action in terms of	f policy qualifiers only	Which in turn would			
		mear	that it is desired that		u signer ueulde carry validity d	a ha pulluy related	of a recommend	ad best before				
L		mean	i mai il is desired lital	policy qualifier	carry valially a	ales of some son	or a recommende					

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
		(ii) Anoth	ner reason why it is in	portant to allow	v empty policy of	content at the time	e of signing is that	, in encapsulating a tra	insaction message in				
		which	n signature data is to	be attached, on	e might want to	or have to place	policy related info	rmation outside the sig	Inature data, for				
		exam	ple using some other	policy mechan	isms (cf. item 2	below). Practical	y, this could perha	aps mean often that tw	o policy identifiers, that				
		within	the signature data a	nd that outside	it, are identical	, but not necessar	ily.						
		2. On policy da	ita or content. The de	sign of [ESF] ha	as that, accordi	ng to the needs of	the singing party	and relying party, poli	by data or content can				
			from the policy source	e the reference	to which is emi	bedded explicitly i	n the signature da	ata in the form of mand	atory policy identilier.				
			<ul> <li>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:</li> <li>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.</li> <li>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</li> </ul>										
		similar speci											
		these protoc											
		a) In Gener											
		consider											
		meant to											
		b) SAML. B											
		messagi											
		informati	on. This security infor	mation is expre	essed in the forr	n of assertions ab	out subject, wher	e a subject is an entity	(either human or				
		compute	r) that has an identity	in some securi	ty domain". In c	order to fit exactly	into this description	on, signature ought to r	epresent the "entity" so				
		intended	, which is really the ro	le of public key	certificate as the	ne common sense	has it presently.	However, the practical	consideration ensues				
		taking in	to account that promu	ligation of SAM	L is rapidly in p	ace. whereas, or	i the other hand, v	we believe that the sigr	lature policy of [ESF]				
			Although termed as "	Access Control	Markun Langu	/. age" the motivati	on of XACMI der	ives from 'a pressing p	eed for a common				
			for expressing secu	ity policy' (IXA	CMI 1) It is in th	is sense that XAC	MI might just be	suitable as the policy b	anguage for [ESE] For				
		this, how	ever, we believe that	one has to mal	ke a careful arc	hitectural conside	ration to cohere th	ne two semantically. (S	ee item 5 for a brief				
		remark o	on this.)										
		d) Web Ser	vices Policy Framewo	ork. Similar to a	pplicability of X	ACML, but with a	more restricted co	ontext of the web servio	ces interoperability.				
		There ar	e on-going investigati	ons as to how [	XACML ] and [\	NS-Policy] can be	made consistent	in practice. Here we w	ould rather insist on the				
		synergy	of [ESF] with [XACML	] for the reasor	n that semantics	s of XACML is mo	re general in natu	re. To add, in conjunct	ion with the overall web				
		services	security standards, o	ne might think o	of applying secu	ire SOAP messag	ing in the form of	Web Services Security	/, for the signature				
		policy qu	eries (including refere	encing). We fee	I that this certai	nly is a potential.			The letter is near done dia				
		3. On policy pr	B. 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 bash calculation of the policy identifier. Also, binding of the policy source and actual policy seems to be rendered by the same.										
		terms of the	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 a	annough only implicit	refers to anoth	J. This may no	and so on (which	er of protection, it	e with [SAM] 1 in coop	aration with [XACMI ])				
		Further sign	ature policy doesn"t	seem to carry it	s own signature	explicitly which	means if it is to b	e signed the signature	ata are to be				
		attached ext	ernally. We believe, t	o complement t	his, that signing	of signature polic	cv has to be desc	ribed in detail. at least	normatively (as XACML				
		TC does). F	or especially, there m	ay arise possib	le semantic am	biguities between	"signature policy"	and "policy signature"	. And it could well				
		happen that	the latter may be pro	vided by some	TSP other than	policy issuer itsel	f. , , ,						
				-		-							

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
		4. On signature	e policy data structure	. Although not	normative, we h	nave a number of	reasons that sign	ature policy specified ir	n [ESF] has to be			
		examined cl	osely. The primary on	e being its pos	ition with respe	ct to other policy a	assertions mention	ned above (see item 2)	, we feel that [ESF]			
		signature po	olicy format has to add	Iress either pos	sible interopera	ability with or defin	itive differentiatio	n from these other stan	dards. Here are a			
		couple of fra	agmental comments:									
		a) On Rules	<ol> <li>The terminology err</li> </ol>	nployed, "Comr	non Rules" ([ES	SF; 11.3]) and "Co	mmitment Rules"	([ESF; 11.4]), seems to	o be rather awkward			
		especiall	ly when compared wit	h other standa	rds. It is suspec	ted that this was i	ntentionally chose	en with some specific a	pplication in mind, but			
		we could	I not have identified th	e relevant pas	sages in the spe	ecification.	·					
		<ul> <li>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.</li> <li>5. On interpreter biling with XACML, this after expected that XACML will fill in the gen where it is guarantee biling the means to prefer comparison.</li> </ul>										
		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.										
		configuring the application domain of signature policy, regardless of whether transaction of the latter takes place through application layer										
		References	protocols or not.									
		IESEI	ETSI TS 101 733 "EI	ectronic Signat	ure Formats"							
		IREC32801	Internet X 509 Public	Key Infrastruct	ure Certificate :	and Certificate Re	vocation List (CR	I) Profile				
		[SAML Core]	Assertions and Proto	col for the OAS	IS Security Ass	sertion Markup La	nguage (SAML).	L) 1 101110.				
		[XACML]	OASIS extensible Ac	cess Control M	arkup Languag	e (XACML).	gua.go (0/).					
		[XAdES]	ETSI TS 101 903 "XN	/L Advance Ele	ectronic Signatu	ires (XAdES)".						
		[WS-Policy]	Web Services Policy	Framework (W	S-Policy).	· · · ·						
	Original			· · · · · · · · · · · · · · · · · · ·	37							
	resolution											
	proposal											
	Resolution	Comment on (a	): The appearance of	a signature pol	icy identifier do	es not preserve u	naltered the state	and quality of signature	e relatively long time (if			
	comment	the algorithm or	the algorithm or the key are broken, the signature policy identifier does not protect the signature): this has to be achieved by other means, like time-									
		stamping. What a signature policy identifier does is to fix rules that the verifier has to follow to validate the signature.										
		The current version of TS 101 733 does not use the SignaturePolicyImplied with NULL value.										
	Resolution	No change.										
	text											

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
TS101733-019	1.3.1		JCPKI-002	17/02/2003	technical	STF242	21/06/2003	already applied					
	Comment text	Pages 49, 67 a RevocationValu crIVals ocspVals otherRevVals }	nd 76: "OPTIONAL" s les ::= SEQUENCE { [0] SEQUENCE OF ( [1] SEQUENCE OF E [2] OtherRevVals ***	hould be descr CertificateList C BasicOCSPRes	ibed after [2] C OPTIONAL sponse OPTIOI	therRevVals mar	ked ****.						
	Original resolution proposal	"OPTIONAL" st	OPTIONAL" should be described after [2] OtherRevVals marked ****										
	Resolution comment	This problem is	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 1 These two shou	7: Timestamp seem u uld be deleted to avoid	unnecessary in d being complic	ES-X Type1 a acy of specific	nd ES-X Type2, s ations.	ince ES-X-L is en	ough.					
	Original resolution proposal												
	Resolution comment	These forms de some of the key validation data:	al with different situat /s of the CAs in the ce then they are added	ions: ES-X Typ ert path can be to the signature	bes 1 and 2 are compromised. e itself.	for those environ ES-X-L are for th	ments where veri ose environments	fier has access to all the where verifier HAS NO	e validation data AND T access to all the				
	Resolution text	No change.											

version									
eferencing,									
eferencing,									
eferencing,									
6 I I - I									
1 SNOUID									
t any indication									
erable target									
version									
is 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.									
nticity.									
erable target									
version									
ovtoncion									
extension									
instances as has been done in X.505 certificate prome standard (NFO 5200).									
the start of									

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 Informatio	n" may be a spelling	mistake for "CF	RL Information".								
	Original resolution proposal												
	Resolution comment	Already applied	Iready 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	se title "Timestamping	g for long life of	signature".								
	Original resolution proposal												
	Resolution comment	Will be correcte	d in next release.										
	Resolution text												

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
			reference						
TS101733-026	1.4.0	10.4	OTHER-009		technical	STF242	25/01/2004	already applied	1.5.1
	Comment text	The Archive Tir attributes are no unsigned attribu The following of id-aa-ets-archiv us(840) rsadsi( Archive timesta ArchiveTimeSta The value of me value) of the fol (a list of 11 diffe For further infor The timestamp length) timestar	nestamp attribute is a bot present these attrib ute. Several instances bject identifier identifie eTimestamp OBJECT 113549) pkcs(1) pkcs mp attribute values ha ampToken ::= TimeSta essageImprint field wi lowing data objects as erent attributes follows mation and definition should be created usi nps.	timestamp of t utes shall be a of this attribute the Nested A DENTIFIER 9(9) smime(16 ave the ASN.1 ampToken thin TimeStamp of TimeStamp ng stronger alg	he user data and dded to the ele e may occur with Archive Timesta ::= { iso(1) men b) id-aa(2) 27} syntax Archive coToken shall be e electronic sign Token see clau gorithms (or lon	nd the entire electi ctronic signature p th an electronic sig imp attribute: hber-body(2) TimeStampToken a hash of the cor hature: se 10.4. ger key lengths) th	ronic signature. If prior to the timesta gnature both over ncatenated values nan in the original	the Certificate values a amp. The Archive Times time and from different (without the type or ler electronic signatures a	nd Revocation Values stamp attribute is an TSAs. ngth encoding for that nd weak algorithm (key
	Original resolution proposal								
	Resolution comment	This section ha	s been re-written in th	e current versio	on.				
	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	ise add "One of" to the beginning of the sentence, because the sentence uses "must".									
	text											
	Original	Please add "On	ease add "One of" to the beginning of the sentence, because the sentence uses "must"									
	resolution											
	proposal											
	Resolution	Noted to be con	sidered for next revis	ion.								
	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	Please add "Or	e of" to the beginning	g of the sentend	ce, because the	e sentence uses "	must".					
	Original resolution proposal	Please add "Or	e of" to the beginning	g of the sentend	ce, because the	e sentence uses "	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				
	Comment text	This profile is appropriate for common use of time stamp.										
	Original resolution proposal											
	Resolution comment	It is agreed that	this profile has gene	eral applicability								
	Resolution text	No change.										
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
TS101861-004	1.2.1	5.2.1	OTHER-010		technical			not yet processed				
	Comment text	This clause cur - "a genTime - a minimum What is the aim	rently includes the re parameter limited to accuracy of one secc of the first requirement	quirements: represent time ond is required;' ent? This could	with one secon " be read to imp	d is required; ly that time repres	sentation of better	accuracy than 1 second	l is not allowed.			
	Original resolution proposal	Replace with: - "the genTim - the time sha	e parameter shall be Ill be to the accuracy	to the precision of one second	n of one second or better;"	d or better;						
	Resolution comment											
	Resolution text											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	reference	uale	type	Source	uale		Version				
TS101861-005	121	521	OTHER-011		technical			not vet processed					
	Comment	This clause stat	es:					not yot processed					
	text	- "an ordering	i parameter missing o	r set to false is	required."								
		What is the rea	son for not allowing o	rdering if the TS	SA wants to pro	vide this service.	Surely, all that th	e aim is to not make it m	nandatory for TSAs to				
		provide ordering	g.	5			<b>,</b> ,,		,				
	Original Delete item.												
	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				
T0404004 000	1.0.1	0			ta ab si a a l			water to water a state					
15101861-006	1.2.1 Commont	6       OTHER-012       Itechnical       Image: constraint of the second seco											
	toxt												
	Original	Line accuracy cu	intentity proposed, the	use of store at	iu iuiwaiu is ina	appropriate.							
	resolution	One on-line pro	tocol and one store a	nd forward prot	ocol must be si	innorted for every	Time Stamping	Authority (TSA)					
	proposal	one on me pro					Time Otamping						
	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										
TS101861-007	1.2.1	7.1.1	OTHER-013		technical			not yet processed					
	Comment	It not explicit as	to which algorithm id	entifier this refe	ers to. Presume	ably, this is Hash/	Algorithm in Mess	sageImprint.					
	text	It is not commo	n practice for "NULL"	to be explicitly	included in the	algorithms param	eters. Why not al	llow the parameters to b	e non-present.				
	Original	Update as indic	ated:					0.1.4.1.1.1					
	resolution	"The AlgorithmIdentifier parameters field is optional. If present, the parameters field shall contain an ASN.1 NULL.											
	proposal	Implementations should accept SHA-1 Algorithmidentifiers with absent parameters as well as NULL parameters.											
	Becelution	Implementation	s should generate SF	IA-1 Algorithmi	dentiners with r	NULL parameters.							
	Resolution												
	Resolution												
	text												
	IGAL	1											

## 5.4 TS 101 862 - Qualified certificate profile

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	Version	Clause	reference	uale	type	Source	uale		Version				
TS101862-001	1.2.1	2	UNSTT-005		editorial	STF242	09/01/2004	applied	1.3.1				
	Comment text	Since TS 101 8 TS version.	62 has been publishe	ed, RFC 2459 h	as been replac	ed by RFC 3280.	Thus it is sugges	ted to accordingly modif	y reference in the next				
	Original	Modify the refer	rence to RFC 2459 in	to RFC 3280.									
	resolution	, ,											
	proposal												
	Resolution	Done as per pro	oposed resolution.										
	comment	0 T0 404 00	0.1/4.0.4										
	text	See 15 101 86.											
Comment ID	Deliverable	Deliverable Original Comment Comment Resolution Resolution Resolution status Deliver											
	version	clause	contribution reference	date	type	source	date		version				
TS101862-002	1.2.1	3.1.1/4.1	UNSTT-005		technical	STF242	09/01/2004	no change					
	Comment	a) Annex I of D	Annex I of Directive 1999/93/EC, specifies: "Qualified certificates must contain:										
	text		 (b) the identification of the certificate-service-provider and the State in which it is established". S 101 862 specifies that the name of the issuer (clause 4.1): "MUST contain a country name stored in the countryName attribute", but nothing is aid about the CSP Identifier. It is therefore herewith proposed the organizationName attribute to be also mandatory:										
		(b) the ident											
		15 101 862 Spe											
		b) Additionally											
		organization	ns or for issuing qualif	ied certificates	with some diffe	rent extensions) i	t is proposed that	an attribute is used to id	dentify the single CA.				
		From the above	e comments stems the	e following prop	osed amendm	ent to clause 4.1 t	ext:						
		"The name of th	ne issuer contained in	the issuer field	d (as defined in	clause 3.1.1 in R	FC 3039) MUST (	contain:					
		1) a country na	ame stored in the cou	ntryName attrib	oute. The specif	ied country SHAL	L be the country	in which the issuer of the	e certificate is				
		established;		a a cifu i a cu tha a u a		a tifi a n							
		2) the organiza	ationiname attribute s	ch one specific	to issue a diffe	nuller. rent qualified cert	ificate type, it is a		at the issuer field				
		contains the se	rialNumber attribute v	vith a value wh	ich SHALL be i	inique for each C/	A within the same	CSP Optionally the CS	SP MAY use the				
		organizationalU	InitName attribute to	specify further	details of the sp	ecific CA."							
	Original	"The name of th	ne issuer contained in	the issuer field	d (as defined in	clause 3.1.1 in R	FC 3039) MUST (	contain:					
	resolution	1) a country na	ame stored in the cou	ntryName attrik	oute. The specif	ied country SHAL	L be the country	in which the issuer of the	e certificate is				
	proposal	established;											
		2) the organizationName attribute specifying the relevant CSP identifier.											
		If one CSP sets	s up different CAs, ea rialNumber attribute v	cn one specific	to Issue a diffe	rent qualified cert	Ificate type, it is a	ISO RECUMIMENDED IN	at the issuer field				
		organizational	InitName attribute to s	specify further (	details of the so	ecific CA "		Cor . Optionally, the Co					
	Resolution	Specific namino	a requirements incorp	orated in TS 10	02 280. X.509 \	.3 Certificate Pro	file for Certificates	s Issued to Natural Pers	ons.				
	comment												
	Resolution	No change to T	S 101 862, see TS 10	02 280.									
	text												

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target					
	version	clause	contribution	date	type	source	date		version					
			reference											
TS101862-003	1.2.1	4.2.1	UNSTT-005		technical	STF242	09/01/2004	no change						
	Comment	Article 2.9 of the	e quoted Directive sta	tes: "certificate	" means an ele	ctronic attestation	which links signa	ture verification data to	a person and confirms					
	text	the identity of th	hat person". In order to	o "confirm the i	dentity" of the s	igner the following	g data are commo	nly deemed necessary	and used:					
		<ul> <li>Date of birth</li> </ul>	1											
		<ul> <li>Place of Birt</li> </ul>	h											
		- Gender												
		<ul> <li>Country of C</li> </ul>	Citizenship											
		For this reason	it is suggested that in	sertion in subje	ctDirectoryAttri	butes of the corre	sponding attribute	es, as listed in RFC 303	9 clause 3.2.1, is at					
		least RECOMM	ENDED in TS 101 86	2, unless a pse	eudonym is use	d "which shall be i	identified as such	" (Directive Annex I, iter	m c). Please see					
		subsequent iten	n 4).	<u> </u>										
	Original	Proposed text:	roposed text: "4.2 SubjectDirectoryAttributes extension 2.1 Identity relevant fields NOTE: Renumbering of the subsequent clauses is required.) order to provide reliable information on the qualified certificate subject's identity, consistently with Directive [1] definition of certificate, the name is ot sufficient. Actually the following data are commonly deemed necessary: date of birth, place of birth, gender, country of citizenship. is therefore RECOMMENDED that a subject's certificate bears at least the following fields in the subjectDirectoryAttributes extension: dateOfBirth:											
	resolution	4.2.1 Identity r												
	proposal	(NOTE: Rent												
		not sufficient A												
		It is therefore P												
		- dateOfBirth												
		<ul> <li>placeOfBirth</li> </ul>	placeOfBirth:											
		- gender:	jender;											
		<ul> <li>countryOfCi</li> </ul>	countryOfCitizenship.											
		Where necessa	here necessary, the countryOfResidence field MAY also be used.											
		Signature verific	cation applications SH	IALL be able to	handle the pre	viously mentioned	d fields."							
	Resolution	Specific naming	requirements incorpo	orated in TS 10	2 280 - X.509 \	/.3 Certificate Pro	file for Certificates	s Issued to Natural Pers	sons					
	comment													
	Resolution	No change to T	S 101 862, see TS 10	2 280.										
	text													
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target					
	version	clause	contribution	date	туре	source	date		version					
TS101962 004	1 2 1	4 2 4			tachnical	STE242	00/01/2004	no chango						
13101002-004	Commont	4.3.1 A requirement i	noodod on how the	l neoudonym is t	he lidentified	DIFZ4Z	09/01/2004	Ino change	idonym" attributos to					
	tovt	carry the pseud	onym. This could leave	to misunderet	andings even i	malicious ones if	a commonly agree	ed manner to identify p	seudonyms is not					
	IEAL	defined in fact	a fictitious name like "	' lohn Doe" rec	anulitys, even i orded in the "cc	mmonName" and	furnished with da	et manner to identity particulate and place of hirth of	ender and citizenshin					
		could be misinte	ernreted as being a "r	eal" name To a	avoid mistakes	it is then proposed	to add a require	ment in TS 101 862 [6]	that pseudonyms					
		MUST be insert	ed in the "pseudonym	" attribute.					and pool doiny mo					
	Original	Proposed text: '	'4.3 Subject field											
	resolution	4.3.1 Pseudor	iym attribute											
	proposal	oposal 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 verific	cation applications SF	IALL be able to	handle this att	ribute as above sp	pecified."							
	Resolution	Specific naming	requirements incorpo	prated in TS 10	2 280 - X.509 \	/.3 Certificate Pro	file for Certificates	s Issued to Natural Pers	sons.					
	comment													
	Resolution	No change to T	S 101 862, see TS 10	2 280.										
	text													

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS101862-005	1.2.1	4.3.2	UNSTT-005		technical	STF242	09/01/2004	no change					
	Comment	Even the data m	nentioned in the previ	ous item 2) mag	y not be enoug	h to uniquely iden	tify one person: in	fact in small towns or	/illages many people				
	text	happen to share	e the same surname a	and quite a few	of them have t	he same given na	me too, so it is po	ssible to find two perso	ns with the same name				
		born in the same	e place on the same of	day. Therefore	it is suggested	that TS 101 862 a	t least MANDATE	S usage of the serial	umber attribute in the				
		subject field. Th	is field, SHALL hold a	at least "an iden	ntifier assigned	by a government	or civil authority",	as per RFC 3039, claus	se 3.1.2. In addition to				
		such identifier a	nd where necessary	to comply with I	RFC 3039 follo	wing sentence: "It	is the CA's respo	nsibility to ensure that t	he serialNumber is				
		sufficient to reso	olve any subject name	e collisions", ea	ch CA SHALL	add a code it assi	gns itself, which S	HALL be unique for ea	ch certificate of that				
		subject. A printa	bleString character s	eparator (e.g. "	/") could be use	ed between the tw	o data. As an exa	mple: "RGGFNC42H3(	0A952P/0001".				
		When the "pseu	idonym" attribute is us	sed, a fictitious	identifier MAY	be used in the ser	alNumber attribu	te, e.g. "PseudonymA/(	00001".				
	Original	Proposed text: "	4.3.2 Serial Number	attribute									
	resolution	The serialNume	senainvumer aunurue onall be used in the subject neid to carry an identifier assigned by a government or civil authority.										
	proposal	If one CA issues	e CA issues the subject several certificates for different usages of foles, it SHALL ensure the serial number differentiate[s] between the subject field would otherwise be identical" (as stated in REC 3039 [4], clause 3.1.2), by adding, to the previously mentioned										
		names where in	is where the subject field would otherwise be identical" (as stated in KFC 3039 [4], clause 3.1.2), by adding, to the previously mentioned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned identifier and the CA assigned and a prity assigned as a prity assigned identifier and the CA assigned and a prity assigned as a prity assigned identifier and the CA assigned as a prity assigned as a prity assigned as a prity assigned as a prity as a prity assigned as a prity assigned as a prity as a										
			rity assigned identifier, one code which is unique for each certificate of that subject. The authority assigned identifier and the CA assigned code to be separated with a printable String character separator that is not used within any of the two code types (e.g., "/"). As an example:										
		BCCENC42H3	L be separated with a printable string character separator that is not used within any of the two code types (e.g. / ). As an example: FNC42H30A952P/0001"										
		When the "nseu	n the "pseudonym" attribute is used, the serialNumer attribute MAY contain a fictitious code, e.g. "PseudonymA/00001"										
		Signature verific	ature verification applications SHALL be able to handle this attribute as above specified "										
	Resolution	Specific naming	ecific naming requirements incorporated in TS 102 280 - X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons										
	comment	opoonio naming											
	Resolution	No change to T	o change to TS 101 862, see TS 102 280.										
	text	J	,										
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS101862-006	1.2.1	4.4	UNSTT-005		technical	STF242	09/01/2004	no change					
	Comment	There has been	a long debate on RF	C 3039 clause	3.2.3 following	text: "If the key us	age nonRepudiat	ion bit is asserted then	it SHOULD NOT be				
	text	combined with a	any other key usage, i	.e. if set, the ke	ey usage non-re	epudiation SHOUL	D be set exclusiv	ely."					
		In order to settle	e it, it is suggested to	mandate the ur	nique use of the	e non-repudiation	bit into TS 101 86	2.					
		Additionally, sin	ce also authentication	n certificates ca	n be "qualified	certificates", it is s	suggested to add t	the following statement	: "Should the key usage				
		digitalSignature	bit be asserted, the H	RFC 3280 provi	SIONS SHALL b	e complied with."							
		It is also sugges	sted that IS 101 862	mandates the k	eyUsage exten	sion to be marked	d critical, to avoid	any possible malicious	misuse of the non-				
	Ordering	repudiation and	of the authentication	certificates.									
	Original	Proposed text:	4.4 Key Usage exten	SION		h		and the Street dive large					
	resolution	If the key usage	nonRepudiation bit is	s asserted then	IT SHALL NOT	be combined with	n any other key us	age, i.e. if set, the key	usage non-repudiation				
	proposal	Should instead	the key usage digita	lSignaturo bit b	a accorted the	PEC 2280 provis	ione SHALL be er	molied with					
		The keyl leade	Tould, Instead, the key usage digital Signature bit be asserted, the RFC 3280 provisions SHALL be complied with.										
		Signature verific	Signature verification applications SHALL be able to bandle this attribute as above specified "										
	Resolution	Specific key use	anon applications of	proorated in TS	102 280 - X 50	9 V 3 Certificate	Profile for Certifics	tes Issued to Natural P	ersons				
	comment				102 200 A.00				0100110.				
	Resolution	No change to T	S 101 862, see TS 10	2 280.									
	text	go to r											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
<b>TO</b> 404000 007			reference			075040	00/04/0004					
TS101862-007	1.2.1		EESSI-002		technical	STF242	30/01/2004	no change				
	Comment	A Certificate Re	vocation List (CRL) is	s just as comple	ex a data struct	ure as a certificate	e. Whilst we have	a qualified certificate pr	ofile in deliverable			
	text	TS 101 862, we	101 862, we do not have a CRL profile in any of the deliverables. This is a significant deficiency that could impede interworking.									
	Original	This is to be addressed by CEN ISSS activity on CRL profiles.										
	resolution		his is to be addressed by ETSI TC-ESI activity on CRL and OCSP profiles.									
	proposal											
	Resolution	This is to be ad										
	comment											
	Resolution	No change.	hange.									
	text	· ·	Č ( )									
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS101862-008	1.2.1		OTHER-014		technical	STF242	09/01/2004	no change				
	Comment	It is suggested	that there are two way	s to indicate th	e country of su	pervision:						
	text	<li>i) by using the</li>	countryName attribut	te type defined	in ITU-T Recor	nmendation X.520	) [10]; (This is what	at our standard mandat	es) or			
		ii) by using the	domainComponent a	attribute type de	efined in RFC 2	247 [12]. (This is t	the approach used	d in Microsoft's Active D	Directory)			
		This is not supp	orted in our standard.	. David would li	ike that to be ad	ded to TS 101 86	62.					
	Original											
	resolution											
	proposal											
	Resolution Specific key usage requirements incorporated in TS 102 280 - X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons											
	comment	, ,	0	•								
	Resolution No change to TS 101 862, See TS 102 280.											
	text	<b>.</b>										

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	reference	date	туре	source	date		version			
TS101862-009	1.2.1		TC-ESI_2-001	11/06/2003	technical	STF242	09/01/2004	applied	1.3.1			
TS101862-009	1.2.1 Comment text	To the maintena TS 101 456 def a) QCP public A certific b) QCP public: A certific TS 101 862 def An Identifier of country under v esi4-qcStaten BY id-etsi-qcs This staten 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 si It is thus reques The big advanta public + SSCD"	TC-ESI_2-001 ance team of TS 101 fines: + SSCD: itu-t(0) ident cate policy for qualified cate policy for qualified cate policy for qualified cate policy for qualified fines id-etsi-qcs-QcCo the statement (repress which law the issuer is nent-1 QC-STATEME s-QcCompliance } nent is a statement by is issued as a Qualified d II of the Directive 19 Council of 13 Decembric signatures, as imple the issuer field of this compliance OBJEC es not permit to make ust be known that an S d-organization(4) etsi( mply using a QCstate sted to define an addit age would be that the	11/06/2003 862. iffied-organizat d certificates is anization(4) ets d certificates is mpliance: ented by an OI operating. NT ::= { IDENT r the issuer tha d certificate ac 099/93/EC of th ber 1999 on a 0 emented in the s certificate. T IDENTIFIER the same disti SSCD has been 0)qualified-cer ment extension ional QCstater CP under whice	ion(4) etsi(0) qu sued to the pub si(0)qualified-ce ssued to the pul iD), stating that TIFIED t this coording te European Pa Community fran e law of the cou R ::= { id-etsi-qcs nction as TS 10 n be used. This tificate-policies( n. ment equivalent ch the certificate	STF242 ualified-certificate- lic, requiring use of rtificate-policies(1 blic. the certificate is is uthe certificate is is nework ntry s 1 } 1 456. In particula can currently only (1456)policy-ident to the "QCP publice is being issued r	og/01/2004 policies(1456) po of secure signatur 456)policy-identif ssued according t ssued according t if a verifier wan y be checked whe ifiers(1) qcp-publi lic + SSCD" CP. may be kept, while	applied         licy-identifiers(1) qcp-pure-creation devices.         iers(1) qcp-public (2)         o the EU-Directive [1], a         ts to make sure that the in the following CP OID         c-with-sscd (1)         e simply adding a QCsta	1.3.1 ublic-with-sscd (1). as implemented in the e signature is a Qualified is being used:			
		NOTE: The rest of the mail exchange has been removed for privacy.										
	Original resolution proposal											
	Resolution comment	New QC statem	nent for SSCD added	to TS 101 862.								
	Resolution text	See TS 101 862	ee TS 101 862 V1.3.1.									

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

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target					
	version	clause	contribution	date	type	source	date		version					
			reference											
TS101903-001	1.1.1		JCPKI-003	17/02/2003	Technical	STF242	25/01/2004	no change						
	Comment	Rationale: Som	e comments regarding	g EESSI Signa	ture Policy									
	text	Author: Japan C	r: Japan Computer Research, 2003/02/17											
		Scope and Intro	be and Introduction											
		The purpose of	e purpose of the present document is to convey some comments upon the policy aspects of the electronic signature format as specified in [ESF] d [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 ecification seems to be incorporation of signature policy; the other is that the policy information issues in general can be regarded as one of the post important milestones in the future evolution of e-business.											
		and [XAdES]. T												
		specification se												
		most important												
		It is now routine	is now routine to standardize the encapsulation of signature data. And a number of these formats bind signature with corresponding public key, and ten if not all the time, together with its certificate or certificate chain. That policy information can function as a means to validate status of ccompanying object is well exemplified in the policy attributes of X.509 certificate profile. Nevertheless, it has to be said that attachment of policy to gnature 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											
		often if not all th												
		accompanying of												
		signature hasn't												
		[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. I o l	be more precise, due	to more loose	semantic consti	raints associated	with digital signati	ire, it is expected that a	pplication domain of					
		the signature po	plicy is far more broad	ly ranged com	pared to certific	ate policy. Accord	ingly, needs to ac	ldress wider area of pra	ctical contexts are felt,					
		and this natural	ly leads to the necess	ity of taking int	o account other	policy related de	velopment efforts	in the Internet commun	ity whose shared aim is					
		to promote flexi	ble online transaction	s (valued or oth	nerwise) while a	pproximating relia	ability of real world	d experience.						
		Policy" has ion	g been traditionally as	sociated, one	way or another,	with the idea of a	luthority, predomi	nantly centrally and stat	ically perceived at that.					
		I ne underlying	principle of certificate	policy closely i	ollows this, ess	entially due to the	way it is bred. A	gainst this, especially to	the extent that each					
		Individual ought	to possess his of her	own policy, is	a picture in whi	cn many policies (	dynamically intera	ict to form the whole. Al	this may be thought					
		UI as what the	Signature policy migr	le envisage, 101	od policion in o	s each spallaí ann		that point of time and a						
		feasible Policy	suggest a way to con	v It is in this se	birit that the follo	owing comments	are delivered alth	ough not always explicit	t t					
		Comments		y. 10 5 11 01 5 5		owing comments a	are delivered, alli	lough hot always explici	ι.					
		1 On the man	dated reference to no	licy. In the data	structure sign	ature policy identi	fier is made mand	latory [ESE: 8.9.1] This	can mean either that:					
		(a) every sig	inature MUST have a	non-trivial sign	ature policy av	ailable for retrieva	l in association wi	th the identifier: or that	(b) signature policy can					
		(a) every signature MOST 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	n of a signature is det	ermined by the	signing of it at	the time when the	latter took place	so that the temporal m	edium between the two					
		actions is	s made frozen. In part	icular, this allo	ws the users to	preserve unaltere	d the state and a	uality of signature relati	vely 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 an	d validation is					
		principal	ly the responsibility of	policy source	policy issuer or	TSP), and the de	termination of act	tual policy content is lef	to the latter, and the					
		issuance	can be protracted to	the time of the	delivery.	,,			····· , ·· · ····					

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference		L								
		(c) In practic	ce, hybrid case is the	most likely to b	e demanded. I	his is because:							
		(I) Perfo	ormance wise, a pract	lical computing	platform wants	to avoid actual co		the policy source to ta	ke place every each				
		ume	arithmetic operations than validation process. Also, applications serving as a service provider would surely have to process hundreds of										
		reque	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										
		mear	mean that policy content be left empty and signer decides its policy related action in terms of policy gualifiers only. Which in turn would										
		mear	that it is desired that	t policy qualifier	carry validity d	lates or some sort	of a recommende	ed best before.					
		(ii) Anotl	her reason why it is in	nportant to allow	w empty policy	content at the time	e of signing is that	, in encapsulating a tra	Insaction message in				
		which	n signature data is to	be attached, or	ne might want to	o or have to place	policy related info	rmation outside the sig	nature data, for				
		exam	example using some other policy mechanisms (cf. item 2 below). Practically, this could perhaps mean often that two policy identifiers, that										
		withir	within the signature data and that outside it, are identical, but not necessarily.										
		2. On policy da	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	be obtained from the policy source the reference to which is embedded explicitly in the signature data in the form of mandatory policy identifier.										
			not specify the policy	tonieni. The p	also the protoc	of a signature poil	cy is not manuale	off to the decision of n	alicy source. Existing				
		similar spec	ification activities alor	na these lines in	clude [SAMI ]	[XACMI1 and [W	S-Policy] We will	examine briefly the nor	ssibility of applying				
		these protoc	cols to the purpose of	obtaining policy	v content for the	e [ESF] signature	data here:		solomy of applying				
		a) In Gener	al. These protocols a	re specified in t	erms of XML, v	vhile [ESF] data st	ructure is defined	in terms of ASN.1. So	it would be natural to				
		consider	consider the use of [XAdES] instead of [ESF], to level the networking laver consistent. Similarly, in the following, the reference "[ESF]" is										
		meant to	be "[XAdES]", when	ever the approp	priateness of the	e context demands	s, without explicitly	y mentioned each time					
		b) SAML. B	By this, we mean to ut	ilise SAML secu	urity assertions	as policy content.	Which would me	an that policy source b	e SAML authority,				
		messagi	ng protocol be SAML	request/respon	se. [SAMLCore	e] states that SAM	L "is an XML-bas	ed framework for excha	anging security				
		informati	on. This security info	rmation is expre	essed in the for	m of assertions at	out subject, wher	e a subject is an entity	(either human or				
		compute	r) that has an identity	' in some securi	ty domain". In o	brder to fit exactly	into this description	on, signature ought to r	epresent the "entity" so				
		taking in	to account that promi	Idation of SAM	l is ranidly in n	lace Whereas or	the other hand v	Ne helieve that the sign	ature policy of [ESE]				
		type can	act as an "external p	olicy" for SAM	to the contrar	V.							
		c) XACML.	Although termed as '	Access Contro	I Markup Langu	lage", the motivati	on of XACML der	ives from 'a pressing n	eed for a common				
		language	e for expressing secu	rity policy' ([XA0	CML]). It is in th	nis sense that XAC	ML might just be	suitable as the policy la	anguage for [ESF]. For				
		this, how	vever, we believe that	one has to mal	ke a careful arc	hitectural conside	ration to cohere th	ne two semantically. (S	ee item 5 for a brief				
		remark c	on this.)										
		d) Web Ser	vices Policy Framewo	ork. Similar to a	pplicability of X	ACML, but with a	more restricted c	ontext of the web servi	ces interoperability.				
		There ar	e on-going investigati	ions as to now [	XACML ] and [	WS-Policy] can be	e made consistent	in practice. Here we w	ould rather insist on the				
		synergy	of [ESF] with [XACIVIL	_] for the reason	n that semantic		re general in natu	Web Services Security	for the signature				
			security standards, o	encina) We fee	applying seco	inly is a notential	ging in the form of	web Services Security	7, IOI the signature				
		3 On policy pr	otection The mechar	nism for policy r	protection is pro	wided by the auth	entication of policy	v source (IESE: 6 111)	The latter is rendered in				
		terms of the	hash calculation of th	ne policy identifi	ier. Also, bindin	a of the policy sou	rce and actual po	blicv seems to be rende	ared by the same				
		mechanism	(although only implici	t, cf. [ESF; 11.1	]). This may no	ot offer enough lev	el of protection, fo	or a complex distributed	policy environment in				
		which, for ex	ample, policy source	refers to anoth	er policy source	e and so on (whicl	n seems to be cas	e with [SAML] in coope	eration with [XACML]).				
		Further, sigr	nature policy doesn"t	seem to carry it	s own signatur	e explicitly, which	means, if it is to b	e signed, the signature	data are to be				
		attached ext	ernally. We believe, t	o complement	this, that signin	g of signature poli	cy has to be desc	ribed in detail, at least	normatively (as XACML				
		TC does). F	or especially, there m	ay arise possib	le semantic am	biguities between	"signature policy"	' and "policy signature"	. And it could well				
		happen that	the latter may be pro	vided by some	ISP other than	n policy issuer itsel	lt.						

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
		<ol><li>On signature</li></ol>	e policy data structure	. Although not	normative, we h	nave a number of	reasons that sign	ature policy specified ir	n [ESF] has to be			
		examined cl	osely. The primary on	e being its pos	ition with respe	ct to other policy a	assertions mentior	ned above (see item 2)	, we feel that [ESF]			
		signature po	licy format has to add	Iress either pos	sible interopera	ability with or defin	itive differentiatio	n from these other stan	dards. Here are a			
		couple of fra	igmental comments:									
		a) On Rules	s. The terminology en	ployed, "Comr	non Rules" ([ES	SF; 11.3]) and "Co	mmitment Rules"	([ESF; 11.4]), seems to	o be rather awkward			
		especial	ly when compared wit	h other standaı	ds. It is suspec	ted that this was i	ntentionally chose	en with some specific a	pplication in mind, but			
		we could	I not have identified th	e relevant pas	sages in the spe	ecification.						
		b) On Exter	nsions. In practice, we	e believe that he	eavy usage of S	SignPolExtensions	s ([ESF; 11.11]) ar	e expected to be inevit	able, for example in			
			ng signatures or othe	r validation data	a for further pro	tection depending	on the circumsta	nces (see item 3). we	feel that it would be a			
		good ide	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									
		5. On interoper	for establishing secur	transactions	It is to this exten	t that we feel pol	icy framework of	XACMI should be take	n into account in			
		configuring t	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	configuring the application domain of signature policy, regardless of whether transaction of the latter takes place through application layer protocols or not									
		References	100.									
		(ESF)	ETSI TS 101 733 "E	ectronic Signa	ature Formats".							
		IRFC32801	Internet X.509 Publi	c Kev Infrastru	cture Certificate	and Certificate R	evocation List (Cl	RL) Profile.				
		[SAMLCore]	Assertions and Prot	ocol for the OA	SIS Security As	sertion Markup L	anguage (SAML).					
		[XACML]	OASIS extensible A	ccess Control I	Markup Langua	ge (XACML).						
		[XAdES]	ETSI TS 101 903 "X	ML Advance E	lectronic Signa	tures (XAdES)".						
		[WS-Policy]	Web Services Policy	y Framework (V	VS-Policy).							
	Original											
	resolution											
	proposal											
	Resolution	Comment on (a	): The appearance of	a signature pol	icy identifier do	es not preserve u	naltered the state	and quality of signature	e relatively long time (if			
	comment	the algorithm or	the key are broken, t	he signature po	olicy identifier d	pes not protect the	e signature): this l	has to be achieved by c	other means, like time-			
		stamping. What	a signature policy ide	entifier does is t	o fix rules that i	the verifier has to	follow to validate	the signature.				
			nion of TS 101 002 da	an not use the	Signature	Implied with NUU	Lyoluo					
	Posolution	The current vers	SIGN OF 15 TUT 903 00	es not use the	SignaturePolic	ymplied with NUL	L value.					
	tovt											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
TS101903-002	111		JCPKI-003	17/02/2003	technical	STF242	21/06/2003	no change				
10101000 002	Comment	Page 17: Times	tamp seems unneces	sarv in XAdES	-X. since XadE	S-X-L is enough.	21/00/2000	ine change				
	text	This should be o	should be deleted to avoid being complicacy of specifications.									
	Original											
	resolution											
	proposal											
	Resolution	These forms de	of forms deal with different situations: XAdES-X Types 1 and 2 are for those environments where verifier has access to all the validation data									
	comment	AND some of th	ome of the keys of the CAs in the cert path can be compromised. XAdES-X-L are for those environments where verifier HAS NOT access to validation data; then they are added to the signature itself.									
	Resolution		מוטמוטרו עמומ. וויפר וויפץ מיפ מעשבע וט וויפ איטומועויב וואבוו.									
	text											
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution reference	date	type	source	date		version			
TS101903-003	1.1.1		JCPKI-003	17/02/2003	technical	STF242	21/06/2003	no change				
	Comment	It makes sense	that signature format	, which is desig	ned to incorpor	ates signature po	licy, is defined in	terms of XML, when cor	nsidered that the			
	text	worldly policy st	andards, like SAML,	XACML, WS-S	ecurity, are spe	cified at the same	e processing layer	using XML.				
		In this sense, it these policy related	would be preferable ( ated standards.	(if not normative	ely, but informa	tively) for the pres	ent standard to ir	vestigate its practicable	e interoperability with			
	Original											
	resolution											
	proposal											
	Resolution	As said before t	he intentions of the E	SI group is to to	ry to be aligned	l with relevant initi	atives on the field	s where it develops its	documents. And indeed			
	comment	the developmen	it									
		of a signature p	olicy format will have	e to take into ac	count developn	nents in XACML						
	Resolution											
	text											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS101903-004	1.1.1		JCPKI-003	17/02/2003	technical	STF242	21/06/2003	no change				
	Comment	Relative to TS 1	ive to TS 101 733 ES Formats, a profile of XML long term signature format was introduced assuming a similar use of CMS SignedData last									
	text	year.										
		Relative to Japa	e 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	matches well than ASN.1 based TS 101 733 from the point of view of long term signature save.									
		To diffuse the u	ise the use of XadES, test programs for interoperability should be implemented.									
		Some errors are	e pointed out in some	parts of XadES	schema so the	at bug information	should be opene	d to public promptly.				
		The manual of 2	XML time-stamping us	sed in the prese	ent document s	hould be describe	d soon after OAS	IS standard formulation	1.			
	Original											
	resolution											
	proposal											
	Resolution	There is a curre	ently taking place inter	operability ever	nt within ETSI.							
	comment	Dealing where of	different implementati	ons are being d	eveloped and i	interoperability am	ong them is being	g assessed. The group	is also building up a			
		number of tests	for facilitating develo	pments of such	tools.							
		A specialist task	c force is currently wo	orking on mainte	enance of all th	e ETSI specificati	ons and will issue	a report on all outstan	ding issues that have			
		yet to be addres	ssed by revised speci	fications.								
	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	In the clause 7.6	6.2 of the XAdES spe	ecification [1] it s	ays:							
	text	OCSP Respons	P Responses (OCSPValues) consist of a sequence of at least one OCSP Response. The <encapsulatedocspvalue> element contains the</encapsulatedocspvalue>									
		base64 encodin	e64 encoding of a DER-encoded OCSP Response. [1, clause 7.6.2]									
		During the XAd	ring the XAdES-PLUGTESTST it turned out that this section has been interpreted differently by the participating implementers in terms of what the									
		actual content o	al content of the < EncapsulatedOCSPValue> has to bee. Some implementers included the whole OCSPResponse others have just included the									
		BasicOCSPRes	icOCSPResponse (contained in the ResponseBytes of the OCSPResponse as defined in RFC 2560 [21]). Therefore, the specification should be									
		more explicit ab	explicit about what to include into the <encapsulatedocspvalue> element.</encapsulatedocspvalue>									
	Original	Since the addition	the additional information that is provided by the OCSPResponse is not needed to be archived, it was first suggested to include the									
	resolution	BasicOCSPRes	icOCSPResponse. The different possibilities are:									
	proposal	<ul> <li>OCSPResponse</li> </ul>	onse: On the one han	d, the additiona	I information pr	ovided by the OC	SPResponse—ar	n integer value indicatin	g if the request was			
		successful-	-is not needed to be a	archived, howev	er, this is how t	he actual version	of the specification	on is to be interpreted n	nost likely. On the other			
		hand, the inf	formation provided by	the <ocspre< th=""><th>ferences&gt; elem</th><th>ent reflects the co</th><th>ontent of the Basic</th><th>COCSPResponse. Ther</th><th>refore, any other OCSP</th></ocspre<>	ferences> elem	ent reflects the co	ontent of the Basic	COCSPResponse. Ther	refore, any other OCSP			
		response typ	be than the BasicOCS	SPResponse ha	s to be referen	ced by a <otherr< th=""><th>ef&gt; element, mos</th><th>t likely.Thus, an OCSP</th><th>response containing a</th></otherr<>	ef> element, mos	t likely.Thus, an OCSP	response containing a			
		different res	ponse type will have	to be included ir	nto a <otherval< th=""><th>lue&gt; element.</th><th></th><th></th><th>_</th></otherval<>	lue> element.			_			
		<ul> <li>ResponseBy</li> </ul>	/tes: The ResponseB	ytes are already	y in DER-encod	led format. They i	nclude an additior	nal object identifier indic	cating the type of the			
		included OC	SP response. The Re	esponse Bytes i	may again conta	ain OCSP respon	ses of different ty	pes. Therefore, the san	ne arguments apply, as			
		for the OCS	PResponse stated in	the paragraph a	above.							
		<ul> <li>BasicOCSPI</li> </ul>	Response: The Basic	OCSPRespons	e contains exac	ctly the data that r	eeds to be archiv	ed and corresponds to	the information			
		provided by	the <ocspref> eler</ocspref>	nent.								
		At the interop th	e participants agrred	to use OCSPR	esponse, since	this is basically w	hat the standards	s said, and furthermore	the only deployed			
		implementation	in Estonia uses that i	interpretation.	-	-						
	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										
TS101903-006	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed					
	Comment	Problem Descri	ption										
	text	The specificatio	n of the <timestamp< th=""><th>Type&gt; data typ</th><th>e is broken in tw</th><th>/o ways:</th><th colspan="6"></th></timestamp<>	Type> data typ	e is broken in tw	/o ways:							
		1. While it is ea	asy to verify the time-s	stamp by proce	ssing all <hash< th=""><th>DataInfo&gt; elemen</th><th>its and comparing</th><th colspan="6">s and comparing the resulting hash value to the hash value</th></hash<>	DataInfo> elemen	its and comparing	s and comparing the resulting hash value to the hash value					
		stored in the	e time-stamp, it is diffic	cult, time-consu	iming and possi	bly even infeasibl	e in the general case to verify, if the time-stamp is applied he time-stamp is applied on the elements that are claimed to e <archivetimestamp> <hashdatainfo> elements have to be</hashdatainfo></archivetimestamp>						
		exactly on th	ne data that is claimed	I by the XAdES	specification. T	hat is, to verify if							
		be time-stan	nped.			<b>_</b>							
		2. For the <aiii< th=""><th>DataObjectsTimeStan</th><th>np&gt;, <individua< th=""><th>IDataObjectsTir</th><th>neStamp&gt; and the</th></individua<></th></aiii<>	DataObjectsTimeStan	np>, <individua< th=""><th>IDataObjectsTir</th><th>neStamp&gt; and the</th></individua<>	IDataObjectsTir	neStamp> and the							
		composed th	hat resolve to exactly	the same data	as the correspo	nding <ds:refere< th=""><th colspan="5" rowspan="3">ence&gt;s in the <ds:signedinfo> do. In the general case it is resolving depends on the context (e.g. the node it is contained</ds:signedinfo></th></ds:refere<>	ence>s in the <ds:signedinfo> do. In the general case it is resolving depends on the context (e.g. the node it is contained</ds:signedinfo>						
		difficult or pr	obably inteasible to c	ompose such a	reference, bec	ause the result of							
		IN). Demorika											
		The input for the	o difforant timo stamp	s used in the a		orsion is formed h	w moone of allos	hDatalatas alamanta T	Those HashDatalates				
		elements have t	to be processed acco	rding to the refe		na model specifie	d in the XMI DSic	specification [3] This is	s in short, resolving the				
		provided LIRI in	the LIRI-attribute of the	ruing to the rele na ∠HashDatali	nfos element a	ng model specifie	orms that are sne	cified by the optional -	Transforms> child				
		element of the	HashDataInfo> elem	ent and finally of	canonicalizing th	pprying the transit	tout of the last tra	insform (or the result of	resolving the URL if				
		there is no trans	sform at all) is a node	list. This mean	s that the result	of processing one	te <hashdatainfo> element is octet data in any case. The</hashdatainfo>						
		resulting octets	of all the included <h< th=""><th>ashDataInfo&gt; e</th><th>elements are the</th><th>en concatenated i</th><th>n the order the &lt;</th><th>HashDataInfos&gt; appea</th><th>r in the document to</th></h<>	ashDataInfo> e	elements are the	en concatenated i	n the order the <	HashDataInfos> appea	r in the document to				
		form the input for	or the time-stamp. The	ese resulting or	tets are in fact	he information the	at is time-stampe	d.					
		The current vers	sion of XAdES specifi	cation therefore	e mandates wha	t the result of pro	cessing an <hasl< th=""><th>nDataInfo&gt; elements ha</th><th>as to be. In the</th></hasl<>	nDataInfo> elements ha	as to be. In the				
		definition of the	<signaturetimestam< th=""><th>p&gt; property it s</th><th>ays for instance</th><th>):</th><th>C C</th><th></th><th></th></signaturetimestam<>	p> property it s	ays for instance	):	C C						
		The <signature< th=""><th>TimeStamp&gt; element</th><th>contains a sing</th><th>gle <hashdatalı< th=""><th>nfo&gt; element that</th><th>refers to the <ds:< th=""><th>SignatureValue&gt; eleme</th><th>ent of the XMLDSig</th></ds:<></th></hashdatalı<></th></signature<>	TimeStamp> element	contains a sing	gle <hashdatalı< th=""><th>nfo&gt; element that</th><th>refers to the <ds:< th=""><th>SignatureValue&gt; eleme</th><th>ent of the XMLDSig</th></ds:<></th></hashdatalı<>	nfo> element that	refers to the <ds:< th=""><th>SignatureValue&gt; eleme</th><th>ent of the XMLDSig</th></ds:<>	SignatureValue> eleme	ent of the XMLDSig				
		signature. That	is, the input for the tin	ne-stamp hash	computation is	the <ds:signature< th=""><th>Value&gt; XML eler</th><th>nent. [1, clause 7.3.1]</th><th></th></ds:signature<>	Value> XML eler	nent. [1, clause 7.3.1]					
		A verifying appl	ication has to make s	ure that the time	e-stamp has be	en applied on the	proper input data	. This is, to verify some	how that processing				
		the <hashdatal< th=""><th>Info&gt; element results</th><th>in the data that</th><th>is claimed by th</th><th>e XAdES specific</th><th>cation. In case of</th><th>the <signaturetimesta< th=""><th>mp&gt; for instance, this is</th></signaturetimesta<></th></hashdatal<>	Info> element results	in the data that	is claimed by th	e XAdES specific	cation. In case of	the <signaturetimesta< th=""><th>mp&gt; for instance, this is</th></signaturetimesta<>	mp> for instance, this is				
		the <ds:signatu< th=""><th>ireValue&gt; element. Th</th><th>ius, the verifyin</th><th>g application ha</th><th>s to check that th</th><th>e octets that are l</th><th>peing time-stamped are</th><th>e a valid representation</th></ds:signatu<>	ireValue> element. Th	ius, the verifyin	g application ha	s to check that th	e octets that are l	peing time-stamped are	e a valid representation				
		of the <ds:signa< th=""><th>atureValue&gt; element.</th><th></th><th></th><th></th><th></th><th></th><th></th></ds:signa<>	atureValue> element.										
		As an URI and a	an arbitrary number of	t transforms ca	n be used to col	mpose such a <h< th=""><th>ashDataInfo&gt; ele</th><th>ment, it is inteasible to</th><th>deduce from the</th></h<>	ashDataInfo> ele	ment, it is inteasible to	deduce from the				
		specified URI al	nd the given transform	ns to the result,	in the general of	case. Thus, the or	ny way to verify w	nat has been time-star	nped is to process the				
			> element and analyze	e the result.	ont actat data r	oprocontations the	at boar the same	information canonicali	zation has been				
		introduced Thu	the only practical w	av to verify the	timestamp inpu	t is to compare the	at bear the same	orm of the data that has	s to be time-stamped				
		according To th	a specification with th	ay to verify the	illestamp inpu	sing the correspo	nding -HashData	Infos element. In this c	esse it would be				
		sufficient to sim	nly create the require	d input for the t	ime-stamp_com	inute the diaest v	alue and compare	it with the digest value	in the time-stamp				
		However the <	HashDataInfo> eleme	nt was introduc	ed to identify th	e input of a diven	time-stamp in ca	ses where the input is a	ambiguous. But it does				
		not serve this p	urpose anyway, as ha	s been shown	above	epar er a given							
		Therefore, a ne	w solution has to be for	ound to identify	the input-data	of a given time-sta	amp in cases wer	e this input cannot be u	nambiguously defined				
		by the XAdES s	pecification.			0			<u> </u>				

version	clause	contribution	date	type	source	date	Resolution status	version
		reference		.,,,,,				
Original	During the intere	operability event the f	ollowing resolution	tion proposal w	as discussed and	agreed on:		
resolution	The <timestam< th=""><th>pType&gt; data type sho</th><th>ould be redefine</th><th>ed to use an ID-</th><th>list to identify the</th><th>elements that ha</th><th>ve been time-stamped.</th><th>An optional</th></timestam<>	pType> data type sho	ould be redefine	ed to use an ID-	list to identify the	elements that ha	ve been time-stamped.	An optional
proposal	<ds:canonicaliz< th=""><th>ationMethod&gt; elemer</th><th>nt should indica</th><th>te which canon</th><th>icalization method</th><th>d to use for canon</th><th>icalizing XML elements</th><th>s. If no canonicalization</th></ds:canonicaliz<>	ationMethod> elemer	nt should indica	te which canon	icalization method	d to use for canon	icalizing XML elements	s. If no canonicalization
	In the case of in	cluded <ds:reference< th=""><th></th><th>ethod as specin</th><th>ed by the actual A</th><th>vite indicates if the</th><th>ation MUST de used.</th><th>ent itself or the data</th></ds:reference<>		ethod as specin	ed by the actual A	vite indicates if the	ation MUST de used.	ent itself or the data
	resulting from p	rocessing the <ds:ref< th=""><th>ference&gt; should</th><th>d be included. I</th><th>the referencedD</th><th>ata-attribute is on</th><th>nitted or the attribute va</th><th>lue is false the element</th></ds:ref<>	ference> should	d be included. I	the referencedD	ata-attribute is on	nitted or the attribute va	lue is false the element
	identified by the	included URI is inclu	ded. If the refer	encedDataattri	oute value is true	the <ds:reference< th=""><th>e&gt; has to be processed</th><th>d according to the</th></ds:reference<>	e> has to be processed	d according to the
	reference proce	ssing model of the XM	/LDSig specific	cation. The resu	It is then used as	input for the time	-stamp. The result of th	e processing must be
	exactly the same	e data as that was us	ed in the comp	utation of the <	ds:Reference> dig	gest value.		
	<xsd:element na<="" th=""><th>ame="TimeStamp" typ</th><th>be="TimeStamp</th><th>oType"/&gt;</th><th></th><th></th><th></th><th></th></xsd:element>	ame="TimeStamp" typ	be="TimeStamp	oType"/>				
	<xsd:complexty< th=""><th>/pe name="TimeStam</th><th>npType"&gt;</th><th></th><th></th><th></th><th></th><th></th></xsd:complexty<>	/pe name="TimeStam	npType">					
	<xsd:sequence></xsd:sequence>	> >ma "Includa" turca "	lo aluda Tura all m		ounded"/s			
	<xsd.element re<="" th=""><th>ame= include_type= f="ds:Canonicalizatio</th><th>nMethod" min(</th><th></th><th>Jounded /&gt;</th><th></th><th></th><th></th></xsd.element>	ame= include_type= f="ds:Canonicalizatio	nMethod" min(		Jounded />			
	<xsd:choice></xsd:choice>							
	<xsd:element na<="" th=""><th>ame="EncapsulatedTi</th><th>imeStamp"&gt;</th><th></th><th></th><th></th><th></th><th></th></xsd:element>	ame="EncapsulatedTi	imeStamp">					
	type="Encapsula	atedPKIDataType"/>						
	<xsd:element na<="" th=""><th>ame="XMLTimeStamp</th><th>p" type="AnyTy</th><th>′pe"/&gt;</th><th></th><th></th><th></th><th></th></xsd:element>	ame="XMLTimeStamp	p" type="AnyTy	′pe"/>				
	<th>&gt; VDe&gt;</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	> VDe>						
	<xsd:complextv< th=""><th>/pe name="IncludeTv</th><th>pe"&gt;</th><th></th><th></th><th></th><th></th><th></th></xsd:complextv<>	/pe name="IncludeTv	pe">					
	<xsd:attribute na<="" th=""><th>ame="uri" type="xsd:a</th><th>anyURI" use="r</th><th>equired"/&gt;</th><th></th><th></th><th></th><th></th></xsd:attribute>	ame="uri" type="xsd:a	anyURI" use="r	equired"/>				
	<xsd:attribute na<="" th=""><th>ame="referencedData</th><th>a" type="xsd:bo</th><th>olean" use="op</th><th>tional"/&gt;</th><th></th><th></th><th></th></xsd:attribute>	ame="referencedData	a" type="xsd:bo	olean" use="op	tional"/>			
	<th>ype&gt;</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	ype>						
Resolution								
Resolution								
text								
_	Original resolution proposal Resolution comment Resolution text	Original resolution proposalDuring the interd The <timestam </timestam  <ds:canonicaliz </ds:canonicaliz  method is special In the case of in resulting from pri identified by the reference proce exactly the same <xsd:element na<br=""></xsd:element> <xsd:element na<br=""></xsd:element> <td< th=""><th>Original resolution proposal     During the interoperability event the fr The <timestamptype> data type shot <ds:canonicalizationmethod> element method is specified the standard cand In the case of included <ds:reference resulting from processing the <ds:ref identified by the included URI is inclu- reference processing model of the XM exactly the same data as that was us       <xsd:element name="TimeStamp" type<br=""><xsd:complextype name="TimeStamp" type<br=""><xsd:element name="TimeStamp" type<br=""><xsd:element ds:canonicalization<br="" name="Include" type="&lt;br&gt;&lt;xsd:element ref="><xsd:choice> <xsd:element encapsulatedpkidatatype"="" name="EncapsulatedT&lt;br&gt;type="></xsd:element> <xsd:element <br="" name="XMLTimeStamp"><xsd:element name="TimeStamp" type<br=""><xsd:element ds:canonicalization<br="" name="Include" type="&lt;br&gt;&lt;xsd:element ref="><xsd:choice> <xsd:element encapsulatedpkidatatype"="" name="EncapsulatedT&lt;br&gt;type="></xsd:element> <xsd:choice></xsd:choice></xsd:choice></xsd:element></xsd:element></xsd:element></xsd:choice></xsd:element></xsd:element></xsd:complextype></xsd:element></ds:ref </ds:reference </ds:canonicalizationmethod></timestamptype></th><th>Original resolution proposal       During the interoperability event the following resolu The <timestamptype> data type should be redefine <ds:canonicalizationmethod> element should indica method is specified the standard canonicalization method in the case of included <ds:reference> elements and resulting from processing the <ds:reference> should identified by the included URI is included. If the reference processing model of the XMLDSig specific exactly the same data as that was used in the comp <xsd:element <br="" name="TimeStamp" type="TimeStamp"><xsd:complextype name="TimeStampType"> <xsd:element include"="" method"="" minof<br="" name="TimeStamp" type="IncludeType"><xsd:element name="EncapsulatedTimeStamp"> <xsd:element name="EncapsulatedTimeStamp"> <xsd:element name="EncapsulatedTimeStamp"> <xsd:element name="XMLTimeStamp" timestamp"="" type="TimeStampType" xmltimestamp"=""></xsd:element> <xsd:complextype name="TimeStampType"> <xsd:complextype name="TimeStampType"> <xsd:element encapsulatedtimestamp"="" include"="" maxoccurs="unt&lt;br&gt;&lt;xsd:element name=" name="Include" type="IncludeType"> <xsd:element <br="" name="Include" type="IncludeType"><xsd:element name="EncapsulatedTimeStamp"></xsd:element></xsd:element></xsd:element></xsd:complextype></xsd:complextype></xsd:element></xsd:element></xsd:element></xsd:element></xsd:complextype></xsd:element></ds:reference></ds:reference></ds:canonicalizationmethod></timestamptype></th><th>Original resolution proposal         During the interoperability event the following resolution proposal was discussed and The <timestamptype> data type should be redefined to use an ID-list to identify the <ds:canonicalizationmethod> element should indicate which canonicalization method method is specified the standard canonicalization method as specified by the actual &gt; In the case of included <ds:reference> elements an additional referencedData-attrib resulting from processing the <ds:reference> should be included. If the referencedD identified by the included URI is included. If the referencedData-attribute value is true reference processing model of the XMLDSig specification. The result is then used as exactly the same data as that was used in the computation of the <ds:reference> dig <xsd:element name="TimeStampType"> <xsd:element <="" name="TimeStampType" sds:<br=""><xsd:element name="TimeStampType"> <xsd:complextype name="TimeStampType"> <xsd:element minoccurs="0" ref="ds:CanonicalizationMethod"></xsd:element> <xsd:element name="EncapsulatedTimeStamp"> type="EncapsulatedPKIDataType"/&gt; <xsd:element name="EncapsulatedTimeStamp"> type="EncapsulatedPKIDataType"/&gt; <xsd:element name="XMLTimeStamp" type="AnyType"></xsd:element>   <xsd:element name="EncapsulatedTimeStamp"> type="EncapsulatedPKIDataType"/&gt;              </xsd:element></xsd:element></xsd:element></xsd:complextype></xsd:element></xsd:element></xsd:element></ds:reference></ds:reference></ds:reference></ds:canonicalizationmethod></timestamptype></th><th>Original resolution proposal         During the interoperability event the following resolution proposal was discussed and agreed on: The <timestamptype> data type should be redefined to use an ID-list to identify the elements that ha <ds:canonicalizationmethod> element should indicate which canonicalization method to use for canon method is specified the standard canonicalization method as specified by the actual XMLDSig specific in the case of included <ds:reference> elements an additional referencedData-attribute indicates if the resulting from processing the <ds:reference> should be included. If the referencedData-attribute is on identified by the included URI is included. If the referencedDataattribute value is true the <ds:reference reference processing model of the XMLDSig specification. The result is then used as input for the time exactly the same data as that was used in the computation of the <ds:reference> digest value.           <xsd:element name="TimeStampType"></xsd:element> <xsd:sequence> <xsd:element name="TimeStampType"></xsd:element> <xsd:element maxoccurs="unbounded" name="Include" type="IncludeType"></xsd:element> <xsd:element name="EncapsulatedTimeStamp"> type="EncapsulatedTimeStampType"/&gt; <xsd:element name="KMLTimeStamp" type="AnyType"></xsd:element> <xsd:element name="XMLTimeStamp" type="AnyType"></xsd:element> <xsd:element name="XMLTimeStamp" type="AnyType"></xsd:element> <xsd:element name="TimeStamp" type="AnyType"></xsd:element>  <xsd:choice> <xsd:choice> <xsd:choice> <xsd:choice> <xsd:choice> <td< th=""><th>Original resolution         call to the second second</th></td<></xsd:choice></xsd:choice></xsd:choice></xsd:choice></xsd:choice></xsd:element></xsd:sequence></ds:reference></ds:reference </ds:reference></ds:reference></ds:canonicalizationmethod></timestamptype></th></td<>	Original resolution proposal     During the interoperability event the fr The <timestamptype> data type shot <ds:canonicalizationmethod> element method is specified the standard cand In the case of included <ds:reference resulting from processing the <ds:ref identified by the included URI is inclu- reference processing model of the XM exactly the same data as that was us       <xsd:element name="TimeStamp" type<br=""><xsd:complextype name="TimeStamp" type<br=""><xsd:element name="TimeStamp" type<br=""><xsd:element ds:canonicalization<br="" name="Include" type="&lt;br&gt;&lt;xsd:element ref="><xsd:choice> <xsd:element encapsulatedpkidatatype"="" name="EncapsulatedT&lt;br&gt;type="></xsd:element> <xsd:element <br="" name="XMLTimeStamp"><xsd:element name="TimeStamp" type<br=""><xsd:element ds:canonicalization<br="" name="Include" type="&lt;br&gt;&lt;xsd:element ref="><xsd:choice> <xsd:element encapsulatedpkidatatype"="" name="EncapsulatedT&lt;br&gt;type="></xsd:element> <xsd:choice></xsd:choice></xsd:choice></xsd:element></xsd:element></xsd:element></xsd:choice></xsd:element></xsd:element></xsd:complextype></xsd:element></ds:ref </ds:reference </ds:canonicalizationmethod></timestamptype>	Original resolution proposal       During the interoperability event the following resolu The <timestamptype> data type should be redefine <ds:canonicalizationmethod> element should indica method is specified the standard canonicalization method in the case of included <ds:reference> elements and resulting from processing the <ds:reference> should identified by the included URI is included. If the reference processing model of the XMLDSig specific exactly the same data as that was used in the comp <xsd:element <br="" name="TimeStamp" type="TimeStamp"><xsd:complextype name="TimeStampType"> <xsd:element include"="" method"="" minof<br="" name="TimeStamp" type="IncludeType"><xsd:element name="EncapsulatedTimeStamp"> <xsd:element name="EncapsulatedTimeStamp"> <xsd:element name="EncapsulatedTimeStamp"> <xsd:element name="XMLTimeStamp" timestamp"="" type="TimeStampType" xmltimestamp"=""></xsd:element> <xsd:complextype name="TimeStampType"> <xsd:complextype name="TimeStampType"> <xsd:element encapsulatedtimestamp"="" include"="" maxoccurs="unt&lt;br&gt;&lt;xsd:element name=" name="Include" type="IncludeType"> <xsd:element <br="" name="Include" type="IncludeType"><xsd:element name="EncapsulatedTimeStamp"></xsd:element></xsd:element></xsd:element></xsd:complextype></xsd:complextype></xsd:element></xsd:element></xsd:element></xsd:element></xsd:complextype></xsd:element></ds:reference></ds:reference></ds:canonicalizationmethod></timestamptype>	Original resolution proposal         During the interoperability event the following resolution proposal was discussed and The <timestamptype> data type should be redefined to use an ID-list to identify the <ds:canonicalizationmethod> element should indicate which canonicalization method method is specified the standard canonicalization method as specified by the actual &gt; In the case of included <ds:reference> elements an additional referencedData-attrib resulting from processing the <ds:reference> should be included. If the referencedD identified by the included URI is included. If the referencedData-attribute value is true reference processing model of the XMLDSig specification. The result is then used as exactly the same data as that was used in the computation of the <ds:reference> dig <xsd:element name="TimeStampType"> <xsd:element <="" name="TimeStampType" sds:<br=""><xsd:element name="TimeStampType"> <xsd:complextype name="TimeStampType"> <xsd:element minoccurs="0" ref="ds:CanonicalizationMethod"></xsd:element> <xsd:element name="EncapsulatedTimeStamp"> type="EncapsulatedPKIDataType"/&gt; <xsd:element name="EncapsulatedTimeStamp"> type="EncapsulatedPKIDataType"/&gt; <xsd:element name="XMLTimeStamp" type="AnyType"></xsd:element>   <xsd:element name="EncapsulatedTimeStamp"> type="EncapsulatedPKIDataType"/&gt;              </xsd:element></xsd:element></xsd:element></xsd:complextype></xsd:element></xsd:element></xsd:element></ds:reference></ds:reference></ds:reference></ds:canonicalizationmethod></timestamptype>	Original resolution proposal         During the interoperability event the following resolution proposal was discussed and agreed on: The <timestamptype> data type should be redefined to use an ID-list to identify the elements that ha <ds:canonicalizationmethod> element should indicate which canonicalization method to use for canon method is specified the standard canonicalization method as specified by the actual XMLDSig specific in the case of included <ds:reference> elements an additional referencedData-attribute indicates if the resulting from processing the <ds:reference> should be included. If the referencedData-attribute is on identified by the included URI is included. If the referencedDataattribute value is true the <ds:reference reference processing model of the XMLDSig specification. The result is then used as input for the time exactly the same data as that was used in the computation of the <ds:reference> digest value.           <xsd:element name="TimeStampType"></xsd:element> <xsd:sequence> <xsd:element name="TimeStampType"></xsd:element> <xsd:element maxoccurs="unbounded" name="Include" type="IncludeType"></xsd:element> <xsd:element name="EncapsulatedTimeStamp"> type="EncapsulatedTimeStampType"/&gt; <xsd:element name="KMLTimeStamp" type="AnyType"></xsd:element> <xsd:element name="XMLTimeStamp" type="AnyType"></xsd:element> <xsd:element name="XMLTimeStamp" type="AnyType"></xsd:element> <xsd:element name="TimeStamp" type="AnyType"></xsd:element>  <xsd:choice> <xsd:choice> <xsd:choice> <xsd:choice> <xsd:choice> <td< th=""><th>Original resolution         call to the second second</th></td<></xsd:choice></xsd:choice></xsd:choice></xsd:choice></xsd:choice></xsd:element></xsd:sequence></ds:reference></ds:reference </ds:reference></ds:reference></ds:canonicalizationmethod></timestamptype>	Original resolution         call to the second	

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS101903-007	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed				
	Comment	The <archiveti< th=""><th colspan="10"><archivetimestamp> definition is broken in two ways:</archivetimestamp></th></archiveti<>	<archivetimestamp> definition is broken in two ways:</archivetimestamp>									
	text	1. The <archiv< th=""><th colspan="10" rowspan="4">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. clause 7.7.1 of the XAdES specification [1] it says:</signeddataobjectproperties></signedsignatureproperties></signedpropertieselement></archivetimestamp></th></archiv<>	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. clause 7.7.1 of the XAdES specification [1] it says:</signeddataobjectproperties></signedsignatureproperties></signedpropertieselement></archivetimestamp>									
		2. The reference										
		these eleme										
		In clause 7.7.1										
		The XAdES <a< th=""><th>rchiveTimeStamp&gt; el</th><th>ement contains</th><th>the following se</th><th>equence of Hash-</th><th>DataInfo element</th><th>S:</th><th></th></a<>	rchiveTimeStamp> el	ement contains	the following se	equence of Hash-	DataInfo element	S:				
		- One <hashl< th=""><th colspan="10">e <hashdatainto> element for each data object signed by the XMLDSIG signature. The result of application of the transforms specified each ashDataInfo&gt; must be exactly the same as the octet stream that was originally used for computing the digest value of the corresponding.</hashdatainto></th></hashl<>	e <hashdatainto> element for each data object signed by the XMLDSIG signature. The result of application of the transforms specified each ashDataInfo&gt; must be exactly the same as the octet stream that was originally used for computing the digest value of the corresponding.</hashdatainto>									
		<hashdatal< th=""><th colspan="10">ashDataInfo&gt; must be exactly the same as the octet stream that was originally used for computing the digest value of the corresponding</th></hashdatal<>	ashDataInfo> must be exactly the same as the octet stream that was originally used for computing the digest value of the corresponding									
		<ds:referen< th=""><th colspan="10">:Reference&gt;. HashDataInfo&gt; element for the <ds:signedinfo> element. The result of application of the transforms specified in this <hashdatainfo> must</hashdatainfo></ds:signedinfo></th></ds:referen<>	:Reference>. HashDataInfo> element for the <ds:signedinfo> element. The result of application of the transforms specified in this <hashdatainfo> must</hashdatainfo></ds:signedinfo>									
		- One <hashi< th=""><th colspan="10">ne <hashdatainfo> element for the <ds:signedinfo> element. The result of application of the transforms specified in this <hashdatainfo> must</hashdatainfo></ds:signedinfo></hashdatainfo></th></hashi<>	ne <hashdatainfo> element for the <ds:signedinfo> element. The result of application of the transforms specified in this <hashdatainfo> must</hashdatainfo></ds:signedinfo></hashdatainfo>									
		De exactly tr	The same as the octet s	the science was	s originally used	i for computing the	e signature value	of the XIVILDSIG signa	ture.			
			Datainio> element for	the <signedsig< th=""><th>ynalureProperti</th><th></th><th></th><th></th><th></th></signedsig<>	ynalureProperti							
				the < signed Da	alaObjectProper	lies> element.						
		 In the first para	aranh it save to includ	o o ∠HoshDoto	Infos element f	or each <ds·refe< th=""><th>rences in the XM</th><th>DSig signature. This o</th><th>by jously includes the</th></ds·refe<>	rences in the XM	DSig signature. This o	by jously includes the			
		reference to the	SignedProperties	In the third an	d the fourth par	aranh it save to i	nclude a -HashD	ataInfos element for th				
		<pre>cSignedSignati</pre>	rePropertiess and th	<ul> <li>SignedData</li> </ul>	OhiectPropertie	s These element	nts are already in	cluded by the reference	to the			
			ties> Additionally the	se two element	s have no xsd·ll	D-attribute specifi	ed thus they can	not be referenced using	n ID-references			
	Original	Omit the <hash< th=""><th>DataInfo&gt; elements f</th><th>or the <signed< th=""><th>SignaturePrope</th><th>rties&gt; and the <si< th=""><th>ignedDataObject</th><th>Properties&gt; Additionally</th><th>/</th></si<></th></signed<></th></hash<>	DataInfo> elements f	or the <signed< th=""><th>SignaturePrope</th><th>rties&gt; and the <si< th=""><th>ignedDataObject</th><th>Properties&gt; Additionally</th><th>/</th></si<></th></signed<>	SignaturePrope	rties> and the <si< th=""><th>ignedDataObject</th><th>Properties&gt; Additionally</th><th>/</th></si<>	ignedDataObject	Properties> Additionally	/			
	resolution	<ul> <li>either add a</li> </ul>	n <hashdatainfo> ele</hashdatainfo>	ement for the <	SignedPropertie	ess and omit the	ds:Reference> to	the <signedproperites< th=""><th>,, S&gt;.</th></signedproperites<>	,, S>.			
	proposal	<ul> <li>or simply learning</li> </ul>	ave the <ds:reference< th=""><th>e&gt; to the signed</th><th>d properties incl</th><th>uded.</th><th></th><th></th><th>,</th></ds:reference<>	e> to the signed	d properties incl	uded.			,			
	<b>1 1</b>	Add xsd:ID-attri	butes to the <signed< th=""><th>SignaturePrope</th><th>rties&gt; and the &lt;</th><th>SignedDataObie</th><th>ctProperties&gt; ele</th><th>ments as well as to the</th><th></th></signed<>	SignaturePrope	rties> and the <	SignedDataObie	ctProperties> ele	ments as well as to the				
		<unsigendsign< th=""><th>atureProperties&gt; and</th><th>the <unsigned< th=""><th>DataObjectProp</th><th>perties&gt; elements</th><th></th><th></th><th></th></unsigned<></th></unsigendsign<>	atureProperties> and	the <unsigned< th=""><th>DataObjectProp</th><th>perties&gt; elements</th><th></th><th></th><th></th></unsigned<>	DataObjectProp	perties> elements						
	Resolution		•		ŕ I							
	comment											
	Resolution											
	text											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	<b>Resolution status</b>	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
TS101002.009	111			25/01/2004	tachnical			not yet proceed				
13101903-006	Commont	Within the ourro	AUES-PI-001	25/01/2004 ES apositionation	n the word "mu	ot" in upod to indi	l noto o roquiromon	t at acvaral places and	habauld therefore any			
	text	"MUST" accordi	ing to REC 2119 [22]	The REC 2110	A defines how th	e key words "MII	ST" "MUST NOT	" "REOLIRED" "SHAL				
	icht.	"SHOULD" "SH	IOUI D NOT" "RECC	MMENDED" "	MAY" and "OP	TIONAL " are to b	e interpreted in th	e sense of requirement	level Therefore the			
		specification sh	ecification should use these key words wherever a requirement is stated.									
		XAdES specific	AdES specification [1], clause 5, first paragraph:									
		The XML name	ne XML namespace URI that must be used by implementations of the present document [1, clause 5]									
		XAdES specification	AdES specification [1], clause 6.2, second paragraph:									
		The <signed< th=""><th colspan="9">he <signedproperties> must be covered by a Reference element of the XML signature. Alignment with the present document mandates that one</signedproperties></th></signed<>	he <signedproperties> must be covered by a Reference element of the XML signature. Alignment with the present document mandates that one</signedproperties>									
		<signedpropert< th=""><th colspan="9">redProperties&gt; element MUST exist. [1, secion 6.2]</th></signedpropert<>	redProperties> element MUST exist. [1, secion 6.2]									
		XAdES specific	S specification [1], clause 6.3, second paragraph: ever the following restrictions apply for using <ds:object> <oualifyingproperties> and <oualifyingpropertiesreference>:</oualifyingpropertiesreference></oualifyingproperties></ds:object>									
		However, the to	vever, the following restrictions apply for using <ds:object>, <qualifyingproperties> and <qualifyingpropertiesreference>:</qualifyingpropertiesreference></qualifyingproperties></ds:object>									
		- All signed pr	operties must occur v	within a single .	QualifyingProp	erties> element [	This element can (	either he a child of the	<ds:ohiect> element</ds:ohiect>			
		(direct incorr	poration), or it can be	referenced by	a <qualifyingpr< th=""><th>opertiesReference</th><th>e&gt; element. See o</th><th>clause 6.3.1 for informa</th><th>tion how to sign</th></qualifyingpr<>	opertiesReference	e> element. See o	clause 6.3.1 for informa	tion how to sign			
		properties.			a saaan jirigi i	0			lion to eight			
		XAdES specification	ation [1], clause 7.2.5	i, last paragrapl	h:							
		At least one ele	ment of <description:< th=""><th>&gt;, <objectident< p=""></objectident<></th><th>ifier&gt; and xmIM</th><th>imeType must be</th><th>present within the</th><th>e property. [1, clause 7.</th><th>.2.5]</th></description:<>	>, <objectident< p=""></objectident<>	ifier> and xmIM	imeType must be	present within the	e property. [1, clause 7.	.2.5]			
		XAdES specific	ation [1], clause 7.2.8	, paragraph 8:								
		At least one o	of the two elements <	ClaimedRoles>	or <certifiedro< th=""><th>ples&gt; must be pre</th><th>sent. [1, clause 7.</th><th>2.8]</th><th></th></certifiedro<>	ples> must be pre	sent. [1, clause 7.	2.8]				
			ation [1], clause 7.7.1	, paragraph 10	: the fellowing of	automoto of ullook	Datalata, alaman	4				
			cnive i imeStamp> eie	ement contains	the following se	quence or <hash< th=""><th>Datainio&gt; elemen</th><th>application of the trans</th><th>forms specified each</th></hash<>	Datainio> elemen	application of the trans	forms specified each			
		- One chashL	Infos must be exactly	the same as the	e octet stream	that was originally	used for comput	ing the digest value of t	the corresponding			
		<ds:referen< th=""><th></th><th></th><th></th><th>that was originally</th><th></th><th>ing the digest value of t</th><th>ine corresponding</th></ds:referen<>				that was originally		ing the digest value of t	ine corresponding			
	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 text	Clause 6.2 of the mandatory Tar	ne XAdES specification get-attribute MUST re	on [1] says: "The efer to the <id>-</id>	e mandatory Ta attribute of the o	rget attribute refe corresponding <ds< td=""><td>rs to the XML sig s:Signature&gt;."</td><td>nature." This should be</td><td>changed to: "The</td></ds<>	rs to the XML sig s:Signature>."	nature." This should be	changed to: "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				
TS101903-010	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed					
	Comment text	For some ASN 7.2.8 of the XA wherever an As	r 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 2.8 of the XAdES specification [1]). This should be changed to mandate the DER (Distinguished Encoding Rules [12]) encoding mechanism nerever an ASN.1 encoding is required.										
	Original resolution proposal												
	Resolution comment												
	Resolution text								-				
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
TS101903-011	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed					
	Comment text	The following p XAdES should specification	roposal was made by probably be able to in	y members of th nclude Trust Sta	e ETSI Technic atus Lists (TSL	al Committee ES [23]), beside certif	I (Electronic Sign fication and revoc	atures and Infrastructure ation information in futu	es): ire versions of 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				
TS101903-012	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed					
	Comment text	In XAdES specification [1] clause 7.2.2, last but one paragraph it says: If the signer uses an attribute certificate to associate a role with the electronic signature, such a certificate MUST be present in the <signerrole> property. [1, clause 7.2.2] This sentence should be moved to clause 7.2.8 'The <signerrole> element' of the XAdES specification</signerrole></signerrole>											
	Original resolution proposal												
	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				
<u>TS101903-013</u>	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	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
--------------	-----------------	--	---	-------------------	--	--------------------	---------------------	---	--------------------	--	--	--	--
	version	clause	contribution	date	type	source	date		version				
			reference										
TS101903-014	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed					
	Comment	The following p	roposal was made by	members of th	e ETSI Technic	al Committee ESI	(Electronic Signa	atures and Infrastructure	es):				
	text	It should be pos	sible in future version	ns of XAdES to	have archival v	ersions that build	on XMLDSig sigr	natures without the man	datory				
		<signedpropert< th=""><th>ties&gt;.</th><th></th><th></th><th></th><th></th><th></th><th></th></signedpropert<>	ties>.										
		With the curren	IVITN THE CUTTENT XAGES VERSIONS IT IS NOT POSSIBLE TO CREATE VALID XAGES A ARCHIVAL VERSIONS OUT OF A PLAIN XMLDSIG SIGNATURE, because the mandatenu a Signad Properties, cannot be added to the signature later. The XAdES encoding the second therefore provide forms that normit XAdES.										
		nandatory <signedproperties> cannot be added to the signature later. The XAdES specification should therefore provide forms that permit XAdES-A versions without the surrently mondatory <signingcortificates and="" delignidentificates="" forms="" permit="" provide="" signature="" th="" that="" xades-a<=""></signingcortificates></signedproperties>											
	Original	versions withou	t the currently manda	itory < Signing I	ime>, <signing< th=""><th>Jentificate&gt; and &lt;</th><th>SignaturePolicyld</th><th>entilier&gt; properties.</th><th></th></signing<>	Jentificate> and <	SignaturePolicyld	entilier> properties.					
	original												
	proposal												
	Resolution												
	comment												
	text												
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS101903-015	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed					
	Comment text	In the actual version of the XAdES specification [1] the <anytype> data type is defined as follows:</anytype>											
		<xsd:complext< th=""><th colspan="10"><xsd:complextype mixed="true" name="AnyType"></xsd:complextype></th></xsd:complext<>	<xsd:complextype mixed="true" name="AnyType"></xsd:complextype>										
		<xsd:sequence></xsd:sequence>											
		<xsd:any namespace="##any"></xsd:any> 											
		This definition d	loes not allow conten	t that has no sc	hema associate	d. Therefore the	definition of the <	AnyType> data type sh	ould read like the				
		following:						, , , , , , , , , , , , , , , , , , , ,					
		<xsd:complext< td=""><td>vpe name="AnvTvpe</td><td>" mixed="true"&gt;</td><td></td><td></td><td></td><td></td><td></td></xsd:complext<>	vpe name="AnvTvpe	" mixed="true">									
		<xsd:seque< td=""><td>nce&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td></xsd:seque<>	nce>										
		<xsd:any< td=""><td>y namespace="##any</td><td>" processConte</td><td>ents="lax"/&gt;</td><td></td><td></td><td></td><td></td></xsd:any<>	y namespace="##any	" processConte	ents="lax"/>								
		<th>ence&gt;</th> <th>-</th> <th></th> <th></th> <th></th> <th></th> <th></th>	ence>	-									
	Original												
	resolution												
	proposal												
	Resolution												
	comment												
	Resolution												
	text												

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	Version	clause	reference	uate	type	300100	uate		Version			
TS101903-016	111		XAdES-PT-001	25/01/2004	technical			not vet processed				
	Comment	In the current v	ersion of the XAdES	specification [1]	the <certid> e</certid>	lement does not h	have an URIattrib	ute for pointing to an ar	chived version of the			
	text	referenced cert	ificate:	op o o moanon [ · .								
		<xsd:complext< th=""><th>ype name="CertIDTy</th><th>pe"&gt;</th><th></th><th></th><th></th><th></th><th></th></xsd:complext<>	ype name="CertIDTy	pe">								
		<xsd:sequence< th=""><th>&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th></xsd:sequence<>	>									
		<xsd:element name="CertDigest" type="DigestAlgAndValueType"></xsd:element> <xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"></xsd:element>  										
		Therefore the d	efinition of the <certi< th=""><th>D&gt; element sh</th><th>ould read like th</th><th>e following to allo</th><th>w pointing to an a</th><th>archived version of the c</th><th>ertificate:</th></certi<>	D> element sh	ould read like th	e following to allo	w pointing to an a	archived version of the c	ertificate:			
		<xsd:complext< th=""><th>ype name="CertIDTy</th><th>pe"&gt;</th><th></th><th></th><th></th><th></th><th></th></xsd:complext<>	ype name="CertIDTy	pe">								
	<pre><xsd:sequence>   </xsd:sequence></pre> <pre></pre>											
												<xsd:ele< th=""><th colspan="10"><xsd:element name="IssuerSerial" type="ds:X509IssuerSerial I ype"></xsd:element></th></xsd:ele<>
	Original	<th colspan="10"></th>										
		resolution										
	nronosal											
	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					_				
TS101903-017	1.1.1	<b>T N</b> (1)	XAdES-PT-001	25/01/2004	technical			not yet processed				
	Comment	The Microsoft .	NET validating XML p	barser fails to particular	arse the current	version of the XA	dES schema, alt	hough the schema has I	been validated using			
	text	the schema val	of the XAdES provided	option	vide web Cons	ortium (W3C). In o	order to reach a la	arger community this iss	sue snould be fixed in			
	Original		or the AAdES specing	cation.								
	resolution											
	proposal											
	Resolution											
	comment											
	Resolution	1										
	text											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS101903-018	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed				
	Comment	In the actual ve	the actual version of the XAdES schema which is part of the XAdES specification the import statement for the XMLDSig schema is missing. Since									
	text	elements from t	ements from the XMLDSig schema are referenced by the XAdES schema an import statement has to be present. Therefore the XAdES schema									
		should read like	ould read like the following:									
			-									
		xml version=</th <th>"1.0" encoding="UTF</th> <th>-8"?&gt;</th> <th></th> <th></th> <th></th> <th></th> <th></th>	"1.0" encoding="UTF	-8"?>								
		<xsd:schema ta<="" th=""><th>irgetNamespace="htt</th><th>p://uri.etsi.org/0</th><th>)1903/v1.1.1#"</th><th></th><th></th><th></th><th></th></xsd:schema>	irgetNamespace="htt	p://uri.etsi.org/0	)1903/v1.1.1#"							
		xmlns:xsd="	http://www.w3.org/20	01/XMLSchem	a"							
		xmIns="http:	://uri.etsi.org/01903/v	1.1.1#"								
		xmlns:ds="h	ttp://www.w3.org/200	)0/09/xmldsig#"								
		elementForr	nDefault="qualified">	•								
			WL 44 11		o/							
		<xsd:import nar<="" th=""><th>nespace="http://www</th><th>/.w3.org/2000/0</th><th>9/xmldsig#"</th><th></th><th></th><th></th><th></th></xsd:import>	nespace="http://www	/.w3.org/2000/0	9/xmldsig#"							
	<b>a</b> : : :	schemaLoca	ation="http://www.w3	.org/1R/2002/R	EC-xmldsig-cor	e-20020212/xmld	sig-core-schema.	xsd"/>				
	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										
TS101903-019	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed					
	Comment	The <qualifying< td=""><td>PropertiesReference</td><td>Type&gt; data typ</td><td>e introduces a r</td><td>new <transforms:< td=""><td>&gt; element in the X</td><td>AdES namespace for t</td><td>he</td></transforms:<></td></qualifying<>	PropertiesReference	Type> data typ	e introduces a r	new <transforms:< td=""><td>&gt; element in the X</td><td>AdES namespace for t</td><td>he</td></transforms:<>	> element in the X	AdES namespace for t	he				
	text	<ds:transforms< td=""><td>Type&gt; rather than us</td><td>ing a reference</td><td>to the element</td><td>type defined in th</td><td>e XMLDSig scher</td><td>na.</td><td></td></ds:transforms<>	Type> rather than us	ing a reference	to the element	type defined in th	e XMLDSig scher	na.					
		The current XA	dES schema definition	n for the <qual< td=""><td>ifyingProperties</td><td>ReferenceType&gt;</td><td>data type is:</td><td></td><td></td></qual<>	ifyingProperties	ReferenceType>	data type is:						
		<xsd:complext< td=""><td>ype name="Qualifying</td><td>gPropertiesRefe</td><td>erenceType"&gt;</td><td></td><td></td><td></td><td></td></xsd:complext<>	ype name="Qualifying	gPropertiesRefe	erenceType">								
		<xsd:seque< td=""><td>nce&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td></xsd:seque<>	nce>										
		<xsd:ele< td=""><td>ment name="Transfo</td><td>orms" type="ds:</td><td>TransformsType</td><td>e" minOccurs="0"/</td><td>/&gt;</td><td></td><td></td></xsd:ele<>	ment name="Transfo	orms" type="ds:	TransformsType	e" minOccurs="0"/	/>						
	<t< td=""></t<>												
		<pre><xsd:attribute name="URI" type="xsd:anyURI" use="required"></xsd:attribute> </pre>											
		<td colspan="11">a/xsa:complex i ype&gt;</td>	a/xsa:complex i ype>										
		This should be	changed to:										
		<xsd:complextype name="QualifyingPropertiesReferenceType"></xsd:complextype>											
	<pre><xsd:sequence></xsd:sequence></pre>												
		<pre><xsd:element minoccurs="0" ref="ds:Transforms"></xsd:element></pre>											
		<xsd:attribute name="URI" type="xsd:anyURI" use="required"></xsd:attribute>											
		<rsd:attribute name="Id" type="rsd:ID" use="optional"></rsd:attribute>											
	Original												
	resolution												
	proposal												
	Resolution												
	comment												
	Resolution												
0	text	Dellasanahila	Original	0	0	Desclution	Deschutten	Desclution status	Dellassekle (energi				
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	uate	туре	source	date		version				
TS101003-020	111			25/01/2004	technical			not vet processed					
13101903-020	Comment	The XAdES eve	males in the (non-no	rmative) annex	D of the curren	t version of the X	AdES specificatio	n [1] are not aligned wit	h the specification				
	text	These example	s should be fixed or i	probably replac	ed by examples	s produced as tes	t cases for the XA	dES-PLUGTESTS TM	event				
	Original				ou by oxampion								
	resolution												
	proposal												
	Resolution	blution											
	comment												
	Resolution												
1	text												

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS101903-022	1.1.1		XAdES-PT-001	25/01/2004	technical			not yet processed				
	Comment	On the one side	the XAdES specification	tion [1] says in	clause 7.6.1, th	ird paragraph:						
	text	In principle, the	inciple, the <certificatevalues> element contains the full set of certificates that have been used to validate the electronic signature, including the</certificatevalues>									
		signer"s certifica	er"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> el</ds:keyinfo>	:KeyInto> element of the signature. [1, clause 7.6.1]									
		On the other sid	the other side the <ds:keyinto> element is not covered by the <archivetimestamp>(s). That is, certificates that are present in the <ds:keyinfo></ds:keyinfo></archivetimestamp></ds:keyinto>									
		and are not incl	are not included into the <certificatevalues> are not time-stamped for archiving purposes.</certificatevalues>									
	Original	There are two p	re are two possible solutions to this issue:									
	resolution	<ul> <li>Mandate the</li> </ul>	e inclusion of all certifi	icates in the ce	rtificate chain in	to the <certificate< th=""><th>Values&gt; element</th><th>•</th><th></th></certificate<>	Values> element	•				
	proposal	- Mandate to	Iandate to include the <ds:keyinfo> element into the <archivetimestamp>(s).</archivetimestamp></ds:keyinfo>									
		This issue need	issue needs further discussion.									
	Resolution											
	comment											
	Resolution											
	text		<u>.</u>			<b>.</b>						
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
TE101002 002	4 4 4			25/01/2004	tachnical			not yet proceed				
15101903-023	I.I.I	In the elever 7	AUES-PI-UUI	25/01/2004	lechnical			not yet processed				
	toxt	The Clause 7.4	4.1 OF THE AAUES SPE	cilication it say	5. Sorts alamanta (	already defined in	alauna 7.2.2 ina	prograting the digest of	anab cortificate and			
	lexi	optionally the is		or identifier [1		alleady defined in		Siporaling the digest of	each certificate and			
		However the X	AdES schoma mande	er luertiner. [1,	ciduse 7.4.1, id	or identifier to be	procent in the -C	orts alamant Tharafar	the word "optionally"			
		should be remo	ved from the quoted a	ales life issuel a			present in the <c< th=""><th></th><th>e the word optionally</th></c<>		e the word optionally			
	Original			Sentence above								
	resolution											
	nronosal											
	Resolution											
	comment											
	Resolution											
	text											

## 5.6 TS 102 023 - Time stamping policy

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version	
TS102023-001	1.1.1	Introduction	UNSTT-006		editorial			not vet processed		
	Comment text	Modify the text: quality of the pa "Another one co the signature wa present docume	"The quality of this evarametric data points to use a time-s as generated before t ent."	vidence is base that anchor the stamp which all he date contair	ed in the process m to the real wo ows to prove th ned in the time-s	s of creating and orld. In this instand at a datum existe stamp token. Polic	managing the dat ce this being the t d before a particu cy requirements to	a structure that represe ime data and how it wa lar time. This technique o cover that case is the	nt the events and the s applied." allows to prove that primary reason of the	
	Original resolution proposal	New text: " Th the parametric o " Another one	ne quality of this evide data points In this ir a consists to usePo	ence is based on Instance this is t Licy requiremer	n the process on he time data ar <u>ats to cover this</u>	of creating and mand how". case".	maging the data s	tructure that represents	s and on the quality of	
	Resolution comment									
	Resolution text									
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version	
TS102023-002	1.1.1	4.3 (2nd para)	UNSTT-006		editorial			not yet processed		
	Comment text	Modify the text: such an organiz	"In any case the orga ation is expected to s	anization will be suitably inform i	held responsib ts end users."	le if the obligatior	ns from the end-us	sers are not correctly fu	Ifilled and therefore the	
	Original resolution proposal	New text: "In a organization"	any case the organiza	ation will be res	ponsible if the c	bbligations from th	ne end-users are r	not correctly fulfilled and	d therefore such 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	
TS102023-003	1.1.1	4.4.3	UNSTT-006		editorial			not yet processed		
	Comment text	Modify the text: "A time-stamp policy may be defined by the user of times-stamp services, whereas the TSA practice statement is always defined by the provider."								
	Original resolution proposal	New text: "A tim	ne-stamp policy may b	be defined by th	ne user of time-s	stamp services	n			
	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										
TS102023-004	1.1.1	7	UNSTT-006		editorial			not yet processed					
	Comment	Modify the text:	"The requirements ar	e indicated in t	erms of the sec	urity objectives for	llowed by more s	pecific requirements for	controls to meet those				
	text	objectives wher	e considered necessa	ary to provide th	he necessary co	onfidence that tho	se objective will b	e met."					
	Original	New text: "The	requirements where	e considered ne	ecessary to pro	vide the necessar	ry confidence that	those objectives"					
	resolution												
	proposal												
	Resolution												
	comment												
	Resolution												
	text						1		r				
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
<b>TO</b> 400000 005			reterence										
15102023-005	1.1.1	1	UNST1-006		Itechnical	TOA :		not yet processed					
	Comment	Modify the text:	"The current docume	nt addresses re	equirements for	ISAs issuing tim	e-stamp tokens w	hich are synchronized	with Coordinated				
	text	universai time (	JIC) and digitally sig	ned by the ISA	λ" 	A = := = ::= = 4:== = = 4	tologue disite						
	Original	New text: In	e current document a	aaresses requi	rements for 15/	As issuing time st	amp tokens digita	lly signed by the TSA It	self that is synchronized				
	resolution	with Coordinate											
	Proposal												
	comment												
	Resolution												
	toyt												
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
	vereien		reference	uuto	.,po	course	ullo						
TS102023-006	1.1.1	2	UNSTT-006		technical			not vet processed					
	Comment	Update the refe	rence "FIPS PUB 140	)-1 (1994): "Seo	curity Requirem	ents For Cryptog	raphic Modules".		L				
	text			(									
	Original	New reference:	FIPS PUB 140-2 (200	01): "Security F	Requirements F	or Cryptographic	Modules".						
	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			
TS102023-007	1.1.1	6.1.1	UNSTT-006		technical			not yet processed				
	Comment text	Modify the text: reference."	"The TSA shall also	ensure adherer	nce to any addit	ional obligations i	ndicated in the tir	ne-stamp either directly	or incorporated by			
	Original resolution proposal	New text: "Th	e TSA shall also ensi	ure adherence	to any additiona	I obligations indic	ated in the time-s	stamp token"				
	Resolution comment											
	Resolution text											
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
TS102023-008	1.1.1	6.2	UNSTT-006		technical			not yet processed				
	Comment text	Modify the text: "NOTE: It is advisable that, when obtaining a time-stamp token, the subscriber verifies that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp token has not been compromised."										
	Original resolution proposal	"NOTE: It is advisable that, when obtaining a time-stamp token, the subscriber verifies that the time-stamp token's digital signature is a valid one, particularly that the private key used to sign the time-stamp token has not been compromised."										
	Resolution comment											
	Resolution text											
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
TS102023-009	1.1.1	6.3	UNSTT-006		technical			not yet processed				
10102020-000	Comment text	Modify the text:       "a) verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification;         NOTE:       During the TSA's certificate validity period, the validity of the signing key can be checked using current revocation status for the TSA's certificate. If the time of verification exceeds the end of the validity period of the corresponding certificate, see annex D for guidance.         b)       take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy."										
	Original resolution proposal	New text: "a) verify that th compromise b) Take into ac	e time-stamp token's ed; count any limitations	digital signatu	re is a valid one of the time-stam	, particularly that	the private key us	sed to sign the time-star p policy;"	np token has not been			
	Resolution comment			<u></u>			•					
	Resolution text											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS102023-010	1.1.1	7.1.2	UNSTT-006		technical			not yet processed				
	Comment	Modify the text:										
	text	"d) The expecte	d life-time of the sign	ature used to s	ign the time-sta	mp token (depend	ds on the hashing	g algorithm being used, t	he signature algorithm			
		being used a	and the private key le	ngth).								
		j) The period c	of time during which I	SA event logs	(see clause 7.4	.10) are retained.						
	Original	New text:	d life the end the stars									
	resolution	a) The expecte	d life-time of the sign	ature associate	ed to the time-st	amp token						
	Proposal	) The period of time during which TSA event logs (see clause 7.4.11)										
	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									
TS102023-011	1.1.1	7.2.1	.2.1 UNSTT-006 technical not yet processed									
	Comment	Modify the text: "The TSA shall ensure that any cryptographic keys are generated in under controlled circumstances.										
	text	b) The generat	) The generation of the TSA's signing key(s) shall be carried out within a cryptographic module(s) which either:									
		<ul> <li>meets th</li> </ul>	e requirements identi	fied in FIPS PL	JB 140-1 [4] lev	el 3 or higher; or"						
	Original	New text: "The	New text: "The TSA shall ensure that any cryptographic keys are generated under controlled circumstances "									
	resolution	D) 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 EIPS PLIB 140-1[4] or EIPS PLIB 140-2 [7] level 3 or higher; or "										
	proposal Decolution	- meets the requirements identified in FIPS PUB 140-1[4] of FIPS PUB 140-2 [7] level 3 of higher, or										
	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									
TS102023-012	1.1.1	7.2.2	UNSTT-006		technical			not yet processed				
	Comment	Modify the text:										
	text	"a) The TSA pri	vate signing key shal	l be held and us	sed within a cry	ptographic modul	e which:					
		- meets th	e requirements identi	fied in FIPS PL	JB 140-1 [4] lev	el 3 or higher; or"						
	Original	New text:										
	resolution	"a) The TSA pri	vate signing key shall	be held and us	sed within a cry	ptographic module	e which:					
	proposal Decolution	- meets th	e requirements identi	tied in FIPS PL	JB 140-1 [4] OF	-IPS PUB 140-2 [	7] level 3 or high	er; or				
	Resolution											
	Resolution											
	text											

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
TS102022-012	111	7.2.4			tachnical			not yet proceed				
13102023-013	Comment	Modify the text:	010311-000		lechnical			not yet processed	<u> </u>			
	text	"NOTE 1: The t - C y th	following additional co clause 7.4.10 requires ear after the expiration ne size of the records	onsiderations a that records cond n of the validity to be kept will	pply when limitin oncerning time- of the TSA's sibe."	ng that lifetime: stamping services gning key. The lor	shall be held for nger the validity p	a period of time as app eriod of the TSA certific	ropriate for at least 1 ate will be, the longer			
	Original resolution proposal	New text: "NOTE 1: The f - C v d	<ul> <li>w text:</li> <li>OTE 1: The following additional considerations apply when limiting that lifetime: <ul> <li>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.</li> </ul> </li> </ul>									
	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			
TS102023-014	1.1.1	7.2.5	7.2.5 UNSTT-006 technical not yet processed									
	Comment text	nent Modify the text: t "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 depending system SHALL reject any attempt to issue TSTs if the signing private key has expired "										
	Original resolution proposal	New text: "a) Operational reasons (e.c c) The TST ge has been su	or technical procedur g. according to what e neration system SHA ibstituted)."	es shall be in p stablished by r LL reject any a	place to ensure national law). ttempt to issue	that a new key is p	put in place when g private key is no	a TSA's key expires or ot valid anymore (e.g. b	is substituted for other ecause it has expired 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			
TS102023-015	1.1.1	7.2.6	UNSTT-006		technical			not yet processed				
	Comment text	Int Modify the title: "Life cycle management of cryptographic module used to sign time-stamps".										
	Original resolution proposal	New title: "Life of	cycle management of	cryptographic	module used to	sign time-stamp t	okens".					
	Resolution comment											
	Resolution	1										
	text											

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
	Verbien	oladoo	reference	uuto	()pc	oouroo	uuto		Verbion			
TS102023-016	1.1.1	7.3.1	UNSTT-006		technical			not yet processed				
	Comment text	Modify the text: "NOTE 2: A pro h) The name o - an identi	tocol for a time-stam f the issuing TSA sha fier for the unit which	p token is defin Il be identified issues the time	ed in RFC 316 <sup>2</sup> in the time-stam e-stamps."	I and profiled in T op token. This sha	S 101 861. Ill include:					
	Original resolution proposal	New text: "NOTE 2: A pro h) The name o - an identi	otocol for requests/res f the issuing TSA fier for the time-stam	sponses of time	e-stamp tokens	s defined in RFC -stamp tokens."	3161 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			
TS102023-017	1.1.1	7.3.2	UNSTT-006		technical			not yet processed				
	Comment text	Modify the text: "NOTE 2: Relyi	Modify the text: "NOTE 2: Relying parties are required to be informed of such events (see clause 7.4.8)."									
	Original resolution proposal	New text: "NOTE 2: Subscribers and relying parties"										
	Resolution comment											
	Resolution text											
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version			
TS102023-018	1.1.1	7.4.5	UNSTT-006		technical			not yet processed				
	Comment text	Modify the text: "c) Media used obsolescence	within the TSA trustw	orthy systems	shall be secure	ly handled to prot	ect media from d	amage, theft, unauthoriz	ed access and			
	Original resolution proposal	New text: "c) Media used life cycle ma	within the TSA trustw anagement shall be su	orthy systems	shall be secure ely prevent obso	ly handled to prot plescence."	ect media from d	amage, theft and unauth	norized access. Media			
	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									
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	tivities, for exam	ple by retaining e	event logs (see cla	ause 7.4.10)."				
	Original	New text:										
	resolution	"e) TSA person	nel shall be accounta	ble for their act	tivities, 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			
T0400000.000	4 4 4	740			teshaisal							
15102023-020	Commont	7.4.0 Madify the texts	010511-000		lechnical			not yet processed				
	toxt	"c) In the case (	of compromise to the	TSA's operatio	n (o a TSA kou		ispacted comprar	nico or loco of colibratio	n the TSA shall not			
	lexi		tomp tokong until stor	n SA S Operatio	rocover from th	o compromiso "	ispected compror		IT THE TSA SHAILING			
	Original	New text:	lew text:									
	resolution	"c) In the case (	of compromise to the	TSA's operatio	on (e.a. TSA priv	vate signing key o	ompromise) "					
	proposal					ato olgrini gitto y o	ompronnoo)					
	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									
TS102023-021	1.1.1	7.4.9	UNSTT-006		technical			not yet processed				
	Comment	Modify the text:										
	text	"a) Before the T	SA terminates its tim	e-stamping ser	vices the follow	ing procedures sh	nall be executed a	as a minimum:				
		- the TSA	shall transfer obligation	ons to a reliable	e party for main	taining event log	and audit archive	s (see clause 7.4.10) ne	cessary to demonstrate			
		the correct operation of the TSA for a reasonable period;"										
	Original	New text:										
	resolution	"a) Before the T	SA terminates its tim	e-stamping ser	vices the follow	ing procedures sh	nall be executed a	as a minimum:				
	proposal	- The TSA	shall transfer obligat	ions to a reliab	le party for main	ntaining event log	and audit archive	es (see clause 7.4.11) n	ecessary to			
	-	demonst	rate the correct opera	ation of the TSA	A for a reasonat	ole period;"						
	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						
TS102023-022	1.1.1	7.4.11	UNSTT-006		technical			not yet processed	
	Comment	Modify the text:							
	text	"f) Records cor	ncerning time-stampir	ng services sha	Il be held for a	period of time after	er the expiration of	f the validity of the TSA	s signing key as
		appropriate	for providing necessa	ary legal eviden	ce and as notif	ied in the TSA dis	sclosure statement	: (see clause 7.1.2)."	
	Original	New text:							
	resolution	"f) "Records co	ncerning time-stampi	ng services	after the expira	tion of the validity	of the TSA's signation	ature verification (public	) key as appropriate"
	proposal								
	Resolution								
	comment								
	Resolution								
	text		1	1	T	1			1
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
			reference			0770.40			
1\$102023-023	1.2.1	4.2	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment	It should be clea	arly defined the TSA's	s key.					
	text	Because reade	rs cannot distinguish	if it is TSA's ke	y or TSU's key.				
	Original								
	resolution								
	proposal	TOLL	<b>TOA O 1</b>	i la c <del>T</del> OL					TOUL
	Resolution	I SUS belong to	a ISA. So it could be	e said that TSU	keys also belo	ng to the TSA. H	owever, since the	key resides in a specific	SISU use of the more
	comment	specific term 18	SU key is considered	more appropria	ate. (However, I	t is not that the he	eading of clause /	.2.1 should be changed	to "ISU key".
	Resolution								
Commont ID	Deliverable	Dolivorabla	Original	Commont	Commont	Baselution	Pasalution	Pacalution status	Deliverable target
Comment ID	Vorsion	clauso	contribution	data	type	Resolution	data	Resolution status	
	Version	clause	reference	uale	type	Source	uale		Version
TS102023-024	121	12		17/02/2003	technical	STE242	21/06/2003	no change	
10102023-024	Comment	We propose to	describe a restriction	on key backun	teennicai	011 242	21/00/2003	no change	
	text	F a "TSA's key	should not be cloned	011 Key backup  "	•				
	Original	L.g. TOASKey	Should not be cloned						
	resolution								
	proposal								
	Resolution	It is not exactly	clear what "cloned" m	eans Require	ments for secu	rity of any backur	kevs are covered	by 7 2 2 b & c	
	comment	it to not oxabily	olour what olohou h			inty of any baonap		by 1.2.2 b a b.	
	Resolution								
	text								

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
TS102023-025	1 2 1	7 1 2 d)		17/02/2003	technical	STE242	21/06/2003	no change					
13102023-023	Comment	Readers easily	understand "The evni	iration date of t	he time-stamp	token TSA assur		In change					
	text	Reducts casily			ine time-stamp		eu,						
	Original												
	resolution												
	proposal												
	Resolution	Time-stamps va	alidity do not expire af	ter this period.	It is only nece	ssary to provide a	additional protection	on to maintain the integr	ty of the token (e.g.				
	comment	using additiona	l signatures).										
	Resolution												
Commont ID	Deliverable	Dolivorablo	Original	Commont	Commont	Posolution	Posolution	Posolution status	Deliverable target				
Comment ID	version	clause	contribution	date	type	Source	date	Resolution status	version				
	Version	Clause	reference	uute	type	300100	uute		Version				
TS102023-026	1.2.1	7.1.2 j)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process					
	Comment	"See clause 7.4	1.10" is wrong. "See c	lause 7.4.11' is	right"								
	text												
	Original	"See clause 7.4	1.10" is wrong. "See c	lause 7.4.11' is	s right"								
	resolution												
	proposal												
	Resolution	Correction note	ed.										
	Resolution												
	text												
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS102023-027	1.2.1	7.2.1 b)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process					
	Comment	FIPS PUB 140-	2 is also required.										
	text Original												
	resolution	FIPS PUB 140-	z is also required.										
	nronosal												
	Resolution	Lise of FIPS PI	IR 140-2 to be consid	ered for next r	vision								
	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				
TS102023-028	1.2.1	7.2.2 a)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process					
	Comment text	FIPS PUB 140-	2 is also required.										
	Original resolution	FIPS PUB 140-	2 is also required.										
	Resolution	Use of FIPS PL	JB 140-2 to be consid	lered for next re	evision.								
	Resolution												
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
TS102023-029	1.2.1	7.2.2 b)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process					
	Comment text	Following note NOTE: Whe TSTs	ollowing note is needed. IOTE: When the backup key is recovered, the TSA needs to assure that it does not use previously used serial numbers in the TSTs for new TSTs.										
	Original resolution proposal	Following note NOTE: Whe TSTs	ollowing note is needed. IOTE: When the backup key is recovered, the TSA needs to assure that it does not use previously used serial numbers in the TSTs for new TSTs.										
	Resolution comment	To be considered for next revision. It is recommended that new keys are generated instead.											
	Resolution text												
Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version				
TS102023-030	1.2.1	7.2.4	JCPKI-005	17/02/2003	editorial	STF242	21/06/2003	in process					
	Comment text	NOTE 1: "See	clause 7.4.10" is wro	ong. "See claus	e 7.4.11" is rigl	nt.							
	Original resolution proposal	NOTE 1: "See	e clause 7.4.10" is wr	ong. "See claus	se 7.4.11" is rig	ht.							
	Resolution comment	Correction note	d.										
	Resolution text												

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS102023-031	1.2.1	7.3.1 e)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change					
	Comment	Following meas	sure is needed.										
	text	If the TSA's clo	ck has been out of the	e stated accura	cy and TSTs w	ere issued before	e it was detected, t	he TSA shall revoke the	e TSTs.				
	Original	Following meas	wing measure is needed.										
	resolution	If the TSA's clo	ck has been out of the	e stated accura	cy and TSTs w	ere issued before	e it was detected, t	he TSA shall revoke the	e TSTs.				
	proposal												
	Resolution	Revocation of ti	me-stamp tokens is n	ot practical. It i	s preferable to	ensure that the T	SA stops issuing t	okens well before there	is a risk that the clock				
	comment	drifts outside ac	cepted accuracy.										
	Resolution												
	text		•			-	-						
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution reference	date	type	source	date		version				
TS102023-032	1.2.1	7.3.2 a)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	in process					
	Comment	The TSA also n	eeds to show to user	s how it can pro	ove its clock's c	orrectness.	•						
	text	For instance, T	he TSA shall keep an	d show tractabi	lity and authen	ticity to UTC as it	s time source to u	sers.					
		An investigation	n of guideline is requir	ed.									
	Original												
	resolution												
	proposal												
	Resolution	Noted to be cor	nsidered for next revis	ion. Synchroniz	zation logs may	/ meet this need.							
	comment												
	Resolution												
	text			-	-			T - · ·					
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
T0400000 000	101	7.0.0!\	reference	47/00/0000	ta abuda al	075040	04/00/0000						
15102023-033	1.2.1	7.3.2 d)	JUPKI-005	17/02/2003	Itechnical	STF242	21/06/2003	in process					
	Comment	vve believe that	tion of suidaling is not	issue time-stan	nps when it is p	processing for a le	eap second".						
	text Original	Some investiga	tion of guideline is rec	quirea.									
	Original												
	resolution												
	Proposal	leave neted He	wavar the importance		of time atoma	na nanjinan nand	a ta ha takan inta	aaaunt					
	Resolution	issue noted. Ho	wever, the importanc	e of availability	or time-stamp	ng services need	s to be taken into	account.					
	Bosolution												
	toxt												
1	lext	1											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
			reference						
TS102023-034	1.2.1	7.4.8	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	
	Comment	It should be pro	vided a way of how to	deal with issue	ed TSTs in the	following cases.			
	text	1. Compromise	of the TSA"s signing	key					
		2. Detected loss	s of calibration						
	Original								
	resolution								
	proposal								
	Resolution	Steps required	already specified in cl	ause 7.4.8.					
	comment								
	Resolution								
-	text		I		-				
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
<b>TO</b> ( 0000 005		7.4.0.)	reterence	47/00/0000			0.4./0.0./0.0.00		
TS102023-035	1.2.1	7.4.8 c)	JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change	l
	Comment	There will be po	ssibility that TST is is	sued after com	promise occur	red and it cannot l	be detected for a	while.	
	text	So we believe t	hat when such cases	happened the	ISA need to sh	now information of	it to relying partie	es and subscribers (e.g.	by time-stamps
		revocation list).							
	Ordering	Some investiga	tion of guideline is rec	quirea.					
	Original								
	resolution								
	proposal								
	Resolution	Since the impac	ct of such a comprom	se is difficult to	predict it is no	t clear whether au	itomatic recovery	is practical. It is prefera	Die to measures in
	Comment	place to avoid s	such a disaster.						
	Resolution								
	text	1							

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS102023-036	1.2.1		JCPKI-005	17/02/2003	technical	STF242	21/06/2003	no change				
	Comment	Referring to TS	102 023, as example	s of a specific -	FSA policy, two	operation regulat	ions were created	in FY2002 report, "Tim	e-stamping usage			
	text	guideline".										
		1. Example of	time-stamping service	e operation reg	ulation using sir	nple protocol.						
		2. Example of	Imple of time-stamping service operation regulation using linking protocol.									
		Also in "Time-st	Interstamping usage guideline, the important matters on use of time-stamping were summarized. Here we discussed about "Time stamp token issued by TSA should have the correct time but the above ETSLTS. A time stamp token issued by TSA should have the correct time but the second statement of									
		Authentication"	ntication" which is not specifically described in the above ETSLIS. A time-stamp token issued by TSA should have the correct time but the									
		token does not	oes not nave a mechanism to prove that the token itself uses a reliable time source to guarantee the time accuracy. The time included in									
		the accuracy	tamp token that TSA insist the accuracy should link to the national standard time based UTC and there should be a mechanism to guarantee									
	Original	the accuracy.										
	resolution											
	proposal											
	Resolution	The requirement	ts for synchronization	with UTC are	specified in clau	use 7.3.2. It is left	open to the imple	mentation to decide wh	ich mechanism is to be			
	comment	used.	······									
	Resolution											
	text											
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target			
	version	clause	contribution	date	type	source	date		version			
			reference									
TS102023-037	1.2.1		MAINT-001		technical			not yet processed				
	Comment	The TS 101 733	3 should be consister	nt with RFC 316	61 and use the '	"time-stamp toker	" within a descript	ion and "TimeStampTo	ken" for formal			
	text	definitions (i.e. /	ASN.1 and XML). The	e TSA policy sh	ould also be co	nsistent.						
	Original											
	resolution											
	proposal											
	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										
TS102023-038	1.2.1		TC-ESI_2-002	13/06/2003	technical			not yet processed					
	Comment	To the maintena	ance team of TS 102	023.									
	text	In clause 7.2.3.	use 7.2.3. we currently only have:										
		7.3.2 Clock Sy	ynchronization with U	ТС									
		b) The TSA clo	he TSA clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibratic										
		Let us consider	two scenarios:										
		Scenario A.	enario A.										
		The clock refere	ence is outside the HS	SM. It is for exa	mple a PCI care	d placed in a PC v	with a crystal cloc	k compensated in temp	erature and				
		synchronized m	nanually every week w	vith UTC by an	operator. The o	perator is able to	set any time whe	n performing the synchr	onization. Someone				
		having an acces	ss to the room and kn	owing some ID	and password	could set any time	e.						
		This scenario re	elies on the security of	t the environme	ent and on the r	espect of procedu	ires.						
		Scenario B.											
		The clock refere	ence is within a HSM	(Tamper Resist	tant - Hardware	Security Module)	, this means that	both the clock and the	TSU signing key are				
		within the same	HSM. The clock is ba	ased upon a cry	ystal clock com	pensated in tempe	erature and synch	ronized every week wit	h UTC. Every week a				
		compensation c	of only XX microsecor	nds (e.g. 100 m	icroseconds) is	allowed. If more i	s being done, the	private key will be zero	ized and a new full				
		installation mus	t be done. Someone	having an acce	ss to the room a	and knowing *eve	rything* cannot de	o more that a clock drift	of XX microseconds.				
		This scenario of	nly relies on the secul	rity features of t	the HSM.								
		Conclusion											
		I see the need f	or two different qualit	ies for the prote	ection whether:								
		1) the security	is achieved both by re	oom access co	ntrol and by pro	cedures to be res	pected by human	-beings, or					
		2) the security	is achieved by securi	ty features built	t-in inside the H	SM.							
		This should lea	d to define two differe	nt TSA policies	unless we r	nandate the later	only.						
	Original				,		o						
	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									
TS102023-039	1.2.1	7.2.2 - b)	TC-ESI_1-005	22/10/2003	technical			not yet processed				
	Comment	Nothing is said	about how long shou	d the exported	key protection	ast.						
	text		-									
	Original	Two possible a	ssible amendments can apply:									
	resolution	1) Reword the	eword the paragraph with the same new text proposed for TS 101 456:									
	proposal	- When ou state of t	utside the signature-c the art, are capable to owing sentence at the	reation device withstand cryp end of the par	(see a) above) t otanalytic attack agraph: "The pr	he CA private sig s for the residual otection must be	ning key shall be life of the encrypt capable to withsta	protected using system ed key or key part. and cryptanalytic attacks	s that, according to the			
		the encrypte	ed key or key part."		«9·«p··· ···o p·							
	Resolution		<i>. . .</i>									
	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	To describe abo <xsd:element n<br="">type="OCSPTr This addition sh</xsd:element>	out OCSP trust condit ame="OCSPTrustCor rustConditionType" mi nould apply on signatu	ion, both in Co ndition" inOccurs="0"/> ire policy claus	mmonRules an e of TS 101 73:	d CommitmentRul 3 in same syntax.	es element schen	na, add following eleme	ent
	Original resolution proposal	To describe abo <xsd:element n<br="">type="OCSPTr This addition sh</xsd:element>	out OCSP trust condit ame="OCSPTrustCor rustConditionType" mi nould apply on signatu	ion, both in Con ndition" inOccurs="0"/> ire policy claus	mmonRules an e of TS 101 73:	d CommitmentRul 3 in same syntax.	es element schen	na, add following eleme	ent
	Resolution comment	This comment i Policy".	s to be fed into separa	ate activities wi	thin ETSI on si	gnature policies - s	see also response	e to "comments regardir	ng EESSI Signature
	Resolution text								

## 5.8 TR 102 041 - Signature policies report

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target		
	version	clause	reference	date	туре	source	uate		version		
TR102041-001	1.2.1	8.3.1	JCPKI-007	17/02/2003	technical	STF242	21/06/2003	no change			
	Comment	In this clause, the	ne Reports describe to	wo types of cor	nmitments, whi	ch are Common F	Rules and Commit	ment Rules.			
	text	However, mean	ing difference betwee	en these rules a	are little bit unde	erstandable. It is h	nelpful for us if you	explain some example	of these Rules,		
		especially comr	nitment rules.								
		Also in this clau	se, description "trust	conditions for u	iser certificate,	timestamps and a	attributes" should b	e added OCSP respon	der's trust conditions.		
		This addition sh	ould apply on signatu	ire policy claus	e of IS 101 73	3 in same syntax.					
	Original	In this clause, th	clause, the Reports describe two types of commitments, which are Common Rules and Commitment Rules.								
	resolution	However, mean	ning difference betwee	en these rules a	are little bit unde	erstandable. It is r	neiptul for us if you	explain some example	of these Rules,		
	proposal	Also in this clau	ly commitment rules.								
		This addition sh	this clause, description trust conditions for user certificate, timestamps and attributes should be added OCSP responder's trust conditions.								
	Resolution	This comment is	s to be fed into separa	ate activities wi	thin ETSI on sid	onature policies -	see also response	to "comments regardir	ng EESSI Signature		
	comment	Policy".				griatare perioree		te commente regaran			
	Resolution										
	text										
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target		
	version	clause	contribution	date	type	source	date		version		
TD 4000 44 000	101		reference	47/00/0000			04/00/0000				
TR102041-002	1.2.1	8.3.2	JCPKI-007	17/02/2003	technical	STF242	21/06/2003	no change	I		
	Comment	Revocation Red	uirements		•						
	Original	Please add CRI	L DISTIDUTION POINTS N		_5.						
	resolution	Please add CR	Distribution points n	ot only full CRI	s						
	proposal										
	Resolution	This comment is	is comment is to be fed into separate activities within ETSI on signature policies - see also response to "comments regarding EESSI Signature								
	comment	Policy".	licy".								
	Resolution	•									
	text										

## 5.9 TS 102 042 - PKC certificate policy

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS102042-001	1.2.1	2	UNSTT-002		editorial			not yet processed					
	Comment	Update the refe	erence "FIPS PUB 140	)-1 (1994): "Seo	curity Requirem	ents For Cryptog	raphic Modules".						
	Original	New reference:	FIPS PUB 140-2 (20	01): "Security R	equirements F	or Cryptographic	Modules"						
	resolution		111 01 00 110 2 (20	or). Coounty r	loquironionio i								
	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										
IS102042-002	1.1.1	4.1 (1st para)	UNS11-002		editorial			not yet processed					
	Comment	Modify the text:	" The certification aut	hority has over	all responsibility	for the provision	of the certificatio	n services identified in c	lause 4.1. The				
	Original	Certification aut	enuncation autionity's key is used to sign the qualified certificates and it is identified in the certification services identified in clause 4.2. The certification										
	Original	New text. The	authority is identified in the certificate as the issuer and its private key is used to sign gualified certificates."										
	proposal	authonity is iden	anonty is identified in the certificate as the issuel and its private key is used to sign qualified certificates.										
	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										
TS102042-003	1.1.1	4.1 (2nd para)	UNSTT-002		editorial			not yet processed					
	Comment	Modify the text:	"However, the key us	sed to generate	the certificates	"							
	text												
	Original	New text: "How	ever, the private key	used to sign the	e certificates,	I							
	resolution												
	proposal												
	Resolution												
	Bosolution												
	tovt												
	text												

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target					
	version	clause	contribution	date	type	source	date		version					
			reference											
TS102042-004	1.1.1	4.2	UNSTT-002		technical			not yet processed						
	Comment	Modify the text:	"Dissemination servio	ce: disseminate	s certificates to	subjects, and if th	ne subject consen	ts, to relying parties. Th	nis service also					
	text	disseminates th	e CA's terms and cor	ditions, and an	y published pol	icy and practice in	formation, to sub	scribers and relying par	rties."					
	Original	New text: "Diss	emination service: dis	seminates cert	ificates to subje	cts, and if subject	consents, makes	them available to relyi	ng parties. This service					
	resolution	also makes ava	s available the CA's terms and conditionsto subscribers ad relying parties."											
	proposal													
	Resolution													
	comment													
	Resolution													
-	text			-	1 -									
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target					
	version	clause	contribution	date	type	source	date		version					
<b>TO</b> 4000 40 005			reference											
IS102042-005	1.1.1	6.2	UNST1-002		technical			not yet processed						
	Comment	Modify the text:	"The CA shall oblige,	through agree	ment (see claus	ses 7.3.1a and 7.3	3.4), the subscribe	er to ensure that the sub	pject fulfils the following					
	text	obligations:				and an an excite the s			ith an annual th					
		a) accurate an	d complete informatio	n is submitted i	to the CA in acc	ordance with the	requirements of tr	his policy, particularly w	ith regards to					
		registration;	is only used in easer	lance with only	limitationa natifi	iad to the aubeerik	or (and clause 7	2 4).						
		b) the key pair	is only used in accord	vance with any	infinitations notifi	ied to the subschit		3.4),						
			NALL if the subscriber	or subject den	eu use or the subie	ubjeci s private ke	у,							
		- subject k	(evs are denerated us	ing an algorithm	m recognized by	v industry as hein	a fit for the uses o	f the certified key as id	entified in the certificate					
		nolicy:	teys are generated at	ing an aigonai	in recognized by									
		- a key ler	noth and algorithm is i	used which is re	ecognized as be	eina fit for the use	s of the certified k	ev as identified in the c	ertificate policy:					
		e) [CONDITIO	NAL1 if the subscriber	or subject aen	erates the subie	ect's kevs and the	private kev is for	creating electronic sign	atures only the subject					
		holds the pr	ivate key once deliver	ed to the subje	ct;	,	,	3 3	, , , ,					
		f) [NCP+] only	use the subject's priv	ate key for sigr	ning or decrypti	ng with the secure	e user device;							
		g) [NCP+] [CO	NDITIONAL] if the su	bject's keys are	e generated und	ler control of the s	ubscriber, genera	te the subject's keys w	ithin the secure user					
		device used	Jevice used for signing or decrypting;											
		h) notify the C/	A without any reasona	able delay, if an	y of the followin	g occur up to the	end of the validity	period indicated in the	certificate:					
		<ul> <li>the subject</li> </ul>	ect's private key has b	een lost, stoler	n, potentially co	mpromised; or								
		- control o	over the subject's priva	ate key has bee	en lost due to co	mpromise of activ	/ation data (e.g. P	IN code) or other reaso	ons; and/or					
		- inaccura	cy or changes to the	certificate conte	ent, as notified t	o the subscriber;								
		i) following co	following compromise, the use of the subject's private key is immediately and permanently discontinued."											

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	reference	date	туре	source	date		version				
	Original	New text: "The	CA shall oblige, throu	ah aareement (	see clause 7.3.	1 h)), the subscrib	Der:						
	resolution	1) to make the	subject aware (in the	case the subso	criber and the s	ubject are not the	same person) of	the CA's terms and con	ditions as provided for				
	proposal	in clause 7.3	3.1.a);										
		2) to ensure th	at the subject fulfils th	e following obli	gations:			1 14 4					
		a) accurate	and complete information	ation is submitt	ed to the CA, di	rectly or through t	ne subscriber, in	accordance with the re-	quirements of this				
		b) the key r	articularly with regards	s to registration	ı, anv other limitat	ions notified to the	subscriber (see	clause 7 3 4).					
		c) reasonal	reasonable care is exercised to avoid unauthorized use of the subject's private key;										
		d) idem;	idem;										
		e) idem;	idem;										
		f) idem;											
		b) notify the	e CA without any reas	onable delay ic	lirectly or throug	the subscriber	if any ·						
		i) idem."		onabio aolay, e			n any,						
	Resolution												
	comment												
	Resolution												
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
TS102042-006	1.1.1	7.2.1	UNSTT-002		technical			not yet processed					
	Comment	Modify the text:	"b) [CHOICE]	wind as st									
	text	[LCP] CA Key g	eneration shall be car	in FIPS PLIB 1	40-1 [2] or 140	2 [6] level 2 o hig	hor						
		[NCP] CA key c	eneration shall be car	rried out within	a device which	either:							
		- meets the re	equirements identified	in FIPS PUB 1	40-1 [2] or 140-	2 [6] level 3 o hig	her;"						
	Original	New text: "b) [0	CHOICE]:										
	resolution	[LCP] CA key g	eneration shall be car	ried out in a pro	oduct, application	on or device which	ensures that the	keys are generated in	a trustworthy manner				
	proposar	- meets the re	equirements identified	in FIPS PUB 1	40-1 [2] level 2	or higher: or							
		<ul> <li>is a trustwor</li> </ul>	rthy system which is a	ssured to EAL	3 or higher in a	ccordance to ISO/	/IEC 15408 [3], or	equivalent security crit	eria.				
		[NCP] CA key g	generation shall be car	rried out within	a device which	either:							
		- meets the re	equirements identified	in FIPS PUB 1	40-1 [2] level 3	or higher; or							
	Resolution	- meets the re	equirements identified	IN CWA 14167	-∠ [4], Or								
	commont												
	Comment												
	Resolution												

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target		
	version	clause	contribution	date	type	source	date		version		
			reference								
TS102042-007	1.1.1	7.2.2	UNSTT-002		technical			not yet processed			
	Comment	Modify the text:	dify the text: "a) [CHOICE]:								
	text	[LCP] The CA p	private signing key sha	all be held and	used in a produ	ct, application or o	device which doe	s not compromise the s	ecurity of the private		
		key and which:									
		<ul> <li>meets the re</li> </ul>	equirements identified	in FIPS PUB 1	140-1 [2] level 2	or higher; or					
		<ul> <li>is a trustwor</li> </ul>	thy system which is a	ssured to EAL	3 or higher in a	ccordance to ISO	/IEC 15408 [3], o	r equivalent security crit	eria.		
		[NCP] The CA p	private signing key sh	all be held and	used within a s	ecure cryptograph	nic device which:				
		<ul> <li>meets the re</li> </ul>	equirements identified	in FIPS PUB 1	140-1 [2] level 3	or higher; or					
		<ul> <li>meets the re</li> </ul>	equirements identified	in CEN Works	hop Agreement	14167-2 [4], or					
		<ul> <li>is a trustwor</li> </ul>	thy system which is a	ssured to EAL	4 or higher in a	ccordance to ISO	/IEC 15408 [3], o	r equivalent security crit	eria. This shall be to a		
		security target of	or protection profile wi	nich meets the	requirements of	the present docu	iment, based on a	a risk analysis and takin	g into account physical		
		and other non-t	ecnnical security mea	sures.							
			taida tha aignatura ar	action product	opplication or d	avian the corresp	, of the CA's prive	ata kay ahall ha anayra	4		
			iside the signature-cre	alion product,	application of o	evice, the secrecy	y of the CAS priv	ale key shall be ensured	J.		
		NOTE. THIS	inay be achieved usir	action device (		UII. Do CA privato sign	ing koy chall be	operwated with an algori	ithm and koy longth		
		that according	to the state of the art	are canable to	withstand crypt	analytic attacks for	or the residual life	of the encrypted with all algorithms	r key part		
		c) The CA priv	ate signing key shall b	ale capable lu	stored and reco	vered only by per	sonnel in trusted	roles using at least du	al control in a physically		
		secured env	vironment (see clause	7 4 4) The nu	mber of person	nel authorized to c	carry out this fund	tion shall be kent to a m	an control in a physically		
		consistent w	ith the CA's practices								
		d) Backup cop	ies of the CA private s	sianina kevs sh	all be subject to	the same or great	ater level of secur	itv controls as kevs curr	rently in use.		
		e) Where the k	evs are stored in a de	dicated key pr	ocessing hardw	are module, acce	ss controls shall I	be in place to ensure the	at the keys are not		
		accessible o	outside the hardware r	nodule."	U	·			2		
	Original	New text: "a) [0	CHOICE]								
	resolution	[LCP] "The CA.	"								
	proposal	FIPS PUB 1	140-1 [2] or FIPS PUE	3 140-2 [6]							
		[NCP] "The CA	private signing key'	:							
		<ul> <li>meets the residual</li> </ul>	equirements identified	in FIPS PUB 1	140-1 [2] or FIPS	S PUB 140-2 [6] le	evel 3 o higher; "				
	Resolution										
	comment										
	Resolution										
	text										

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TC400040.000	4 4 4	700			taabaical				l
15102042-008	1.1.1	7.2.9	UNST1-002		technical			not yet processed	
	Comment	Modify the text:	"d) Where the secure	user device ha	as associated us	ser activation data	a (e.g. PIN code),	the activation data sha	Il be securely prepared
	text	and distributed	separately from the si	gnature-creatio	n module.				
		NOTE: Sepa	aration may be achieve	ed by ensuring	distribution and	delivery at differe	ent times, or via a	different route."	
	Original	New text: d) V	Vhere the secure user	device has as	sociated user ad	ctivation data se	eparately from the	e secure user device.	
	resolution	NOTE: "Sep	aration may be achiev	ed by ensuring	distribution of a	activation data and	d delivery of secu	ire user device"	
	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						
TS102042-009	1.1.1	7.3.1	UNSTT-002		technical			not yet processed	
	Comment	Modify the text:							
	text	"b) [CONDITIO]	NAL]: If the subject is	a person and n	ot the same as	the subscriber, th	e subject shall be	informed of his/her ob	oligations.
		c) The CA sha	Il communicate this in	formation throu	gh a durable (i.	e. with integrity ov	/er time) means c	of communication, which	n may be transmitted
		electronicall	y, and in readily unde	rstandable lang	juage.				
		NOTE 1: A mo	del PKI disclosure sta	atement which r	may be used as	the basis of such	a communication	n is given in annex B.	
		d) The service	provider shall collect	either direct evi	dence, or an at	testation from an	appropriate and a	authorized source, of the	e identity (e.g. name)
		and, if applic	cable, any specific attr	ibutes of subje	cts to whom a c	ertificate is issued	d. Submitted evid	ence may be in the form	n of either paper or
		electronic do	ocumentation. Verifica	ition of the subj	ect's identity sh	all be by appropri	ate means and in	accordance with nation	nal law.
		e) [CHOICE]:							
		[LCP] No	o requirement.						
		[NCP] If	the subject is a physic	cal person evide	ence of the sub	ect's identity (e.g	. name) shall be c	checked against a phys	ical person either
		directly c	or indirectly using mea	ins which provid	des equivalent a	assurance to phys	sical presence (se	e note 2). Evidence for	verifying other entities
		shall invo	olve procedures which	n provide the sa	ame degree of a	ssurance.			
		NOTE 2: An ex	xample of evidence ch	necked indirectl	y against a phy	sical person is do	cumentation pres	ented for registration w	hich was acquired as
		the re	esult of an application	requiring physi	ical presence.				
		f) [CONDITIO	NAL] If the subject is a	a physical perso	on, evidence sh	all be provided of	:		
		- full name	e (including surname a	and given name	es);				<i>.</i>
		- date and	I place of birth, referen	nce to a nationa	ally recognized	dentity document	, or other attribute	es which may be used t	o, as far as possible,
		distinguis	sh the person from off	hers with the sa	ame name.				
			ecommended that the	place be given	i în accordance	to national conve	ntions for register	ring births.	
		g) [CONDITIO	NAL] If the subject is a	a physical perso	on who is identi	ried in association	i with a legal pers	on, or organizational er	ntity (e.g. the
		subscriber),	evidence snall be pro	VIDED OF:	a) of the authior	.4.			
		- IUII name	e (including surname a	and given name	es) of the subject	il, dontitu dogumont	or other ottribute	a of the subseriber whi	ah may ha usad ta sa
		- date and	place of pirth, referen	nce to a nationa	thore with the e			es of the subscriber whi	ch may be used to, as
		full nome	and logal status of the	person norm of	and porcon or c	ther organization	al antity (a. a. tha	subscribor):	
			anu leyal status of th	associated le	lo a compony r	ogistration) of the	a entity (e.g. the	subscriber),	zational ontitu:
			that the subject is as	sociated with th	legi company i	or other organiza	tional entity	person of other organiz	zalional entity,
			NALL I If the subject is as	an organization	al ontity ovidor	ce shall be provid	lional entity.		
		- full name	of the organizational	entity:	a entity, eviden				
		- reference	e to a nationally recor	nized registrati	on or other attr	ibutes which may	he used to as fa	r as nossible distinguis	sh the organizational
		entity fro	m others with the san	name		ibutes which may		i as possible, distinguie	sh the organizational
			NALL I If the subject is a	a device or syst	em operated by	or on behalf of a	n organizational e	entity, evidence shall be	e provided of
		- identifier	of the device by which	h it may be refe	erenced (e.a. In	ternet domain nar	ne).		provided on
		- full name	e of the organizational	entity:			,,		
		- a nationa	ally recognized identity	v number, or of	her attributes w	hich may be used	l to, as far as pos	sible, distinguish the or	ganizational entity from
		others w	ith the same name	,			, ao iai ao poo		
		i) The subscrit	ber shall provide a phy	vsical address.	or other attribut	es, which describ	e how the subscr	iber may be contacted.	
		k) The CA shall	Il record all the inform	ation necessary	v to verify the si	ubiect's identity, in	cluding any refer	ence number on the do	cumentation used for
		verification.	and any limitations or	its validity.	,				
L	1								

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target				
	version	clause	contribution	date	type	source	date		version				
			reference										
		<ol> <li>The CA sha</li> </ol>	ll record the signed ag	greement with t	he subscriber in	ncluding:							
		- agreeme	ent to the subscriber's	obligations (se	e clause 6.2);								
		<ul> <li>if require</li> </ul>	d by the CA, agreeme	ent by the subs	criber to user s	ecure user device	;						
		<ul> <li>consent</li> </ul>	to the keeping of a re	cord by the CA	of information	used in registration	n, subject device	provision, including whe	ether this is to the				
		subscrib	er or to the subject wh	nere they differ,	, and any subse	equent revocation	(see clause 7.4.1	<ol> <li>and passing of this i</li> </ol>	nformation to third				
		parties u	nder the same condit	ions as require	d by this policy	in the case of the	CA terminating its	s services;					
		- whether,	and under what conc	litions, the subs	scriber requires	and the subject c	onsents to the pu	blication of the certification	te;				
		- confirma	tion that the information	on held in the c	ertificate as be	ing correct.							
		NOTE 4: The s	subscriber may agree	to different asp	pects of this agr	eement during dif	ferent stages of re	egistration. For example	<ol> <li>agreement that the</li> </ol>				
		inforr	nation held in the cert	lificate is correc	ct may be carrie	d out subsequent	to other aspects	of the agreement.					
		NOTE 5: This	agreement may be in	electronic form	). 			、 <b>.</b> 、 .	<b>A</b>				
		m) The records	identified above shall	be retained to	r the period of t	ime as indicated to	o the subscriber (	see c) above) and as n	ecessary for the				
		purposes to	r providing evidence o	of certification in	n legal proceed	ngs."							
	Original	New text: "b) [C	ext: "b) [CONDITIONAL]: If the subject is a person and not the same as the subscriber, the subject shall be informed of his/her obligations.										
	resolution	<ol> <li>Inis comma</li> </ol>	should be cancelled	from this claus	e (Subject regis	tration) and insert	ed in "Subscriber	s obligations" (this kind	of information is				
	proposal	provided at	the moment of signing	g the agreemen	it by the subscr	ber).							
		I) The CA sha	Il record the signed										
		- ir require	tion that the information	ent by the subs	criber to use se	cure user device;							
		- coniima	uon mai me mornau	on neid in the c	w of the country	ect.	action Sonvice Dr	ovidar is astablished "					
	Resolution		ceedings according to				cation Service I I						
	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										
TS102042-010	1.1.1	7.2.8	UNSTT-002		technical			not yet processed					
	Comment	Modify the text:											
	text	"e) [CONDITIOI	NAL] If a copy of the s	subject's public	key is not requ	ired to be kept by	the CA (see claus	e 7.2.4), on delivery to	the subject, only the				
		subject (or,	if the key is not for ele	ctronic signatu	res, the subscri	ber) shall have ac	cess to its private	key. Any copies of the	subject's private key				
		held by the	held by the CA shall be destroyed."										
	Original	New text:	w text:										
	resolution	"e) [CONDITIOI	) [CONDITIONAL] If a copy of the subject's private key is no required"										
	proposal												
	Resolution												
	comment												
	Resolution												
	text												

Comment ID	Deliverable version	Deliverable clause	Original contribution	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
			reference						
TS102042-011	1.1.1	3.1	UNSTT-002		technical			not yet processed	
	Comment	Missing definition	on.						
	text								
	Original	New text: "Exte	nded Normalized Cer	tificate Policy:	normalized cert	ficate policy requi	ring use of a sec	ure user device."	
	resolution								
	proposal								
	Resolution								
	Comment								
	Resolution								
Comment ID	Deliverable	Deliverable	Original	Commont	Commont	Pesolution	Pesolution	Perclution status	Deliverable target
Comment ID	version	clause	contribution	date	type	Source	date	Resolution status	version
	Vereien	oladoo	reference	duto	.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Source	uuto		Verbion
TS102042-012	1.1.1	7.4.4	UNSTT-002		technical			not yet processed	
	Comment	Modify the text:	"Certificate generation	n, subject devi	ce provision an	d revocation mana	agement		•
	text	d) The facilities	s concerned with certi	ficate generation	on, subject devi	ce provision and r	evocation manag	gement shall be operate	d in an environment
		which physi	cally protects the serv	vices from com	promise through	unauthorized ac	cess to systems of	or data.	
		e) Physical pro	ptection shall be achie	ved through th	e creation of cle	arly defined secu	rity perimeters (i.	e. physical barriers) aro	und the certificate
		generation,	subject device provisi	ion and revoca	tion manageme	nt services. Any p	arts of the premi	ses shared with other or	ganizations shall be
		outside this	perimeter.	nitu a sentus la sla	all ha imanlanaan		fe eiliter her reiner er		
		1) Physical and	and the feeilities use	d to support the	all be implement		naching nousing s	vstern resources, the sy	stern resources
		certificate d	and the lacinities use	vice provision a	and revocation n	ie CAS priysical a	cas shall address	the physical access co	entrol natural disaster
		protection f	ire safety factors fail	ire of supportin	a utilities (e.a. r	ower telecommu	inications) struct	ure collapse plumbing l	eaks protection against
		theft, breaki	ng and entering, and	disaster recove	erv. etc.			are concepte, planning i	ouno, protocuori againet
		g) Controls sha	all be implemented to	protect agains	t equipment, inf	ormation, media a	nd software relat	ting to the CA services b	peing taken off-site
		without auth	orization.			·		0	C
		NOTE 1: See	ISO/IEC 17799 for gu	idance on phys	sical and enviro	nmental security.			
		NOTE 2: Othe	r functions may be su	pported within	the same secur	ed area provided	that the access is	s limited to authorized p	ersonnel."
	Original	New text: "Cert	ificate generation, sub	pject device pro	vision and revo	cation manageme	ent		
	resolution	e) Physical pro	ptection shall be achie	ved through th	e creation of cle	arly defined secu	rity perimeters (	) around the certificate	generation, subject
	proposal	device provi	ision and revocation n	nanagement se	ervices. Any par	ts of the premises	snared with othe	er organizations shall be	e outside this perimeter.
		NOTE 1: AS a	erined at the beginnin	g of the docum	ient, a subject (	device provision s	ervice prepares a	and provides a signature	e-creation device to
		appli	cable only to subject	CA gives Regis device prepara	tion (and NOT r	es the responsibility	ity to provide sign	lature devices to subject	as comma e) is
		appii a) idem	cable only to subject	device prepara					
		NOTE 2:							
		NOTE 3:"							
	Resolution								
	comment								
	Resolution								
	text								

Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	reference	date	туре	source	Gate		version
TS102042-013	111	745	UNSTT-002		technical			not vet processed	
	Comment	Modify the text:	011011 002		toorninoar			not yot proceeded	
	text	"c) Media used	within the CA shall be	e securelv hand	ded to protect n	nedia from damac	e. theft and unau	thorized access."	
	Original	New text:					- ,		
	resolution	"c) Media used	within the CA shall be	e securely hand	dled to protect n	nedia from damag	e, theft, and una	uthorized access. Media	life cycle management
	proposal	shall be suc	h to proactively preve	nt obsolescend	e."				
	Resolution								
	comment								
	Resolution								
	text				-		I	1	
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target
	version	clause	contribution	date	type	source	date		version
T0100040.014	4 4 4	740			tashaisal				
15102042-014	1.1.1 Commont	7.4.8 Madify the taxts	UNSTI-002		technical			not yet processed	
	toxt	c) In the case	of compromise the C/	\ shall as a min	vimum provide t	he following unde	rtakings:		
	IEXI	- inform a	ll subscribers relving	narties and oth	er CAs with wh	ich it has agreem	ents or other form	of established relations	s of the compromise."
	Original	New text:	il ouboonboro, rorying			ion it has agreen			
	resolution	"a) In the case	of compromise						
	proposal	- Inform a	Il subscribers (and the	ese ones in turr	n will inform the	subjects) and any	entity with whick	n it has agreements or o	ther form of established
		relations	, among which relying	g parties and C	As"		•	·	
	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
T0102042-015	1 1 1	740			taabaical			not yet pressed	
15102042-015	Commont	7.4.9 Modify the text:	UNSTI-002		technical			not yet processed	
	tovt	a) Before the (	A General	ices the followi	na procedures s	shall be evecuted	as a minimum:		
	ICAL	- the CA s	hall inform all subscri	hers relving na	arties and other	CAs with which it	has agreements	or other form of establish	shed relations."
	Original	New text: "CA c	ieneral	bolo, lolying pe			nao agreemente		
	resolution	a) before the C	A terminatesthe CA	shall					
	proposal	- inform a	Il subscribers (and the	ese one in turn	will inform the s	ubjects) and any	entity with which	it has agreements or oth	ner form of established
		relations	, among which relying	parties and C	As."	, , ,	,	0	
	Resolution			<b>z</b> .					
	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									
TS102042-016	1.1.1	7.4.11	UNSTT-002		technical			not yet processed				
	Comment	Modify the text:	"The CA shall ensure	that all relevar	nt information co	oncerning a certifi	cate is recorded f	or an appropriate perio	d of time, in particular			
	text	for the purpose	of providing evidence	of certification	for the purpose	s of legal proceed	dings.					
		NOTE 1: Reco	ords concerning certifi	cates include re	egistration inforr	mation (see clause	e 7.3.1) and infor	mation concerning signi	ificant CA			
		envir	onmental, key manag	ement and cert	tificate manager	ment events.						
		In particular:										
		General										
		a) The confide	ntiality and integrity of	f current and ar	chived records	concerning certific	cates shall be ma	intained.				
		<ul> <li>b) Records cor</li> </ul>	ncerning certificates s	hall be complet	ely and confide	ntially archived in	accordance with	disclosed business pra	ctices.			
		c) Records cor proceedings	Records concerning certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. The subject, and within the constraints of data protection requirements (see clause 7.4.10) the subscriber, shall have access to registration and other information relating to the subject.									
		registration	and other information	relating to the	subject.							
		NOTE 2: This	may be used, for example	mple, to suppor	t the link betwe	en the certificate a	and the subject.					
		a) The precise	time of significant CA	environmental	, key managem	ent and certificate	e management ev	ents shall be recorded.				
		NOTE 3: It is f	ecommended that the	e CA states in it	s practices the	accuracy of the cl	ock used in timing	g or events, and now the				
		f) The events	icerning certificates s		a period or time	e as indicated in tr	ie CAS leinis and	a conditions (see clause	t 1.3.4).			
		time that the	shall be logged in a w	ay mat mey ca	inot be easily u			isier to long-term media	a) within the period of			
		NOTE 4. This	may be achieved for	evample throu	ah the use of w	rite only media a	record of each re	movahla madia usad a	nd the use of off site			
		hack	un	example, unou	gir the use of w	nie only media, a						
		a) The specific	events and data to be	e loaged shall h	be documented	by the CA						
		Registration		e logged shall k		by the O/t.						
		h) The CA sha	ll ensure all events re	lating to registra	ation including r	equests for certifi	cate re-kev or rer	newal are logged				
		i) The CA sha	Il ensure that all regis	tration informat	ion including the	e following is reco	rded:	iowal, aro loggoa.				
		- type of d	ocument(s) presented	d by the applica	int to support re	distration:						
		- record of	f unique identification	data. numbers.	or a combination	on thereof (e.g. ar	oplicant's drivers	license number) of iden	tification documents. if			
		applicab	le;		,			,				
		- storage	ocation of copies of a	pplications and	identification d	ocuments, includi	ng the signed sub	oscriber agreement (see	e clause 7.3.1 l);			
		- any spec	cific choices in the sub	scriber agreen	nent (e.g. conse	nt to publication c	of certificate);	Ŭ (	,.			
		- identity of	of entity accepting the	application;								
		- method	used to validate identi	fication docume	ents, if any;							
		- name of	receiving CA and/or s	submitting Regi	stration Authori	ty, if applicable.						
		j) The CA sha	Il ensure that privacy	of subject inform	mation is mainta	ained."						
	Original	New text: "The	CA shall ensure that a	all relevant info	rmation concerr	ning a qualified ce	rtificate is recorde	ed for an appropriate pe	eriod of time, in			
	resolution	particular for the	e purpose of providing	g evidence of ce	ertification for th	e purposes of leg	al proceedings a	ccording to the national	law of the country			
	proposal	where the Certi	fication Service Provid	der is establishe	ed."							
		Registration						<i>,</i>				
		i) The Ca shal	I ensure that all regist	tration information	on any speci	fic choices in the	subscriber agreei	ment (e.g. subjects' con	sent to publication of			
		certificate)."										
	Resolution											
	comment											
	Resolution											
	text											

Comment ID	Deliverable version	Deliverable clause	Original contribution reference	Comment date	Comment type	Resolution source	Resolution date	Resolution status	Deliverable target version
TS102042-017	1.1.1	3.2	UNSTT-002		technical			not yet processed	
	Comment	Modify the text:	"NCP+ Normalized C	ertificate Policy	/ requiring use of	of a secure user of	levice"		
	text								
	Original	New text: "NCP	+ Extended Normalized	ed Certificate F	olicy."				
	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										
TS102042-018	1.1.1		TC-ESI_3-002		technical			not yet processed					
	Comment	Comment	nment										
	text	We have not loo	oked at possible confli	cts, which may	arise when the	re are more than	one certificates is	sued to a key pair, e.g.	generated and residing				
		on a card. Thes	e certificates may be	issued by differ	rent CAs, under	different CPs.							
		I have, so far, ic	lentified one potential	conflict. Assun	ne that two CAs	issue two differer	nt certificates to th	ne same key, one speci	fying key usage for el.				
		signatures only,	atures 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. With	nout a flag in the CP th	ne situation is r	not transparent t	o auditors either.							
		We should cons	sider to look at:										
		a) whether the	re are other potential of	conflicts for the	configuration d	escribed above, a	ind						
		b) how to addre	how to address them.										
		Maintenance of	intenance of the policies is probably the right place to deal with this.										
		Discussion											
		Rey multiple us	aye. howerk to support the	use of a signal	tures and creati	na an anvironmar	t which will prom	oto truct, and protocting	the interests of				
		consumers relvi	ng on e-signatures: is	an objective u	nder EESSI and	the Directive		ole liusi, and protecting	g the interests of				
		It is technically	nossible that the same	an objective u	av he included in	n more than one c	ertificate (This co	ould well be the case for	or example where the				
		key pair is gene	rated by the subscribe	er which he se	nds to more that	n one certification	authority) In der	neral there may be not	hing objectionable in				
		this, but for som	e applications, this m	av be undesira	ble, particularly	where higher leve	els of assurance a	are required.					
		Issue revolves a	around:										
		a) the quality o	f the key pair generate	ed; and									
		b) the creation	of a close association	between the k	ey pair and an a	application for whi	ich it is to be used	J.					
		Qualified certific	ates are designed to	offer a high lev	el of assurance	which needs to b	e maintained in a	Il aspects of the service	e. TS 101 456 [1] does				
		not prohibit sub	scriber generation of l	keys. It should	be preferred that	t the certification	authority takes re	sponsibility for generati	ing the keys. This is not				
		currently part of	Electronic Signatures	Directive, nor	conformance g	uidance.							
		Qualified certific	cates may be used to	support an artic	cle 5.1 e-signatu	ure; they may also	be used for auth	entication in general us	se.				
		Article 5.1 signa	tures must be recogn	ized in legal pr	oceedings as th	e equivalent of ha	and written signat	ures. Other electronic s	ignatures may be				
		recognized as s	uch, although probab	ly only if they s	atisfy at least th	e definition of an	advanced electro	nic signature under arti	cle 2.2.				
		It is suggested,	therefore, that subscr	iber key pairs i	ssued for the pu	irpose of creating	any type electron	iic signature which is in	tended to fulfil the				
		function of a ha	nd written signature, i		s to be treated a	is a nandwritten s	Ignature by a rely	ing party, should be res	stricted to that purpose.				
		In respect of bo	th qualified certificates	s AND any e-si	gnature which is	s intended to be a	nandwritten sign	ature equivalent, there	is a need that they				
		Signaturos in th	a right level of assurat	we main function	i party who may	reasonably rely c	ni uns.						
		they indicate	a will or intention by	the signer to ta	uke on a commit	ment (The exact	nature of the corr	mitment may be ambic	wous except by				
		reference to	the document to which	the signer to ta	or to some othe	r evidence). and		innument may be ambig	Juous except by				
		- a signature i	s evidence of itself i	e of the act of the	sianina								
		Therefore, there	e are two elements wh	hich electronic s	signatures cann	ot prove:							
		a) the intention	to express a commit	ment; and									
		b) the intention	to create the signatu	re.									
		Even an Article	5.1 electronic signatu	re created usin	g public key cry	ptography, i.e. die	gital signatures, a	re not (unless there is o	other evidence) capable				
		of demonstratin	g the signer's intentior	ns. However, ir	ntent is an essei	ntial element of sig	gning and there is	an urgent need to find	a means of				
		incorporating th	is factor into an electr	onic signature,	which is intended	ed as a handwritte	en signature.	-					
		One factor whic	h could provide evide	nce of the inter	ntion to create a	signature equival	ent to a h/w one,	is to "bind" the signing	key to the application.				
		This could be a	chieved by restricting	the use of a ke	y to a "signing"	application, i.e. by	/ including it in a d	certificate (qualified) wh	nich specifies a key				
		usage.											

		The relying part	y needs to know (in	order to rely on	a "e-signature e	equivalent to hand	written signature	") that the signer will not	be able to deny his
		intention to mak	e the signature as a	handwritten one	e. This requires	two steps:			
		<ul> <li>making it cle</li> </ul>	ar to the signer that	his key, certifica	ate, must only b	e used to create a	an e-signature, er	nforcing that obligation e	ither by technical or
		(second bes	t) by legal means;						
		<ul> <li>ensuring a m</li> </ul>	neans of signature c	reation which m	akes it clear to	the signer that he	is creating is equ	ial to a h/w one; prevent	ing (as far as possible)
		the use of hi	s key pair for any oth	ner purpose.					
		As a preference	, the sscd on which	the keys are sto	ored should also	be dedicated to a	a hw sign, but this	s may carry unrealistic c	osts implications. The
		reason is that w	ill give an opportunit	y to include som	nething on the c	asing of the sscd	which will alert th	ne signer to its significan	ce as a signing device.
		The fact that:							
		<ul> <li>key usage is</li> </ul>	restricted, and						
		<ul> <li>the signer pr was making.</li> </ul>	obably knew that ke	y usage was res	stricted will prov enforced by lay	vide prima facie ev v was being under	vidence that the s	igner knew what kind of	electronic signature he
		Enforcement:				i nao song unao			
		It has been arou	ed that certification	authorities shou	uld be free to de	cide for themselve	es whether to enf	orce obligations against	a subscriber. There
		may be many re	asons for NOT takin	a any enforcem	nent action.			eree esingatione againet	
		- the certificat	ion authority does no	of regard the bre	each as being si	onificant.			
		<ul> <li>the certificat</li> </ul>	ion authority itself ha	is not suffered a	any loss neither	will its inaction is	not (currently) in	contravention of any au	uditing criteria or
		quidance:					not (our officity) in		
		- the subscrib	er is a customer the	re is a real conf	lict of interest -	it is not a good ma	arketing practice	to bring legal proceeding	as against customers:
		and				in to not a good in	g processo		ge againer easternere,
		- cost of legal	proceedinas.						
		The reliability of	signatures = to $h/w$	signatures is a i	matter of public	interest, therefore	e, the responsibili	ty for ensuring their effe	ctiveness should not
		just be left to the	e discretion of a certi	fication authorit	v. The role of th	e certification aut	hority should be t	to take such steps as ar	e reasonably within its
		, competence and	d power to ensure a	sinale use of ke	vs used to crea	te such signature	s. This could be r	provided for by including	appropriate
		requirements in	TS 101 456 [1] and	TS 102 042 [2]	(or for the time	being, in any appr	opriate maintena	ance document).	
		In due course, it	t is to be hoped (and	expected) that	national laws w	ill impose the sam	ne level of respor	sibility of a signer as cu	rrently exist in relation
		to a handwritten	signature. However	, this cannot ha	ppen for so long	as there is ambi	auity surrounding	the electronic signature	e creation.
	Original		4		• •			ε τ <u>τ</u>	
	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						
TS102042-019	1.1.1	7.2.9	OTHER-005		technical			not yet processed	
	Comment	I am wondering	whether we omitted	a clause in TS	101 456 [1] to s	tate that the CA s	hall inform their s	ubscribers about the kir	d of environment that
	text	he shall use for	the SSCD, pointing	to CWA 14170 [	[12]: Security re	quirements for Sig	gnature Creation	Systems.	
	Original	Add to clause 7	.2.9:					· ·	
	resolution	"NOTE: It is re	ecommended that th	e CA advises si	ubscribers as to	the environments	in which the SS	CD should be used. This	s includes the
	proposal	chara	cteristics of the devi	ces and applica	tions used, and	the purpose or in	tention of the act	of signing."	
	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							
TS102042-020	1.1.1	7.2.5	OTHER-006		technical			not yet processed		
	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								
	text	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	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								
	proposal	other purposes if this results in the violation of THE SECURITY MEASURES OR ANY OTHER SPECIFIC LIMITATIONS PROVIDED FOR in this								
		VOIE: It is recommended that different CA keys are used to issue certificates under different policies.								
		) An alternative resolution is to delete this clause.								
		ian 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 Y	vouid result in violation of the QUP. Same for NUP.							
	Decelution	inis is not a requirement that can be understood easily. Actually, I think that the new wording is meaningless.								
	Resolution									
	Becelution									
	test									
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Pesolution	Pesolution	Posolution status	Deliverable target	
Comment iD	version	clause	contribution	date	type	Source	date	Resolution status	version	
	Version	Clause	reference	uate	type	300100	uate		Version	
TS102042-021	111	747	OTHER-007		technical			not vet processed		
10102012 021	Comment	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)". Update clause 7.4.7, note 1 to explicitly reference CWA 14167-1 [11] and add the reference to the bibliography/references.								
	text									
	Original									
	resolution		· ·	5	-	-		0 1 9		
	proposal									
	Resolution									
	comment									
	Resolution									
	text			-			-	7		
Comment ID	Deliverable	Deliverable	Original	Comment	Comment	Resolution	Resolution	Resolution status	Deliverable target	
	version	clause	contribution	date	type	source	date		version	
			reference						ļ	
TS102042-022	1.1.1	8	OTHER-008		technical			not yet processed	l	
	Comment	It is currently no	ot clear when a new ce	ertification polic	cy is necessary.					
	text									
	Original	Add to clause 8								
	resolution	ION  "No changes should be made to a certificate policy which could affect a relying party's consideration on the reliability of the certificate issued b								
	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	
--------------	------------------------------------	---	--	-----------------	-----------------	----------------------	--------------------	-------------------	-------------------------------	
TS102042-023	1.1.1	7.2.2 - b) - NCP	TC-ESI_1-004	22/10/2003	technical			not yet processed		
	Comment text	CA private signing keys, when exported, can be protected not only by means of encryption, but also by means of other mechanisms, like Shamir's or Blakley's threshold secret sharing mechanism.								
	Original resolution proposal	Change clause protected using encrypted key c	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 and crypted key or key component."							
	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						
TS102042-024	1.1.1	Annex D	TC-ESI_1-007	26/10/2003	technical			not yet processed	
	Comment	Correct the inco	onsistencies in annex	D, the cross re	eference betwee	n RFC 2527 and	TS 101 456.		
	text								
	Original	Amendment pro	mendment proposed: 3.4: change "7.3.5" into "7.3.6"						
	resolution	* 3.4: change							
	proposal	* 4.4: change	e "7.3.5" into "7.3.6"						
		* 5.2: change	e "7.4.5" into "7.4.3" (n	ote 1)					
		* 6.3: add "6.	2, " before "7.2"						
		* 6.4: add *7.	2.7, " before "7.2.9"						
		0.5. aug 7.4	4.5, Deloie 7.4.0	2)					
		* 6.7: add "7	4.5 " before "7.4 (1101e	2)					
		0.7. add 7.							
		NOTE 1: The procedural controls, as per RFC 2527, are: "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).							
							e (22)		
							0.().		
		For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule). Identification and authentication requirements for each role may also be defined."						rule). Identification and	
		NOTE2: The	life cycle security cont	trols, as per RF	C 2527, are:				
		"This subcompo	This subcomponent addresses system development controls and security management controls.						
		System development controls include development environment security, development personnel security, configuration management security							
		during product	maintenance, softwar	e engineering	practices, softwa	are development i	methodology, mo	dularity, layering, use of	failsafe design and
		implementation	techniques (e.g., def	ensive progran	nming) and deve	elopment facility s	ecurity. (<- this is	not addressed by TS 1	01 456)
		Security manag	gement controls includ	le execution of	tools and proce	dures to ensure t	hat the operation	al systems and network	s adhere to configured
		security. These	tools and procedures	include check	ing the integrity	of the security so	ftware, firmware,	and hardware to ensure	Heir correct operation.
		(<- this is addre	essed in clause 7.4 of	IS 101 456)				<i>.</i>	
		This subcompo	nent can also address	s life-cycle sec	urity ratings bas	ed, for example, o	on the Trusted So	oftware Development Me	sthodology (ISDM)
		level IV and V,	independent life-cycle	security contr	ois audit, and th	e Software Engin	eering institute's	Capability Maturity Mod	ei (SEI-CIVIVI). (<- this
	Pasalution	is not addresse	eu by 15 101 456).						
	Resolution								
	Bosolution								
	Resolution								
	τεχτ								

# 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			
2.4 Inte	rpretation and Enforcement	5.4			
2.5 Fee	S	N/A			
2.6 Pub	lication and Repositories	7.3.5, 7.3.6			
2.7 Cor	npliance Audit	N/A			
2.8 Cor	fidentiality Policy	7.3.1			
2.9 Inte	llectual Property Rights	N/A			
3 IDEN					
3.1 Initi	al Registration	7.3.1			
3.2 ROL	Itine Rekey	7.3.2			
3.3 Rek	ey After Revocation No Key Compromise	7.3.2			
3.4 Rev		7.3. <del>0</del> 0			
4 OFER	tificate Application	731			
4.1 Cer 4.2 Cer	tificate Application	733			
4.2 Cer	tificate Accentance	7.3.1			
4.0 Cer	tificate Suspension and Revocation	7 3 56			
4.5 Sec	urity Audit Procedures	N/A			
4.6 Rec	ords Archival	7 4 11			
4.7 Kev	Changeover	732			
4.8 Cor	npromise and Disaster Recovery	7.4.8			
4.9 CA	Termination	7.4.9			
5 PHYS	SICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS				
5.1 Phy	sical Security Controls	7.4.4			
5.2 Pro	cedural Controls	7.4. <del>5</del> 3 (see note 1)			
5.3 Per	sonnel Security Controls	7.4.3			
6 TECH	INICAL SECURITY CONTROLS				
6.1 Key	Pair Generation and Installation	7.2.8, 7.2.9			
6.2 Priv	ate Key Protection	7.2.8			
6.3 Oth	er Aspects of Key Pair Management	7.2, 6.2			
6.4 Acti	vation Data	7.2.7, 7.2.9			
6.5 Cor	nputer Security Controls	7.4.5, 7.4.6, 7.4.7			
6.6 Life	Cycle Security Controls	7. <del>3</del> 4 (see note 2)			
6.7 Net	work Security Controls	7.4.5, 7.4.6			
6.8 Cry	ptographic Module Engineering Controls	7.2			
7 CER	IFICATE AND CRL PROFILES	7.0.0			
7.1 Cer	lificate Profile	7.3.3			
		N/A			
0 SPEC	vification Change Presedures	7 1			
8.1 Spe	lication and Notification Procedures	7.1			
8.3 Cer	tification practice statement Approval Procedures	7.1			
NOTE 1	he procedural controls as per REC 2527 are:	7.1			
	"In this subcomponent, requirements for recognizing trusted roles are	described, together			
	with the responsibilities for each role.(22).				
	For each task identified for each role, it should also be stated how ma	any individuals are			
	required to perform the task (n out m rule).Identification and authentic	ation requirements for			
	each role may also be defined."				
NOTE2:	The life cycle security controls, as per RFC 2527, are:				
	"I his subcomponent addresses system development controls and se	curity management			
	controls.				
	System development controls include development environment security, development				
	engineering practices, software development methodology, modularity, lovaring, use of				
	failsafe design and implementation techniques (e.g. defensive programming) and				
	development facility security (this is not addressed by TS 101 456).				
	Security management controls include execution of tools and procedures to ensure that the				
	operational systems and networks adhere to configured security. These tools and procedures				
	include checking the integrity of the security software, firmware, and hardware to ensure their				
	correct operation (this is addressed in clause 7.4 of TS 101 456).				
	This subcomponent can also address life-cycle security ratings based, for example, on the				
	I rusted Software Development Methodology (TSDM) level IV and V, independent life-cycle				
	security controls audit, and the Software Engineering Institute's Capability Maturity Model				
1	(SET-GIVIN) (THIS IS NOT ADDRESSED DV 15 101 456).				

# A.1.2 TS 102 042 - Normalized certificate policy

## A.1.2.1 Export of the CA private key

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

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	7.3.56
4 OPERATIONAL REQUIREMENTS	
4.1 Certificate Application	7.3.1

4.2       Certificate Issuance       7.3.3         4.3       Certificate Acceptance       7.3.1         4.4       Certificate Acceptance       7.3.66         4.5       Security Audit Procedures       N/A         4.6       Records Archival       7.4.11         4.7       Key Changeover       7.3.2         4.8       Compromise and Disaster Recovery       7.4.8         4.9       CA Termination       7.4.9         5       PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS       5.1         5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.4         5.3       Personnel Security Controls       7.4.53 (see note 1)         5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.4.6         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2.7, 7.2.9         6.4       Activation Data       7.2.7, 7.4.6, 7.4.7         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Cryptographic Module Engineering Controls<		
4.3       Certificate Acceptance       7.3.1         4.4       Certificate Suspension and Revocation       7.3.66         4.5       Security Audit Procedures       N/A         4.6       Records Archival       7.4.11         4.7       Key Changeover       7.3.2         4.8       Compromise and Disaster Recovery       7.4.8         4.9       CA Termination       7.4.9         5       PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS         5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.4.3         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.3.3         7.1       Certificate Profile       7.3.3		
4.4       Certificate Suspension and Revocation       7.3.56         4.5       Security Audit Procedures       N/A         4.6       Records Archival       7.4.11         4.7       Key Changeover       7.3.2         4.8       Compromise and Disaster Recovery       7.4.8         4.9       CA Termination       7.4.9         5       PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS       5.1         5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.53 (see note 1)         5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.4.3         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8, 7.2.9         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         7.0       CERTIFICATE AND CRL PROFILES       7.2         7.1       Certificate Profile       7.3.3         7.2       CRETIFICATION ADMINI		
4.5       Security Audit Procedures       N/A         4.6       Records Archival       7.4.11         4.7       Key Changeover       7.3.2         4.8       Compromise and Disaster Recovery       7.4.8         4.9       CA Termination       7.4.9         5       PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS       5         5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.53 (see note 1)         5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       6.1         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6, 7.4.6         6.7       Network Security Controls       7.4.5, 7.4.6, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.2         7       CERTIFI		
4.6       Records Archival       7.4.11         4.7       Key Changeover       7.3.2         4.8       Compromise and Disaster Recovery       7.4.8         4.9       CA Termination       7.4.9         5       PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS         5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.53 (see note 1)         5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.4.3         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Cryptographic Module Engineering Controls       7.4.5, 7.4.6         7       CERTIFICATE AND CRL PROFILES       7.2         7.1       Certificate Profile       7.3.3         7.2       CERTIFICATE AND CRL PROFILES       7.1         7.1       Certification Change Procedures       7.1         8.1       Specification Change Procedures		
4.7       Key Changeover       7.3.2         4.8       Compromise and Disaster Recovery       7.4.8         4.9       CA Termination       7.4.9         5       PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS       5         5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.4         5.3       Physical Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.4.3         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2.7, 7.2.9         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Cryptographic Module Engineering Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.2         7.1       Certificate Profile       7.3.3         7.2       CCRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1		
4.8       Compromise and Disaster Recovery       7.4.8         4.9       CA Termination       7.4.9         5       PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS       7.4.9         5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.53 (see note 1)         5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.4.3         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.4.5, 7.4.6         7       CERTIFICATE AND CRL PROFILES       7.2         7.1       Certificate Profile       7.3.3         7.2       CERTIFICATE AND CRL PROFILES       7.1         7.1       Certification Change Procedures       7.1         8.1       Specification Change Procedures       7.1         8.2       Pub		
4.9       CA Termination       7.4.9         5       PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS       7.4.4         5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.53 (see note 1)         5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.4.3         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.2.8         7       CERTIFICATE AND CRL PROFILES       7.2         7.1       Cettificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Practice statement Approval Procedures       7.1         8.1       Specification practice statement Approval Procedures       7.1         8.2		
5       PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS         5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.53 (see note 1)         5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.4.3         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.1         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       7.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3 <t< td=""></t<>		
5.1       Physical Security Controls       7.4.4         5.2       Procedural Controls       7.4.63 (see note 1)         5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.2.8         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.1         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       7.1         8.1       Specification And Notification Procedures       7.1         8.1       Specification practice statement Approval Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.4       Subcomponent, requirements for recognizing trusted roles are described,		
5.2       Procedural Controls       7.4.53 (see note 1)         5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       6.1         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2.6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.3.3         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.4       Publication and Notification Procedures       7.1		
5.3       Personnel Security Controls       7.4.3         6       TECHNICAL SECURITY CONTROLS       7.2.8         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2.6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.2         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.3       Certification change of each role.(22).       For each task identified for each role.(22).         For each task identified for each role.(22).       For each task		
6       TECHNICAL SECURITY CONTROLS         6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.1         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.1       Specification Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recogniz		
6.1       Key Pair Generation and Installation       7.2.8, 7.2.9         6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.4.5, 7.4.6         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.1         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the respons		
6.2       Private Key Protection       7.2.8         6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.34 (see note 2)         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.2         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authen		
6.3       Other Aspects of Key Pair Management       7.2, 6.2         6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.34 (see note 2)         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.3         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
6.4       Activation Data       7.2.7, 7.2.9         6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.34 (see note 2)         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.2         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
6.5       Computer Security Controls       7.4.5, 7.4.6, 7.4.7         6.6       Life Cycle Security Controls       7.34 (see note 2)         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.3.3         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
6.6       Life Cycle Security Controls       7.34 (see note 2)         6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.3.3         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       7.3.3         7.2       CRL Profile       7.1         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
6.7       Network Security Controls       7.4.5, 7.4.6         6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.3.3         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
6.8       Cryptographic Module Engineering Controls       7.2         7       CERTIFICATE AND CRL PROFILES       7.3.3         7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
7       CERTIFICATE AND CRL PROFILES         7.1       Certificate Profile         7.2       CRL Profile         8       SPECIFICATION ADMINISTRATION         8.1       Specification Change Procedures         7.1       Specification Change Procedures         7.1       8.2         Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures         7.1       The procedural controls, as per RFC 2526, are:         "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
7.1       Certificate Profile       7.3.3         7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
7.2       CRL Profile       N/A         8       SPECIFICATION ADMINISTRATION       8.1         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
8       SPECIFICATION ADMINISTRATION         8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
8.1       Specification Change Procedures       7.1         8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       7.1         "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).       For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
8.2       Publication and Notification Procedures       7.1         8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are: "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22). For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
8.3       Certification practice statement Approval Procedures       7.1         NOTE 1:       The procedural controls, as per RFC 2526, are:       "In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).         For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
<ul> <li>NOTE 1: The procedural controls, as per RFC 2526, are:         <ul> <li>"In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22).</li> <li>For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."</li> </ul> </li> </ul>		
"In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.(22). For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
with the responsibilities for each role.(22). For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule).Identification and authentication requirements for each role may also be defined."		
For each task identified for each role, it should also be stated how many individuals are required to perform the task (n out m rule). Identification and authentication requirements for each role may also be defined."		
required to perform the task (n out m rule). Identification and authentication requirements for each role may also be defined."		
each role may also be defined."		
NOTE 2: The life cycle security controls, as per RFC 2527, are:		
This subcomponent addresses system development controls and security management		
System development controls include development environment security, development		
personnel security, configuration management security during product maintenance, software		
engineering practices, software development methodology, modularity, layering, use of		
failsafe design and implementation techniques (e.g., defensive programming) and		
development facility security (this is not addressed by TS 101 456).		
Security management controls include execution of tools and procedures to ensure that the		
operational systems and networks adhere to configured security. These tools and procedures		
include checking the integrity of the security software, firmware, and hardware to ensure their		
correct operation (this is addressed in clause 7.4 of TS 101 456).		
This subcomponent can also address life-cycle security ratings based, for example, on the		
Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle		
security controls audit, and the Software Engineering Institute's Capability Maturity Model		
(SEI-CMM) (this is not addressed by TS 101 456).		

# A.1.3 TS 102 023 - Time-stamping policy

## A.1.3.1 Export of the CA private key

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

#### Contribution: comment

Clause 7.2.2 - item b):

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

#### Contribution: proposed resolution

Two possible amendments can apply:

- 1) Reword the paragraph with the same new text proposed for TS 101 456:
  - When outside the signature-creation device (see a) above) the CA private signing key shall be protected using systems that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key part.

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 data ....separately from the secure user device.

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

#### ✓ 7.3.1 Subject Registration

- b) [CONDITIONAL]: If the subject is a person and not the same as the subscriber, the subject shall be informed of his/her obligations.
- j) This comma should be cancelled from this clause (Subject registration) and inserted in "Subscriber's obligations" (this kind of information is provided at the moment of signing the agreement by the subscriber).
- 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

[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	
D contribution JCPKI-007	
Source	Japan and China PKI Forums
/ersion 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	<ul> <li>Accuracy</li> </ul>	/ 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<sup>™</sup>

158

## 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<sup>™</sup> 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-PLUGTESTS<sup>TM</sup> 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-PLUGTESTS<sup>TM</sup> 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