

Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates



Reference

RTS/ESI-000058

Keywords

e-commerce, electronic signature, security

ETSI

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

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

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

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

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 2007.
All rights reserved.

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

Contents

Intellectual Property Rights	5
Foreword.....	5
Introduction	5
1 Scope	6
2 References	7
3 Definitions and abbreviations.....	8
3.1 Definitions	8
3.2 Abbreviations	9
4 General concepts	10
4.1 Certification authority	10
4.2 Certification services.....	10
4.3 Certificate policy and certification practice statement	11
4.3.1 Purpose	11
4.3.2 Level of specificity	12
4.3.3 Approach	12
4.3.4 Other CA statements.....	12
4.4 Subscriber and subject.....	12
5 Introduction to qualified certificate policies.....	13
5.1 Overview	13
5.2 Identification	13
5.3 User Community and applicability.....	14
5.3.1 QCP public + SSCD	14
5.3.2 QCP public.....	14
5.4 Conformance	14
5.4.1 General.....	14
5.4.2 QCP public + SSCD	15
5.4.3 QCP public.....	15
6 Obligations and liability	15
6.1 Certification authority obligations.....	15
6.2 Subscriber obligations	15
6.3 Information for relying parties	16
6.4 Liability	16
7 Requirements on CA practice.....	17
7.1 Certification Practice Statement (CPS)	17
7.2 Public key infrastructure - Key management life cycle.....	18
7.2.1 Certification authority key generation	18
7.2.2 Certification authority key storage, backup and recovery.....	19
7.2.3 Certification authority public key distribution.....	19
7.2.4 Key escrow	19
7.2.5 Certification authority key usage	20
7.2.6 End of CA key life cycle.....	20
7.2.7 Life cycle management of cryptographic hardware used to sign certificates	20
7.2.8 CA provided subject key management services.....	21
7.2.9 Secure-signature-creation device preparation	21
7.3 Public key infrastructure - Certificate Management life cycle	21
7.3.1 Subject registration	21
7.3.2 Certificate renewal, rekey and update.....	23
7.3.3 Certificate generation.....	24
7.3.4 Dissemination of Terms and Conditions.....	25
7.3.5 Certificate dissemination	25
7.3.6 Certificate revocation and suspension.....	26

7.4	CA management and operation	27
7.4.1	Security management.....	27
7.4.2	Asset classification and management	28
7.4.3	Personnel security	28
7.4.4	Physical and environmental security.....	29
7.4.5	Operations management	30
7.4.6	System Access Management.....	31
7.4.7	Trustworthy Systems Deployment and Maintenance	32
7.4.8	Business continuity management and incident handling	33
7.4.9	CA termination	33
7.4.10	Compliance with Legal Requirements.....	34
7.4.11	Recording of Information Concerning Qualified Certificates.....	35
7.5	Organizational	36
8	Framework for the definition of other qualified certificate policies	37
8.1	Qualified certificate policy management.....	37
8.2	Exclusions for non public QCPs.....	38
8.3	Additional requirements	38
8.4	Conformance	38
Annex A (informative):	Potential liability in the use of electronic signatures	40
Annex B (informative):	Model PKI disclosure statement.....	43
B.1	Introduction	43
B.2	The PDS structure	43
Annex C (informative):	Electronic signature Directive and qualified certificate policy cross-reference	45
Annex D (informative):	IETF RFC 3647/RFC 2527 and qualified certificate policy cross-reference	46
Annex E (informative):	Revisions made since version 1.2.1	49
E.1	Additional Requirements.....	49
E.2	Update Requirements	49
E.3	Clarifications	49
E.4	Editorial.....	49
E.5	Revisions made since version 1.3.1.....	49
Annex F (informative):	Bibliography.....	50
History	51

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 Specification (TS) 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 measures in order to minimize the operational and financial threats and risks associated with public key crypto systems.

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 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.

The present document applies also to certification authorities that include attributes in qualified certificates. Policy requirements for Attribute Authorities, i.e. for authorities that issue Attribute Certificates, are specified in TS 102 158 [14].

1 Scope

The present document specifies policy requirements relating to Certification Authorities (CAs) issuing qualified certificates (termed certification-service-providers issuing qualified certificates in the Directive [1]). It defines policy requirements on the operation and management practices of certification authorities issuing qualified certificates such that subscribers, subjects certified by the CA and relying parties may have confidence in the applicability of the certificate in support of electronic signatures.

The policy requirements are defined in terms of:

- a) the specification of two closely related qualified certificate policies for qualified certificates issued to the public, one requiring the use of a secure-signature-creation device;
- b) a framework for the definition of other qualified certificate policies enhancing the above policies or for qualified certificates issued to non-public user groups.

The policy requirements relating to the CA include requirements on the provision of services for registration, certificate generation, certificate dissemination, revocation management, revocation status and, if required, signature-creation device provision. Other certification-service-provider functions such as time-stamping, attribute certificates and confidentiality support are outside the scope of the present document. In addition, the present document does not address requirements for certification authority certificates, including certificate hierarchies and cross-certification. The policy requirements are limited to requirements for the certification of keys used for electronic signatures.

These policy requirements are specifically aimed at qualified certificates issued to the public, and used in support of qualified electronic signatures (i.e. electronic signatures that are legally equivalent to hand-written signatures in line with article 5.1 of the European Directive on a community framework for electronic signatures [1]). It specifically addresses the requirements for CAs issuing qualified certificates in accordance with annexes I and II of this Directive [1]. Requirements for the use of secure-signature-creation devices as specified in annex III, which is also a requirement for electronic signatures in line with article 5.1, is an optional element of the policy requirements specified in the present document.

Certificates issued under these policy requirements may be used to authenticate a person who acts on his own behalf or on behalf of the natural person, legal person or entity he represents.

These policy requirements are based around the use of public key cryptography to support electronic signatures.

The present document may be used by competent independent bodies as the basis for confirming that a CA meets the requirements for issuing qualified certificates.

It is recommended that subscribers and relying parties consult the certification practice statement of the issuing CA to obtain further details of precisely how a given certificate policy is implemented by the particular CA.

The present document does not specify how the requirements identified may be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE: See CEN Workshop Agreement 14172 "EESSI Conformity Assessment Guidance".