SLOVENSKI STANDARD
SIST EN 319 411-3 V1.1.1:2013

01-marec-2013

Elektronski podpisi in infrastruktura (ESI) - Zahteve politike in varnosti za ponudnike storitev zaupanja, ki izdajajo digitalna potrdila - 3. del: Zahteve politike za overitelje digitalnih potrdil, ki izdajajo digitalna potrdila javnih ključev

Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 3: Policy requirements for Certification Authorities issuing public key certificates

Ta slovenski standard je istoveten z: **ETSI EN 319 411-3 V1.1.1 (2013-01)**

ICS:

03.080.99	Druge storitve	Other services
35.030	Informacijska varnost	IT Security
35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST EN 319 411-3 V1.1.1:2013 **en**

ETSI EN 319 411-3 V1.1.1 (2013-01)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates

Reference
DEN/ESI-000088

Keywords
e-commerce, electronic signature, Lightweight Certificate Policy, Normalized Certificate Policy, public key, 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/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights 5
Foreword 5
Introduction 5
1 Scope 7
2 References 8
2.1 Normative references 8
2.2 Informative references 8
3 Definitions, abbreviations and notation 9
3.1 Definitions 9
3.2 Abbreviations 10
3.3 Notation 10
4 General concepts 11
4.1 General Policy Requirements Concepts 11
4.2 Certification Authority 11
4.3 Certification services 11
4.4 Certificate policy and certification practice statement 12
4.4.1 Other CA statements 12
4.5 Subscriber and subject 13
5 Introduction to certificate policies 13
5.1 Overview 13
5.2 Identification 14
5.3 User community and applicability 14
5.4 Conformance 14
5.4.1 Conformance claim 14
5.4.2 Conformance requirements 15
6 Obligations, warranties and liability 15
6.1 Certification Authority obligations and warranties 15
6.2 Subscriber obligations 15
6.3 Information for relying parties 16
6.4 Liability 16
7 Requirements on CA practices 16
7.1 Certification practice statement 16
7.2 Public key infrastructure - Key management life cycle 17
7.2.1 Certification Authority key generation 17
7.2.2 Certification Authority key storage, backup and recovery 18
7.2.3 Certification Authority public key distribution 18
7.2.4 Key escrow 19
7.2.5 Certification Authority key usage 19
7.2.6 End of CA key life cycle 19
7.2.7 Life cycle management of cryptographic hardware used to sign certificates 19
7.2.8 CA provided subject key management services 20
7.2.9 Secure user device preparation 20
7.3 Certificate management life cycle 21
7.3.1 Subject registration 21
7.3.2 Certificate renewal and update 23
7.3.3 Certificate generation 23
7.3.4 Dissemination of terms and conditions 24
7.3.5 Certificate dissemination 25
7.3.6 Certificate revocation and suspension 25
7.4 CA management and operation 27
7.4.1 Security management 27

7.4.2 Asset classification and management 27
7.4.3 Personnel security 27
7.4.4 Physical and environmental security 27
7.4.5 Operations management 27
7.4.6 System access management 28
7.4.7 Trustworthy systems deployment and maintenance 29
7.4.8 Business continuity management and incident handling 29
7.4.9 CA termination 30
7.4.10 Compliance with legal requirements 30
7.4.11 Recording of information concerning certificates 30
7.5 Organizational 31

8 Framework for the definition of other certificate policies 31
8.1 Certificate policy management 31
8.2 Additional requirements 32
8.3 Conformance 32

Annex A (informative): Model PKI disclosure statement 34

A.1 Introduction 34

A.2 The PDS structure 35

Annex B (informative): IETF RFC 3647 and present certificate policy document cross reference 36

Annex C (informative): Revisions made since TS 102 042 V2.1.3 38

Annex D (normative): Auditors qualification 39

Annex E (informative): Bibliography 40

History 41

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://ipr.etsi.org).

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 000314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.4].

The present document was previously published as TS 102 042 [i.6].

National transposition dates	
Date of adoption of this EN:	15 January 2013
Date of latest announcement of this EN (doa):	30 April 2013
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 October 2013
Date of withdrawal of any conflicting National Standard (dow):	31 October 2013

Introduction

Electronic commerce, in its broadest sense, 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 and protect the confidentiality of electronic exchanges. This is commonly achieved by using cryptographic mechanisms which are supported by a Trust Service Provider issuing certificates, commonly called a Certification Authority (CA).

For participants of electronic commerce to have confidence in the security of these cryptographic mechanisms 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.

EN 319 401 [10] identifies general policy requirements for Trust Service Providers supporting Electronic Signatures regardless the service they provide. EN 319 411-2 [i.5] provides a baseline for policy requirements for certification authorities issuing qualified certificates in line with the Directive 1999/93/EC [i.1] of the European Parliament and of the Council on a Community framework for electronic signatures (hereinafter referred to as "the Electronic Signature Directive"). The present document is based on the same approach as EN 319 411-2 [i.5] but is applicable to the general requirements of certification in support of cryptographic mechanisms, including other forms of electronic signature as well as the use of cryptography for authentication and encryption. Moreover, where requirements identified have general applicability they are carried forward into the present document. Annex A of the present document identifies significant differences to EN 319 411-2 [i.5] Both documents reference EN 319 401 [10] for the common general requirements.

Article 5.2 of the Electronic Signature Directive states that an electronic signature "*is not denied legal effectiveness … solely on the grounds that …[it is] not based on a qualified certificate …*". Hence, certificates issued by certification authorities operating in accordance with the present document are applicable to electronic signatures as described in article 5.2.

The present document includes options for supporting the same level of quality by certification authorities issuing qualified certificates (as required article 5.1 of the Electronic Signature Directive 1999/93/EC [i.1]) but "normalized" for wider applicability and for ease of alignment with other similar specifications and standards from other sources and institutions. Through such harmonization the quality level set by the Electronic Signature Directive can become embodied in more widely recognized and accepted specifications.

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 Certificate, are specified in TS 102 158 [i.9].

The present document is derived from the requirements specified in TS 102 042 "Policy requirements for certification authorities issuing public key certificates" [i.6]. Policy requirements relating to web server certificates previously covered in later versions of TS 102 042 [i.6] are to be addressed in a separate part of EN 319 411.

1 Scope

The present document specifies policy requirements relating to Trust Service Providers (TSP) issuing public key certificates. It defines policy requirements on the operation and management practices of certification authorities issuing and managing certificates such that subscribers, subjects certified by the TSP and relying parties may have confidence in the applicability of the certificate in support of cryptographic mechanisms.

The policy requirements are defined in terms of three reference certificate policies and a framework from which TSPs can produce a certificate policy targeted at a particular service.

The first reference policy defines a set of requirements for TSPs providing a level of quality the same as that offered by qualified certificates, without being tied to the Electronic Signature Directive (1999/93/EC [i.1]) and without requiring use of a secure user (cryptographic) device. This is labelled the "Normalized" Certificate Policy (NCP). It is anticipated that the NCP may be used as the basis for realizing the quality level set by the Qualified Certificate Policy (as defined in EN 319 411-2 [i.5]) but without the legal constraints of the Electronic Signature Directive (1999/93/EC [i.1]).

In addition to the NCP quality level, the present document specifies two alternative variants of NCP, the requirements of which may be used where alternative levels of service can be justified through risk analysis. The alternatives are referred to as:

- the Lightweight Certificate Policy (LCP) for use where a risk assessment does not justify the additional costs of meeting the more onerous requirements of the NCP (e.g. physical presence);
- the extended Normalized Certificate Policy (NCP+) for use where a secure user device is considered necessary.

Certificates issued under these policies requirements may be used in support of any asymmetric mechanisms requiring certification of public keys including electronic and digital signatures, encryption, key exchange and key agreement mechanisms.

The present document may be used by competent independent bodies as the basis for confirming that a CA provides a reliable service in line with recognized practices.

Subscribers and relying parties should consult the certificate policy and certification practice statement of the issuing TSP to obtain details of the requirements addressed by its certificate policy and how the certificate policy is implemented by the particular TSP.

The policy requirements relating to the TSP include requirements on the provision of services for registration, certificate generation, certificate dissemination, revocation management, revocation status and if required, secure subject device provision. Support for other trusted third party functions such as time-stamping and attribute certificates 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 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 TS 119 403 [i.2] for guidance on assessment of TSP processes and services against the present document. The present document references EN 319 401 [10] for policy general requirements common to all classes of TSP service.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] FIPS PUB 140-1: "Security Requirements for Cryptographic Modules".

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

[3] ISO/IEC 15408 (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".

[4] CEN Workshop Agreement 14167-2 (2004): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)".

[5] CEN Workshop Agreement 14167-3 (2004): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)".

[6] CEN Workshop Agreement 14167-4 (2004): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile (CMCSO PP)".

NOTE: CEN Workshop Agreement 14167 is currently under revision to become the basis of a European Norm in CEN TC 224.

[7] ISO/IEC 9594-8/ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[8] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[9] ISO/IEC 17021: "Conformity assessment - Requirements for bodies providing audit and certification of management systems".

[10] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting electronic signatures".

[11] ISO/IEC 19790: "Information technology - Security techniques - Security requirements for cryptographic modules".

[12] CENELEC EN 45011: "General requirements for bodies operating product certification systems".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.2] ETSI TS 119 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General requirements and guidance".

[i.3] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.4] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: Overview".

[i.5] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates ".

[i.6] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[i.7] ISO/IEC 27002 (2005): "Information technology - Security techniques - Code of practice for information security management".

[i.8] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[i.9] ETSI TS 102 158: "Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates".

[i.10] CEN Workshop Agreement 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".

[i.11] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

3 Definitions, abbreviations and notation

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 319 401 [10] and the following apply:

attribute: information bound 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

certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the Certification Authority which issued it

Certificate Policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

NOTE: This is a specific type of TSP Policy as specified in EN 319 401 [10].

Certificate Revocation List (CRL): signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

NOTE: See ITU-T Recommendation X.509 [7].

Certification Authority (CA): authority trusted by one or more users to create and assign certificates

NOTE: See clause 4.2 for further explanation of the concept of Certification Authority.

Certification Practice Statement (CPS): statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates

NOTE: See RFC 3647 [i.3].

Lightweight Certificate Policy (LCP): certificate policy which offers a quality of service less onerous than the qualified certificate policy

NOTE: The qualified certificate policy is as defined in EN 319 411-2 [i.5].

Normalized Certificate Policy (NCP): certificate policy which offers a quality of service equivalent to the qualified certificate policy

NOTE: The qualified certificate policy is as defined in EN 319 411-2 [i.5].

Public-key certificate (PKC): public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the CA which issued it

NOTE: See ITU-T Recommendation X.509-200811 [7].

relying party: recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate

NOTE: See RFC 3647 [i.3].

secure user device: device which holds the user's private key, protects this key against compromise and performs cryptographic functions on behalf of the user

subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

subscriber: entity subscribing with a Certification Authority on behalf of one or more subjects

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in EN 319 401 [10] and the following apply:

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service provider

NOTE: The more general term Trust Service Provider is used in preference to CSP in the present document except in relation to external references.

EAL	Evaluation Assurance Level
LCP	Lightweight Certificate Policy
MLA	Multilateral Agreement
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
PDS	PKI Disclosure Statement
PIN	Personal Identifier Number
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
RA	Registration Authority

3.3 Notation

The requirements identified in the present document include:

a) mandatory requirements strictly to be followed in order to conform to the present document. Such requirements are indicated by clauses without any additional marking;

b) requirements strictly to be followed if applicable to the services offered under the applicable certificate policy. Such requirements are indicated by clauses marked by "[CONDITIONAL]";

c) requirements that include several choices which ought to be selected depending on the quality of the service offered under the applicable certificate policy. Such requirements are indicated by markings by "[CHOICE]" with a subsequent indicator relating to the relative quality:

- "[LCP]", "[NCP]", "[NCP+]"

4 General concepts

4.1 General Policy Requirements Concepts

The concepts described in EN 319 401 [10] clause 4 apply.

4.2 Certification Authority

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates is called the Certification Authority. The Certification Authority has overall responsibility for the provision of the certification services identified in clause 4.3. The Certification Authority is identified in the certificate as the issuer and its private key is used to sign certificates.

A Certification Authority is a Trust Service Provider, as described in EN 319 401 [10], and also a form of certification service provider as defined in the Electronic Signatures Directive 1999/93/EC [i.1], which issues public key certificates.

4.3 Certification services

The service of issuing certificates is broken down in the present document into the following component services for the purposes of classifying requirements:

- **Registration service:** verifies the identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service.
- **Certificate generation service:** creates and signs certificates based on the identity and other attributes verified by the registration service.
- **Dissemination service:** disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the TSP's terms and conditions, and any published policy and practice information, to subscribers and relying parties.
- **Revocation management service:** processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.
- **Revocation status service:** provides certificate revocation status information to relying parties. This may be based upon certificate revocation lists or a real time service which provides status information on an individual basis. The status information may be updated on a regular basis and hence may not reflect the current status of the certificate.

And optionally:

- **Subject device provision service:** prepares, and provides or makes available signature-creation devices, or other secure user device, to subjects.

NOTE: Examples of this service are:

- a service which generates the subject's key pair and distributes the private key to the subject;
- a service which prepares the subject's signature-creation module and enabling codes and distributes the module to the registered subject.

This subdivision of services is only for the purposes of clarification of policy requirements and places no restrictions on any subdivision of an implementation of the CA services.