ETSI TS 102 042 V2.4.1 (2013-02)

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

Reference
RTS/ESI-0002042version241

Keywords
e-commerce, electronic signature,
extended validation certificat, public key, security,
SSL/TLS certificates

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

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://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 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, 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 certification-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.

TS 101 456 [15] 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 TS 101 456 [15] 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 TS 101 456 [15].

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 [13].

Due to recent and increasingly sophisticated attacks on websites, e.g. via spoofing and DNS servers "poisoning", the CA/Browser Forum - CAB Forum - (http://www.cabforum.org/) released the EV Certificate Guidelines (EVCG [16]), and the Baseline Requirements for the issuance and management of publicly-trusted certificates (BRG [19]).

ETSI - Electronic Signature and Infrastructure (ESI) - includes in the present document provisions consistent with the requirements for issuing Extended Validation Certificates (EVC), as specified in the above mentioned CAB Forum EVC Guidelines (EVCG [16]) as well as Publicly trusted TLS/SSL certificates, as specified in the mentioned CAB Forum PTC guidelines (BRG [19]) As a consequence, EVC and PTC issued by CAs operating in compliance with the EVC and PTC related provisions as indicated in the present document can be assessed as meeting the requirements specified by the CAB Forum in their EVCG [16] and BRG [19] plus recognised good practice for CA's issuing certificates.

1 Scope

The present document specifies policy requirements relating to Certification Authorities (CAs) issuing public key certificates, including Extended Validation Certificates (EVC) and Publicly trusted TLS/SSL certificates (PTC). It defines policy requirements on the operation and management practices of certification authorities issuing and managing certificates such that subscribers, subjects certified by the CA 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 six reference certificate policies and a framework from which CAs can produce a certificate policy targeted at a particular service.

The first reference policy defines a set of requirements for CAs 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 (signing or decrypting) 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 TS 101 456 [15]) 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 six 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 (signing or decrypting) is considered necessary;
- the Extended Validation Certificates Policy (EVCP) for use with code signing or TLS/SSL where provisions, additional to those indicated in NCP, are required to issue EVCs, consistently with what is specified in the EV Certificates Guidelines [16] issued by the CAB Forum;
- the enhanced Extended Validation Certificates Policy (EVCP+) for use with code signing or TLS/SSL where, in addition to the requirements to issue EVCs, a secure user device (signing or decrypting) is considered necessary;
- the Domain Validation Certificates Policy (DVCP) for use with TLS/SSL where provisions, additional to those indicated in NCP, are required to issue DVCs, consistently with what is specified in the BRG [19] issued by the CAB Forum;
- the Organizational Validation Certificates Policy (OVCP) for use with TLS/SSL where provisions, additional to those indicated in NCP, are required to issue OVCs, consistently with what is specified in the BRG [19] issued by the CAB Forum.

NOTE 1: TLS/SSL is used to denote access to web based services protected using the Transport Layer Security (TLS) protocol [i.4] or earlier equivalent Secure Socket Layer (SSL) protocol.

EVCP and EVCP+ are based on NCP and NCP+ respectively, therefore, except where explicitly specified, all the relevant NCP and NCP+ requirements apply in addition to those specifically required for EVC.

DVCP and OVCP are based on NCP as well, so except where explicitly specified, all the relevant NCP requirements apply in addition to those specifically required for DVC and/or OVC.

Applicability of these certificates is specified by clause 5.3.

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. As far as it regards to EVC and DVC/OVC it can be used by:

- Auditors, operating in a European framework for evaluation of Certification Authorities, to evaluate whether these Certification Authorities meet the requirements for issuing EVC and/or DVC/OVC as Specified in the CAB Forum EV Certificate Guidelines [16] and/or the BRG [19] respectively.

- Certification Authorities, operating under the previous versions of this Technical Specification, that intend to adapt their policies and practices to issuing EVC and/or DVC/OVC.
- Certification Authorities planning to issue EVC and/or DVC/OVC within a context that fits European standard practices for CAs.

It is recommended that subscribers and relying parties consult the certificate policy and certification practice statement of the issuing CA to obtain details of the requirements addressed by its certificate policy and how the certificate policy is implemented by the particular CA.

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, 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, except where explicitly specified in the cases of EVCP and/or EVCP+ and DVCP/OVCP.

Consistently with EVCG [16] and BRG [19], within the clauses of the present document related to issuing certificates the keyword "SHOULD" has the meaning specified in RFC 2119 [18] that indicates that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications are understood and carefully weighed before choosing a different course.

If an implementation of the present document is to be certified conformant through assessment by an independent auditor, annex E states requirements to ensure proper qualification of that auditor.

NOTE 2: See TS 119 403 [i.2] for guidance on assessment of CA processes and services against the present document.

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

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

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

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

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

NOTE: This document is currently under revision.

[6] 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".

NOTE: This document is currently under revision.

[7] 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".

NOTE: This document is currently under revision

[8] 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: This document is currently under revision.

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

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

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

NOTE: ISO/IEC 17799 (2005) was re-numbered as ISO/IEC 27002 on 2007-07-01.

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

NOTE: Obsoletes IETF RFC 2527 [i.3].

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

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

[15] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[16] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates" version 1.3.

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

[18] IETF RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels".

[19] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

[20] CA/Browser Forum: "Network and Certificate System Security Requirements".

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 2527: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.4] IETF RFC 5246: "The Transport Layer Security Protocol Version 1.2".

[i.5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.6] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[i.7] ISO 27006: "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".

[i.8] ISO 27001: "Information technology - Security techniques - Information security management systems - Requirements".

3 Definitions, abbreviations and notation

3.1 Definitions

For the purposes of the present document, the following terms and definitions 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: 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: See clause 4.3 for explanation of the relative role of certificate policies and certification practice statement.

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

NOTE: See Recommendation ITU-T X.509 [9].

certification authority: authority trusted by one or more users to create and assign certificates

NOTE: See clause 4.1 for further explanation of the concept of certification authority.

certification practice statement: statement of the practices which a certification authority employs in issuing managing, revoking, and renewing or re-keying certificates

NOTE: See RFC 3647 [12].

code signing certificate: certificate used for signing code in order to secure it

Domain Validation Certificate (DVC): certificate which has no validated organizational identity information for the subject. It only identifies the subject by its domain name

Domain Validation Certificate Policy (DVCP): NCP enhanced incorporating requirements of the BRG [19] as applicable to domain validated certificates

electronic signature: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data

EV certificate: See Extended Validation certificate.

extended normalized certificate policy: normalized certificate policy requiring use of a secure user device

Extended Validation Certificate (EVC): certificate that is issued and maintained in compliance with the Extended Validation Certificate Policy or the enhanced Extended Validation Certificate

Extended Validation Certificate Policy (EVCP): NCP enhanced to incorporate requirements in EVCG [16]

Enhanced Extended Validation Certificate (EVCP+): EVCP requiring use of a secure user device

high security zone: physical location where a CA's private key or cryptographic hardware is located

lightweight certificate policy: certificate policy which offers a quality of service less onerous than the qualified certificate policy as defined in TS 101 456 [15]

normalized certificate policy: certificate policy which offers a quality of service equivalent to the qualified certificate policy as defined in TS 101 456 [15]

Organizational Validation Certificate (OVC): certificate that includes validated organizational identity information for the subject

Organizational Validation Certificate Policy (OVCP): NCP enhanced to incorporate requirements in BRG [19] as applicable to organizational validated certificates

Publicly-trusted certificate (PTC): certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software

Publicly-trusted certificate – Baseline Requirements (PTC-BR): publicly trusted certificates incorporating the requirements in BRG [19]

NOTE: This includes policy requirements relating to OVCP and DVCP.

qualified certificate: certificate which meets the requirements laid down in annex I of the Directive 1999/93/EC [i.1] and is provided by a certification-service-provider who fulfils the requirements laid down in annex II of the Directive 1999/93/EC [i.1]

qualified certificate policy: certificate policy suited to issuance and maintenance of Qualified Certificates

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 [12].

secure user device: device which holds the user's private key, protects this key against compromise and performs signing or decryption 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

NOTE: The subject may be a subscriber acting on its own behalf.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BRG	Baseline Requirements Guidelines
CA	Certification Authority
CAB	CA/Browser
CABF	CA/Browser Forum
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DNS	Domain Name System
DVC	Domain Validation Certificate
DVCP	Domain Validation Certificate Policy
EAL	Evaluation Assurance Level
EVC	Extended Validation Certificate

EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
EVCP+	enhanced Extended Validation Certificate Policy
IT	Information Technology
LCP	Lightweight Certificate Policy
MLA	Master Licence Agreement
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
NCPetc	All variants of NCP
NetSec-CAB	Network Security Requirements- CA/Browser Forum
OCSP	Online Certificate Status Protocol
OVC	Organizational Validation Certificate
OVCP	Organizational Validation Certificate Policy
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructure
PTC	Publicly-Trusted Certificate

NOTE: Within the context of the present document PTC is used synonymously with DVC and OVC.

PTC-BR	Publicly-Trusted Certificate- Baseline Requirements

NOTE: Within the context of the present document PTC-BR is used synonymously with DVCP and OVCP.

QCP	Qualified Certificate Policy
RA	Registration Authority
TLS/SSL	Transport Layer Security/Secure Socket Layer protocol

NOTE: RFC 5246 [i.4] or earlier equivalent Secure Socket Layer protocol.

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]"; and where relevant an identifier for the applicable certificate policy as follows:

- "[LCP]", "[NCP]", "[NCP+]", "[EVCP]", "[EVCP+]", "[PTC-BR]";
- PTC-BR is used to denote requirements applicable to OVCP and DVCP;
- [NCPetc] is used to indicated NCP and all the policies derived from NCP: i.e. [NCP+]", "[EVCP]", "[EVCP+]", "[PTC-BR]".

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+]", "[NCPetc], "[EVCP]", "[EVCP+]","[PTC-BR]", "[DVCP]" "[OVCP]":

- PTC-BR is used to denote requirements applicable to OVCP and DVCP;
- [NCPetc] is used to indicated NCP and all the policies derived from NCP: i.e. [NCP+]", "[EVCP]", "[EVCP+]", "[PTC-BR]".

d) text copied from EVCG [16] and BRG [19] is italicised.

4 General concepts

4.1 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 4.2. The certification authority is identified in the certificate as the issuer and its private key is used to sign certificates.

The certification authority may make use of other parties to provide parts of the certification service. However, the certification authority always maintains overall responsibility and ensures that the policy requirements identified in the present document are met. For example, a certification authority may sub-contract all the component services, including the certificate generation service. However, the key used to sign the certificates is identified as belonging to the CA, and the CA maintains overall responsibility for meeting the requirements defined in the present document.

A certification authority is a certification-service-provider, as defined in the Electronic Signatures Directive 1999/93/EC [i.1] which issues public key certificates.

4.2 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 CA'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:

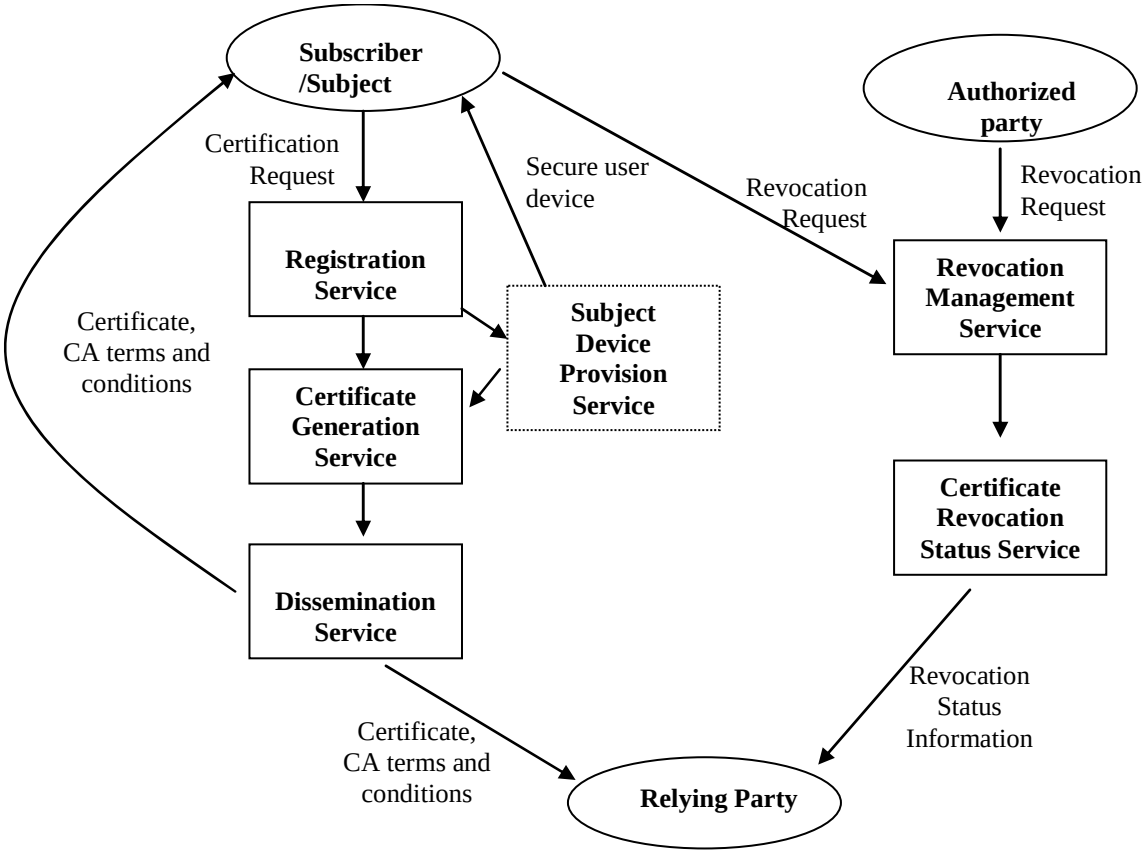
- **Subject device provision service:** prepares and provides signature-creation devices, or other secure user device, to subjects.

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.

Figure 1 illustrates the interrelationship between the services.



NOTE: Figure 1 is for illustrative purposes. Clause 7 specifies the specific requirements for each of the services.

Figure 1: Illustration of subdivision of certification services used in the present document

4.3 Certificate policy and certification practice statement

This clause explains the relative roles of certificate policy and certification practice statement. It places no restriction on the form of a certificate policy or certification practice statement specification.

4.3.1 Purpose

In general, the purpose of the certificate policy, referenced by a policy identifier in a certificate, states "what is to be adhered to", while a certification practice statement states "how it is adhered to", i.e. the processes it will use in creating and maintaining the certificate. The relationship between the certificate policy and certification practice statement is similar in nature to the relationship of other business policies which state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out.

If any changes are made to a certificate policy which affects the applicability then the policy identifier should be changed.

4.3.2 Level of specificity

A certificate policy is a higher level document than a certification practice statement; it may apply to a community to which more Cas belong that abide by the common set of rules specified in that CP. A certification practice statement defines how one specific certification authority meets the technical, organizational and procedural requirements identified in a certificate policy.

NOTE: Even lower-level documents may be appropriate for a CA detailing the specific procedures necessary to complete the practices identified in the certification practice statement. This lower-level documentation is generally regarded as internal operational procedure documents, which may define specific tasks and responsibilities within an organization. While this lower-level documentation may be used in the daily operation of the CA and reviewed by those doing a process review, due to its internal nature this level of documentation is considered private and proprietary and therefore beyond the scope of the present document. For example, the policy may require secure management of the private key(s), the practices may describe the dual-control, secure storage practices, while the operational procedures may describe the detailed procedures with locations, access lists and access procedures.

4.3.3 Approach

The approach of a certificate policy is significantly different from a certification practice statement. A certificate policy is defined independently of the specific details of the specific operating environment of a certification authority, whereas a certification practice statement is tailored to the organizational structure, operating procedures, facilities, and computing environment of a certification authority. A certificate policy may be defined by the users of certification services, whereas the certification practice statement is always defined by the provider.

4.3.4 Other CA statements

In addition to the policy and practice statements a CA may issue terms and conditions. Such a statement of terms and conditions is broad category of terms to cover the broad range of commercial terms or PKI specific, etc. Terms that are not necessarily communicated to the customer, they may, nevertheless apply in the situation.

The PKI disclosure statement is that part of the CA's terms and conditions which relate to the operation of the PKI and which it is considered that the CA ought to disclose to both subscribers and relying parties.

4.4 Subscriber and subject

In some cases certificates are issued directly to individuals for their own use. However, there commonly exist other situations where the party requiring a certificate is different from subject to whom the certificate applies. For example, a company may require certificates for its employees to allow them to participate in electronic business on behalf of the company, or a computer system may perform automated commerce on behalf of the owner organization. In such situations the entity subscribing to the certification authority for the issuance of certificates is different from the entity which is the subject of the certificate. Another common example is the case of server certificates, where the certificate is required for a computer system acting on behalf of the owner organization.

In the present document to clarify the requirements which are applicable to the two different roles that may occur two different terms are used for the "subscriber" who contracts with the certification authority for the issuance of certificates and the "subject" to whom the certificate applies. The subscriber bears responsibility towards the CA for the use of the private key associated with the public key certificate but the subject is the individual entity that is authenticated by the private key and that has control over its use.

In the case of certificates issued to individuals for their own use the subscriber and subject can be the same entity. In other cases, such as certificates issued to employees or computer systems as mentioned above, the subscriber and subject are different. The subscriber would be, for example, the employer or owner organization. The subject would be the employee or computer system.

Within the present document we use these two terms with this explicit distinction wherever it is meaningful to do so, although in some cases the distinction is not always crystal clear.

5 Introduction to certificate policies

5.1 Overview

A certificate policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" [9].

The policy requirements are defined in the present document in terms of certificate policies. Certificates issued in accordance with the present document include a certificate policy identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application. The present document specifies seven certificate policies:

1) A Normalized Certificate Policy (NCP) which offers the same quality as that offered by the Qualified Certificate Policy (QCP) as defined in TS 101 456 [15] but without the legal constraints implied by the Electronic Signature Directive (1999/93/EC) [i.1] and without requiring the use of a Secure Signature Creation Device.

NOTE 1: The certificate policy NCP is particularly suited to the support of Advanced Electronic Signatures, as defined by the Electronic Signature Directive (1999/93/EC) [i.1], for legal entities if they use physical means to provide reasonable confidence that the signing key remains under their sole control.

2) An extended Normalized Certificate Policy (NCP+) which offers the same quality as that offered by the Qualified Certificate Policy (QCP) as defined in TS 101 456 [15] but without the legal constraints implied by the Electronic Signature Directive (1999/93/EC) [i.1] and, instead of requiring the use of a Secure Signature Creation, requires the use of a secure user device.

NOTE 2: The certificate policy NCP+ is particularly suited to the support of Advanced Electronic Signatures, as defined by the Electronic Signature Directive (1999/93/EC) [i.1], for human beings as well as legal entities since the use of a secure user device provides confidence that the signing key remains under the sole control of the signatory.

3) A Lightweight Certificate Policy (LCP) which incorporates less demanding policy requirements.

4) An Extended Validation Certificate Policy (EVCP) that includes, except where explicitly indicated, all the Normalized Certificate Policy (NCP) requirements, plus additional provisions suited to support EVC issue, usage and maintenance as specified in EVCG [16], section 7.1.2.

5) An enhanced Extended Validation Certificate Policy (EVCP+) that includes, except where explicitly indicated, all the extended Normalized Certificate Policy (NCP+) requirements, enhanced with additional provisions suited to support EVC issue, usage and maintenance as specified in EVCG [16], section 7.1.2 when the EVCs owner shall operate make use of a secure device.

6) A Domain Validation Certificate Policy (DVCP): NCP enhanced incorporating requirements of the BRG [19] as applicable to domain validation certificates.

7) An Organizational Validation Certificate Policy (OVCP): NCP enhanced incorporating requirements in BRG [19] as applicable to organizational validation certificates.

Clause 8 specifies a framework for other certificate policies which enhance or further constrain the above policies.

5.2 Identification

The identifiers for the certificate policies specified in the present document are:

a) NCP: Normalized Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) ncp (1)
```

b) NCP+: Normalized Certificate Policy requiring a secure user device

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) ncpplus (2)
```

c) LCP: Lightweight Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) lcp (3)
```

d) EVCP: Extended Validation Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) evcp (4)
```

e) EVCP+: Extended Validation Certificate Policy requiring a secure user device

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) evcpplus (5)
```

f) DVCP: Domain Validation Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) dvcp (6)
```

g) OVCP: Organizational Validation Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0)
other-certificate-policies(2042)
policy-identifiers(1) ovcp (7)
```

By including one of these object identifiers in a certificate the CA claims conformance to the identified certificate policy.

NOTE: Either Cas own OIDs and/or ETSI OIDs and/or CAB OIDs as indicated in EVCG [16] for d) and e), and BRG [19] for f) and g) can be used.

5.3 User community and applicability

The policies NCP, NCP+ and LCP defined in the present document place no constraints on the user community and applicability of the certificate. The applicability of other certificates is as described below.

5.3.1 EV Certificates

The specific purpose of EV Certificates is clarified in EVCG [16], section 6 "Basic Concepts of the EV Certificate" that states:

*"6.1 **Purpose of EV Certificate:** EV Certificates are intended for establishing Web-based data communication conduits via TLS/SSL protocols and for verifying the authenticity of executable code*

6.1.1 Primary Purposes:

(1) Identify the legal entity that controls a website

(2) Enable encrypted communications with a website

(3) Identify the source of executable code

6.1.2 Secondary Purposes: *… to help establish the legitimacy of a business claiming to operate a website or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware and other forms of online identity fraud.*

6.1.3 Excluded Purposes: *EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behaviour of the Subject."*

Additionally, EVCG [16] Appendix G "Code-signing: Introduction (Informative) – 1. Purpose" states:

> ***"Purpose of EV Code Signing Certificates".*** *EV Code Signing Certificates are intended to be used to verify the identity of a holder of an EV code signing certificate (Subscriber) and the integrity of its code. They provide assurance to a user or platform provider that code verified with the certificate has not been modified from its original form and is distributed by the legal entity identified in the EV Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information.*
>
> *EV Code Signing Certificates may help to establish the legitimacy of signed code, help to maintain the trustworthiness of software platforms, help users to make informed software choices, and limit the spread of malware.*
>
> *No particular software object is identified by an EV Code-Signing Certificate, only its distributor is identified."*

5.3.2 Publicly Trusted Certificates-Baseline Requirements

The purpose of PTC is clarified in BRG [19], section 2 that states:

"The primary goal of these Requirements is to enable efficient and secure electronic communication, while addressing user concerns about the trustworthiness of Certificates. The Requirements also serve to inform users and help them to make informed decisions when relying on Certificates."

Certificates issued under PTC-BR are aimed at for publicly trusted certificates used to identify web servers accessed via the TLS or SSL protocol.

5.4 Conformance

5.4.1 Conformance claim

The CA shall only claim conformance to the present document as applied in the certificate policy (or policies) identified in the certificate that it issues if:

a) It either claims conformance to the identified certificate policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance.

NOTE 1: This evidence can be, for example, a report from an auditor confirming that the CA conforms to the requirements of the identified policy. The auditor may be internal to the CA organization but should have no hierarchical relationship with the department operating the CA.

b) It has a current assessment of conformance to the identified certificate policy by a competent independent party. The results of the assessment shall be made available to subscribers and relying parties on request.

NOTE 2: This assessment should be carried out by a competent independent auditor. See TS 119 403 [i.2] and BRG [19] section 17

NOTE 3: Cas may issue certificates for internal and testing purposes provided that such certificates are not made available to for any other uses.

c) If the CA is later shown to be non-conformant in a way that significantly affects the ability of the CA to meet the objectives identified in the present document, then it shall cease issuing certificates using the identifiers in clause 5.2 until it has demonstrated or been assessed as conformant, otherwise the CA shall take steps to remedy the non-conformance within a reasonable period.

NOTE 4: Even if a CA is known to be critically non-conformant, it may issue certificates for internal and testing purposes provided that such certificates are not made available to for any other uses.

d) The CA compliance shall be checked on a regular basis and whenever major change is made to the CA operations.

e) [EVCP], [EVCP+] and [PTC-BR]: The CA and its Root CA before issuing EVC and/or PTC shall successfully and respectively complete a point-in-time readiness assessment audit against the present document for the primary certification of the CA (readiness) and a period-in-time assessment has to be stated with the supervisory audit at least every year.

5.4.2 Conformance requirements

A conformant CA shall demonstrate that:

a) it meets its obligations as defined in clause 6.1;

b) it has implemented controls which meet the requirements, including options applicable to the implemented policies, as specified in clause 7.

6 Obligations, warranties and liability

6.1 Certification authority obligations and warranties

The CA shall ensure that all requirements on CA, as detailed in clause 7, are implemented as applicable to the selected certificate policy (see clauses 5.4.2 and 8.3).

The CA has the responsibility for conformance with the procedures prescribed in this policy, even when the CA functionality is undertaken by sub-contractors.

The CA shall provide all its certification services consistent with its certification practice statement.

6.2 Subscriber obligations

The CA shall oblige through agreement (see clause 7.3.1 m)) the subscriber to address all the following obligations. If the subject and subscriber are separate entities, the subscriber shall make the subject aware of those obligations applicable to the subject (as listed below):

a) accurate and complete information is submitted to the CA in accordance with the requirements of this policy, particularly with regards to registration;

b) the key pair is only used in accordance with any limitations notified to the subscriber (see clause 7.3.4);

c) reasonable care is exercised to avoid unauthorized use of the subject's private key;

d) [CONDITIONAL] if the subscriber or subject generates the subject's keys:

   i) subject keys are generated using an algorithm recognized by industry as being fit for the uses of the certified key as identified in the certificate policy;

   ii) a key length and algorithm is used which is recognized as being fit for the uses of the certified key as identified in the certificate policy during the validity time of the certificate.

NOTE 1: See TS 102 176-1 [14] giving guidance on algorithms and their parameters.

e) [CONDITIONAL] if the subscriber or subject generates the subject's keys and the private key is for creating electronic signatures the subject's private key can be maintained under the subject's sole control;

f) [NCP+] only use the subject's private key for signing or decrypting with the secure user device;

g) [NCP+] [CONDITIONAL] if the subject's keys are generated under control of the subscriber or subject, generate the subject's keys within the secure user device used for signing or decrypting;

h) notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

   i) the subject's private key has been lost, stolen, potentially compromised; or

ii) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or

iii) inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject.

i) following compromise, the use of the subject's private key is immediately and permanently discontinued;

j) in the case of being informed that the CA which issued the subject's certificate has been compromised, ensure that the certificate is not used by the subject.

NOTE 2: Where [EVCP] or [EVCP+] is involved, additional guidance is provided in EVCG [16], namely from section 9.3 and from appendix A. For EV code signing certificates, appendixes G and H apply.

NOTE 3: Where [PTC-BR] is involved, additional guidance is provided in BRG [19], section 10.3 and Appendix A.

6.3 Information for relying parties

The terms and conditions made available to relying parties (see clause 7.3.4) shall include a notice that if it is to reasonably rely upon a certificate, it shall:

a) verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party (see clause 7.3.4); and

NOTE 1: Depending on CA's practices and the mechanism used to provide revocation status information, there may be a delay of up to 1 day in disseminating revocation status information. Where [EVCP] or [EVCP+] is involved, please refer to clause 7.3.6), item h), iii).

NOTE 2: Where [PTC-BR] is involved, please refer to clause 7.3.6 item h) iv).

b) take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions supplied as required in clause 7.3.4; and

c) take any other precautions prescribed in agreements or elsewhere.

NOTE 3: Depending on CA's practices related to the problem reporting and response capability, where [EVCP] or [EVCP+] is involved, refer to section 11.3 of EVCG [16].

NOTE 4: Depending on CA's practices related to the problem reporting and response capability, where [PTC-BR] is involved, refer to section 13.1.2 of BRG [19].

6.4 Liability

The CA shall specify any disclaimers or limitations of liability in accordance with applicable laws.

Where [EVCP] or [EVCP+] is involved, please refer to section 7.1.3 of EVCG [16].

Where [PTC-BR] is involved, please refer to section 18 of BRG [19].

7 Requirements on CA practice

The CA shall implement the controls that meet the following requirements.

The present document includes the provision of services for registration, certificate generation, dissemination, revocation management and revocation status (see clause 4.2). Where requirements relate to a specific service area of the CA then it is listed under one of these subheadings. Where no service area is listed, or "CA General" is indicated, a requirement is relevant to the general operation of the CA.

These policy requirements are not meant to imply any restrictions on charging for CA services.

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objective will be met.

NOTE: The details of controls required to meet an objective is a balance between achieving the necessary confidence whilst minimizing the restrictions on the techniques that a CA may employ in issuing certificates. In case of clause 7.4 (CA management and operation) reference is made to other more general standards which may be used as a source of more detailed control requirements. Due to these factors the specificity of the requirements given under a given topic may vary.

7.1 Certification practice statement

The CA shall have a statement of the practices and procedures.

NOTE 1: This policy makes no requirement as to the structure of the certification practice statement.

In particular:

a) The CA's certification practice statement shall address all the requirements identified in the applicable certificate policy.

b) [EVCP] and [EVCP+]: The CA's certification practice statement shall include the item 1 and item 3 from sections 7.1.2 and 15.1 of EVCG [16].

c) The CA's certification practice statement shall identify the obligations of all external organizations supporting the CA services including the applicable policies and practices.

d) The CA shall make available its certification practice statement, and other relevant documentation, as necessary to assess conformance to the certificate policy:

   1) to subscribers and relying parties;

   2) [EVCP] and [EVCP+]: EVCG [16], section 6.2.1 item 1 c);

   3) [PTC-BR]: BRG [19], section 8.2.2.

NOTE 2: The CA is not generally required to make all the details of its practices public.

e) The CA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of the certificate as specified in clause 7.3.4.

f) The CA shall have a high level management body with final authority and responsibility for approving the certification practice statement.

g) The senior management of the CA is responsible for ensuring that the certification practices established to meet the applicable requirements specified in the present document are properly implemented.

h) The CA shall define a review process for certification practices including responsibilities for maintaining the certification practice statement.

i) The CA shall give due notice of changes it intends to make in its certification practice statement and shall, following approval as in e) above, make the revised certification practice statement immediately available as required under c) above.

j) The CA shall document the algorithms and parameters employed.

k) [EVCP] and [EVCP+]: The CA SHALL address the provisions specified in EVCG [16], sections 7.1.3 and 15.2.

l) [PTC-BR]: The CA SHALL address the provisions specified in BRG [19], sections 8.2.1, 8.2.2 and 8.3.

7.2 Public key infrastructure – Key management life cycle

7.2.1 Certification authority key generation

Certificate generation

The CA shall ensure that CA keys are generated in controlled circumstances.

In particular:

a) Certification authority key generation shall be undertaken in a physically secured environment (see clause 7.4.4) by personnel in trusted roles (see clause 7.4.3) under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

b) [CHOICE]:

[LCP] CA key generation shall be carried out in a product, application or device which ensures that the keys are generated in a trustworthy manner and do not compromise the security of the private key and which:

i) meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 2 or higher; or

ii) is a trustworthy system which is assured to EAL 3 or higher in accordance to ISO/IEC 15408 [4], or equivalent security criteria.

[NCPetc] CA key generation shall be carried out within a device which either:

iii) meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 3 or higher; or

iv) meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [6], CWA 14167-3 [7] or CWA 14167-4 [8]

NOTE 1: These CWAs will be replaced as specified in clause 2.1.

v) is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [4], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

NOTE 2: The rules of clause 7.2.2 b) to e) apply also to key generation even if carried out in a separate system.

c) Certification authority key generation shall be performed using an algorithm recognized by industry as being fit for the CA's signing purposes.

d) The selected key length and algorithm for CA signing key shall be one which is recognized by industry as being fit for the CA's signing purposes.

[EVCP] and [EVCP+]: EVCG [16] appendix A (1) and (2) also apply.

[PTC-BR]: BRG [19] Appendix A (1) and (2) apply.

NOTE 3: See TS 102 176-1 [14] giving guidance on algorithms and their parameters. EVCG [16] appendix A or BRG [19] Appendix A will prevail in case of conflict for EVC or PTC respectively.

e) A suitable time before expiration of its CA signing key (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this policy.

NOTE 4: In order to meet this requirement these operations need to be performed timely enough to allow all parties that have relationships with the CA (subjects, subscribers, relying parties, higher level Cas, etc.) to be timely aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a CA which will cease its operations before its own certificate-signing certificate expiration date.

f) [EVCP] and [EVCP+]: EVCG [16], section 14.1.5 applies. In case of EV code signing certificates Appendix H of EVCG [16] applies.

g) [PTC-BR]: BRG [19], section 17.7 applies.

7.2.2 Certification authority key storage, backup and recovery

Certificate generation

The CA shall ensure that CA private keys remain confidential and maintain their integrity.

In particular:

a) [CHOICE]:

[LCP] The CA private signing key shall be held and used in a product, application or device which does not compromise the security of the private key and which:

i) meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3], level 2 or higher; or

ii) is a trustworthy system which is assured to EAL 3 or higher in accordance to ISO/IEC 15408 [4]; or equivalent security criteria.

[NCPetc] The CA private signing key shall be held and used within a secure cryptographic device which:

iii) meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 3 or higher; or

iv) meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [6], CWA 14167-3 [7], CWA 14167-4 [8]

NOTE 1: These CWAs will be replaced as specified in clause 2.1.

v) is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [4], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

b) [CHOICE]:

[LCP] When outside the signature-creation product, application or device, the secrecy of the CA's private key shall be ensured.

NOTE 2: This may be achieved using physical security or encryption.

[NCPetc] When outside the signature-creation device (see a) above) the CA private signing key shall be protected in a way that ensures the same level of protection as provided by the signature creation device.

c) The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 7.4.4). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

d) Backup copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

e) Where the keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module.

7.2.3 Certification authority public key distribution

Certificate generation and certificate distribution

The CA shall ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties.

In particular:

a) CA signature verification (public) keys shall be made available to relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.

NOTE: For example, certification authority public keys may be distributed in certificates signed by itself, along with a declaration that the key authenticates the CA, or issued by another CA. By itself a self signed certificate cannot be known to come from the CA. Additional measures, such as checking the fingerprint of the certificate against information provided by a trusted source, is needed to give assurance of the correctness of this certificate.

7.2.4 Key escrow

a) [CONDITIONAL] If the subject's key is to be used for electronic signatures with the meaning of Directive 1999/93/EC [i.1], then the CA shall not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow).

b) [CONDITIONAL] If a copy of the subject's key is kept by the CA then the CA shall ensure that the private key is kept secret and only made available to appropriately authorized persons.

7.2.5 Certification authority key usage

The CA shall ensure that CA private signing keys are not used inappropriately.

In particular:

Certificate generation

a) CA signing key(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 purpose.

b) The certificate signing keys shall only be used within physically secure premises.

7.2.6 End of CA key life cycle

The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle.

In particular:

Certificate generation

a) The use of the corresponding CA's private key, shall be limited to that compatible with the hash algorithm, the signature algorithm and signature key length used in the generating certificates, in line with current practice as in clause 7.2.1 d).

b) All copies of the CA private signing keys shall be destroyed or put beyond use at the end of their life cycle.

7.2.7 Life cycle management of cryptographic hardware used to sign certificates

This clause is not applicable to LCP.

[NCPetc]: The CA shall ensure the security of cryptographic device throughout its lifecycle.

Certificate generation

[NCPetc]: In particular the CA shall ensure that:

a) Certificate and revocation status information signing cryptographic hardware is not tampered with during shipment.

b) Certificate and revocation status information signing cryptographic hardware is not tampered with while stored.

c) The installation, activation, back-up and recovery of the CA's signing keys in cryptographic hardware shall require simultaneous control of at least of two trusted employees.

d) Certificate and revocation status information signing cryptographic hardware is functioning correctly.

e) CA private signing keys stored on CA cryptographic hardware are destroyed upon device retirement. This destruction does not affect all copies of the private key. Only the physical instance of the key stored in the cryptographic hardware under consideration will be destroyed.

7.2.8 CA provided subject key management services

The CA shall ensure that any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured.

Certificate generation

[CONDITIONAL] If the CA generates the subject's keys:

a) CA-generated subject keys shall be generated using an algorithm recognized by industry as being fit for the uses identified in the certificate policy during the validity time of the certificate.

b) CA-generated subject keys shall be of a key length and for use with a public key algorithm which are recognized by industry as being fit for the purposes stated in the certificate policy during the validity time of the certificate:

   i) [EVCP] or [EVCP+]: guidance SHALL be taken from the EVCG [16], appendix A but SHALL not override a) and b).

   ii) [PTC-BR]: guidance SHALL be taken from Appendix A of BRG [19] but SHALL not override a) and b).

c) CA-generated subject keys shall be generated and stored securely before delivery to the subject.

d) The subject's private key shall be delivered to the subject in a manner such that the secrecy and integrity of the key is not compromised.

   i) [PTC-BR]: requirements from BRG [19], section 10.2.4 applies.

e) [CONDITIONAL] If a copy of the subject's private key is not required to be kept by the CA, or other authorized entity, (see clause 7.2.4), once delivered to the subject, the private key can be maintained under the subject's sole control. Any copies of the subject's private key held by the CA shall be destroyed.

7.2.9 Secure user device preparation

[NCP+] and [EVCP+]: The CA shall ensure that if it issues to the subject secure user device this is carried out securely.

In case of an EV code signing certificate follow indications of Appendix H, item 10 of EVCG [16].

Subject device provision

[CONDITIONAL]: In particular, if the CA issues a secure user device:

a) Secure user device preparation shall be securely controlled by the service provider.

b) Secure user device shall be securely stored and distributed.

c) Secure user device deactivation and reactivation shall be securely controlled.

d) Where the secure user device has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the signature-creation module.

NOTE: Separation may be achieved by ensuring distribution of activation data and delivery of secure signature creation device at different times, or via a different route.

7.3 Public key infrastructure – Certificate management life cycle

7.3.1 Subject registration

The CA shall ensure that evidence of subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.

In particular:

Registration

a) Before entering into a contractual relationship with a subscriber, the CA shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 7.3.4.

b) [CONDITIONAL]: If the subject is a person and not the same as the subscriber, the subject shall be informed of his/her obligations.

c) The CA shall communicate this information through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.

NOTE 1: A model PKI disclosure statement which may be used as the basis of such a communication is given in annex B.

d) The service provider shall collect either direct evidence, or an attestation from an appropriate and authorized source, of the identity (e.g. name) and, if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the subject's identity shall be at time of registration by appropriate means and in accordance with national law.

[EVCP] and [EVCP+]: Guidance on Information Verification requirements SHALL be taken from the EVCG [16], section 10.

[PTC-BR]: Guidance on verification practices SHALL be taken from BRG [19], section 11.

e) [CHOICE]:

- [LCP] No requirement.
- [NCPetc] If the subject is a physical person evidence of the subject's identity (e.g. name) shall be checked against a physical person either directly or shall have been checked indirectly using means which provides equivalent assurance to physical presence (see note 2). Evidence for verifying other entities shall involve procedures which provide the same degree of assurance.

NOTE 2: An example of evidence checked indirectly against a physical person is documentation presented for registration which was acquired as the result of an application requiring physical presence.

f) [CONDITIONAL] If the subject is a physical person, evidence shall be provided of:

i) full name (including surname and given names consistent with the applicable law and national identification practices);

ii) date and place of birth, reference to a nationally recognized identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

NOTE 3: It is recommended that the place be given in accordance to national conventions for registering births.

g) [CONDITIONAL] If the subject is a physical person who is identified in association with a legal person, or organizational entity (e.g. the subscriber), evidence shall be provided of:

i) full name (including surname and given names, consistently with the applicable law and national identification practices) of the subject;

ii) date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name;

iii) full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber);

iv) any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;

v) evidence that the subject is associated with the legal person or other organizational entity.

h) [CONDITIONAL] If the subject is an organizational entity, evidence shall be provided:

i) of full name of the organizational entity (private organization, government entity or non-commercial entity);

[EVCP] and [EVCP+]: Guidance on Information Verification requirements SHALL be taken from the EVCG [16], sections 10.2 to 10.6;

[OVC]: Requirements from section 11.2 of BRG [19] applies;

ii) of reference to a nationally recognized registration, or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name.

NOTE 4: This provision MAY be also enforced when registering subjects related to non EV certificates.

i) [CONDITIONAL] If the subject is a device or system operated by or on behalf of an organizational entity, evidence shall be provided of:

i) identifier of the device by which it may be referenced (e.g. Internet domain name);

[EVCP] and [EVCP+]: Domain verification requirements SHALL be taken from the EVCG [16], section 10.6;

[PTC-BR]: Requirements from section 11.1 of BRG [19] apply;

ii) full name of the organizational entity;

[EVCP] and [EVCP+]:Requirements from sections 10.2 to 10.6 of EVCG [16] apply;

[OVC]: Requirements from section 11.2 of BRG [19] apply;

iii) a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name.

j) The CA shall record all the information necessary to verify the subject's identity and, if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.

k) If an entity other than the subject is subscribing to the CA services (i.e. the subscriber and subject are separate entities – see clause 4.4) then evidence shall be provided that the subscriber is authorized to act for the subject as identified (e.g. is authorized for all members of the identified organization).

[EVCP] and [EVCP+]: Guidance on roles SHALL be taken from the EVCG [16], section 10.7.

[PTC-BR]: Requirements from sections 11.2.1 and 11.2.2 of BRG [19] apply.

l) The subscriber shall provide a physical address, or other attributes, which describe how the subscriber may be contacted.

[EVCP] and [EVCP+]: Guidance on Verification of the applicant's location should be taken from the EVCG [16], section 10.4.

[PTC-BR]: Requirement from section 11.2.1 of BRG [19] applies.

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

i) agreement to the subscriber's obligations (see clause 6.2);

ii) if required by the CA, agreement by the subscriber to user secure user device;

iii) consent to the keeping of a record by the CA of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clause 7.4.11), the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the CA terminating its services;

iv) whether, and under what conditions, the subscriber requires and the subject consents to the publication of the certificate;

v) confirmation that the information held in the certificate is correct.

NOTE 5: The subscriber may agree to different aspects of this agreement during different stages of registration. For example, agreement that the information held in the certificate is correct may be carried out subsequent to other aspects of the agreement.

NOTE 6: This agreement may be in electronic form.

vi) [EVCP] and [EVCP+]: Guidance on Verification of the signatures and of the approval of EV request SHALL be taken from the EVCG [16], sections 10.8 and 10.9;

vii) [PTC-BR]: Requirements from section 10.3.2 of BRG [19] apply;

n) The records identified above shall be retained for the period of time as indicated to the subscriber (see c) above) and as necessary for the purposes for providing evidence of certification in legal proceedings.

i) [EVCP] and [EVCP+]: Requirement from EVCG [16], section 13.2.2 applies.

ii) [PTC-BR]: Requirement from BRG [19], section 15.3.2 applies.

NOTE 7: The factors that need to be taken into account in identifying "applicable law" are:

i) the law of the country where the CA is established should always be considered;

ii) where subjects are registered through a registration authority in another country to where the CA is established then that RA should also apply its own country's regulations;

iii) where some subscribers are also in another country then contractual and other legal requirements applicable to those subscribers should also be taken into account.

o) [CONDITIONAL] If the subject's key pair is not generated by the CA, the certificate request process shall ensure that the subject has possession of the private key associated with the public key presented for certification.

p) The CA shall ensure that the requirements of the applicable national data protection legislation are adhered to (including the use of pseudonyms if applicable) within their registration process.

q) The CA's verification policy shall only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

r) [EVCP] and [EVCP+]: the CA shall abide by EVCG [16] requirements in section 10.11.1.The Acceptable methods of verifications are specified in EVCG [16] requirements in section 10.11.2.

s) [EVCP] and [EVCP+] : For a dual control procedure follow EVCG [16], section 12.1.3.

t) [EVCP] and [EVCP+]: The subscriber shall satisfy the requirements stated in EVCG [16], section 7.2.

u) [EVCP] and [EVCP+]: Certificate requests shall obtain the information from the subscriber as specified in EVCG [16], section 9.2.

v) [PTC-BR]: Requirements from sections 10.1, 10.2, 11.3, 11.4, 11.5 and 11.6 of BRG [19] apply.

w) [EVCP] and [EVCP+]: Requirements from section 6.2.1 item 1) and 2) of EVCG [16] apply.

x) [PTC-BR]: Requirements from section 7.1 of BRG [19] apply.

7.3.2 Certificate renewal, rekey and update

The CA shall ensure that requests for certificates issued to a subject who has previously been registered with the same CA are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes.

NOTE: The subscriber may, if the CA offers this service, request a certificate renewal for example where relevant attributes presented in the certificate have changed or when the certificate is nearing expiry.

In particular:

Registration

a) The CA shall check the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject are still valid.

b) If any of the CA terms and conditions have changed, these shall be communicated to the subscriber and agreed to in accordance with clause 7.3.1 a), b), c) and m).

c) If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information is verified, recorded, agreed to by the subscriber in accordance with clause 7.3.1 d) to l).

d) The CA shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised.

7.3.3 Certificate generation

The CA shall ensure that it issues certificates securely to maintain their authenticity.

In particular:

Certificate generation

a) The certificates shall include, in accordance with X.509 [9] and RFC 5280 [17]:

   i) identification of the CA (certification-service-provider) and the country in which it is established;

   ii) the name of the subject, or a pseudonym which shall be identified as such;

   iii) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

   iv) the public key which corresponds to the private key under the control of the subject;

   v) an indication of the beginning and end of the period of validity of the certificate;

   vi) the serial number of the certificate;

   vii) the electronic signature of the certification authority issuing it;

   viii) limitations on the scope of use of the certificate, if applicable; and

   ix) limits on the value of transactions for which the certificate can be used, if applicable;

   x) [EVCP] and [EVCP+]: Requirements in clauses 8.1 and 8.2 of EVCG [16] on certificate content and on policy identification shall be applied. Guidance on Validity period SHALL be taken from the EVCG [16], section 8.3. In the case of EV certificate for SSL/TSL EVCG [16], appendix B applies. In case of an EV code signing certificate Appendix H of EVCG [16] applies.

   xi) [PTC-BR]: Requirements in section 9 of BRG [19] on certificate content and profile shall be applied. Appendix B of BRG [19] for certificate extensions shall also be applied.

b) The CA shall take measures against forgery of certificates, and, in cases where the CA generates the subjects' private key, guarantee confidentiality during the process of generating such data.

c) The procedure of issuing the certificate is securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject-generated public key.

d) [CONDITIONAL] if the CA generated the subject's key:

   i) the procedure of issuing the certificate is securely linked to the generation of the key pair by the CA;

   ii) [LCP], [NCPetc] the private key is securely passed to the registered subject;

   iii) [NCP+] the secure user device containing the subject's private key is securely passed to the registered subject.

e) The CA shall ensure that over the life time of the CA a distinguished name which has been used in a certificate by it is never re-assigned to another entity.

f) The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed CA system components.

g) The CA shall verify that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are used.

h) The CA shall verify that the certificate issuance by the root CA requires and individual authorized by the CA personnel management procedure:

   i) [PTC-BR]: Requirement of BRG [19], section 12 applies.

7.3.4 Dissemination of terms and conditions

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties.

In particular:

a) The CA shall make available to subscribers and relying parties the terms and conditions regarding the use of the certificate:

   i) the certificate policy being applied, including a clear statement as to whether the policy is for certificates issued to the public and whether the policy requires the use of any particular product, application or device for the purposes of applying the key-pair associated with the certificate being issued;

   ii) any limitations on its use;

   iii) the subscriber's obligations as defined in clause 6.2, including whether the policy requires the use of any particular product, application or device for the purposes of applying the key-pair associated with the certificate being issued;

   iv) information on how to validate the certificate, including requirements to check the revocation status of the certificate, such that the relying party is considered to "reasonably rely" on the certificate (see clause 6.3);

   v) any limitations of liability, including the purposes/uses for which the CA accepts (or excludes) liability;

   vi) the period of time which registration information (see clause 7.3.1) is retained;

   vii) the period of time which CA event logs (see clause 7.4.11) are retained;

   viii) procedures for complaints and dispute settlement;

   ix) the applicable legal system; and

   x) if the CA has been assessed to be conformant with the identified certificate policy, and if so through which scheme.

b) The information identified in a) above shall be available through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.

NOTE 1: A model PKI disclosure statement which may be used as the basis of such a communication is given in annex B. Alternatively this communication may be provided as part of a subscriber/relying party agreement. These terms and conditions may be included in a certification practice statement provided that they are conspicuous to the reader.

NOTE 2: Regarding contractual terms and conditions for certificates issued to the public attention is drawn to requirements of consumer legislation including implementation of Directive 93/13/EEC [i.6] on unfair terms in consumer contracts.

7.3.5 Certificate dissemination

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties.

In particular:

Dissemination

a) Upon generation, the complete and accurate certificate shall be available to the subscriber or subject for whom the certificate is being issued.

b) Certificates are available for retrieval in only those cases for which the subject's consent has been obtained.

c) The CA shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 7.3.4).

d) The applicable terms and conditions shall be readily identifiable for a given certificate.

e) [CHOICE]:

i) [LCP] the information identified in b) and c) above shall be available as specified in the CA's Certification Practice Statement;

ii) [NCPetc] the information identified in b) and c) above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CA, the CA shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement.

f) [CONDITIONAL] If the CA is issuing certificate to the public the information identified in b) and c) above shall be publicly and internationally available.

7.3.6 Certificate revocation and suspension

The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests.

In particular:

Revocation management

a) The CA shall document as part of its certification practice statement (see clause 7.1) the procedures for revocation of certificates including:

i) who may submit revocation reports and requests;

ii) how they may be submitted;

iii) any requirements for subsequent confirmation of revocation reports and requests;

NOTE 1: For example, a confirmation may be required from the subscriber if a compromise is reported by a third party.

iv) whether and for what reasons certificates may be suspended;

v) the mechanism used for distributing revocation status information;

vi) the maximum delay between receipt of a revocation request or report and the change to revocation status information being available to all relying parties.
This shall be at most [CHOICE]:

- [LCP] 72 hours;
- [NCPetc] 24 hours.

b) Requests and reports relating to revocation (e.g. due to compromise of subject's private key, death of the subject, unexpected termination of a subscriber's or subject's agreement or business functions, violation of contractual obligations) shall be processed on receipt:

i) [EVCP] and [EVCP+]: Requirement from EVCG [16], sections 9.3.2 (5) and 9.3.3 (5) apply;

ii) [PTC-BR]: Requirement from BRG [19], section 10.3.2 (5) apply.

c) [EVCP] and [EVCP+]: Requirement from EVCG [16], sections 11.2.1 and 11.3.3 apply. For [PTC-BR], requirements from sections 13.1 and 13.1.4 of BRG [19] apply.

d) Requests and reports relating to revocation shall be authenticated, checked to be from an authorized source. Such reports and requests will be confirmed as required under the CA's practices.

e) A certificate's revocation status may be set to "suspended" whilst the revocation is being confirmed. The CA shall ensure that a certificate is not kept suspended for longer than is necessary to confirm its status.

NOTE 2: Support for certificate suspension is optional.

f) The subject, and where applicable the subscriber, of a revoked or suspended certificate, shall be informed of the change of status of the certificate.

g) Once a certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.

h) [CHOICE]:

   i) [LCP] Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least every 72 hours;

   ii) [NCPetc] Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least every 24 hours;

   iii) [EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.1, item 1) and item 2);

   iv) [PTC-BR]: Requirement from BRG [19], section 13.2;

i) Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used as the sole means of providing revocation status information:

   i) every CRL shall state a time for next scheduled CRL issue; and

   ii) a new CRL may be published before the stated time of the next CRL issue;

   iii) the CRL shall be signed by the certification authority or an authority designated by the CA.

NOTE 3: In order to maximize interoperability it is recommended that the CA issue Certificate Revocation Lists as defined in Recommendation ITU-T X.509 [9].

Revocation status

j) [CHOICE]:

   i) [LCP] Revocation status information shall be available as specified in the CA's Certification Practice Statement;

   ii) [NCPetc] Revocation status information, shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement;

   iii) [EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.1 applies;

   iv) [PTC-BR]: Requirements from section 13.2 of BRG [19] apply.

NOTE 4: Revocation status information may be provided, for example, using on-line certificate status service or through distribution of CRLs through a repository.

k) [EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.1.

l) [EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.2.

m) Response time requirement:

   i) [EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.3 applies;

   ii) [PTC-BR]: Requirement from BRG [19], section 13.2.3 applies.

n) The integrity and authenticity of the status information shall be protected.

o) [CONDITIONAL] If the CA is issuing certificates to the public, Revocation status information shall be publicly and internationally available.

p) Revocation status information shall include information on the status of certificates at least until the certificate expires.

q) If the code signing is supported, in case of an EV code signing certificate, the CA should follow the revocation procedures indicated in Appendix H item 13 of EVCG [16].

7.4 CA management and operation

Requirements from NetSec-CAB [20] apply.

7.4.1 Security management

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.

In particular:

CA General

a) The CA shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis shall be regularly reviewed and revised if necessary.

   i) [EVCP] and [EVCP+]: Requirement from EVCG [16], section 13.3.2 applies;

   ii) [PTC-BR]: Requirement from BRG [19], section 16.2 applies.

b) The CA shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the CA and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the CA. The CA shall retain responsibility for the disclosure of relevant practices of all parties.

c) The CA management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the CA's information security policy and ensuring publication and communication of the policy to all employees who are impacted by the policy.

d) The CA shall have a system or systems for quality and information security management appropriate for the certification services it is providing.

e) The information security infrastructure necessary to manage the security within the CA shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the CA management forum.

NOTE 1: See ISO/IEC 27002 [11] for guidance on information security management including information security infrastructure, management information security forum and information security policies.

f) The security controls and operating procedures for CA facilities, systems and information assets providing the certification services shall be documented, implemented and maintained.

NOTE 2: It is recommended that this documentation (commonly called a system security policy) identifies all relevant targets, objects and potential threats related to the services provided and the safeguards required to avoid or limit the effects of those threats. It is recommended that the documentation describes the rules, directives and procedures regarding how the specified services and the associated security assurance are granted in addition to stating policy on incidents and disasters.

g) The CA shall ensure that the security of information shall be maintained when the responsibility for CA functions has been outsourced to another organization or entity.

h) [EVCP] and [EVCP+]: Requirements of EVCG [16], section 13.3 shall also be taken into account.

i) [PTC-BR]: Requirements of sections 14.2 and 16 of BRG [19] shall be taken into consideration.

7.4.2 Asset classification and management

The CA shall ensure that its assets and information receive an appropriate level of protection.

In particular:

CA General

a) The CA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

7.4.3 Personnel security

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations.

In particular:

CA General

a) The CA shall employ a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.

NOTE 1: CA personnel may fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two.

i) [EVCP] and [EVCP+]: section 12.1.1 of EVCG [16] applies;

ii) [PTC-BR]: section 14.1.2 of BRG [19] applies.

b) Appropriate disciplinary sanctions shall be applied to personnel violating CA policies or procedure.

c) Security roles and responsibilities, as specified in the CA's security policy, shall be documented in job descriptions. Trusted roles, on which the security of the CA's operation is dependent, shall be clearly identified.

d) CA personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Where appropriate, these shall differentiate between general functions and CA specific functions.

NOTE 2: Job descriptions may include skills and experience requirements.

e) Personnel shall exercise administrative and management procedures and processes that are in line with the CA's information security management procedures (see clause 7.4.1).

NOTE 3: See ISO/IEC 27002 [11] for guidance.

Registration, certificate generation, subject device provision, revocation management

f) Managerial personnel shall be employed who possess experience or training in the electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

g) All CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations.

h) Trusted roles include roles that involve the following responsibilities:

i) Security Officers: overall responsibility for administering the implementation of the security practices. Additionally approve the generation/revocation/suspension of certificates;

ii) System Administrators: authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation, subject device provision and revocation management;

iii) System Operators: responsible for operating the CA trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery;

iv) System Auditors: authorized to view archives and audit logs of the CA trustworthy systems.

i) CA personnel shall be formally appointed to trusted roles by senior management responsible for security.

j) The CA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.

i) In some countries it may not be possible for CA to obtain information on past convictions. Where this is allowed, it is recommended that the employer asks the candidate to provide such information and turn down an application in case of refusal;

ii) Where [EVCP] and [EVCP+] are involved, section 12.1.1 (2) (D) of EVCG [16] applies.

k) [EVCP] and [EVCP+]: this applies to EVCG [16], sections 12.1.2 and 12.1.3.

l) [PTC-BR]: requirement of section 14.1 of BRG [19] applies.

7.4.4 Physical and environmental security

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized.

In particular:

CA General

a) Physical access to facilities concerned with certificate generation, subject device preparation, and revocation management services shall be limited to properly authorized individuals.

b) Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities. And,

c) Controls shall be implemented to avoid compromise or theft of information and information processing facilities.

Certificate generation, subject device provision (in particular preparation) and revocation management

d) The facilities concerned with certificate generation, subject device preparation (see clause 7.2.9) and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

e) Any persons entering this physically secure area shall not be left for any significant period without oversight by an authorized person.

f) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation, subject device preparation (see clause 7.2.9) and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.

g) 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 preparation (see clause 7.2.9) and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc.

h) Controls shall be implemented to protect against equipment, information, media and software relating to the CA services being taken off-site without authorization.

NOTE 1: See ISO/IEC 27002 [11] for guidance on physical and environmental security.

NOTE 2: Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

i) [EVCP] and [EVCP+]: EVCG [16], section 13.3.3 applies.

j) [PTC-BR]: Requirement of section 16.5 of BRG [19] applies.

7.4.5 Operations management

The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure.

In particular:

CA General

a) The integrity of CA systems and information shall be protected against viruses, malicious and unauthorized software.

b) Damage from security incidents and malfunctions shall be minimized through the use of incident reporting and response procedures.

c) Media used within the CA shall be securely handled to protect media from damage, theft and unauthorized access.

NOTE 1: Every member of personnel with management responsibilities is responsible for planning and effectively implementing the certificate policy and associated practices as documented in the certification practice statement.

d) Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

e) Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of certification services.

f) [PTC-BR]: Requirements of section 16.5 of BRG [19] applies.

Media handling and security

g) All media shall be handled securely in accordance with requirements of the information classification scheme (see clause 7.4.2). Media containing sensitive data shall be securely disposed of when no longer required.

System planning

h) [CHOICE]:

  i) [LCP] no requirement;

  ii) [NCPetc] capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Incident reporting and response

i) The CA shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.

j) Audit processes, meeting requirements specified in clause 7.4.11, shall be invoked at system start up, and cease only at system shutdown.

k) Audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity.

  i) [EVCP] and [EVCP+]: Requirement from EVCG [16], sections 11.2 and 11.3.3 apply;

  ii) [PTC-BR]: Requirement from BRG [19], section 15.2 applies.

Certificate generation, revocation management

Operations procedures and responsibilities

l) CA security operations shall be separated from normal operations.

NOTE 2: CA security operations' responsibilities include:

i) operational procedures and responsibilities;

ii) secure systems planning and acceptance;

iii) protection from malicious software;

iv) housekeeping;

v) network management;

vi) active monitoring of audit journals, event analysis and follow-up;

vii) media handling and security;

viii) data and software exchange.

These responsibilities will be managed by CA security operations, but, may actually be performed by non-specialist, operational personnel (under supervision); as defined within the appropriate security policy, and, roles and responsibility documents.

7.4.6 System access management

The CA shall ensure that CA system access is limited to properly authorized individuals.

In particular:

CA General

a) Controls (e.g. firewalls) shall be implemented to protect the CA's internal network domains from external network domains accessible by third parties.

NOTE 1: Firewalls may be configured to prevent protocols and accesses not required for the operation of the CA.

b) Sensitive data shall be protected against unauthorized access or modification. Sensitive data shall be protected (e.g. using encryption and an integrity mechanism) when exchanged over networks which are not secure.

NOTE 2: Sensitive data includes registration information.

c) The CA shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access.

d) The CA shall ensure access to information and application system functions are restricted in accordance with the access control policy and that the CA system provides sufficient computer security controls for the separation of trusted roles identified in CA's practices, including the separation of security administrator and operation functions. Particularly, use of system utility programs is restricted and tightly controlled. Access shall be restricted only allowing access to resources as necessary for carrying out the role(s) allocated to a user.

e) CA personnel shall be successfully identified and authenticated before using critical applications related to certificate management.

f) CA personnel shall be accountable for their activities, for example by retaining event logs (see clause 7.4.11):

i) [EVCP] and [EVCP+]: Requirement from section 13.2.1 of EVCG [16] applies.

g) Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

NOTE 3: Sensitive data includes registration information.

h) [EVCP] and [EVCP+]: EVCG [16], section 13.1 item C applies.

Certificate generation

i) The CA shall ensure that local network components (e.g. routers) are kept in a physically secure environment and their configurations periodically audited for compliance with the requirements specified by the CA.

j) Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

NOTE 4: This may use, for example, an intrusion detection system, access control monitoring and alarm facilities.

Dissemination

k) Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.

Revocation management

l) Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

NOTE 5: This may used, for example, an intrusion detection system, access control monitoring and alarm facilities.

Revocation status

m) Revocation status application shall enforce access control on attempts to modify revocation status information.

7.4.7 Trustworthy systems deployment and maintenance

The CA shall use trustworthy systems and products that are protected against modification.

NOTE 1: Requirements for the trustworthy systems may be ensured using, for example, systems conforming to CWA 14167-1 [5] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [4].

NOTE 2: It is recommended that the risk analysis carried out on the CA's services (see clause 7.1) identifies its critical services requiring trustworthy systems and the levels of assurance required.

In particular:

CA General

a) An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the CA or on behalf of the CA to ensure that security is built into IT systems.

b) Change control procedures exist for releases, modifications and emergency software fixes for any operational software.

7.4.8 Business continuity management and incident handling

The CA shall ensure in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible.

NOTE 1: Other disaster situations include failure of critical components of a CA system, including hardware and software.

In particular:

CA General

a) The CA shall define and maintain a continuity plan to enact in case of a disaster.

CA systems data back up and recovery

b) CA systems data necessary to resume CA operations shall be backed up and stored in safe places suitable to allow the CA to timely go back to operations in case of incident/disasters.

NOTE 2: ISO/IEC 27002 [11], clause 10.5.1: Information back-up.

c) Back up and restore functions shall be performed by the relevant trusted roles specified in clause 7.4.3.

NOTE 3: If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.

CA key compromise

d) The CA's business continuity plan (or disaster recovery plan) shall address the compromise or suspected compromise of a CA's private signing key as a disaster and the planned processes shall be in place.

e) Following a disaster the CA shall, where practical, take steps to avoid repetition of a disaster.

Revocation status

f) In the case of compromise the CA shall as a minimum provide the following undertakings:

   i) inform the following of the compromise: all subscribers and other entities with which the CA has agreements or other form of established relations, among which relying parties and Cas. In addition, this information shall be made available to other relying parties;

   ii) indicate that certificates and revocation status information issued using this CA key may no longer be valid.

NOTE 4: It is recommended that when a CA is informed of the compromise of another CA, any CA certificate that it has issued for the compromised CA is revoked.

Algorithm compromise

g) Should any of the algorithms, or associated parameters, used by the CA or its subscribers become insufficient for its remaining intended usage then the CA shall:

   i) inform all subscribers and relying parties with whom the CA has agreement or other form of established relations. In addition, this information shall be made available to other relying parties;

   ii) revoke any affected certificate.

7.4.9 CA termination

The CA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

In particular:

CA General

a) Before the CA terminates its services the following procedures shall be executed as a minimum:

   i) the CA shall inform the following of the termination: all subscribers and other entities with which the CA has agreements or other form of established relations, among which relying parties and CA. In addition, this information shall be made available to other relying parties;

   ii) the CA shall terminate all authorization of subcontractors to act on behalf of the CA in the performance of any functions related to the process of issuing certificates;

   iii) the CA shall perform necessary undertakings to transfer obligations for maintaining registration information (see clause 7.3.1), revocation status information (see clause 7.3.6) and event log archives (see clause 7.4.11) for their respective period of time as indicated to the subscriber and relying party (see clause 7.3.4);

   iv) the CA shall destroy, or withdraw from use, its private keys, as defined in clause 7.2.6.

NOTE: The CA is not required to have a prior relationship with the relying party.

b) The CA shall have an arrangement to cover the costs to fulfil these minimum requirements in case the CA becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

c) The CA shall state in its practices the provisions made for termination of service. This shall include:

   i) the notification of affected entities;

   ii) the transfer of its obligations to other parties;

   iii) the handling of the revocation status for unexpired certificates that have been issued.

7.4.10 Compliance with legal requirements

The CA shall ensure compliance with legal requirements.

In particular:

CA General

a) CA shall ensure it meets all applicable statutory requirements (including such as requirements of the Data Protection Directive [i.5] – see next item) for protecting records from loss, destruction and falsification. Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clause 7.4.11).

b) The CA shall ensure that the requirements of applicable data protection legislation as the European Data Protection Directive [i.5], as implemented through national legislation, are met.

NOTE: European Data Protection [i.5] issues specific to this policy are addressed in:

   i) Registration (including use of pseudonyms) (see clause 7.3.1);

   ii) Confidentiality of records (see clauses 7.4.11 a) and 7.3.3 f));

   iii) Protecting access to personal information (see clause 7.4.6);

   iv) User consent (see clause 7.3.1 m)).

c) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

d) The information that users contribute to the CA shall be completely protected from disclosure without the user's agreement, a court order or other legal authorization.

7.4.11 Recording of information concerning certificates

The CA shall ensure that all relevant information concerning a certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

NOTE 1: Records concerning certificates include registration information (see clause 7.3.1) and information concerning significant CA environmental, key management and certificate management events.

In particular:

General

a) The confidentiality and integrity of current and archived records concerning certificates shall be maintained.

b) Records concerning certificates shall be completely and confidentially archived in accordance with disclosed business practices.

c) Records concerning certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. The subject, and within the constraints of data protection requirements (see clause 7.4.10) the subscriber, shall have access to registration and other information relating to the subject.

NOTE 2: This may be used, for example, to support the link between the certificate and the subject.

d) The precise time of significant CA environmental, key management and certificate management events shall be recorded.

NOTE 3: It is recommended that the CA states in its practices the accuracy of the clock used in timing of events, and how this accuracy is ensured.

e) Records concerning certificates shall be held for a period of time as indicated in the CA's terms and conditions (see clause 7.3.4) in accordance with applicable legislation.

   i) [EVCP] and [EVCP+]: Requirements from EVCG [16], sections 13.2.1 and 13.2.2 apply;

   ii) [PTC-BR]: Requirements from BRG [19], section 15.3 applies.

f) The events shall be logged in a way that they cannot be easily deleted or destroyed (except for transfer to long-term media) within the period of time that they are required to be held.

NOTE 4: This may be achieved, for example, through the use of write only media, a record of each removable media used and the use of off site backup.

g) The specific events and data to be logged shall be documented by the CA.

   i) [EVCP] and [EVCP+]: Requirements from EVCG [16], sections 13.1 applies;

   ii) [PTC-BR]: Requirements from BRG [19], section 15.1 and 15.2 apply.

Registration

h) The CA shall ensure all events relating to registration including requests for certificate re-key or renewal, are logged.

i) The CA shall ensure that all registration information including the following is recorded:

   i) type of document(s) presented by the applicant to support registration;

ii) record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents, if applicable;

iii) storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.3.1 m));

iv) any specific choices in the subscriber agreement (e.g. consent to publication of certificate) see clause 7.3.1 m);

v) identity of entity accepting the application;

vi) method used to validate identification documents, if any;

vii) name of receiving CA and/or submitting Registration Authority, if applicable.

j) The CA shall ensure that privacy of subject information is maintained.

Certificate generation

k) The CA shall log all events relating to the life-cycle of CA keys.

l) The CA shall log all events relating to the life-cycle of certificates.

Subject device provision

m) The CA shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA.

n) If applicable, the CA shall log all events relating to the preparation of secure user devices.

Revocation management

o) The CA shall ensure that all requests and reports relating to revocation, as well as the resulting action, are logged.

7.5 Organizational

The CA shall ensure that its organization is reliable.

In particular that:

CA general

a) Policies and procedures under which the CA operates shall be non-discriminatory.

b) The CA shall make its services accessible to all applicants whose activities fall within its declared field of operation.

c) The CA is a legal entity according to national law.

d) The CA has adequate arrangements to cover liabilities arising from its operations and/or activities.

e) The CA has the financial stability and resources required to operate in conformity with this policy.

f) The CA has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of electronic trust services or any other related matters.

g) The CA has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

Certificate generation, revocation management

h) The parts of the CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies; in particular its senior executive, senior staff and staff in trusted roles, shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

i) The parts of the CA concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

7.6 Additional requirements

7.6.1 Additional testing

The CA shall provide different options to allow third parties to check and test their certificates.

[PTC-BR]: Requirements from BRG [19], appendix C applies.

7.6.2 Cross certificates

The CA shall disclose all cross certificates that identify the CA as the subject.

[PTC-BR]: Requirements from BRG [19] section 8.4 applies.

8 Framework for the definition of other certificate policies

This clause provides a general framework for other policies for Cas issuing public key certificates. A CA may claim conformance to this general framework as defined in clause 8.3. In general terms this requires conformance to the requirements in clauses 6 and 7 excluding those applicable only to Cas issuing certificates to the public.

8.1 Certificate policy management

The authority issuing the certificate policy shall ensure that the certificate policy is effective.

In particular:

a) The certificate policy shall identify which of the certificate policies defined in the present document it adopts as the basis, plus any variances it chooses to apply.

b) There shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the certificate policy.

c) A risk assessment shall be carried out to evaluate business requirements and determine the security requirements to be included in the certificate policy for the stated community and applicability.

d) Certificate policy(s) shall be approved and modified in accordance with a defined review process, including responsibilities for maintaining the certificate policy.

e) A defined review process shall exist to ensure that the certificate policy is supported by the CA's Certification Practice Statement.

f) The CA shall make available the certificate policies supported by the CA to its user community.

NOTE: The CA's user community includes the subscribers/subjects eligible to hold certificates issued under the policy and any parties which may require relying upon those certificates.

g) Revisions to certificate policies supported by the CA shall be made available to subscribers and relying parties.

h) The certificate policy shall incorporate, or further constrain, all the requirements identified in clauses 6 and 7.

i) A unique object identifier shall be obtained for the certificate policy of the form required in Recommendation ITU-T X.509 [9].

8.2 Additional requirements

Subscribers and relying parties shall be informed, as part of implementing the requirements defined in clause 7.3.4, of the ways in which the specific policy adds to or further constrains the requirements of the certificate policy as defined in the present document.

[EVCP] and [EVCP+]: for code signing services Appendix J of EVCG [16] applies.

8.3 Conformance

The CA shall only claim conformance to the present document and the applicable certificate policy:

a) if the CA claims conformance to the identified certificate policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or

NOTE 1: This evidence can be, for example, a report from an auditor confirming that the CA conforms to the requirements of the identified policy. The auditor may be internal to the CA organization but should have no hierarchical relationship with the department operating the CA.

b) if the CA has a current assessment of conformance to the identified certificate policy by an independent party. The results of the assessment shall be made available to subscribers and relying parties on request;

c) if the CA is later shown to be non-conformant in a way that significantly affects the ability of the CA to meet the objectives identified in the present document, it shall cease issuing certificates using its certificate policy identifier until it has demonstrated or been assessed as conformant, otherwise the CA shall take steps to remedy the non-conformance within a reasonable period;

NOTE 2: Even if a CA is known to be critically non-conformant, it may issue certificates for internal and testing purposes provided that such certificates are not made available to for any other uses.

d) the CA compliance shall be checked on a regular basis and whenever major change is made to the CA operations.

A conformant CA shall demonstrate that:

e) it meets its obligations as defined in clause 6.1;

f) it has implemented controls which meet the requirements specified in clause 7;

g) uses a certificate policy which meets the requirements specified in clause 8.1;

h) it has implemented controls which meet the additional requirements of the certificate policies employed;

i) it meets the additional requirements specified in clause 8.2;

j) [EVCP] and [EVCP+]: it meets the requirements specified in EVCG [16].

k) [PTC-BR]: it meets the requirements specified in BRG [19].

Annex A (informative): Significant differences to TS 101 456

The present document is based upon TS 101 456 [15] and includes much text that is in common. The significant differences between the present document and TS 101 456 [15] are outlined below.

Other changes are generally due to:

a) alternative wording being considered to be necessary to clarify the requirements. Such changes are likely to be incorporated in future editions of TS 101 456 [15], subject to ratification;

b) differences in the scope requiring generalization of wording (e.g. qualified certificate changed to public key certificate).

A.1 Scope

TS 101 456 [15] is limited to CA's issuing qualified certificates whereas the present document is for any CA issuing public key certificates. Certificates issued under the policy requirements defined in the present document 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.

TS 101 456 [15] specifies two "qualified certificate policies". The present document specifies two Normalized Certificate Policies that is of equivalent quality to that specified in TS 101 456 [15] but without the legal constraints if the Electronic Signatures Directive (1999/93/EC) [i.1].

In addition, the present document specifies a Lightweight Certificate Policy where certain requirements are eased for use where the risks do not justify the additional costs of meeting the more onerous requirements of the NCP (e.g. physical presence).

Two additional certificate policies are added to address EVC aspects: [EVCP] and [EVCP+].

Another two more additional certificate policy are added to address DVC and OVC (covered both as PTC) aspects: [DVCP] and [OVCP] which are simplified in [PTC-BR].

A.2 TS 101 456 specific requirements

The following requirement clauses in TS 101 456 [15] are removed or replaced because they relate to requirements which are only applicable to the narrow scope of TS 101 456 [15].

NOTE: Scope and other introductory clauses not directly specifying requirements are not included.

Clauses: All of 5, 6.4, 7.3.3 a) requirements specific to qualified certificates.

A.3 Alternative quality requirements

The clauses in the present document offer alternative requirements to support a choice between:

a) Lightweight quality of service which is less onerous than TS 101 456 [15].

b) Normalized quality of service which is equivalent to TS 101 456 [15], including options for use of a secure user device which is a generalized form of secure signature creation device.

c) Two EVC related policies to address EVC related issues: [EVCP] and [EVCP+].

d) Two "baseline" policies to address DVC and OVC related issues: [DVCP] and [OVCP] respectively.

As marked with LCP/NCP/NCP+/EVCP/EVCP+/DVCP/OVCP.

A.4 Alternative functionality requirements

The clauses in the present document are conditional due to the wider variation of services supported by the present document as marked with [CONDITIONAL].

Annex B (informative): Model PKI disclosure statement

B.1 Introduction

The proposed model PKI disclosure statement is designed for use by a CA issuing certificates as a supplemental instrument of disclosure and notice. A PKI disclosure statement may assist a CA to respond to regulatory requirements and concerns. Further, the aim of the model PKI disclosure statement is to foster industry "self-regulation" and build consensus on those elements of a certificate policy and/or certification practice statement that require emphasis and disclosure.

Although certificate policy and certification practice statement documents are essential for describing and governing certificate policies and practices, many PKI users, especially consumers, find these documents difficult to understand. Consequently, there is a need for a supplemental and simplified instrument that can assist PKI users in making informed trust decisions. Consequently, a PKI disclosure statement is not intended to replace a certificate policy or certification practice statement.

This annex provides an example of the structure for a PKI disclosure statement, illustrating the harmonized set of statement types (categories) that would be contained in a deployed.

B.2 The PDS structure

The PDS contains a clause for each defined statement type. Each clause of a PDS contains a descriptive statement, which MAY include hyperlinks to the relevant certificate policy/certification practice statement sections.

Table B.1

Statement types	Statement descriptions	Specific Requirements of certificate policy (see clause 7.3.4)
CA contact info:	The name, location and relevant contact information for the CA/PKI.	
Certificate type, validation procedures and usage:	A description of each class/type of certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate usage.	Any limitations on its use. Whether the policy is for certificate issued to the public.
Reliance limits:	The reliance limits, if any.	Indication that the certificate is only for use with electronic signatures. The period of time which registration information and CA event logs (see clause 7.4.11) are maintained (and hence are available to provide supporting evidence).
Obligations of subscribers:	The description of, or reference to, the critical subscriber obligations.	The subscriber's obligations as defined in clause 6.2, including whether the policy requires use of a secure user device.
Certificate status checking obligations of relying parties:	The extent to which relying parties are obligated to check certificate status, and references to further explanation.	Information on how to validate the certificate, including requirements to check the revocation status of the certificate, such that the relying party is considered to "reasonably rely" on the certificate (see clause 6.3).
Limited warranty and disclaimer/Limitation of liability:	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	Limitations of liability (see clause 6.4).
Applicable agreements, certification practice statement, Certificate:	Identification and references to applicable agreements, certification practice statement, certificate policy and other relevant documents.	Certificate policy being applied.
Privacy policy:	A description of and reference to the applicable privacy policy.	See note.
Refund policy:	A description of and reference to the applicable refund policy.	
Applicable law, complaints and dispute resolution:	Statement of the choice of law, complaints procedure and dispute resolution mechanisms (anticipated to often include a reference to the International Chambers of Commerce's arbitration services).	The procedures for complaints and dispute settlements. The applicable legal system.
CA and repository licenses, trust marks, and audit:	Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.	If the CA has been certified to be conformant with a certificate policy, and if so through which scheme.
NOTE: Cas under this policy are required to comply with the requirements of Data Protection Legislation.		

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

NOTE: There is a difference in organization between RFC 3647 [12] and the present document, and in some cases a RFC 3647 [12] is more detailed. The same clause from the present document may be related to several sections in RFC 3647 [12].

Table C.1: Cross-reference RFC 3647 [12] clauses and policy references

RFC 3647 section	Present document reference
1 INTRODUCTION	
1.1 Overview	5.1
1.2 Document name and identification	5.2
1.3 PKI participants	5.3 7 Introductory text
1.4 Certificate usage	5.3
1.5 Policy administration	ETSI see covering pages
1.5.1 Organization administering the document	ETSI
1.5.2 Contact person	See cover pages
1.5.3 Person determining CPS suitability for the policy	-
1.5.4 CPS approval procedures	7.1
1.6 Definitions and acronyms	3
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES	
2.1 Repositories	7.3.5
2.2 Publication of certification information	7.3.5, 7.3.6, 7.3.4
2.3 Time or frequency of publication	7.3.5, 7.3.6
2.4 Access controls on repositories	7.4.6
3 IDENTIFICATION AND AUTHENTICATION	
3.1 Naming	7.3.3
3.2 Initial identity validation	7.3.1
3.3 Identification and authentication for re-key requests	7.3.2
3.4 Identification and authentication for revocation request	7.3.6
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	
4.1 Certificate Application	7.3.1
4.2 Certificate application processing	7.3.3
4.3 Certificate issuance	7.3.3
4.4 Certificate acceptance	7.3.1
4.5 Key pair and certificate usage	6.2, 6.3
4.6 Certificate renewal	7.3.2
4.7 Certificate re-key	7.3.2
4.8 Certificate modification	7.3.2
4.9 Certificate revocation and suspension	7.3.6
4.10 Certificate status services	7.3.6
4.11 End of subscription	-
4.12 Key escrow and recovery	7.2.4
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	
5.1 Physical controls	7.4.1, 7.4.4, 7.4.5
5.2 Procedural controls	7.4.5, 7.4.3, 7.4.6
5.3 Personnel controls	7.4.3
5.4 Audit logging procedures	7.4.11
5.5 Records archival	7.4.11
5.6 Key changeover	7.2
5.7 Compromise and Disaster Recovery	7.4.8
5.8 CA or RA termination	7.4.9
6 TECHNICAL SECURITY CONTROLS	
6.1 Key pair generation and installation	7.2.1, 7.2.3, 7.2.8, 7.2.9
6.2 Private Key Protection and Cryptographic Module Engineering Controls	7.2.1, 7.2.2, 7.2.6, 7.2.7
6.3 Other aspects of key pair management	7.2.1, 7.2.2, 7.2.5
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 technical controls	7.4.5, 7.4.6, 7.4.7

RFC 3647 section	Present document reference
6.7 Network security controls	7.4.6
6.8 Time-stamping	N/A
7 CERTIFICATE, CRL, AND OCSP PROFILES	
7.1 Certificate profile	7.3.3 a)
7.2 CRL profile	7.3.6
7.3 OCSP profile	-
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS	
8.1 Frequency or circumstances of assessment	5.4.1
8.2 Identity/qualifications of assessor	TS 119 403 [i.2]
8.3 Assessor's relationship to assessed entity	TS 119 403 [i.2]
8.4 Topics covered by assessment	5.4.2, 5.4.3, 8.4
8.5 Actions taken as a result of deficiency	5.4.1, 8.4
8.6 Communication of results	5.4.1
9 OTHER BUSINESS AND LEGAL MATTERS	
9.1 Fees	7 intro
9.2 Financial responsibility	7.5
9.3 Confidentiality of business information	
9.4 Privacy of personal information	7.3.1 o), 7.3.3 e), 7.4.10, 7.4.11 j)
9.5 Intellectual property rights	Cover pages
9.6 Representations and warranties	4.5.2
9.7 Disclaimers of warranties	4.5.2
9.8 Limitations of liability	6.4
9.9 Indemnities	-
9.10 Term and termination	-
9.11 Individual notices and communications with participants	7.3.4
9.12 Amendments	ETSI Procedures
9.13 Dispute resolution provisions	7.5
9.14 Governing law	-
9.15 Compliance with applicable law	7.4.10
9.16 Miscellaneous provisions	-
9.17 Other provisions	7.5

Annex D (informative): Revisions made since previous versions

D.1 Changes from V1.1.1 to V2.1.1

D.1.1 Additional Requirements

Reference and provision related to EVC, namely EVCP and EVCP+, have been added in the following clauses: Introduction, 1, 2.1, 3.1, 3.2, 4.3.2, 4.3.5, 5.1, 5.2, 5.4.1, 6.2, 6.4, 7.1, 7.2.1, 7.2.8, 7.3.1 (items h) iii) and r), 7.3.6 (items c), h) iii), 7.3.6 i), 7.3.6 k), 7.3.6.l, 7.3.6 m), 7.4.3 Note 5, A.1, A.3.

Clause 4.5 has been added related to EVC.

The following items have been added which significantly affect the requirements: 5.4.1 c), 5.4.1 d), 6.2 j), 7.1 i), 7.2.1 e), 7.3.1 k), 7.3.3 b), 7.3.6 l, 7.4.1 a) last sentence, 7.4.1 d), 7.4.3 b), 7.4.4 e), 7.4.5 d), 7.4.5 i), 7.4.5 j), 7.4.6 b), 7.4.8 a), b), c), 7.4.8 g), 7.4.9 a) 2nd item (recording of revocation status information), 8.3 c), d).

D.1.2 Update Requirements

The following items have been updated to extend choices or otherwise modify requirements:

5.4.1 b), 6.2 Lead in, 7.2.1 b), 7.2.2 a), 7.2.8 d), 7.2.8 e), 7.3.1 j), 7.3.2 c), 7.3.3.a), 7.4.3 g) 4th item, 7.4.6 b), 7.4.6 d), 7.4.8 f), 7.4.9 b), 8.4 b), annex C.

D.1.3 Clarifications

The following clauses have been reworded to achieve a better clarity.

4.3.2, 6.2 1st paragraph, 6.2 d) ii), 6.2 e), g), h), i), 6.3 Note 1, 7.1 f), 7.2.2 b), 7.2.4, 7.2.6 a), 7.2.8 a), b), 7.2.9 Note, 7.3.1 (introduction) 7.3.1 d), 7.3.1 e), f), g), 7.3.1 l (moved), 7.3.1 Note 6, 7.3.1 m) 3rd item, 7.3.1 p, 7.3.1 some repetition text on data protection removed, 7.3.2 d), 7.3.4 Note 2, 7.3.6.h) i), 7.3.6 ii), 7.3.6 Note 3, 7.4.1 d) (moved from 7.5), 7.4.3 a) (merged with equivalent item in 7.5), 7.4.3 Note 2, 7.4.3 f), 7.4.3 Note 4, 7.4.4 d), f), g), 7.4.7 Note 1 => 2, 7.4.8 Note 2 => 3, 7.4.8 Note 4, 7.4.9 a) 1st item, 7.4.10 a), b & Note, 7.4.11 e), 7.5 (two items moved to 7.4.1 d & 7.4.3 a), 8.3 Notes 1 & 2.

D.1.4 Editorial

A number of other editorial changes were made which do not affect the technical content of the present document.

D.1.5 Annex E

Introduction of the auditors' qualification.

D.2 Changes from V2.1.1 to V2.1.2

D.2.1 Additional Requirements

Clause 8.3 j has been added related to EVC.

The following items have been added which significantly affect the requirements: 7.2.1 d. And reference to X.509 / RFC 5280 [17] in 7.3.3 a).

D.2.2 Update Requirements

The following items have been updated to extend choices or otherwise modify requirements:

4.5.1, 6.2 Note 2, 6.3 Note, 7.1 b), 7.1 d) 2, 7.1 k), 7.2.1 e), 7.2.1 f), 7.3.1 d), 7.3.1 h) i), 7.3.1 h) iii), 7.3.1 i) i), 7.3.1 k), 7.3.1 l, 7.3.1 m) vi), 7.3.1 n), 7.3.1 r), 7.3.1 s), 7.3.2 a), 7.3.3 a) x), 7.3.6 c), 7.3.6 h) iii), 7.3.6 j), 7.3.6 k), 7.3.6 l, 7.3.6 m), 7.4.3 Note 4, 7.4.5 Note 2, 7.4.11 Note 2.

D.2.3 Clarifications

The following clauses have been reworded to achieve a better clarity.

Bibliography TTP.NL Part 3.

D.3 Changes from V2.1.2 to V2.2.1

D.3.1 Update Requirements

The following items have been updated to extend choices or otherwise modify requirements:

3.1, 5.1 4), 5.1 5), 6, 6.1, 6.3 Note 2, 6.4, 7.1 b), 7.1 d) 2), 7.2.1, 7.2.8, 7.3.1, 7.3.6 Note 2, 7.3.6 c), 7.4.1, 7.4.1 Note 1, 7.4.3, 7.4.3 Note 5, 7.4.6 Note 3, 8.2, Annex C 9.6 and 9.7.

D.4 Changes from V2.2.1 to V2.3.1

D.4.1 Update Requirements

The following items have been updated to add support for CABF Publicly trusted TLS/SSL certificates, to extend choices or otherwise modify requirements:

1, 2.1, 2.2, 3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.3.2, 5.4.1, 6.2, 6.3, 6.4, 7.1, 7.2.1, 7.2.2, 7.2.7, 7.2.8, 7.3.1, 7.3.3, 7.3.6, 7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.4.6, 7.4.11, 8.3, A.1, A.3, Annex C, D, E and F.

D.4.2 Clarifications

Annex F: Bibliography has been removed.

D.5 Changes from V2.3.1 to V2.4.1

Reference [16] was updated to refer to version 1.3 specifically.

Annex E (normative): Auditors qualification

This annex states requirements of bodies that may audit conformance of implementations of the present document if conformance is to be certified.

The body carrying out the audit shall be accredited for the purpose of auditing organisations implementing the present document by an official accreditation body (such as the signatories to the MLA of the European Cooperation for Accreditation http://www.european-accreditation.org and International Accreditation Forum http://www.iaf.nu) as conforming to ISO/IEC 17021 [10] or EN 45011 [1].

The auditing body shall also be accredited as having the competence specified in TS 119 403 [i.2] or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 27006 [i.7] to carry out ISO 27001 [i.8] audits.

The "Independent Auditors Report" shall confirm that "the examination was conducted in accordance with European Standards/Specifications, in particular the present document and TS 119 403 [i.2] and, where applicable, has considered all current CA/Browser Forum Requirements".

History

Document history		
V1.1.1	April 2002	Publication
V1.2.1	May 2005	Publication
V1.2.2	June 2005	Publication
V1.2.3	December 2006	Publication
V1.2.4	March 2007	Publication
V1.3.4	December 2007	Publication
V2.1.1	May 2009	Publication
V2.1.2	April 2010	Publication
V2.2.1	December 2011	Publication
V2.3.1	November 2012	Publication
V2.4.1	February 2013	Publication