ETSI TR 102 437 V1.1.1 (2006-10)

Technical Report

Electronic Signatures and Infrastructures (ESI); Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)

Reference

DTR/ESI-000023

Keywords

e-commerce, electronic signature, security

ETSI

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

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

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Security (SEC).

The present document is largely based on the "TTP.NL Guidance on TS 101 456 [15]", issued by ECP.NL - The Electronic Commerce Platform for the Netherlands that kindly offered their document as a basis for the present document.

Introduction

Electronic commerce is getting momentum as a way of doing business and communicating across public and private networks. An important requirement of electronic commerce is the ability to identify the originator of electronic information in the same way that documents are signed using a hand-written signature. This is commonly achieved by using electronic signatures which are supported by a certification-service-provider issuing certificates, commonly called a certification authority. The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures [1] (hereinafter referred to as "the Directive") identifies a special form of electronic signature which is based on a "qualified certificate". Annex I of this Directive specifies requirements for qualified certificates. Annex II of the Directive specifies requirements on certification-service-providers issuing qualified certificates (i.e. certification authorities issuing qualified certificates). Annex III specifies requirements for secure signature creation devices.

For users of electronic signatures to have confidence in the authenticity of the qualified electronic signatures they need to have confidence that the CA that issued the qualified certificate the electronic signature is based upon has properly established procedures and protective measure in order to minimize the operational and financial threats and risks associated with public key crypto systems.

ETSI ESI issued, and keeps updated, the Technical Specification TS 101 456 [15] that specifies baseline policy requirements on the operation and management practices of certification authorities issuing qualified certificates to the public, that are used in support of qualified electronic signatures (i.e. electronic signatures that are legally equivalent to hand-written signatures in line with article 5.1 of the European Directive on a community framework for electronic signatures [1]). The use of a secure-signature-creation device, as required through annex III of the Directive, is an optional element of these policy requirements.

The present document provides guidelines on interpreting the TS 101 456 [15] requirements for use by independent bodies and their assessors, certification service providers and other interested parties. Guidance is provided both to the assessors, by specifying which verifications they are recommended to do, and to the certification authorities, by indicating documents and other factual reference they should provide to assessors.

Interrelation of standards

In figure 1 a schema is shown displaying the CA's areas (organization, systems, products, crypto modules) and the corresponding assessment scopes.

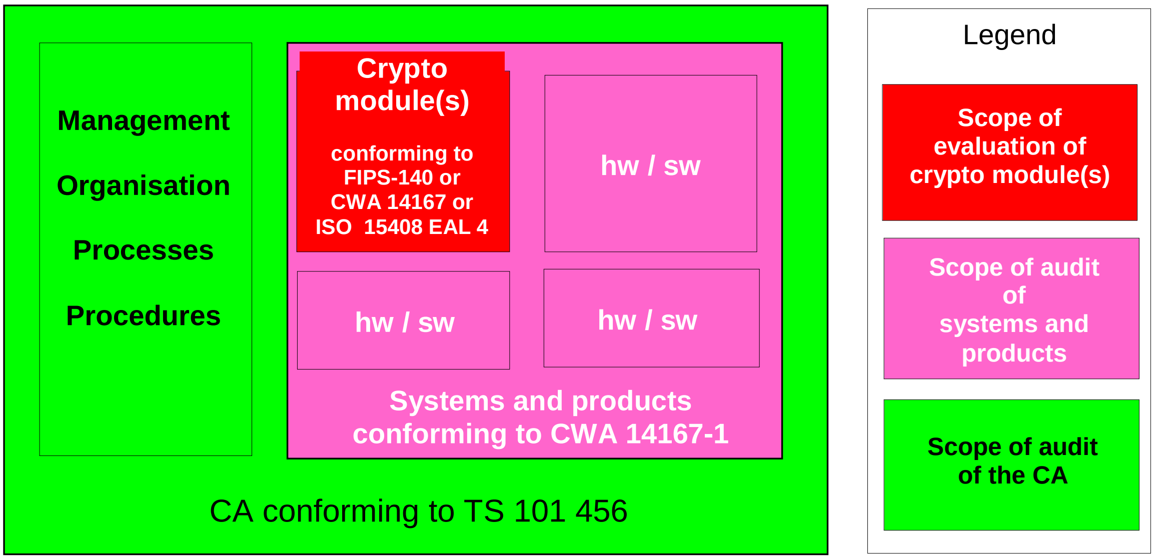
Management
Organisation
Processes
Procedures
Crypto module(s)
conforming to FIPS-140 or CWA 14167 or ISO 15408 EAL 4
hw / sw
hw / sw
hw / sw
Systems and products conforming to CWA 14167-1
CA conforming to TS 101 456
Legend
Scope of evaluation of crypto module(s)
Scope of audit of systems and products
Scope of audit of the CA

Figure 1: Illustration of interrelation of standards regarding electronic signatures

More specifically:

- CA management, organization, processes and procedures are to be assessed against TS 101 456 [15];
- CA systems and products are to be assessed against CWA 14167-1 [8];
- CA crypto systems are to be assessed against CWA 14167-2 [9], -3 [10], -4 [11] as appropriate, or FIPS 140-1, -2 [5], or suitable ISO/IEC 15408 [7] protection profiles or security target to EAL 4.

This implies the following:

- For the management system: auditing of documentation and implementation.
- For trustworthy systems: executing an EDP-audit against CWA 14167-1 [8] or verifying a statement that an EDP-audit against CWA 14167-1 has been carried out with positive results.
- For Crypto Modules: demanding statements, that fulfil certain conditions (based on the right standards, supplied by the right organizations and persons, etc.).

Further assessment guidelines on TS 101 456 [15] are provided in CWA 14172-2 [18]. In addition, guidance on assessment of trustworth systems against CWA 14167-1 [8] is given in CWA 14172-3 [18]. The present document incorporates guidance on TS 101 456 [15]:

- As given in most notes included in TS 101 456 [15].
- As given in CWA 14172-2, by referring to the relevant sections.
- With additional guidance covering further issues identified in applying TS 101 456 [15].

The guidance taken from these 3 sources are provided in tables of the following form:

Subject	**TS 101 456 Guidance Note / CWA 14172-2 Guidance / Additional Guidance**
	Best practice

1 Scope

The present document provides guidance on interpreting the requirements specified in TS 101 456 (V1.4.1) [15]. This guidance is intended for use by bodies that supervise (e.g. as per Directive articles 3.3), approve or accredit CAs (e.g. as per articles 3.2 of Directive [1]), assessors, certification service providers and other interested parties.

The present document purpose is to facilitate assessors in evaluating compliance of certification authorities with TS 101 456 [15] and, consequently, to facilitate certification authorities in implementing TS 101 456 [15] requirements.

The original text of TS 101 456 [15] is repeated in the present document to provide a comprehensive source.

TEXT COPIED VERBATIM FROM TS 101 456 [15] IS IN ITALIC.

2 References

For the purposes of this Technical Report (TR) the following references apply:

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

The following references are taken from TS 101 456.

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

NOTE: The above is referred to as "the Directive" in the present document.

[2] IETF RFC 3647 (2003): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

NOTE: Obsoletes IETF RFC 2527.

[3] ITU-T Recommendation X.509 (2000)/ISO/IEC 9594-8 (2001): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[4] 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.

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

NOTE: FIPS 140-1 certified devices are perfectly admissible and a valid alternative to FIPS 140-2.

[6] ETSI TS 101 862: "Qualified certificate profile".

[7] ISO/IEC 15408 (2005) (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".

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

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

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

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

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

[13] ISO/IEC 17799 (2005): "Information technology - Security techniques - Code of practice for information security management".

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

Additional references

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

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

[17] ETSI TS 102 176-2: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices".

[18] CWA 14172-2: "EESSI Conformity Assessment Guidance on ETSI TS 101 456".

[19] CWA 14172-3: "EESSI Conformity Assessment Guidance on Trustworthy Systems".

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

[21] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)".

[22] IETF RFC 4211: "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)".

[23] PKCS #5 v2.0: "Password-Based Cryptography Standard".

[24] TTP.NL Part 1: "Requirements and Guidance for the Certification of the Public Key Infrastructure of Certification Service Providers".

[25] TTP.NL Part 2: "Requirements and Guidance for the Certification of Information Security Management of Certification Service Providers".

[26] TTP.NL Part 3: "General Requirements and Guidance for the Accreditation of Certification Service Providers issuing Qualified Certificates".

[27] "Scheme approval profiles for Trust Service Providers".

NOTE: See http://www.tscheme.org/.

[28] ITU-T Recommendation X.843 | ISO/IEC 15945: "Information technology - Security techniques - Specification of TTP services to support the Application of Digital Signatures".

[29] ITU-T Recommendation X.842 | ISO/IEC 14516: "Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services".

[30] ISO/IEC TR 13335-1 (1996): "Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security".

[31] ISO/IEC TR 13335-2 (1997): "Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security".

[32] ISO/IEC TR 13335-3 (1998): "Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security".

[33] ISO/IEC TR 13335-4 (2000): "Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards".

[34] ANSI X9.79: "Public Key Infrastructure (PKI) - Practices and Policy Framework".

[35] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts - Statement by the Council and the Parliament re article 6 (1) - Statement by the Commission re article 3 (1), first indent.

[36] Commission Decision 2000/709/EC of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.

[37] ANSI X9.17: "Financial Institution Key Management (wholesale)".

[38] NIST Special Publication 800-57: "Recommendation for key management - Part 1: General guideline".

[39] CWA 14169: "Secure signature-creation devices "EAL 4+"".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 456 [15] apply.

NOTE: For further explanations of the general concepts used in TS 101 456 [15] see clause 4.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 101 456 [15] and the following apply:

CM	Cryptographic module

3.3 Additional terms used in the present document

The present document is a Technical Report providing Guidance on TS 101 456 [15] and not a Technical Specification, therefore its provisions are not mandatory for assessors or implementors. The consequences of not following the guidance, indicated by "should" in the current document, should be understood and carefully weighed before choosing an alternative course.

On the other hand, requirements on the CA deriving directly from TS 101 456 [15] provisions are specified as "SHALL" where applicable.

4 General Concepts

See TS 101 456 [15] for description of the general concepts used.

Subject	**CWA 14172-2 Guidance**
Certification authority assessment	Please refer to CWA 14172-2 section 3.4 for guidance on requirements for independent bodies concerned with assessment, assessors and assessment teams.
	Best practice
	Guidance element G.2.4 states: The following requirements apply to the assessment team as a whole: a) In each of the following areas at least one assessor in the team should satisfy the independent body's criteria for taking responsibility within the assessment team: i. ..., ii. knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of certification service and information security Guidance Element G.2.20 provides guidance on: 1 cooperation between the assessment team and the CA 2 acceptability by the assessment team of independent assessments performed by separate teams on service components 3 need, in the case of separate assessment of some service components, for the independent body to: a. have the separate assessment reports available, b. verify the compliance of the separate assessment bodies with the provision of the CWA 14172-2 guidance.

5 Introduction to qualified certificate policies

5.1 Overview

As specified in TS 101 456 [15]:

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" [3].

The policy requirements are defined in the present document in terms of certificate policies. These certificate policies are for qualified certificates, as defined the Directive [1], and hence are called qualified 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 [TS 101 456 [15] *specifies two qualified certificate policies:*

1) *a qualified certificate policy for qualified certificates issued to the public, requiring use of secure signature-creation devices.*

Subject	**TS 101 456 [15] Guidance Note**
Qualified certificates issued to the public	NOTE 1: The exact meaning of public is left to interpretation within the context on national legislation. A CA may be considered to be issuing qualified certificates to the public if the certificates are not restricted to uses governed by voluntary agreements under private law among participants.
	Best practice
	The assessing team should have sufficient qualification on the applicable legislation to verify if its provisions on the meaning of "public" are met.

2) *a qualified certificate policy for qualified certificates issued to the public;*

Clause 8 (of TS 101 456 [15]) *specifies a framework for other qualified certificate policies which:*

a) *enhance or further constrain the above policies; and/or*

b) *are for qualified certificates issued to "closed groups" other than the public.*

NOTE 2: The present document makes use of the principles defined in RFC 3647 [2] and the framework defined in ANSI X9.79 (see bibliography). The aim of the present document is to achieve best possible harmonization with the principles and requirements of those documents.

5.2 Identification

The identifiers for the qualified certificate policies specified in TS 101 456 [15] are:

a) ***QCP public + SSCD:*** *a certificate policy for qualified certificates issued to the public, requiring use of secure signature-creation devices*

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456)
policy-identifiers(1) qcp-public-with-sscd (1)
```

b) ***QCP public:*** *a certificate policy for qualified certificates issued to the public*

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456)
policy-identifiers(1) qcp-public (2)
```

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

Subject	TS 101 456 [15] Guidance Note
Qualified Certificates identifier	NOTE: TS 101 862 [6] clause 5.3 requires that an esi4-qcStatement-1 statement included in a Qualified Certificate Statement extension, as defined in TS 101 862 [6] clause 5.2.1: ▪ SHOULD be present for Qualified Certificates compliant with TS 101 862 issued until June 30, 2005, ▪ SHALL be present for Qualified Certificates compliant with TS 101 862 issued after June 30, 2005.
	Best practice
	An assessor should verify if certificates issued after 30 June 2005 have the qcStatements extension implemented

A CA shall also include the identifier(s) for the certificate policy (or policies) being supported in the terms and conditions made available to subscribers and relying parties to indicate its claim of conformance.

Subject	Additional Guidance
Indicate QCP applicability	If a CA adopts the QCP+SSCD or QCP public, or any other policy defined under the QCP framework, to which the CA can demonstrate conformance, then it shall include the corresponding OID in the certificates it issues.
	Best practice
	No Stipulations.

5.3 User Community and applicability

As specified in TS 101 456 [15].

5.3.1 QCP public + SSCD

The certificate policy QCP public + SSCD is for certificates:

a) which meet the requirements laid down in annex I of the Directive [1];

b) are issued by a CA who fulfils the requirements laid down in annex II of the Directive [1];

c) which are for use only with secure-signature-creation devices which meet the requirements laid down in annex III of the Directive [1];

d) are issued to the public.

Qualified certificates issued under this policy may be used to support electronic signatures which "satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data", as specified in article 5.1 of the Directive [1].

5.3.2 QCP public

The certificate policy QCP Public is for certificates:

a) which meet the requirements laid down in annex I of the Directive [1];

b) are issued by a CA who fulfils the requirements laid down in annex II of the Directive [1];

c) are issued to the public.

Qualified certificates issued under this policy may be used to support electronic signatures which "are not denied legal effectiveness and admissibility as evidence in legal proceedings", as specified in article 5.2 of the Directive [1].

5.4 Conformance

5.4.1 General

As specified in TS 101 456 [15]:

The CA shall only use the identifier for either of the qualified certificate policies as given in clause 5.2:

a) if the CA claims conformance to the identified qualified 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 qualified 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 can be carried out either under a "voluntary accreditation" scheme as defined in article 2.13 of the Directive [1], or other form of assessment carried out by a competent independent auditor See CEN Workshop Agreement 14172 "EESSI Conformity Assessment Guidance" (see bibliography).

c) if the CA is later shown to be non-conformant in a way that significantly affects its ability to meet the requirements for qualified certificates identified in the Directive [1] 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;

Subject	TS 101 456 [15] Guidance Note
Certificates issued for testing purposes	NOTE 3: 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.
	Best practice
	An assessor should verify that procedures are in place to ensure that while a CA is not assessed as conformant it does not issue any qualified certificates with legal value to its. subscribers/users.

Subject	TS 101 456 [15] Guidance Note
Conformance may depend on applicable legislation	NOTE 4: The means required to demonstrate conformance may depend on legal requirements for the country where the CA is established.
	Best practice
	The assessing team should have sufficient qualification on the applicable legislation to verify compliance with this requirement.

Subject	CWA 14172-2 [18] Guidance
Guidance on requirements for independent bodies, assessors, and assessment teams	The independent body responsible for assessment should clearly document the procedures used for assessment and the qualifications required of assessors.
	Best practice
	The following CWA 14172-2 [18]Guidance Elements apply: • G.2.1: Guidance on requirements for independent bodies; • G.2.2: Guidance on qualification criteria for individual assessors; • G.2.3: Guidance on a Code of Conduct for assessors; • G.2.4: Guidance on assessment team competence; • G.2.5: Guidance on the use of technical experts.

Subject	CWA 14172-2 [18] Guidance
Guidance on how to conduct and perform the assessment	Please refer to CWA 14172-2 section 3.4 for indications on these requirements.
	Best practice
	The Guidance Elements from G.2.6 to G.2.18 apply.

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

Subject	Additional Guidance
The CA compliance shall be checked on a regular basis and whenever major change is made to the CA operations.	CA conformance should be checked for significant changes annually with a full re-assessment first after three years and then every four years.
	Best practice
	The CA should keep the history of all the security incidents occurred since the previous assessment along with the changes applied to practices and security policies, based on the risk assessment revisions meanwhile occurred (see Guidance to clause 7.4.1), to be submitted to assessors. NOTE: if the assessing team is not provided with this history, it might find it difficult to perform its task exhaustively.

5.4.2 QCP public + SSCD

A conformant CA must demonstrate that:

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

b) it has implemented controls which meet all the requirements specified in clause 7.

5.4.3 QCP public

A conformant CA must demonstrate that:

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

b) it has implemented controls which meet the requirements specified in clause 7, excluding those specified in clause 7.2.9 and excluding the subscriber obligation given in clause 6.2 e) and f).

Subject	Additional Guidance
Migration from TS 101 456 [15] V1.2.1 to 1.3.1 and to 1.4.1	The applicability of the mentioned versions of TS 101 456 [15] are considered equivalent and applications can accept certificates certified by CAs under new or old policies as being equivalent.
	Best practice
	Assessment against the latest version of TS 101 456 [15] (V1.4.1) can be carried out at the next scheduled full re-assessment of the CA as described in the guidance below item 5.4.1 item d). The subsequent re-assessment can be scheduled on a four years basis as per the suggested schedule.

6 Obligations and liability

As specified in TS 101 456 [15].

6.1 Certification authority obligations

The CA shall ensure that all requirements on CA, as detailed in clause 7, are implemented as applicable to the selected qualified certificate policy (see clauses 5.4.2, 5.4.3, 8.4).

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.

Subject	Additional Guidance
Responsibility conformance	• When CA functionality is undertaken by sub-contractors the CA shall demonstrate conformance of these sub-contractors with the prescribed procedures. • When CA functionality is **not** undertaken by sub-contractors the CA shall demonstrate conformance with the procedures in adequately defined process and work descriptions describing the obligations and responsibilities within the CA.
	Best practice
	The conformance of subcontractors may be demonstrated by the CA by statements in contracts (e.g. service level agreements) describing the obligations and responsibilities for each party and by presenting a report of conformance to TS 101 456 [15] by a third party.

Subject	CWA 14172-2 [18] Guidance
Responsibility conformance	Please refer to CWA 14172-2 section 3.6 for indications on this requirement
	Best practice
	For additional guidance please refer to the following CWA 14172-2 Guidance elements: • G.2.21 on policies and practices enforcement also on subcontractors; • G.2.22 on CA management system; • G.2.23 on lines of authority, responsibility and allocation of functions.

6.2 Subscriber obligations

The CA shall oblige through agreement (see clause 7.3.1 i) 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) submit accurate and complete information to the CA in accordance with the requirements of this policy, particularly with regards to registration;

Subject	Additional Guidance
CA obliges subscriber to submit accurate and complete information	The assessor should assess the certification contract provisions relating to subscriber registration.
	Best practice
	No stipulations.

b) only use the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber (see clause 7.3.4);

Subject	Additional Guidance
Key pair usage	• The CA should ensure that certification contracts have stipulations that the key pair is used for electronic signatures only. • If applicable, the CA should demonstrate that other limitations than key usage are notified to the subscriber.
	Best practice
	No Stipulations.

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

Subject	Additional Guidance
Avoid unauthorized use private key	The CA should ensure that certification contracts have stipulations that the subscriber will exercise reasonable care to avoid unauthorized use of the subject's private key.
	Best practice
	The CA may give additional Guidance on private key protection, e.g. through the use of passwords (including password rules), PIN-code protection or through the use of additional user authentication mechanisms, such as biometrics.

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

i) generate subject's keys using an algorithm recognized as being fit for the purposes of qualified electronic signatures;

ii) use a key length and algorithm which is recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate;

Subject	Additional Guidance
Algorithms being fit for the purpose	• The CA should provide evidence that the subscriber or subject is obliged to use algorithms and key length that are generally recognized as suitable (by experts). • The assessor should assess, based on the precise details, as provided by the CA, of the algorithm(s) and key length(s) used by the subscriber, if they meet the TS 101 456 [15] requirements.
	Best practice
	TS 102 176-1 [16] specifies algorithms and key lengths to be used that meet the qualified signature requirements.

iii) the subject's private key can be maintained under the subject's sole control.

Subject	Additional Guidance
The subject must have the possibility to maintain their private key under their sole control	• The CA should make available evidence that procedures are in place such that: o no copies can be done of the private key during or after its generation; o the access to the private key is controlled in a way that can reasonably prevent unauthorized access. • The assessor should assess the precise details, as provided by the CA, of the mechanisms used to protect access to the private key. These mechanisms must allow the subject to prevent any one but the subject to access the private key.
	Best practice
	The assessment team should verify that key pair is: 1. generated and kept in the secure signature creation device; or 2. generated in a secure hardware device that injects it into the secure signature creation device; or 3. when generated in software, generated in a way such that the private key is always kept protected, i.e. that only the legitimate subject can access it. The access mechanisms can be based on passwords (password composition rules should be specified), PINs (PIN composition rules should be specified), biometrics.

e) if the certificate policy requires use of an SSCD (i.e. QCP public + SSCD), only use the certificate with electronic signatures created using such a device;

NOTE 2: The above item is NOT applicable to qualified certificate policy: QCP public.

Subject	Additional Guidance
Use certificate with electronic signatures created using a SSCD	The assessor should check the relevant clause in the certification contract.
	Best practice
	No stipulations.

Subject	Additional Guidance
Use of an SSCD	The assessor should check that the SSCDs are tested and certified by Notified Bodies.
	Best practice
	Notified Bodies are bodies as specified in European Commission Decision 2000/709/EC [36].

f) if the certificate is issued by the CA under certificate policy QCP public + SSCD and the subject's keys are generated under control of the subscriber or subject, generate the subject's keys within the SSCD to be used for signing;

NOTE 3: The above item is NOT applicable to qualified certificate policy: QCP public.

Subject	Additional Guidance
Key pair generated by the subject inside the SSCD	The assessor should check the relevant clause in the certification contract.
	Best practice
	No stipulations

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

i) *the subject's private key has been lost (e.g. by forgetting the PIN number needed to use the key), stolen, potentially compromised; or*

ii) *control over the subjects 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.*

Subject	Additional Guidance
Reasonable delay of notifying CA	The CA should ensure that the subscriber agreements have stipulations defining reasonable delay in notifying the CA.
	Best practice
	The assessing team should ascertain that the certification contracts specify that, should the revocation requests be submitted beyond such "reasonable delay", the subject should be responsible for any misuse of the private key occurred outside the "reasonable delay". It is to be noted, however, that any such assertion by the subject is intrinsically uncorroborated, therefore it is recommended that the "reasonable delay" does not encompass a point in time before the latest previous CRL issuance (or a similar reference in time for the OCSP responder data base).

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

Subject	Additional Guidance
Private key discontinued upon compromise	The assessor should check the relevant clause in the certification contract.
	Best practice
	No stipulation.

i) *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;*

Subject	Additional Guidance
The subject shall discontinue their certificate usage upon information of CA compromise	The assessor should check the relevant clause in the certification contract.
	Best practice
	No stipulations.

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*

Subject	TS 101 456 [15] Guidance Note
Period between revocation request and revocation information	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.
	Best practice
	The assessment team should ascertain that, also consistently with provision in TS 101 456 [15] clause 7.3.6.a, 6th bullet, revocation requests are made available to all parties with a delay of at most 1 day since the CA received them.

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.*

Subject	TS 101 456 [15] Guidance Note
CA liability to the parties	NOTE 2: The liability of CAs issuing qualified certificates to the public specified in article 6 of the Directive applies to parties who "reasonably rely" on a certificate.
	Best practice
	Parties who "reasonably rely" on a certificate issued by the CA are those to which an object signed with this certificate is relevant.

6.4 Liability

CAs issuing qualified certificates to the public are liable as specified in article 6 of the Directive [1] (see annex A for further guidance on liability).

Subject	Additional Guidance
Liability	A CA shall not add clauses in the certification contracts which run counter to the liability obligations given in the Directive.
	Best practice
	The assessment team should ascertain that the liability clauses in the certification contracts do not conflict with the applicable law that is assumed as compliant with article 6 of the Directive [1].

7 Requirements on CA practice

Subject	CWA 14172-2 [18] Guidance
Certification practice statement	Please refer to CWA 14172-2 [18] for guidance.
	Best practice
	Guidance element G.2.24 addresses the need to verify compliance with specific requirements in TS 101 456 [15], clause 7.

NOTE 1: This clause is applicable to both qualified certificate policies identified in clause 5: QCP public, and QCP public + SSCD, except where indicated.

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

NOTE 2: A reference to the article within the Directive on which the requirement is based is given after each paragraph.

The present document is concerned with CA's issuing qualified certificates. This includes the provision of services for Registration, certificate generation, certificate 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. Each control objective is followed by a reference to the relevant requirement given in the Directive [1].

NOTE 3: 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 qualified 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 ensure that it demonstrates the reliability necessary for providing certification services (see the Directive [1], annex II (a)).

In particular:

a) The CA shall have a statement of the practices and procedures used to address all the requirements identified in the qualified certificate policy.

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

Subject	**Additional Guidance**
Statement of the practices	The Assessor should: • ascertain if the CSP has a CPS or at least a document that is meant to describe the practices that the CSP employs in issuing (qualified) certificates; • ascertain the completeness of the CPS as to the requirements identified in the qualified certificate policy.
	Best practice
	• Many CPSs are drafted in accordance with the RFC 2527 or 3647 [2] standards for Certificate Policy and Certification Practice Statements. The TS 101 456 [15] has included a cross-reference list in Annex D for statements to be addressed in RFC 2527 or RFC 3647 [2]. • In general, a CPS contains also legal statements. A CPS is often incorporated by reference in End User contracts.

Subject	**CWA 14172-2 [18] Guidance**
Statement of the practices	Please refer to CWA 14172-2 for guidance.
	Best practice
	Guidance element G.2.26 CAs encourages CAs to adopt the CPS structure described in document RFC 2527 "Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework" or in other standards that update, replace or extend RFC 2527. NOTE: RFC 2527 is now obsoleted by RFC 3647 [2].

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

c) The CA shall make available to subscribers and relying parties its certification practice statement, and other relevant documentation, as necessary to assess conformance to the qualified certificate policy.

Subject	TS 101 456 [15] Guidance Note
CPS states the obligations of all external organizations	NOTE 2: The CA is not generally required to make all the details of its practices public.
	Best practice
	• The obligations are stated as a high level description with the objective to demonstrate reliability to the public. Some detailed obligations between the CA and the external organizations are confidential to the public and stated in Service Level Agreements and Service Contracts. (RFC 2527, chapter 2 now superseded by RFC 3647 [2] these obligations are scattered in the specific CA, RA, subjects relevant sections). • The above mentioned detailed confidential obligations should not be specified in the CPS, as the CPS will be made publicly available. A CSP acting with external organizations will stipulate service provision contracts and service level agreement(s) with its contractors. A CP may be incorporated by reference in these documents.

d) *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.*

Subject	Additional Guidance
Terms and conditions disclosure to subscribers and third parties	The assessor should verify if the Terms and Conditions are actually freely and completely available to any user from outside the CA internal network.
	Best practice
	The Terms and Conditions can be published on the CA web site and/or on the supervision/accreditation body web site.

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

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

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

Subject	Additional Guidance
Terms: "High level management body"; "Senior management"	No Stipulations.
	Best practice
	• Usually the Senior management is the top level management reporting to the CEO and is responsible towards outside of the CA for the possible consequences of the CPS non correct implementations; the High Level Management Body is a smaller group of managers usually with technical and organizational responsibilities related to the CA management; in some organizations Senior and High level Management may consist of the same persons. • In general the High Level Management responsible for approving the CPS consists of a multidisciplinary task force made of differently competent officers, for instance: security officer, general management, legal, Head of Administrative Organization.

h) *The CA shall give due notice of changes it intends to make in its Certification Practice Statement (CPS) and shall, following approval as in (e) above, make the revised Certification Practice Statement immediately available as required under (c) above.*

i) *The CA shall document the signature algorithms and parameters employed.*

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 (see the Directive [1], annex II (g) and annex II (f)).

In particular:

a) Certification authority key generation shall be undertaken in a physically secure 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.

Subject	**Additional Guidance**
Root Key Ceremony	The CA should keep, and provide to the assessment team, evidence that the process in which CA keys are generated ("Root Key Ceremony") is under suitable control. Consistently with the provision in clause 7.4.1.f) of the QCP: "*the security controls and operating procedures for CA facilities, systems and information assets providing the certification services shall be documented, implemented and maintained*" the CA should implement the following requirements: • The root key ceremony should be described in detail in a script. In particular: - All "security critical operations" should be documented in detail (e.g. critical commands, like those regarding the cryptographic module, should be written exactly). - A description of the responsibilities (roles) of the persons present at the root key ceremony must be documented. It must be clear what (signed) assurance these persons are actually giving. • Before the actual execution of the script, extensive testing by the CSP of the script in a testing environment is necessary. • A CSP may consider to obtain a third party opinion on the script before it is executed. Where a third party consultancy was requested the assessing team may verify this party's comments. (The, possibly financial, ramifications of an inadequate Root Key Ceremony later in time can be considerable, e.g. as distributed root keys in browsers need to be redistributed.)
	Best practice
	The assessing team: • Should verify that the root key ceremony script exists in a manner that its integrity and authenticity can be relied upon, e.g. this script is securely kept by a responsible manager. • Should verify that reliable proof of this testing exist. • Is not required to assess the reliability of the third party that verified the script.

b) CA key generation shall be carried out within a device which either:

- *meets the requirements identified in FIPS 140-2 [5], level 3 or higher; or*
- *meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [9], CWA 14167-3 [10] or CWA 14167-4 [11]; or*
- *is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [7], 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 1: The rules of clause 7.2.2 (b to e) apply also to key generation even if carried out in a separate system.

Subject	Additional Guidance
Cryptographic Module (CM)	• The CA should make available evidence that the cryptographic module (CM) is certified by a competent certification body against an evaluation report from a competent evaluation body, according to the criteria specified in the TS 101 456 [15]. • The assessor should verify that the CM is installed in accordance with the assumptions used under which the CM was certified. • See clause 7.4.7. for guidance on trustworthy systems.
	Best practice
	• FIPS 140-1 has been replaced by FIPS 140-2 (March 2001), but devices certified as per FIPS 140-1 shall still be accepted and deemed as valid. • FIPS 140-1/2 [5] deals only with the CM and does not cover the interfacing ICT systems / applications (usually based on NT or Unix and additional software). • The auditor can check on Common Criteria websites (e.g. http://www.cesg.gov.uk/, http://www.bsi.bund.de/ or www.commoncriteria.de) for information related to certified PKI products. • Archived PIN codes should be securely kept, e.g. placed in tamper-evident envelopes and stored in a safe(box) whereby each envelope is in a separate safe(box) only accessible by designated individuals. In this case, access control to these safebox must be consistent with the overall security organization.

Subject	**CWA 14172-2 [18] Guidance**
Assessment of cryptographic module	Please refer to CWA 14172-2, section 3.6 for indications on this requirement.
	Best practice
	Guidance Element G.2.27 addresses what the assessment team should verify about compliance of the devices, namely evidence of the devices proper certification.
Subject	**Additional Guidance**
Initialization Cryptographic Module (CM)	See also clause 7.2.7 on life cycle management of cryptographic modules. The CA should make available evidence for all of the above.
	Best practice
	Please find listed below some of the most important CM related aspects, the abidance by which an assessor should verify: • Processes for a CM, of which at least the following partial list can be identified: - Activation: putting the CM in a state suitable for a specific task (e.g. Initialization, Generation, Usage, Destruction). - Initialization: setting all security parameters and tokens. - Key Generation: whereby all cryptographic keys are generated (based on the configuration set-up during initialization). - Key Usage: whereby specific cryptographic keys are used. - Key Backup: whereby specific cryptographic keys are backed up. - Key Restore: whereby specific cryptographic keys are restored. - Key Export: whereby specific cryptographic keys are exported. - Key Destruction: whereby specific cryptographic keys are destroyed. • Secure CM shipment from the manufacturer to the CA, e.g. using "tamper evident" packaging. • Adequate CM control during its lifecycle. This means, for instance, that a CM should not be first used in a testing environment with low security characteristics and later in a production environment with high security characteristics unless it is possible to detect tamper attempts, or to reset the CM to its pristine status in a trusted way. • Adequate re-initialized by the CSP of the relevant security parameters in the CM (in particular, seeding of a deterministic pseudo random number generator like Annex C of ANSI X9.17 [37]). The CA should document in detail (i.e., including the required keying commands) the procedure for re-initializing the CM. • Appropriate internal test functions set adoption by the CSP for the CM (for example as required by FIPS 140-1/2 [5]), to verify that it is properly functioning. The procedure for realizing this should be documented by the CA in detail (i.e. including the required commands).

c) *Certification authority key generation shall be performed using an algorithm recognized as being fit for the purposes of qualified certificates.*

d) *The selected key length and algorithm for CA signing key shall be one which is recognized as being fit for the purposes of qualified certificates as issued by the CA.*

NOTE 2: See ETSI TS giving guidance on algorithms and their parameters to be published as TS 102 176-1 shortly after the TS 101 456 1 document has been published.

Subject	**Additional Guidance**
Key length and algorithm for CA signing key	The CA should provide evidence that the choice of the algorithm and key length used by the CA to issue qualified certificates is based on an adequate assessment/research in the field of cryptography.
	Best practice

Subject	Additional Guidance
	The assessment team should take into account at least the following: • TS 102 176-1 [16], that provides guidance on algorithms and key lengths; • Whether at least the following factors have been taken unto account when choosing a certain key length: o the life span of the key o the margins of security the CA needs o the expected progress in computing power and cryptanalysis. • In the TS 102 176-1 [16] it is remarked that if a small public exponent (e.g. equal to three) is used, then it is less secure. It is good practice to avoid public exponents with less than 16 Bits. On the other side it is unusual to use exponents with more than 64 Bits. NOTE: The auditor can determine which public RSA exponent *e* is used by using the following OpenSSL command on the CA certificate: `x509 -inform DER -in <certificate file name> -text –noout`

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.*

Subject	Additional Guidance
A suitable time before expiration of its CA signing key the CA shall generate a new certificate-signing key pair	The CA should specify how does the CA timely renew its key pair, and its Security Policies should specify (at a different depth level) the security related measures on how this implemented.
	Best practice
	The assessment team can take the following into account: • RFC 4210 [21] details a procedure for a root CA key changeover. • If the CA is not a RootCA then other mechanisms apply, basically similar to those adopted for end entities key pair update.

Subject	TS 101 456 [15] Guidance Note
These operations must be performed a suitable time before expiration	NOTE 3: These operations must 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.
	Best practice
	The assessment team should take into account that this time may be defined by some applicable legislations. For example, ninety days before certificate expiration.

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 (see the Directive 1, annex II (g) and annex II (f)).

In particular:

a) *The CA private signing key shall be held and used within a secure cryptographic device which:*

- *meets the requirements identified in FIPS PUB 140-1, or FIPS 140-2 5, level 3 or higher; or*

Subject	Additional Guidance
Requirements identified in FIPS PUB 140 1, or FIPS 140-2	FIPS 140-1 has been replaced by FIPS 140-2 (March 2001), but previous validations against FIPS 140-1 will still be recognized.
	Best practice
	No stipulation.

- *meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [9], 14167-3 [10], CWA 14167-4 [11]; or*
- *is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [7], 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.*

Subject	Additional Guidance
cryptographic module (CM) activation	The CA should provide evidence that the CM is only activated in a sufficiently controlled environment.
	Best practice
	• See also clause 7.2.7. • Before the CM can be used it must be activated; FIPS 140-1/2 [5] defines the "User" and "Crypto (or Security) Officer" roles in which it can be activated. The activation is usually done with special "datakeys" (e.g. smartcards). The auditor should have an accurate overview of the set-up and the usage of the datakeys and their physical and/or logical protection (e.g. pin codes). The datakeys should be locked in several vaults under the control of the datakey owner.

Subject	Additional Guidance
Physical protection of activated cryptographic module (CM)	The CA should provide evidence that the activated CM (and its peripherals like "datakeys") has been adequately protected against unauthorized access during its lifetime (including its period at the manufacturer).
	Best practice
	The assessment team should verify if suitable protection measures have been implemented by the CA to ensure its CM protection against unauthorized access during its entire life cycle, among which, for example: • the CM manufacturer has provided evidence that the manufacturing cycle was certified according to an accepted criteria (FIPS 140-1/2 [5], CWA 14167-2 [9], etc.) • the CM was securely delivered from the manufacturer to the CA; • the CM was securely stored before being put in service (e.g. in a safe accessible only by authorized officers); • the physical location of the CM is kept under (camera) surveillance and to declare this location as a "no lone" zone (see TS 101 456 [15], clause 7.4.4.e)); • Entry logs to the room where the activated CM is located, are kept and archived.

b) *When outside the secure cryptographic 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 secure cryptographic device.*

Subject	Additional Guidance
CA private key protection	• Where protection is achieved through storage in a CM: o the CA should provide evidence that the CM is certified by a competent certification body against an evaluation report from a competent evaluation body, according to the criteria specified in the TS 101 456 [15]; o the assessor should verify that the CM is installed in accordance with the assumptions used under which the CM was certified. • Where protection is achieved through algorithms, like encryption or shared secret algorithms: o The CA should provide evidence that the choice of the algorithm and, where applicable, key length used by the CA to protect the CA private signing key is based on an adequate assessment/research in the field of cryptography.
	Best practice
	• Currently, there is no formal EESSI standard regarding key length and algorithms for protecting the CA signing key, for example through encryption or secret sharing. Neither TS 102 176-1 [16] nor TS 102 176-2 [17] provide guidance on this subject. When encryption is used it is a good practice to use a secure algorithm with a random key with at least 168 bits. The best practice would be to use AES-256. This probably provides adequate security most likely until 2015 and possibly until 2036, please refer to NIST Special Publication 800-57 [38]. • The CM should allow exporting the private key only under a randomly generated key of at least 90 bits.

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 secure 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.*

Subject	Additional Guidance
Security of backup copies key.	The CA should provide evidence that the process in which the CA signing key is backed-up is adequately controlled, this includes the requirement that for this process an adequate, documented procedure should be in place.
	Best practice
	• Making backups is a security critical operation: - a documented backup script should exist which must be tested prior to execution. This is to assure that produced backups are correctly formed; - the CA must draft and archive a report on creation of backups. • The backup of the CA key is often a "cloned" CM and "cloned" datakeys. The security of these clones must have at least the same level as the operational CM and datakeys. Cloned datakeys should also be locked in different safes or safeboxes that are only accessible by designated individuals. Access control to these safes and safeboxes must be consistent with the overall security organization. • Where the backup security is achieved through systems like the Shamir's and Blakley's "m" out of "n" secret sharing, the "n" parts and their access codes should be protected with a security level comparable to the operational CM.

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 (see the Directive 1*, annex II (g) and annex II (f)).*

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.

Subject	TS 101 456 [15] Guidance Note
Integrity and authenticity of the CA key.	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.
	Best practice
	The CA should provide evidence that the process in which the CA certificate is distributed to relying parties adequately protects its integrity and authenticity. For example the following practices can be used. • To provide trust on the self-signed CA certificate among other methods, one or both of the following ones can be used: o the self-signed certificates can be placed on a marked medium that can only be written once (e.g. a CD-ROM or WORM) and that can be provided with a mark of authenticity (e.g. a conventional signature) or can be securely distributed through a secure device or trusted communications channel; o the hash of a self-signed certificate can be published in a newspaper, telephone book or even a secure access website. The control mechanism (e.g. viewing the detail information from a browser's certificate management applet) should be described in the CP or CPS. • TS 102 176-1 [16] provides indications on the hash algorithms reliability. • It is good practice to verify the cryptographic correctness of subCA certificates before handing them over to relying parties. • Assessors should verify if the adopted mechanism is reliably implemented. For instance: they should verify if the way the published CA certificate/public key digest is correctly and timely fed into the applications involved in the CA certificate verification.

7.2.4 Key escrow

Subject private signing keys shall not be held in a way which provides a backup decryption capability, allowing authorized entities under certain conditions to decrypt data using information supplied by one or more parties (commonly called key escrow) (see the Directive [1], annex II (j)).

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, may also be used to sign other types of certificates, as well as revocation status information, as long as operational requirements for the CA environment, as specified in clauses 7.2.1 to 7.2.3, 7.2.5 to 7.2.7 and 7.4, are not violated;

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

Subject	**Additional Guidance**
Proper use of CA keys.	The CA should provide evidence that the CA private signing keys are not used inappropriately, e.g. a balanced log journal of the CM can be such an evidence.
	Best practice
	The assessment team should verify that suitable measures are implemented to ensure abidance by the referenced provisions, for example the following ones. • The use of a CA private signing key must be limited to the certificate and (where applicable) certificate revocation lists signing task only as specified in TS 101 456 [15], clause 7.2.5 letter a). • A CA private signing key is not used in cryptographic services other than certificate signing and (where applicable) CRL signing. For instance, a CA private signing key shall not be used to establish an SSL connection. • Assurance that a CA private signing key is not used inappropriately must also come from the (physical) control surrounding the cryptographic module, in which the CA private signing key resides. • The certificate associated with the CA private signing key has its key usage fields set according to its function (e.g. CRLsign and Certificate Signing (keyCertSign)) and must not have any other key usage set (e.g. Data Encipherment). See TS 101 862 [6], annex A.

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 (see the Directive 1, annex II (g) and annex II (f)).

In particular:

Certificate generation

a) *all copies of the CA private signing keys shall be destroyed or put beyond use.*

Subject	Additional Guidance
Destruction of signing CA keys	• The CA should provide evidence that the process (including procedures and training) in which CA keys are destroyed or put beyond use is sufficiently controlled. • The CA should provide evidence that all previous CA keys (including its copies or related tokens) are destroyed or put beyond use.
	Best practice
	The assessing team should verify, regarding the destruction of the signing CA keys, that evidence exists specifying the procedures in force. Additionally, if these procedures have already been implemented, the assessors should verify that evidence exists that they have been enacted conforming to the practices in force. Example of suitable practices follow: - The actual operations are documented in a detailed script which should be tested prior to execution. - A description of the responsibilities (roles) of the persons present at the key destruction should be documented. It should be clear what (signed) assurance these persons are actually giving. - All components (e.g. the "datakeys") related to the signing key must be involved in the destruction process. - The actual destruction should be reported and archived. - If a partial or encrypted CA key is not readily available for destruction it may be considered sufficient that other partial keys, or the key encrypting key, are destroyed provided that it can be demonstrated that the key cannot be put back into use. - Depending on the hardware used, it may be good practice to physically destroy the datakeys or smartcards related to the destroyed signing key, after they have been destroyed logically. - The datakeys or smartcards must not be used twice unless there is assurance that reusing will not affect security.

7.2.7 Life cycle management of cryptographic hardware used to sign certificates

The CA shall ensure the security of cryptographic hardware throughout its lifecycle (see the Directive 1, *annex II (f)).*

Certificate generation

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; and*

e) *CA private signing keys stored on CA cryptographic hardware are destroyed upon device retirement.*

Subject	Additional Guidance
Security of Cryptographic Module (CM) during its lifetime.	• The CA should provide evidence (including records of security-related actions) that the CM (and its peripherals like "datakeys") is and has been adequately protected against unauthorized access during its lifetime. • The CA should provide evidence that: - the CM was securely initialized and tested before being used in production; - the CM is adequately tested periodically while in production; - the CM was securely destroyed at end of its life-cycle.
	Best practice
	The assessment team should verify that evidence exists of suitable practices in force, fro example: • designating the above mentioned controlled environment as a "no lone" zone, i.e. a zone where no (even trusted) employee is allowed to be alone for a significant period of time (see also clause 7.4.4. e); • activation of a CM (in either user or Crypto officer mode) is only done when required; • installation, initialization, generation, usage, and destruction or management of CMs is performed in the presence of no less than two designated employees; • appropriate controls should be in force for the reparation of CMs at the manufacturer (if at all applicable). See clause 7.2.1; • all important events (to be formally determined) relating to the CM should be reported and archived.

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 (see the Directive 1, annex II (f) and (j)).

Certificate generation

If the CA generates the subject keys:

a) *CA-generated subject keys shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures 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 is recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate.*

NOTE: *See ETSI TS giving guidance on algorithms and their parameters to be published as TS 102 176-1 shortly after the current document has been published.*

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, if required via the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole control.*

e) *Once delivered to the subject any copies of the subject's private key held by the CA shall be destroyed.*

Subject	Additional Guidance
Algorithm and key-length used for CA-generated subject keys.	The CA should provide evidence that the choice of the key generation algorithm and key length used by the CA is based on an adequate assessment/research in the field of cryptography.
	Best practice
	TS 102 176-1 [16] provides information on suitable algorithms and key lengths.

7.2.9 Secure-signature-creation device preparation

NOTE 1: This clause is NOT applicable to the qualified certificate policies: QCP public.

The CA shall ensure that if it issues SSCD this is carried out securely (see the Directive [1], annex III).

Subject device provision

In particular, if the CA issues a SSCD:

a) secure-signature-creation device preparation shall be securely controlled by the service provider;

b) secure-signature-creation device shall be securely stored and distributed;

c) secure-signature-creation device deactivation and reactivation shall be securely controlled;

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

NOTE 2: 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.

NOTE 3: Requirement for SSCD preparation listed above may be fulfilled, for example, using a suitable protection profile, defined in accordance with ISO/IEC 15408 [7] or equivalent.

Subject	**Additional Guidance**
Secure handling of SSCDs	Protection profile CWA 14169 [39] can be used as a reliable protection profile, since it has been listed in European Commission Decision of 14 July 2003, published on the 15/7/2005 issue of the Official Journal of the European Union among "*reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC [1] of the European Parliament and of the Council*".
	Best practice
	The assessment team should verify, for example: • That the following CWA 14169 [39]requirements are met: - Private signing key for end-user is either generated in a SSCD of type 1 and sent to the actual SSCD of type 2 or 3 over a trusted channel or is generated in a SSCD of type 3. In the first case, the private signing key must be destroyed from the SSCD of type 1. - The activation data (typically a PIN code) is not printed or stored in the clear; e.g. so-called PIN mailers must be used. - There must be adequate assurance that the SCCD and the user activation code are delivered to the right person. • That suitable practice are in force to securely prepare activation data and to distribute them separately from the SSCD. For example: o The SSCD and/or activation data are handed over to the end-user by the CSP. The end-user is then typically also given the required software/hardware. o The SCCD is sent by registered mail whereby the recipient is required to authenticate himself with a national ID card, where applicable; the activation data (PIN code) may be either sent by separate mail in a neutral envelope or handed over to the user at his/her registration at the registration facility.

7.3 Public key infrastructure - Certificate Management life cycle

7.3.1 Subject registration

The CA shall ensure that subjects are properly identified and authenticated; and that subject certificate requests are complete, accurate and duly authorized (see the Directive 1*, annex II (d)).*

Subject	Additional Guidance
"Properly identified and authenticated"	The assessor should review the identification and authentication procedures implemented by the CSP.
	Best practice
	These procedures - should be found in the following documents: • Certification Practice Statement • Operating Handbooks • Detailed Working Instructions

In particular:

Registration

Subject	TS 101 456 [15] Guidance Note
Term: "Specific attributes"	NOTE 1: When registering, a subject is identified as a person with specific attributes. The specific attributes may indicate, for example, an association within an organization possibly with a role.
	Best practice
	The term "specific attribute" is to be interpreted as "attribute" as defined in TS 101 456 [15] (see clause 3). In the context of registration this can include any information that helps identify the person.

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 (see the Directive [1], annex II (k)).*

b) *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.*

Subject	TS 101 456 [15] Guidance Note
The CA shall communicate Terms and Conditions through a durable means and in readily understandable language.	NOTE 2: A model PKI disclosure statement which may be used as the basis of such a communication is given in annex B.
	Best practice
	PKI disclosure statement is just one possible means to convey this information. The assessing team should verify if the communications means is "durable", depending on its format, and in clear language.

c) *The service provider shall verify at time of registration by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or shall have been checked indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation.*

Subject	Additional Guidance
Term: "by appropriate means in accordance with national law"	n order to comply with "appropriate means", the assessor should investigate whether: • The service provider verifies the identity of the end user against a legally valid means of identification.
	Best practice
	Reference material: a valid means of identification can be a legal identification document as specified by the relevant national law, but certain bodies may validly implement other identification means, as per the applicable law.

Subject	Additional Guidance
Checking the evidence of the identity	The CA should provide evidence that the person's identity is adequately checked, for example in the following ways: • The registration facility can check the evidence of the identity by requiring physical presence of the Person (end user) either **directly** or **indirectly**; • Evidence checked **directly** means that the Person will physically appear at the registration facility. • Evidence checked **indirectly** means that the procedure as mentioned under Directly has been performed at an earlier stage by the same registration authority or another authority trusted to support registration.
	Best practice
	The assessor should investigate whether: • The process of Indirect person's identity checking provides equivalent assurance to directly checked identity (i.e. requiring physical presence at the registration facility). • The submitted evidence of indirect person's checks is in the form of either paper or electronic documentation. Electronic documentation should have incorporated adequate security measures in order to provide assurance equivalent to evidence checked directly.

NOTE 4: Attribute certificates are outside the scope of the present document as they contain no public signing key.

d) Where the subject is a person evidence shall be provided of:

- *full name (including surname and given names consistent with the applicable law and national identification practices);*
- *date and place of birth, a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.*

Subject	TS 101 456 [15] Guidance Note
Evidence shall be provided of: - full name - date and place of birth, a nationally recognized identity number, or other attributes	NOTE 5: It is recommended that the place be given in accordance to national conventions for registering births.
	Best practice

NOTE 6: The CA is liable as regards the accuracy "of all information contained in the certificate" (see annex A).

Subject	Additional Guidance
Evidence shall be provided of: - full name - date and place of birth, a nationally recognized identity number, or other attributes	In some countries some documents used to prove someone's identity may not bear the full name, but only some initials, as well as maiden name or married name for women. Additional problems may be found regarding the place of birth, that may vary after issuance of some identity documents
	Best practice
	The national / applicable law obviously prevail over technical rules, therefore, information provided in legally valid identity documents are acceptable for registration. Similar practice applies for persons registered is association with an organization in item e) below. Assessors should have available the applicable rules of law relevant to subject registration, to verify if the CA practices regarding registration are compliant with the rules of law in force.

e) *Where the subject is a person who is identified in association with a legal person, or other organizational entity, evidence shall be provided of:*

- *full name (including surname and given names) of the subject;*
- *date and place of birth, a nationally recognized identity number, or other attributes of the subject which may be used to, as far as possible, distinguish the person from others with the same name;*
- *full name and legal status of the associated legal person or other organizational entity;*
- *any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity;*
- *evidence that the subject is associated with the legal person or other organizational entity.*

d) *The CA shall record all the information used to verify the subjects' 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.*

g) *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).*

Subject	Additional Guidance
Subscriber authorization	Where a subject is being registered as a member of an organization and the subscriber is an official acting on behalf of that organization the registration authority should check that the subscriber is authorized to act for that organization. This implies that the person acting on behalf of the subscribing organization, provides evidence of the actual existence of such organization." The registration check made under item e) above of "*evidence that the subject is associated with the legal person or other organizational entity"* should also verify that the subject is an authorized member of the organization.
	Best practice
	The assessors should verify if the registration procedures require the registration officer to verify if: 1. the subscribing persons (legal or natural) provide evidence of their own identities; 2. the subscribing person is lawfully representing the subject's organization; 3. there is evidence of the subject's association with the same organization. The assessor should verify, in accordance with the applicable laws and/or statutory or customary rules, if these procedures are actually abided by.

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

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

- *agreement to the subscriber's obligations (see clause 6.2);*
- *if required by the CA, agreement to use a SSCD;*

NOTE 7: The above item above does not apply for QCP Public.

- *consent to the keeping of a record by the CA of information used in registration (see clause 7.4.11 h), i) and j)), subject device provision (see clause 7.4.11 items m), n) and any subsequent revocation (see clause 7.4.11 o)), identity and any specific attributes of the subject 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;*
- *whether, and under what conditions, the subscriber requires and the subject's consents to the publication of the certificate;*
- *confirmation that the information held in the certificate is correct.*

Subject	**TS 101 456 [15] Guidance Note**
Recording of the information regarding subjects, subscribers and agreements subscribed by the subject	NOTE 8: The subscriber or the subject 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 9: Other parties (e.g. the associated legal person) may be involved in establishing this agreement. NOTE 10: This agreement may be in electronic form. The assessors should: 1. have available all the relevant agreements, either in paper or electronic form; 2. ensure that the agreement and registration procedures address the identified requirements.
	Best practice
	No stipulation.

Subject	**Additional Guidance**
Consent to keeping of a record	The assessor should investigate whether the user agreement includes the *users consent* for the following, where applicable: • keeping a record of registration information; • passing this information to third parties; • publishing the certificate.
	Best practice
	No stipulations.

j) *The records identified above shall be retained for the period of time as indicated to the subscriber (see a) and b) above) and as necessary for the purposes for providing evidence of certification in legal proceedings according to the applicable law.*

Subject	**TS 101 456 [15] Guidance Note**
The registration related records shall be retained for the period of time required by the "applicable law"	NOTE 11: 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.
	Best practice
	The assessing Team should identify all the involved countries and should sight the record keeping requirements in the light of the three items above.

k) *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.*

Subject	**Additional Guidance**
Proof of possession of the private key	The assessor should ascertain whether the certification procedure ensures that the subject has possession of the private key associated with the public key presented for certification.
	Best practice
	RFC 4210 [21] and RFC 4211 [22] address Proof of Possession of the private key.

l) *If the subject's key pair is not generated by the CA and the certificate policy requires use of an SSCD (i.e. QCP public + SSCD), the certificate request process shall ensure that the public key to be certified is from a key pair effectively generated by a SSCD.*

Subject	**Additional Guidance**
Ensuring that the certification related key pair is generated by a SSCD	The assessor should ascertain whether the key generation and certification procedure ensure that the public key to be certified is from a key pair effectively generated by a SSCD.
	Best practice
	This can be achieved in several ways, that require the SSCD to generate the core of the certification request, and to protect it in a way that allows the CA to ascertain that the key pair is actually generated by the SSCD.

7.3.2 Certificate renewal, rekey and update

The CA shall ensure that requests for certificates issued to a subject who has already previously been registered 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 (see the Directive [1], annex II (g)).

Subject	**TS 101 456 [15] Guidance Note**
Certificate renewal	NOTE: The subscriber may, if the CA offers this service, request a certificate renewal for example where relevant attributes presented CA the certificate have changed or when the certificate lifetime is running out.
	Best practice
	Where the CA provides this service it should provide the assessing team with evidence of appropriate examples where users in the mentioned conditions have actually been able to renew their certificates. The Assessing team should also verify (by examining the procedures and/or through test cases) if this is actually possible.

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 is 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) and i).*

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 c) to g).*

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.*

Subject	**Additional Guidance**
Term: "Cryptographic security is sufficient"	"Cryptographic security is still sufficient" means "recognized as being fit for the purposes of qualified certificates" as mentioned in Guidance clause 7.2 after note 2.
	Best practice
	No stipulations.

7.3.3 Certificate generation

The CA shall ensure that it issues certificates securely to maintain their authenticity (see the Directive [1], annex II (g)).

In particular:

Certificate generation

a) *the certificates are generated and issued in accordance with annexes I of the Directive [1]. Qualified certificates must contain:*

- *an indication that the certificate is issued as a qualified certificate;*
- *the identification of the CA [Certification-Service-Provider] and the State in which it is established;*
- *the name of the signatory or a pseudonym, which shall be identified as such;*
- *provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;*
- *signature-verification data which correspond to signature-creation data under the control of the signatory;*
- *an indication of the beginning and end of the period of validity of the certificate;*
- *the identity code of the certificate;*
- *the advanced electronic signature of the certification-service-provider issuing it;*
- *limitations on the scope of use of the certificate, if applicable; and*
- *limits on the value of transactions for which the certificate can be used, if applicable.*

NOTE 1: A standard format for qualified certificates meeting the requirements of annex I of the Directive [1] is defined in TS 101 862 [6].

b) *The CA shall take measures against forgery of certificates, and, in cases where the CA generates signature-creation data, guarantee confidentiality during the process of generating such data; (see II (g) of the Directive [1]).*

Subject	Additional Guidance
Measures against forgery of certificates, and confidentiality during the signature key pair generating process performed by the CA;	The assessor should investigate whether the practices and security policies in force specifically enforce procedures ensuring: 1. signature creation data are not available in clear; 2. procedures for forwarding the public key to the certificate generation process ensure the coupling between public and private key; 3. the CA certificate signing key cannot reasonably be used off control or for arbitrary usage.
	Best practice
	Examples of implementing the above requirements are: 1. the signature key pairs are created in a HSM certified as specified in clause 7.2.1 letter b) and the private key never leaves the HSM in clear; 2. the public key leaves the generating HSM inside a cryptographic envelope signed within the generating device with the corresponding private key; 3. the certificate signing private key is kept in an HSM certified as specified in clause 7.2.2 letter a) and is operated as specified in clauses 7.2.5 and 7.4.

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.*

Subject	Additional Guidance
The certificate is securely linked to the associated registration, including the provision of any subject generated public key.	The assessor should investigate whether the exchange of registration data is adequately linked to the correct possibly subject generated public key, by: • checking whether the certificate generation procedure securely provides for the association between the registration data and the possibly subject generated public key; • checking whether the submission of the subject generated public key is reliably associated to the subject registration data.
	Best practice
	RFC 4210 [21] and RFC 4211 [22] provide a suitable indication on how the above requirements can be implemented.

d) *if the CA generated the subjects key:*

- *the procedure of issuing the certificate is securely linked to the generation of the key pair by the CA;*
- *the private key (or SSCD - see clause 7.2.9) is securely passed to the registered subject.*

Subject	Additional Guidance
The Private key (or SSCD) is securely passed to the registered subject.	The assessor should investigate whether the related practice provides sufficient checks to ensure that no one except the registered subject may tamper with the private key (or SSCD).
	Best practice
	Examples on how to abide by the above requirements are: 1. The SSCD is delivered to the subject along a channel different from the one along which the activating data are delivered. 2. The private key is encrypted with a key derived from a passphrase/PIN long enough to be reasonably secure (PKCS#5 [23] provides a reliable mechanism to derive an encryption key from a password), that is delivered to the subject along a channel different from the one along which the private key is delivered.

e) *The CA shall ensure over time the uniqueness of the distinguished name assigned to the subject within the domain of the CA. (i.e. over the life time of the CA a distinguished name which has been used in an issued certificate shall never be 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.*

NOTE 2: See also clause 7.4.10 on Data Protection requirements.

Subject	Additional Guidance
The registration data confidentiality and integrity to be ensured when exchanged.	The assessor should investigate whether the registration data are exchanged in a secure way, abiding also by the applicable Data Protection requirements.
	Best practice
	Examples on how to abide by the above requirements are: 1. adoption of secure channels like SSL/TLS, VPN, IPSec, 2. data are encrypted in a way that only the intended recipient can decrypt, e.g. through asymmetric encryption.

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.*

Subject	Additional Guidance
Registration data exchange between distributed CA components	The assessor should investigate whether the exchange of registration data is adequately secured.
	Best practice
	The above requirements can be abided by protecting the communication between the PKI(CA) components and between subscriber and the CA system to ensure integrity and confidentiality (investigate security functionalities). In this case the CA System should maintains files in which the communication events are logged.

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 (see the Directive [1], annex II (k)).

In particular:

a) *The CA shall make available to subscribers and relying parties the terms and conditions regarding the use of the certificate including the Directive [1], annex II (k):*

- *the qualified 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 uses of a SSCD;*
- *any limitations on its use;*
- *the subscriber's obligations as defined in clause 6.2, including whether the policy requires uses of a SSCD;*
- *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);*
- *limitations of liability including the purposes/uses for which the CA accepts (or excludes) liability;*
- *the period of time which registration information (see clause 7.3.1) is retained;*
- *the period of time which CA event logs (see clause 7.4.11) are retained;*
- *procedures for complaints and dispute settlement;*
- *the applicable legal system; and*
- *if the CA has been certified to be conformant with the identified qualified 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 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 [12] on unfair terms in consumer contracts.

Subject	**Additional Guidance**
Term: durable means of communication	The assessor should investigate whether the information is made available through a durable means of communication. This means that the information carrier, the application and the file format can stand the test of time (e.g. the subscriber certificate validity period added to the archival period required by law.
	Best practice
	No stipulations.

Subject	**Additional Guidance**
Term: "Readily understandable language"	The assessor should take notice of the fact that: • the terms and conditions shall be in accessible and understandable wording, for the CA's audience, from a technical, as well as from a legal point of view.
	Best practice
	Reference material: other end user ICT/Telecommunication terms and conditions.

Subject	**TS 101 456 [15] Guidance Note**
Term: "PKI Disclosure Statement (PDS)"	NOTE 1: A model PKI disclosure statement which may be used as the basis of such a communication is given in TS 101 456 [15] annex B. Alternatively this 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.
	Best practice
	In case a PDS is used, the assessor should investigate: • If there is additional documentation available to the end user that provides a detailed overview of the rights and obligations. • If this end user is informed adequately in accordance with clause 7.3.1 a. A PDS is a supplementary and simplified instrument to a CP/CPS that can assist PKI users, often not expert in the PKI technology, in making informed trust decisions. A PDS is not intended to replace a CP or CPS.

7.3.5 Certificate dissemination

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties (see the Directive 1*, annex II (l)).*

In particular:

Dissemination

a) upon generation, the complete and accurate certificate shall be available to 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;

Subject	Additional Guidance
Certificates availability only if the subjects gave their consent	The assessor should ascertain that certificates are not available for retrieval in those cases for which the subjects" consent was not obtained.
	Best practice
	The assessor may ask for issuance of a test certificate without giving this consent and verify that this certificate is not publicly available.

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) *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 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;*

f) *The information identified in b) and c) above shall be publicly and internationally available.*

Subject	Additional Guidance
Certificates (upon authorization) and terms and conditions shall internationally be available to relying parties 24 × 7	The assessor should ascertain that practices exist specifying the maximum delay in recovering from incidents and indicating the emergency procedures to enforce, should the 24 × 7 rule may not be met due to force majeur cases.
	Best practice
	These practices, may usually be within the broader business continuity, or disaster recovery, procedures, but it must be possible to selectively access those relative to the PKI. They should indicate the way back up copies are performed, the existence of a disaster recovery site, the procedures to keep the operational systems up to date, the personnel education plan, the procedures to enact in case of emergency, etc. consistently with what can be found in specialized DRM / BC dedicated sites.

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 (see the Directive [1], annex II (b)).

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:*

- *who may submit revocation reports and requests;*
- *how they may be submitted;*
- *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.

- *whether and for what reasons certificates may be suspended;*
- *the mechanism used for distributing revocation status information;*
- *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 1 day.*

Subject	Additional Guidance
Procedures for revocation of certificates	1. The one day delay encompasses the entire process, from the revocation/suspension request being received by the CA from an authorized party (e.g. from subject), through the request processing up to the revocation request rejection or to the certificate revocation publication. 2. The entire revocation / suspension request handling process must be logged by the CA suitably for a subsequent audit. 3. Particular attention is to be given to the way the revocation / suspension requesting party authentication and authorization verification is performed.
	Best practice
	1. It is recommended that the basic authorized parties are: a. The subject. b. The subscriber (i.e. the physical or legal person under which subscription the subject was issued the certificate). c. The Registration Authority or the CA themselves, that may have become aware of unacceptable behaviour by the subject or the subscriber. The Registration Authority may also act on behalf of the belonging CA or upon warrant by a Judge or equivalent authority. 2. The one day delay rule must take into account the technical time necessary to process the revocation / suspension request. 3. By including this delay in the 1 day processing, it is may be possible for the revocation requests that are submitted too close to the next CRL publishing time if CRL are published regularly every 24 hours. If this delay is significant (e.g. more than 5 minutes) it may be necessary to issue additional CRLs or issue CRLs more regular frequency than every 24 hours. 4. The revocation / suspension related logging system must ensure all log records are securely registered and kept, and must have an application that allows to easily inspect the log file. 5. The revocation / suspension requesting party must be authenticated. Examples of three basic ways to do this follow: a) via suitably long passphrase/PIN, subject to specific composition rules, to be used: i. on a web site; ii. through a contact centre; b) via a signed document sent via e-mail or submitted through a suitable web page application; c) requester's showing up at the competent authority such as the Registration Authority. In case a. the following possible examples may apply: 1. If a telephone automatic reply is used, only PINs can be used as the voice recognition technology under certain conditions may not be reliable; both tone and impulse mechanisms should be supported. 2. If a telephone automatic reply is not used, the suspension request handling system must take into account the possibility that a suspension is subsequently withdrawn, thus re-enabling the certificate; if the PIN is disclosed in its entirety, its confidentiality is broken; an example of an actually used solution: only a random chosen PIN digits subset is requested for input, and the authentication allows for a limited number of attempts (3 to 5 depending on the key length). This allows for PIN re-use in a subsequent request for revocation or for new suspension. Case a) should not be used for third parties, such as subscribers, since, given the possible repeated requests for subjects" certificates revocation, the Password/PIN confidentiality would be at risk. Only cases b) and c) should be used.

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.*

Subject	Additional Guidance
Revocation requests to be processed on receipt	Revocation requests may be of two types: 1. requests that require immediate revocation (e.g. private key compromise); 2. requests submitted in advance for planned revocation (e.g.: when subjects cease from their job in a planned and friendly way). The first type shall be processed upon receipt and should give way to insertion of the certificate revocation in the next available certificate status update (CRL or on-line service), the second type should be processed upon submission, to ascertain their due time.
	Best practice
	The assessor should verify that both request types are processed upon request, and should ascertain that: 1. Type one requests are immediately enacted upon submission to be published the soonest possible, consistently with the publication mechanism adopted (CRL, OCSP). NOTE: Where CRLs are used, it is deprecated to immediately publish "urgent" revocations regardless of the scheduled next CRL issuance time. CRLs can be issued shortly before such time, to prevent possible "last minute" system malfunctions to impede the CRL timely publication, but they should not be published whenever the revocation request is submitted, to prevent man-in-the-middle / replay attacks. 2. Type two requests are published timely before the due enacting time.

c) *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.*

d) *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.

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

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

g) *Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least daily and:*

- *every CRL shall state a time for next CRL issue; and*
- *a new CRL may be published before the stated time of the next CRL issue;*
- *the CRL shall be signed by the certification authority or an entity designated by the CA.*

NOTE 3: In order to maximize interoperability it is recommended that the CA issue Certificate Revocation Lists as defined in ISO/9594-8 [3].

Subject	Additional Guidance
Publication interval	The assessor should investigate the interval between the publication of CRLs, as published in the CPS. This interval shall be set to at least daily (once per 24 hours). There is no prescription for the time of issuance of the CRL. However, consideration should be given to the impact of processing time leading a revocation request missing a regular 24 hour certificate issuance period. (see previous additional guidances).
	Best practice
	No stipulations.

h) *Revocation management services 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 service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement.*

Subject	Additional Guidance
Upon system failure, [omissis] this service is not unavailable for longer than a maximum period of time as denoted in the CPS	This requirement relates to usual system failures, it does not apply to disasters, where specific publicly available Disaster Recovery/ Management Policies come into force.
	Best practice
	Assessors should verify if: 1. the CA CPS provisions address this subject; 2. in the existing recordings there is evidence that incidents in the past did not affect the revocation service availability as declared in the CA CPS.

Revocation status

i) *Revocation status information, shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which is 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.*

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

Subject	Additional Guidance
Availability of revocation management services and certificate status information	1. The assessor should investigate the availability of revocation management services and of revocation status information. In case (one of) the above mentioned services has been outsourced, the assessor should check the existence of contracts with third parties/delegates as to whether the CA has enforced the relevant obligations mentioned in TS 101 456 [15]. 2. This requirement applies also in case of disaster. As relying parties should not accept signatures unless they have certificate status information, steps should be taken to ensure the availability of already published status information even in the case disaster causing failure of a failure of services from a single location.
	Best practice
	Item 1: No stipulations. Item 2: The CA should have in place a shadowing / mirroring system of the repositories where CRLs are published and/or OCSP responders are in place from more than one location.

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

k) *Revocation status information shall be publicly and internationally available.*

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

7.4 CA management and operation

7.4.1 Security management

The *CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards (see the Directive [1], annex II (e), 2nd part).*

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.*

Subject	Guidance
The CA shall carry out a risk assessment	The CA should provide the assessors with the results of the risk assessment, with the practice statements and with the security policies in force to evaluate if the identified risks have all been addressed. NOTE: While CPS are commonly made publicly available, security policies are essentially for CA internal use, i.e. their confidentiality is to be protected. As a consequence the highly security relevant issues are only specified in the security policies and access to security policies can be selective depending on the addressed topics.
	Best practice
	The conformity assessors should evaluate if all the risks identified have been addressed in the practices statements and/or in the security policies.

Subject	Guidance
The risk analysis shall be regularly reviewed and revised if necessary.	The CA should annually review the risk assessment to identify any major changes, also taking into account incidents occurred since the previous risk assessment. The CA should provide the conformity assessors with the reviewed practices statements and security policies.
	Best practice
	The conformity assessors should verify that all the practices statements and the security policies, modified as per the risk assessment revisions, are complied with.

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.*

Subject	Guidance
Certification services outsourcing	The CA should provide the assessor with information on all arrangements for outsourcing.
	Best practice
	No stipulation.

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.*

Subject	Guidance
A high level steering forum is responsible for the CA's information security policy	The CA should provide the assessing team with documentation on the forum components and responsibilities, as well as the duties of the certification services related employees, as well as with description of the mechanisms to keep employees informed on the certification service procedures and policies.
	Best practice
	The assessor should verify that the steering forum is formally established and that procedures are in place to ensure all related employees are timely informed of any certification services procedures and policies update.

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

Subject	Additional Guidance
Term: a system or systems for quality	The assessor should review if the CA has implemented and documented a system or systems for quality and information security management.
	Best practice
	Quality and information security management system requirements usually do not mention a specific period in which internal audits and management review of the quality system should take place. CAs should carry out internal audits followed by management reviews of the CAs quality system at least once each year.

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.*

Subject	TS 101 456 [15] Guidance Note
Information security infrastructure management.	NOTE 1: See ISO/IEC 17799 [13] for guidance on information security management including information security infrastructure, management information security forum and information security policies. Other alternative guidance documents are given in bibliography.
	Best practice
	No stipulation.

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

Subject	TS 101 456 [15] Guidance Note
Security controls and operating procedures management	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.
	Best practice
	No stipulation.

g) *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.*

Subject	Additional Guidance
Security Management	The CA shall have a documented information security management system (ISMS), available to the assessor. This should at least include or refer to: • A definition of Information Security (IS), overall policy, objectives and scope. • Legal and contractual IS requirements. • Organization of Information Security, including: - A framework for information security, e.g. the allocation of responsibilities to assets (see below), and important processes, e.g. the core CA processes, user management & authorization, and business continuity. - Complete asset inventory, classification and allocation of responsibilities to individuals (see below). - Requirements on risk-analysis to be used. - Requirements on information security plans. - Security requirements on outsourcing. - Finance of information security. - Adopted baselines (e.g. for Unix, Windows NT, Firewalls etc.). - Handling of security incidents, including regular reporting to senior management. - When and by whom the information security policy and plans are reviewed and perhaps adjusted. - When and how a third party audits information security. - The way security awareness and training is addressed.The Management of the CA should formally approve the security policy and other documentation specifying the Information Security Management System. Included in the allocated responsibilities, should be that of an Information Security Officer (ISO) responsible for: • The daily management of information security. • Managing the decisional process on security related issues/questions. • Incident handling. • Maintaining the information security policy. One or more System Security Policies shall cover the security of all important (security relevant) business processes of the CA and shall be available to the assessor.
	Best practice
	• For Information Security Management ISO/IEC 17799 [13] can be referred to. • The information security policy and information security plan(s) should be consistent with the CPs and CPSs that the CA supports. • It is crucial that the security of important assets and processes is unambiguously assigned to individuals and that these individuals are sufficiently aware of their tasks, authorities and responsibilities.

	(continued) • Tasks, authorities and responsibilities should be linkable to actual persons. If tasks, authorities and responsibilities are described in terms of "roles" then there should be a document, mapping roles to actual persons. • The goal of a risk-analysis is to find a right balance between the value of assets, the threats jeopardizing it and the controls preventing the threat becoming manifest. Conducting a risk-analysis becomes easier for the CA when they use guidance on: i. value (see asset classification below); ii. threats (e.g. which are relevant); and iii. controls (e.g. lists thereof). A risk-analysis can be quantitative (using probabilities) or qualitative; both are currently commonly used. • The adoption of existing baselines, e.g. for router, firewalls, operating systems, procedures, provides an efficient way to enhance security. • Security audits of outsourced components of a CA can provide assurance on the security of the outsourced components. • The document approval procedure can be part of the Information Security Management System. • The approval procedure for documents may be partly delegated, e.g. to the Information Security Officer. Such delegation should be described in the approval procedure. • It is good practice to realize one integral Information Security Plan containing all information relating to information security; this Information Security Plan may be integrated with the CPS employed by the CA, but in this case part of this ISP will be classified and therefore it should not included in the CPS. • The Information Security Plan and Policy can take the form of internal webpages with attachments; due to its nature iv. version control should be adequately addressed; v. parts of this handbook should be classified; vi. secret core information (e.g. passwords) should not be placed in an Information Security Plan.

7.4.2 Asset classification and management

*The CA shall ensure that its assets and information receive an appropriate level of protection. (see the Directive [*1*], annex II (e)).*

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.*

Subject	Additional Guidance
Asset Classification	• Management of asset classification (including updating) should be clearly assigned to a person or body within the CA. • The CA should make readily available to the assessor a complete and up-to-date inventory of all relevant assets. This should include a description of their security properties and make clear the ownership of each asset. • The CA's main security relevant processes should be documented and a relation with the assets used in these processes should be made. • Each asset should be classified according to the CA's classification methodology. Its inventory number and its classification should be clearly marked on the asset itself, when possible.
	Best practice
	• For Asset Classification section 5 of ISO/IEC 17799 [13] can be referred. • With respect to asset classification, it is good practice: i. To define classifications up to the criteria CIA (Confidentiality, Integrity and Availability) in terms of High, Medium and Low. ii. To document a taxonomy for each of the nine possibilities. iii. To designate an asset that has one of its criteria rated as "high", as "security critical"; an asset that has one of its criteria rated as medium is designated as "security related". • "Properties" of assets depend of their nature, this may include for example: iv. computer rooms: keys or codes giving access to it v. cabinets, safes: keys of codes giving access vi. computers (hardware): BIOS passwords or physical keys vii. computers (OS): the accounts enabled with their various security levels (administrators, specific users etc.). viii. CA applications: several users (master users, security officers, CRL users). ix. CMs: datakeys, physical keys x. Datakeys: PIN codes • It is good practice to start with classifying the CA's main security relevant processes and then to let the classification of the assets depend on this classification. • When possible, engraving the inventory number on the asset is good industry practice.

7.4.3 Personnel security

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations (see Directive [1], annex II (e) 1st part).

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.

Subject	TS 101 456 [15] Guidance Note
Sufficient number of suitably skilled personnel	NOTE 1: It is recommended that CA personnel fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two.
	Best practice
	In addition to formal credentials (e.g. security certification like CISSP) and proven specific experience, certification services personnel should undergo regular, although not necessarily periodical, training sessions. Where it is publicized that these training sessions are held, the assessors should have the records of these sessions available.

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

Subject	Additional Guidance
Appropriate disciplinary sanctions	Security policies, certification practices and similar documents should highlight that disciplinary sanctions can be enforced against personnel violating policies and procedures, as per statutory and customary rules of raw in force.
	Best practice
	No stipulation.

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.*

Subject	TS 101 456 [15] Guidance Note
Job descriptions	NOTE 2: It is recommended that the job descriptions include skills and experience requirements.
	Best practice
	No stipulation

Subject	Additional Guidance
Job descriptions	The CA should provide the assessing teams with a complete and up-to-date list of all job descriptions. The role of the function within the distinguished CA business processes and assets should be made clear. Each job should be classified, e.g. as trusted, security-related or non-trusted.
	Best practice
	The assessors should verify if persons are aware of what are their job descriptions and, where applicable, is assignment has been done formally.

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 17799 [13] for guidance.

Registration, certificate generation, subject device provision, revocation management

f) *Managerial personnel shall be employed who possess experience or training in 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.*

Subject	Additional Guidance
Managerial personnel skill	Certification service managers should have background experience and / or formal credentials, and, in addition, should undergo regular, although not necessarily periodical, training sessions should be in place. Where it is publicized that these training sessions are held the CA should provide the assessors with the records of these sessions.
	Best practice
	Assessors should verify if credentials and training sessions evidence match the specific tasks requirements.

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:*

- *Security Officers: Overall responsibility for administering the implementation of the security practices. Additionally approve the generation/revocation/suspension of certificates.*
- *System Administrators: Authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation, subject device provision and revocation management.*
- *System Operators: Responsible for operating the CA trustworthy systems on a day to day basis. Authorized to perform system backup and recovery.*
- *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.*

Subject	**TS 101 456 [15] Guidance Note**
Personnel background screening	NOTE 4: 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.
	Best practice
	Assessors should verify if that any information collected under this requirement is done so legitimately.

Subject	Additional Guidance
Personnel Security	- The responsibility of reviewing Personnel Security should be assigned to a person or body within the CA. - A complete and up-to-date inventory of all job descriptions at the CA should be available. The role of the function within the distinguished CA business processes and assets should be made clear. Each job should be categorized, e.g. as trusted, security-related or non-trusted. - There should be evidence that CA staff is properly made aware of security issues related to their job (responsibilities, threats, etc.), e.g. during formal training. - A complete and up-to-date inventory of all staff employed at the CA should be readily available to the assessor; third party employees should be clearly marked in this inventory. There should be a clear relation between job description inventory and the staff inventory. - All CA personnel should have signed a confidentiality statement (non-disclosure agreement). An inventory of these statements should be readily available to the assessor. Personnel with a trusted role within the CA should have signed a statement indicating that they are free from conflicting interests that might prejudice the impartiality of the CA operations. An inventory of these statements should be readily available to the assessor. Personnel with a trusted role within the CA should submit a "Statement of good conduct", prior to entrance into office. These statements should be readily available to the assessor. The CA should periodically (e.g. yearly) review the trustworthiness of personnel with trusted roles. (FOR INSTANCE personnel MAY fill in and sign a statement on basis of which their trustworthiness can be re-determined). The CA should provide the assessing team with all necessary documentations of the above to provide evidence that provisions have been enforced.
	Best practice
	- For personnel security section 6 of BS 7799:1999-1 (ISO/IEC 17799 [13]) can be referred to. - It is good practice for a CA to let staff of third party contractors sign a separate confidentiality statement (non-disclosure agreement) in addition to the confidentiality agreement covered with the third party contractor. - It is good practice for a CA to refrain from giving third party personnel trusted roles within the CA. - It is good practice for a CA to arrange a meeting between the Information Security Officer and newly hired staff on their first working day and to discuss information security and their role in it. This also presents an opportunity to let the new staff member sign confidentiality (non-disclosure agreement) and independence statements. - Where statutory or legal rules prevent from asking personnel to subscribe statements that commit them to a specific behaviour, the CA be require them to subscribe a statement of having read and understood statements that describe their duties and responsibilities. The assessing team should verify that the documentation provided by the CA demonstrate evidence that provisions have been enforced.

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 (see Directive 1999/93/EC [1] annex II (f)).

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 17799 [13] 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.

Subject	**Additional Guidance**
Physical and environmental security	The CA should make available to the assessor the following: 1. A clear description of its physical environment. This description should discuss: i. security zones implemented and their protection properties (preventive, repressive, detective and corrective); ii. the relation with the security critical assets; iii. which members of the CA staff have access to what zones. 2. Documentation describing the protection (preventive, repressive, detective and corrective) against fire/smoke, power failures, water, storm etc. The CA should implement them, based on a documented risk-analysis. 3. A complete and up-to-date inventory of the CA staff having access to security zones. 4. Documentation on access control systems. 5. Documentation on requirement about access codes to high-security zones; they should be regularly changed. 6. Documentation providing evidence that devices and procedures ensure that any person entering the physically secure area is always in presence of an authorized person. 7. Documentation on to whom the responsibility is assigned of maintaining the above description, risk-analysis and inventory. The CA management should assign them to a person or body within the CA. Periodically reviewing of the above description is a management task.
	Best practice
	• For physical and environmental security section 7 of BS 7799:1999-1 (ISO/IEC 17799 [13]) can be referred. • Reviewing physical and environmental security at least yearly is good industry practice. Refer also to Guidance table before clause 7.4.1 letter b).

7.4.5 Operations management

The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure (see the Directive [1], annex II (e)).

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.*

Subject	TS 101 456 [15] Guidance Note
Policy and practice enforcement	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.
	Best practice
	The CA Managers should give evidence of departmental plans on certificate policies and practices implementation and of their systematic assessment on compliance with these plans.

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.*

Media handling and security

f) *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

g) *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

h) *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.*

i) *Audit processes, meeting requirements specified in clause 7.4.11, shall be invoked at system startup, and cease only at system shutdown.*

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

Subject	Additional Guidance
Incident reporting and response	• The CA should provide assessors with a concise, documented description of incident handling. Amongst other things, the present document should define the notion "security incident" and should clearly assign tasks, authorities and responsibilities. • Similarly, evidence should be available that the incident handling procedure is adequately communicated to the CA staff. • The CA should assign the responsibility of maintaining, updating and periodically reviewing antivirus and other protection programs to a person or body within the staff. • The CA should have in place an adequate change management procedure; the responsibility of maintaining, updating and periodically reviewing this should be assigned to a person or body within the staff. • The CA should proactively keep abreast of emerging, relevant security problems and related patches. In addition the CA should be able to timely and adequately address emerging security problems. Responsibility for both tasks should be clearly defined.
	Best practice Assessors should verify that the CA is pro-active in the following. • Timely acquiring information on sources of security problems, for example on security problems emerging from staff, manufacturers, the "hacker community", or special mailing lists. The CA can also participate in a Computer Security Incident Response Team (CSIRT). • To prevent media obsolescence it is good practice to test such media timely before the probable media decay time. • It is good practice to timely install security patches in a secure manner. • A proper definition of "security incident" is required to provide CA staff guidance on categorizing and reporting relevant incidents. • It is good practice to periodically (e.g. yearly) report on security incidents / problems to the CA management.

Certificate generation, revocation management

Operations procedures and responsibilities

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

NOTE 2: CA security operations' responsibilities include:

- *operational procedures and responsibilities;*
- *secure systems planning and acceptance;*
- *protection from malicious software;*
- *housekeeping;*
- *network management;*
- *active monitoring of audit journals, event analysis and follow-up;*
- *media handling and security;*
- *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.

Subject	Additional Guidance
Operations procedures and responsibilities	• The CA management should assign the responsibility of maintaining the above description, risk-analysis and inventory to a person or body within the CA. Periodically reviewing of the above description is a management task. • The CA should document in detail all security critical operations (e.g. root key generation, end-user registration, end-user certificate production, certificate revocation, CRL production etc.) in procedures, including the roles, staff, responsibilities and assets concerned. This documentation should clarify to the assessor which actual employee performs which role and has which responsibility.
	Best practice
	Procedures as mentioned above are best made part of an integral Information Security Plan and/or CPS.

7.4.6 System Access Management

The CA shall ensure that CA system access is limited to properly authorized individuals (see Directive [1], annex II (f)).

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.

Subject	TS 101 456 [15] Guidance Note
Network Perimeter defence implementation	NOTE 1: It is recommended that firewalls be configured to prevent protocols and accesses not required for the operation of the CA.
	Best practice
	It is a good practice to regularly monitor the firewall related logs and to install an intrusion detection/prevention systems. These systems must be regularly updated.

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.

Subject	Additional Guidance
Sensitive data protection	The CA should provide the assessors with sufficient information on whether the registration data are exchanged in a secure way, and if they are stored in a way to ensure only authorized persons may have access to them.
	Best practice
	The assessment team should verify how the registration data security and confidentiality are ensured. Examples on how to abide by the above requirements are: 1. adoption of secure channels like SSL/TLS, VPN, IPSec, 2. data are encrypted in a way that only the intended users or recipients can decrypt, e.g. through asymmetric encryption or through password based encryption (PKCS#5 [23] provides a reliable mechanism to derive an encryption key from a password).

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 shall be 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).*

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.

Certificate generation

h) *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.*

Subject	Additional Guidance
Local network components configurations periodically audited	The network component configurations (the initial one and all the subsequent ones) should be formally defined and kept by a responsible manager. Their implementation should be recorded on event minutes. The CA should specify these practices in its procedures and / or operating manuals.
	Best practice
	Assessors should inspect if the certification service provider's procedures and / or operating manuals indicate the relevant practices and if requirements specified are met.

i) *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

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

Revocation management

k) *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

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

Subject	Additional Guidance
System Access Management	The CA should provide assessors with documents on the following. • The CA should assign the responsibility of maintaining the system access controls to a person or body within the CA. The system access controls should be periodically reviewed. • The CA should document in detail and keep to date the security configuration of all security relevant assets that should be based on a risk-analysis. .Configuration documentation should clearly indicate all preventive, repressive, detective and corrective controls. A reference copy of this documentation should be kept by the Security Manager. • System access management. • Adequate user management is implemented at the CA, at least for its security related assets. • Adequate account policies are in place for security relevant assets, e.g. computers, operation system, applications, computer rooms, safes. • An up-to-date list of all persons having access to a security related asset of the CA and their level of access. This should be readily available. Historic access records should also be available.
	Best practice
	• The assessing team should verify if the documentations above meet the requirements, among which if the actual configuration matches the reference documentation. • For adequate user management section 9 of ISO/IEC 17799 [13] can be referred to. • The "system access" controls are best made part of an integral Information Security Plan. • A security audit performed by a third party, including a penetration test, on the CA core ICT infrastructure before going into production is good practice. The audit report can provide extra assurance to the assessor on adequate system access management. • The use of technical "security baselines" (for routers, firewalls, operating systems, applications etc.) can enhance security very efficiently.

7.4.7 Trustworthy Systems Deployment and Maintenance

The CA shall use trustworthy systems and products that are protected against modification (see the Directive [1], annex II (f)).

Subject	TS 101 456 [15] Guidance Note
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 [8] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [7]. NOTE 2: It is recommended that the risk analysis carried out on the CA's services (see clause 7.4.1) identifies its critical services requiring trustworthy systems and the levels of assurance required.
	Best practice
	No stipulation

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.*

Subject	Additional Guidance
Trustworthy Systems Deployment and Maintenance	• If a CA uses CA systems accompanied with an EDP Audit statement as a result of an EDP Audit against CWA 14167-1 [8] or equivalent it means that these systems are evaluated by the manufacturers or by the CA. The CA should provide the assessing team with documentation regarding installation, maintenance and use. • The CA should provide the assessing team with evidence that all security critical systems used by the CA for its certificate management are "hardened", that is, the systems are configured such that: all functionality (software, services, network protocols, logical access (e.g. "guest" accounts, physical access (e.g. floppy drives, network adapters)) that is not strictly necessary for the correct functioning of the system are removed, permanently when possible. • The CA should provide the assessing team with evidence that appropriate logging of events is installed on security critical systems used by the CA for its certificate management as well as regularly monitoring of those. Responsibility for monitoring should be clearly defined.
	Best practice
	• The assessor should check the documentation regarding installation, maintenance and use of systems consistently with CWA 14167-1 [8] or equivalent standards that specify security requirements on trustworthy systems (TWSs used for Managing Certificates). Using approved TWSs that have proved conformance to this CWA is the easiest way to meet the policy requirements. • For many platforms, guidelines and even tools are available to "harden" them. Some platforms are even directly available in a "hardened" version.

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 (see the Directive [1], annex II (a)).

In particular:

CA General

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

Subject	Additional Guidance
Term: *"as soon as possible"*	The CA should provide the assessors with its own Business continuity plan and/or the disaster recovery plan. The CA's Business Continuity Plan or the disaster recovery plan should describe: • The consecutive phases and the actions that have to be undertaken after a disaster situation; • The required timeframe between the disaster and the restored status of the CA-system; • The timeframe should be in accordance with the estimated throughput-time of all the required activities. The Disaster Recovery Plan should also include a policy document, that should be public, specifying the non confidential information to be made available to the certification service uses, such as the maximum time required to resume operations should it be necessary to switch to a back up site. The CA CPS should specify that in case of disaster a specific Disaster Recovery/Management policy come into force, and should specify which is the expected delay in resuming the revocation management service.
	Best practice
	The assessing team should review the CA's Business continuity plan and/or the disaster recovery plan to verify if they meet the above requirements

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.*

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

Subject	TS 101 456 [15] Guidance Note
Back up and restore of CA systems data necessary to resume CA operations	NOTE 1: If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.
	Best practice
	No stipulation

Subject	Additional Guidance
Back up and restore of CA systems data necessary to resume CA operations	NOTE: In line with ISO/IEC 17799 [13] clause 8.4.1: "Back-up copies of essential business information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans."
	Best practice
	No stipulation

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.*

Revocation status

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

- *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.*

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

Subject	**TS 101 456 [15] Guidance Note**
Undertakings following CA key compromise: notification mechanisms	NOTE 2: It is recommended that, when a CA is informed of the compromise of another CA, any CA certificate that has been issued for the compromised CA is revoked.
	Best practice
	No stipulation

Subject	**Additional Guidance**
Undertakings following CA key compromise: notification mechanisms	The assessor should review whether the CA has implemented (in accordance with the CA's Business Continuity plan or Disaster Recovery Plan) controls and measures that facilitate a fast notification to relevant parties that the CA key has been compromised and that the certificates and certificate status information are no longer trustworthy.
	Best practice
	The CA may have taken the following measures or may have implemented the following mechanisms to facilitate a fast notification to relevant parties: • E-mail distribution list for subscribers and business relations and a pre-defined notification e-mail. • A standard web-site notification (web-site and directory) for the relevant groups (including relying parties). • A pre-defined notification for a (real-time) on-line news service (e-mail or web page). • An emergency telephone line (recorded message) or a help desk for the relevant parties.

Algorithm compromise

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

- Inform all subscribers and relying parties with which the CA has agreement or other form of established relations. In addition, this information shall be made available to other relying parties.

- Revoke any affected certificate.

Subject	Additional Guidance
Algorithm compromise notification mechanisms	The CA should provide the assessing team with documentation demonstrating that it has implemented measures that facilitate a quick notification to relevant parties that the algorithms, or associated parameters, used by the CA or its subscribers become insufficient for its remaining intended usage and are no longer trustworthy.
	Best practice
	The assessor should review whether the CA has implemented the above measures. The CA may have taken the following measures or may have implemented the following mechanisms to facilitate a fast notification to relevant parties: • E-mail distribution list for subscribers and business relations and a pre-defined notification e-mail. • A standard web-site notification (web-site and directory) for the involved users (including relying parties). • A pre-defined notification for a real-time on-line news service (e-mail or web page). • An emergency telephone line (recorded message) or a help desk for the relevant parties.

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 as covered by the certificate policy, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings (see the Directive [1], annex II (i)).

In particular:

CA General

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

- *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 CAs. In addition, this information shall be made available to other relying parties.*

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

- *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;*

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

Subject	Additional Guidance
Undertakings to transfer obligations for maintaining registration information and event log archives	The CA should provide the assessors with documentation and contracts that prove that the CA has implemented controls and measures to facilitate the seamless transfer of the registration information and event logs to an external organization in case of CA termination for scenarios that may be foreseen.
	Best practice
	The assessing team should verify if the documentations prove the above requirements. The CA decision to terminate operation must be taken and made public with a suitable early notice, in order to timely inform all the involved partied. The CA should have taken the following measures or should have implemented the following mechanisms to facilitate the transfer: • Selection of external organization (continuity requirements). • (Service) contract with an external organization (IT Service Organization, Notary or semi-governmental organization) to store the data and to process a realistic number of data-requests in the future.

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

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.*

Subject	Additional Guidance
Arrangement to cover costs	The CA should provide the assessing team documentation proving that proves that the CA has arrangements in force to cover the costs to fulfil the minimum requirements.
	Best practice
	The assessor should review the above documentation, contracts or other evidence. The CA may have taken the following measures or may have implemented the following arrangements to be able to cover the costs by itself: • An insurance policy, a financial arrangement that is not affected by legal or financial claims or any consequence of bankruptcy of the organization. • The arrangement stipulates that the costs for data continuity are fully covered for the necessary period.

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

- *the notification of affected entities;*
- *the transfer of its obligations to other parties;*
- *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 (see the Directive [1], article 8).

In particular:

CA General

a) *CA shall ensure it meets all applicable statutory requirements (including requirements of the Data Protection Directive [4] – 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);*

Subject	Additional Guidance
Term: important records	The CA should provide the assessing team with documentation providing evidence that records which hold personal data (in accordance with applicable Data Protection Laws and regulations) are adequately protected in accordance with the European Directive. Important records include (whether in paper or in electronic form): • Registration information (included but not limited to personal data of the subscribers and/or end users). • Delivery and Service Contracts with external parties. • Certification related information, such as when certificates were issued and to whom; this information can be the certificates themselves or data that lead to the same result. • Certificate Status Information. • Event Log archives.
	Best practice
	The assessor, in addition to verifying if the provided documentation demonstrates abidance by the above requirements, can also seek information on whether the CA has conducted a Privacy Audit.

b) *the CA shall ensure that the requirements of the European data protection Directive [4], as implemented through national legislation, are met;*

NOTE: *Data protection issues specific to this policy are addressed in:*

- *Registration (including use of pseudonyms) (see clause 7.3.1).*
- *Confidentiality of records (see clauses 7.4.11 a and 7.3.3 f).*
- *Protecting access to personal information (see clause 7.4.6).*
- *User consent (see clause 7.3.1 i)*

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.*

Subject	Additional Guidance
Term: completely protected from disclosure	• The term completely protected does not imply an impossible to achieve 100 % security. It implies that the CA should implement adequate protection against disclosure of the information that can be ascribed to the CA. • The CA should provide the assessing team with documentation proving that the CA has implemented appropriate security measures and if the CA has implemented a procedure for the disclosure of information compliant with Legal requirements.
	Best practice
	The assessor should review if the CA has implemented the above appropriate security measures and procedure The following measures can be taken: • Paper documents are stored in a filing system that can be locked. This filing system may be in a room that has restricted and controlled personnel access. • Electronic documents are stored in a database that is encrypted and for which the accessibility is restricted to authorized personnel only.

7.4.11 Recording of Information Concerning Qualified Certificates

The CA shall ensure that all relevant information concerning a qualified certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings (see the Directive [1], annex II (i)).

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

Subject	**Additional Guidance**
Records include Registration Information	Refer to the Guidance specified in clause 7.3.1, after item i).
	Best practice
	No additional stipulations.

In particular:

General

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

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

c) Records concerning qualified 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.

Subject	**TS 101 456 [15] Guidance Note**
The precise time shall be recorded	NOTE 3: It is recommended that the CA states in its practices as the accuracy the clock used in timing of events, and how this is accuracy ensured.
	Best practice
	The usual practice is for the Certification service provider to have a trusted UTC time source like, for instance, a GPS receiver or a link to the national precise time provider. This time source should provide with the precise time all the provider's services. The assessor should also verify if the protocols adopted to transmit the time and/or the implemented organizational measure ensure that the time preciseness is not affected.

e) Records concerning qualified certificates shall be held for a period of time as appropriate for providing necessary legal evidence in support of electronic signatures in accordance with applicable legislation.

Subject	TS 101 456 [15] Guidance Note
Period of time as appropriate for providing necessary legal evidence	NOTE 4: The duration of the record retention period is difficult to pinpoint, and requires weighing the need for reference to the records against the burden of keeping them. The records could be needed at least as long as a transaction relying on a valid certificate can be questioned. For most transactions, statutes of limitation will eventually place a transaction beyond dispute. However, for some transactions such as real property conveyances, legal repose may not be realized until after a lengthy time elapses, if ever. NOTE 5: Where differing periods of times are applied to certificates being used for different purposes, they should have different specific qualified certificate policy identifiers. Where differing periods are applied to different parts of the registration and event log records, this should be indicated to the subscriber and relying party as specified in clauses 7.3.1 and 7.3.4. The assessor should interpret "the period of time as appropriate for" as a general term for recording paper and electronic data, in full abidance of the legislations in force in the country the CA is established in and the Registration Authorities are established in, if different.
	Best practice
	The assessor should access the rules of law in force in the relevant countries and should ascertain if they are met by the implemented measures.

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.*

Subject	TS 101 456 [15] Guidance Note
The events shall be logged in a way that they cannot be easily deleted or destroyed	NOTE 6: 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.
	Best practice
	Care is to be taken about the decay in the time of the media, even certain CD or DVD, depending on the technology used. Therefore the service provider should verify the media readability with a periodicity consistent with such decay time. The assessing team should verify if procedures exist to implement such measures.

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

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:*

- *type of document(s) presented by the applicant to support registration;*
- *record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents, if applicable;*
- *storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.3.1 i));*
- *any specific choices in the subscriber agreement (e.g. consent to publication of certificate) see clause 7.3.1 i);*
- *identity of entity accepting the application;*
- *method used to validate identification documents, if any;*
- *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 SSCDs.*

Revocation management

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

Subject	Additional Guidance
Recording of all logs and registration information.	Where the applicable legislation allows for it, these recordings can be held on electronic media.
	Best practice
	The assessing team should verify if the related applicable legislation is complied with. The same caveats apply as specified in the previous Guidance table, in order to meet the legal storage requirements. A suitable number of copies of these recordings, kept in different places, may also be necessary, to be pro-active regarding disasters.

7.5 Organizational

The CA shall ensure that its organization is reliable (see Directive 1*, annex II (a)).*

In particular that:

CA general

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

Subject	CWA 14172-2 [18] Guidance
Certification practice statement	Please refer to CWA 14172-2 [18] for guidance.
	Best practice
	Guidance element G.2.25 warns that difference in charging services may be discriminatory, thus conflicting with TS 101 456 [15], clause 7.5 a)

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.*

Subject	Additional Guidance
Term: legal entity	Legal entity means a natural person, or a legal person. The CA should provide the assessors with documents that demonstrate that the CA is a legal entity, as per the applicable national law, that is entitled to conclude contracts and may carry out CA activities.
	Best practice
	The assessor should be informed (refer to reference to CWA 14172-2 [18], guidance element G.2.4 indicated in clause 4) on which documents are necessary as per the applicable law to specify that a CA is a legal entity.

Subject	CWA 14172-2 [18] Guidance
Term: legal entity	Please refer to CWA 14172-2 [18] for guidance.
	Best practice
	Guidance element G.2.28 addresses the case where the CA is part of a larger legal entity. It makes it clear that in this case the structure of the entire legal entity may be subject to assessment. It also specifies an exception for CAs that are part of government.

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.*

Subject	Additional Guidance
Term: financial stability and resources	Financial stability and resources means: The CA should be able to demonstrate that supervision of the finances of the CA by the responsible management has included actions to maintain the financial stability and resources required for the operation of certification services. The CA should provide the assessors with documents demonstrating the above supervision.
	Best practice
	The assessing team should verify if the documentation provided by the CA give enough evidence of the required stability.

Subject	CWA 14172-2 [18] Guidance
Financial stability and resources	Please refer to CWA 14172-2 [18] for guidance.
	Best practice
	Guidance element G.2.29 specifies that, where the financial resources are arranged under an insurance, the insurance terms are not subject to assessment, except assessing whether the CA is financially capable to withstand the liabilities excludes from the insurance 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.*

Subject	CWA 14172-2 [18] Guidance
Resolution of complaints and disputes	Please refer to CWA 14172-2 [18] for guidance.
	Best practice
	Guidance element G.2.30 addresses the resolution of complaints and disputes.

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 particular its senior executive, senior staff and staff in trusted roles, must 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.*

Subject	CWA 14172-2 [18] Guidance
Impartial certificate generation and revocation management	Please refer to CWA 14172-2 [18] for guidance.
	Best practice
	Guidance element G.2.31 addresses impartiality. It specifies these decisions on certificate issuance and revocation should not depend on other organizations, be thy external to or internal to the legal entity to which the CA belongs. In the second case "*the management of the legal entity should provide documented assurance that these services of the CA are authorised to operate independently regarding decisions relating to granting and revocation of qualified certificates*".

Subject	Additional Guidance
Independence of certificate generation and revocation management.	The CA should provide the assessors with evidence of independence of the certificate generation and revocation activities from other organizations; Note that the independence requirement does not apply to registration authorities. The CA should have formal rules and structures for the appointment and operation of any committees which are involved in the certification process; such committees should be free from any commercial, financial and other pressures that might influence decisions.
	Best practice
	The assessor should evaluate if the provided documentation gives evidence of meeting of the above requirements.

8 Framework for the definition of other qualified certificate policies

As stated in TS 101 456 [15]:

This clause provides a general framework for other policies for CAs issuing qualified certificates. A CA may claim conformance to this general framework as defined in clause 8.4. 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.

NOTE: This clause is NOT applicable to either qualified certificate policies identified in clause 5: QCP public, and QCP public + SSCD.

8.1 Qualified certificate policy management

The CA 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 qualified certificate policy;*

c) *a risk assessment shall be carried out to evaluate business requirements and determine the security requirements to be included in the qualified certificate policy for all the areas identified above;*

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

e) *a defined review process shall exist to ensure that the qualified certificate policies are supported by the CAs Certification Practices Statement (CPS);*

f) *the CA shall make available the qualified certificate policies supported by the CA to all appropriate subscribers and relying parties;*

g) *revisions to qualified certificate policies supported by the CA shall be made available to subscribers and relying parties;*

h) *the qualified certificate policy shall incorporate, or further constrain, all the requirements identified in clauses 6 and 7 with the exclusions indicated below. In the case of any conflict the requirements of the present document prevail;*

i) *a unique object identifier shall be obtained for the certificate policy of the form required in ITU-T Recommendation X.509 [3].*

Subject	Additional Guidance
1. Qualified certificate policy approval process 2. Risk assessment	The CA should provide the assessors with documents proving that: a. a body exists with authority to approve the qualified certificate policy; b. a QCP review process officially exists and is enforced; c. a body exists (that may be coincident with the previous one) to approve CPS; d. a procedure officially exists and is enforced to make the QCP timely available to the interested users; e. a process exists and is enforced to obtain OIDs for the QCP and to request for new OID whenever the QCP requirements change in a manner to be incompatible with the previous OID. Where the CA is part of a wider organization (e.g. a consortium) the QCP approval authority may be outside the CA legal entity.
	Best practice
	The assessing team should verify if the received documentation proves meeting the above requirements

8.2 Exclusions for non public QCPs

Certificates issued under a certificate policy for qualified certificates not issued to the public need not apply the following qualified certificate policy requirements:

Subject	TS 101 456 [15] Guidance Note
Certificate policy for qualified certificates not issued to the public	NOTE: A CA is not considered to be issuing qualified certificates to the public if the certificates are restricted to uses governed by voluntary agreements under private law among participants
	Best practice
	Where the QCP is not issued to the public the assessors should be provided with the official documents that: • identify the intended users (subjects, subscribers, relying parties); • where applicable the agreements signed by these users accepting the CA policies and practices.

a) *liability as defined in clause 6.3;*

b) *independence of providers of certificate generation and revocation management services as specified in clause 7.5 h), i);*

c) *dissemination of certificates publicly as specified in clause 7.3.5 f);*

d) *public availability of revocation status information as specified in clause 7.3.6 k).*

8.3 Additional requirements

Subscribers and relying parties shall be informed, as part of implementing the requirements defined in clause 7.3.4:

a) *if the policy is not for public use and whether exclusions identified in clause 8.2 apply;*

b) *whether the policy includes requirements for use of a SSCD;*

c) *the ways in which the specific policy adds to or further constrains the requirements of the qualified certificate policy as defined in the present document.*

8.4 Conformance

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

a) *if the CA claims conformance to the identified qualified 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 qualified 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 can be carried out either under a "voluntary accreditation" scheme as defined in article 3.13 of the Directive [1], or other form of assessment carried out by a competent independent auditor See CEN Workshop Agreement 14172 "EESSI Conformity Assessment Guidance".

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 requirements for qualified certificates identified in the Directive [1] it shall cease issuing certificates using the qualified certificate policy, until it has demonstrated or been assessed as conformant, otherwise the CA shall take steps to remedy the non-conformance within a reasonable period;*

Subject	TS 101 456 [15] Guidance Note
If the CA is shown to be non-conformant it shall cease issuing certificates using the qualified certificate policy	NOTE 3: 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.
	Best practice
	The same Conformance Guidance applies as in table in clause 5.4 after item c) specifying TS 101 456 [15], note 3.

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

Subject	TS 101 456 [15] Guidance Note
The CA compliance shall be checked on a regular basis	NOTE 4: The means required to demonstrate conformance may depend on legal requirements for the country where the CA is established.
	Best practice
	The same Conformance Guidance applies as in table in clause 5.4 after item c) specifying TS 101 456 [15], note 4.

Subject	Additional Guidance
CA compliance regular verification and whenever major change is made to the CA operations.	CA conformance should be checked for significant changes annually with a full re-assessment first after three years and then every four years. The CA should keep the history of all the security incidents occurred since the previous assessment along with the changes applied to practices and security policies, based on the risk assessment revisions meanwhile occurred (see Guidance to clause 7.4.1), to be submitted to assessors.
	Best practice
	The assessing team should verify if the documentation received proves compliance with the above requirements.

A conformant CA must 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, excluding:*

- *clause 7.2.9 if the CA does not require use of a SSCD;*
- *those clauses specified in clause 8.2 if the CA is not providing a service to the public;*

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

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

i) *it meets the additional requirements specified in clause 8.3.*

Subject	Additional Guidance
1. Requirements for independent bodies, assessors, and assessment teams. 2. Conformity assessment process.	See third and fourth Guidance Tables in clause 5.4 after item c).
	Best practice
	No stipulations.

History

Document history		
V1.1.1	October 2006	Publication