TTP.NL Guidance

on

ETSI TS 101 456

Project TTP.NL Guidance on ETSI TS 101 456

30 May 2002 – ECP.NL, CCvD-TTP.NL

Table of Contents

Foreword

Since 1998/1999 the TTP.NL initiative has been active in the area of electronic signatures. The activities in this period resulted in the TTP. NL Criteria Part 1, 2 and 3 for PKI processes, information security management and organisational reliability of Trusted Third Parties (TTPs).

In 2000 the TTP.NL initiative started with the implementation of a trusted, internationally interoperable infrastructure for conformity assessment of TTPs. Based on the European Directive for electronic signatures, the voluntary accreditation scheme for TTPs was finalised in 2001. The scheme in turn is based on the European technical specification ETSI TS 101 456, which incorporates the TTP.NL Criteria Part 1, 2 and 3.

The implementation of the TTP.NL scheme is taking longer then expected. This is partly caused by the relatively slow penetration of the use of electronic signatures as such. However in the Netherlands public services in particular are at present stimulating the use of electronic signatures to safeguard communications with citizens, companies and internal parties. The market is preparing their service delivery, which creates demand for conformity assessment and accredited certification of certification service providers.

In order to reduce obstacles for certification of service providers, the Dutch Department of Transport (Verkeer & Waterstaat) has sponsored a project to solve interpretation problems arising from ETSI TS 101 456. This report represents the end result of that project. The TTP.NL Guidance on ETSI TS 101 456 report can be seen as a final step in stimulating the implementation of the TTP.NL scheme and the transfer to market parties of knowledge on the assessment of TTPs.

The Central Council of Experts on TTP.NL (CCvD-TTP.NL) is an independent body that is hosted by ECP.NL. CCvD-TTP.NL manages the elaboration of interpretation problems arising from the TTP.NL scheme and the underlying ETSI standard. For this project the CCVD-TTP.NL has instituted a working group in which all concerned parties are represented, to write the actual guidance report. In December 2001 this working group produced an interim report cataloguing the issues in ETSI TS 101 456 on which guidance was required. This interim report was used as a starting point for writing interpretation notes on all the issues identified.

In the working group the following organizations were represented: KPN, DigiNotar, PinkRoccade Megaplex, KPMG, PricewaterhouseCoopers and ECP.NL. The working group was chaired by Anton Pronk of ECP.NL.

Members of the working group:

DigiNotar	Ilja van Kempen and Tony de Bos
KPN	Jako Swanenburg
PinkRoccade Megaplex	Johan Wagenvoord and Henk Dekker
KPMG	Patrick Paling
PwC	Frank Schasfoort and Eric Verheul
ECP.NL	Jacob Boersma and Anton Pronk

The working group reported to CCvD-TTP.NL and ECP.NL.
A subgroup of the CCvD has judged the contents and provided quality control:

Members of the quality control subgroup:

SQC	Jan Sauer
KEMA	Gerard Duin
IBM	Rob Weemhoff

This final report, as approved by CCvD-TTP.NL, shall be used as binding advice to Certification Bodies that are members of the CCvD-TTP.NL.

1 Scope

This document provides guidance on the requirements in ETSI TS 101 456 V 1.2.1 (2002-04) – "Policy requirements for certification authorities issuing qualified certificates". This guidance is intended for use by independent bodies and their assessors, certification service providers and other interested parties.

2 References

2.1 Relationship between legal and normative framework

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".
The *Wet elektronische handtekeningen* (the Dutch electronic signature law) determines the legal status of electronic signatures in the Netherlands. This law is based on the Directive.
Annex II of the Directive specifies requirements on certification-service-providers issuing qualified certificates (i.e. certification authorities issuing qualified certificates). ETSI TS 101 456 [a] specifies baseline policy requirements on the operation and management practices of certification authorities issuing qualified certificates in accordance with the Directive.

The table below shows the different certificate types as specified in the Directive, the Dutch electronic signature law and ETST TS 101 456:

Legal framework				Normative framework		
TTP-Services	Articles European Directive	Articles (proposed) Dutch law	Type of certificate	Certificate Policies (CPs)	Trustworthy Systems (TWSs)	Crypto Modules (CMs)
ESignature	5.1	BW, Titel 1 van Boek 3, Afdeling 1A, art. 15a t/m 15c en Titel 3 van Boek 6, Afdeling 4A, art. 196b; Telecommunicatiewet art. 1.1, 2.1, 2.2, 11.5a, 18.15 t/m 18.18	Qualified certificate	ETSI TS 101 456 [QCP+SSCD]	CEN CWA 14167-1 or equivalent	FIPS PUB 140-2 level 3, or CEN CWA 14167-2, or ISO/ IEC 15408 level EAL 4
	5.2	BW, Titel 1 van Boek 3, Afdeling 1A, art. 15a t/m 15c en Titel 3 van Boek 6, Afdeling 4A, art. 196b; Telecommunicatiewet art. 1.1, 2.1, 2.2, 11.5a, 18.15, 18.16, 18.18	Qualified certificate	ETSI TS 101 456 [QCP]	CEN CWA 14167-1 or equivalent	FIPS PUB 140-2 level 3, or CEN CWA 14167-2, or ISO/ IEC 15408 level EAL 4
		BW, Titel 1 van Boek 3, Afdeling 1A, art. 15a en 15c	Ordinary certificate	Not known		

Table 1: Legal and Normative framework

2.2 Interrelation of standards

A schematic representation of the interrelation of standards is shown below in figure 1.

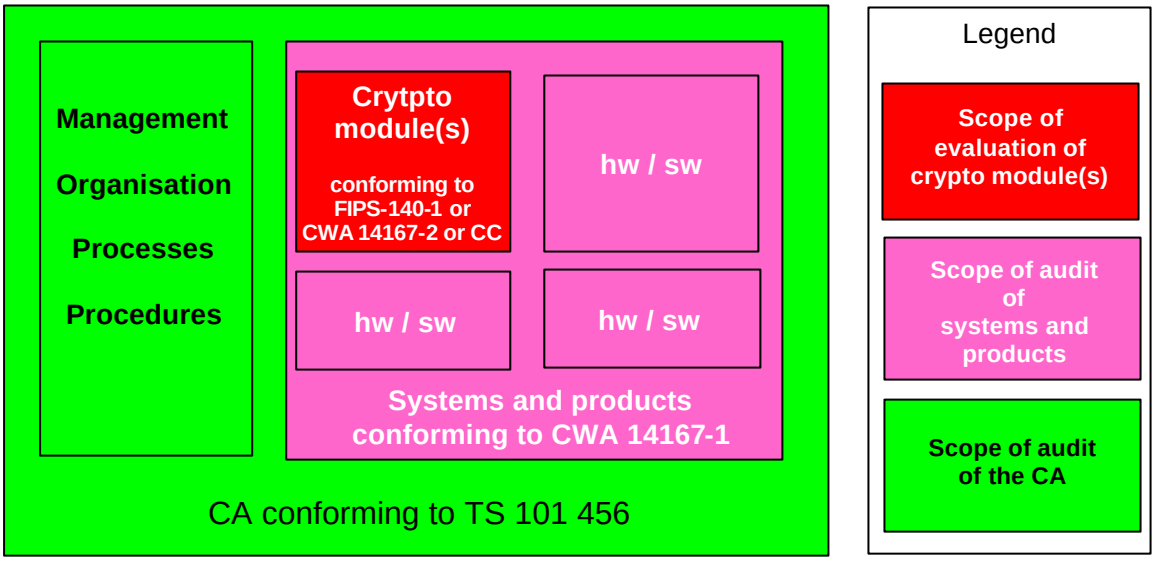

Figure 1: Illustration of interrelation of standards regarding electronic signatures

2.3 Audit scope

The framework for certification separates the management system audit from the product audit. An illustration of this can be seen in Figure 2:

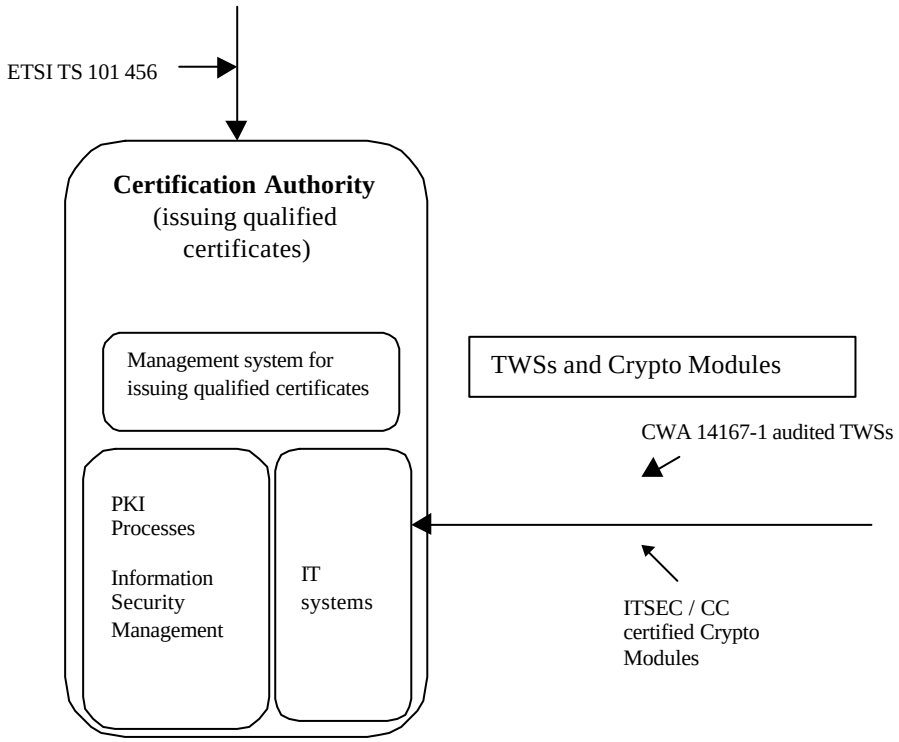

Figure 2: Separation of management system audit from the product audit

This implies the following:

- For the management system: auditing of documentation and implementation.
- For trustworthy systems: executing an EDP-audit against CWA 14716-1 or verifying a statement that an EDP-audit against CWA 14716-1 has been carried out with positive results.
- For CMs: demanding statements, that fulfil certain conditions (based on the right standards, supplied by the right organizations and persons, etc.).

2.4 Normative documents

[a] ETSI TS 101 456 Policy Requirements on CAs issuing Qualified Certificates
[b] CWA 14172-2 EESSI Conformity Assessment Guidance on ETSI TS 101 456
[c] CWA 14172-3 EESSI Conformity Assessment Guidance on Trustworthy Systems

More normative documents are referenced in 3.2.

3 Guidance ETSI TS 101 456

This chapter contains the original text of chapters 1 through 7 of ETSI TS 101 456 v1.2.1 (2002-04). TTP.NL acknowledges ETSI's ownership of this material and will revise this guidance document in the event that ETSI publishes a similar document.

The numbers of the chapter / section headings of TS 101 456 hereunder are preceded by the number 3, which is the number of this chapter of the guidance document. Thus, 3.1 hereunder is chapter 1 of the TS 101 456, 3.2 is chapter 2, etc.

The references within the text of TS 101 456 hereunder have been kept unchanged (i.e. are not preceded by the number 3). Thus, a reference in the text to e.g. clause 4.2 points to section heading 3.4.2 of this guidance document.

TTP.NL Guidance notes and Best practice comments have been inserted in the text of TS 101 456 immediately under the related Subject in the box format as shown below:

Subject	Guidance
Use of TTP.NL guidance	The term 'shall' is used throughout the guidance to indicate those provisions which, reflecting the requirements of ETSI TS 101 456, are mandatory. Any variation from the guidance should be an exception. Such variation should only be permitted on a case-by-case basis after it has been demonstrated that the exception meets the relevant requirements and the intent of this guidance in an equivalent way.
	Best practice
	Guidance on ETSI TS 101 456 requirements are presented in: – ETSI TS 101 456 Notes [a]; – EESSI Guidance [b]; – TTP.NL Guidance.

3.1 Scope

The ETSI TS 101 456 [a] document specifies policy requirements relating to certification authorities (CAs) issuing qualified certificates (termed certification-service-providers issuing qualified certificates in the Directive [1]). It defines policy requirements on the operation and management practices of certification authorities issuing qualified certificates such that subscribers, subjects certified by the CA and relying parties may have confidence in the applicability of the certificate in support of electronic signatures.

The policy requirements are defined in terms of:

a) the specification of two closely related qualified certificate policies for qualified certificates issued to the public, one requiring the use of a secure-signature-creation device;

b) a framework for the definition of other qualified certificate policies enhancing the above policies or for qualified certificates issued to non-public user groups.

The policy requirements relating to the CA includes requirements on the provision of services for registration, certificate generation, certificate dissemination, revocation management, revocation status and if required, signature-creation device provision. Other certification-service-provider functions such as time-stamping, attribute certificates

and confidentiality support are outside the scope of the present document. In addition, the present document does not address requirements for certification authority certificates, including certificate hierarchies and cross-certification. The policy requirements are limited to requirements for the certification of keys used for electronic signatures.

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

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

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

The present document (ETSI TS 101 456) may be used by competent independent bodies as the basis for confirming that a CA meets the requirements for issuing qualified certificates.

It is recommended that subscribers and relying parties consult the certification practice statement of the issuing CA to obtain further details of precisely how a given certificate policy is implemented by the particular CA.
The present document does not specify how the requirements identified may be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

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

<table>
<tr><th>Subject</th><th>Guidance</th></tr>
<tr><td rowspan="3">Scope of the certification of conformity of CAs</td><td>ETSI TS 101 456 addresses three types of certificate policies:
1 Qualified certificates issued to the public requiring the use of an SSCD;
2 Qualified certificates issued to the public, without SSCD;
3 Framework for other qualified certificate policies.

The assessor has to determine the scope of certification of the CA. The scope description should include a description of / a reference to:
• the standard to which the CA complies, or in case the assessed organization does not cover the full CA activity but one or more of the CA services as described in section 3.4.2 hereunder, the standard and the particular clauses to which the service(s) comply;
• in case of the full CA activity: the type(s) of certificate(s) issued;
• in all cases: the CP, CPS and Terms and Conditions that are valid at the time of the assessment;
• in all cases: the organizational structure (including for the full CA activity any subcontractors).
The certification body shall include the scope description in the certificate of conformity or in an appendix to the certificate.</td></tr>
<tr><td>Best practice</td></tr>
<tr><td>No stipulations.</td></tr>
</table>

Subject	Guidance
Assessment of CAs	Refer to CWA 14172 Part 2 “EESSI Conformity Assessment Guidance - Certification Authority services and processes” [b] for guidance on: • Requirements for independent bodies; • Qualification criteria for individual assessors; • Code of conduct for assessors; • Assessment team competence; • Use of technical experts; • Conformity assessment process; • Use of ETSI TS 101 456.
	Best practice
	No stipulations.

3.2 References

The following documents contain provisions which, through referenced in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[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 2527 (1999): "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[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 140-1 (1994): "Security Requirements For Cryptographic Modules".

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

[7] ISO/IEC 15408 (1999) (parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".

[8] CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".

3.3 Definitions and abbreviations

3.3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

advanced electronic signature: electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;
b) it is capable of identifying the signatory;
c) it is created using means that the signatory can maintain under his sole control; and
d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable (see Directive 1999/93/EC).

certificate: public key of a user, together with some other information, rendered un-forgeable by enciphering with the private key of the certification authority which issued it (see ITU-T Recommendation X.509)

certificate policy: named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements (see ITU-T Recommendation X.509)

NOTE: See clause 4.3 for explanation of the relative role of certificate policies and certification practice statement.

certification authority: authority trusted by one or more users to create and assign certificates (see ITU-T Recommendation X.509)

NOTE: A certification authority is a certification-service-provider issuing certificates. See clause 4.2 for further explanation of the concept of certification authority.

certification practice statement: statement of the practices which a certification authority employs in issuing certificates (see IETF RFC 2527)

certification-service-provider (CSP): entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (see Directive 1999/93/EC)

NOTE: The present document is concerned with certification service providers issuing qualified certificates (or component services for issuing qualified certificates - see clause 4.1). The present document is not concerned with other types of CSP functions such as time-stamping and key escrow.

electronic signature: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data (see Directive 1999/93/EC)

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

Qualified Certificate Policy (QCP): certificate policy which incorporates the requirements laid down in annex I and annex II of the Directive 1999/93/EC

qualified electronic signature: advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device, as defined in article 5.1 of the Directive 1999/93/EC

relying party: recipient of a certificate which acts in reliance on that certificate and/or digital signatures verified using that certificate (see IETF RFC 2527)

signature-creation data: unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (see Directive 1999/93/EC)

NOTE: In qualified certificates based on public key cryptography, as covered by the present document, the signature-creation data is, for example, a private key. Hence, within the present document the term private key is used for the signature-creation data.

signature-creation device: configured software or hardware used to implement the signature-creation data (see Directive 1999/93/EC)

secure-signature-creation device: signature-creation device which meets the requirements laid down in annex III of Directive 1999/93/EC

signature-verification data: data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature (see Directive 1999/93/EC)

NOTE: In qualified certificates based on public key cryptography, as covered by the present document, the signature-verification data is, for example, a public key. Hence within the present document the term public key is used for the signature-verification data.

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

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

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

3.3.2 Abbreviations

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

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
SSCD	Secure Signature Creation Device

3.4 General Concepts

3.4.1 Certification authority

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates is called the certification authority. The certification authority has overall responsibility for the provision of the certification services identified in clause 4.1. The certification authority's key is used to sign the qualified certificates and it is identified in the certificate as the issuer.

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

CA, and the CA maintains overall responsibility for meeting the requirements defined in the present document and liability for the issuing of certificates to the public as required in the Directive [1].

A certification authority is a certification-service-provider, as defined in the Directive [1], which issues certificates.

3.4.2 Certification services

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

- **Registration service:** verifies the identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service.

NOTE 1: This service includes proof of possession of non-CA generated subject private keys.

- **Certificate generation service:** creates and signs certificates based on the identity and other attributes verified by the registration service.

- **Dissemination service:** disseminates certificates to subjects, and if the subject consents, to relying parties. This service also disseminates the CA's terms and conditions, and any published policy and practice information, to subscribers and relying parties.

- **Revocation management service:** processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.

- **Revocation status service:** provides certificate revocation status information to relying parties. This service may be a real-time service or may be based on revocation status information which is updated at regular intervals.

and optionally:

- **Subject device provision service:** prepares and provides a signature-creation device to subjects.

NOTE 2: Examples of this service are:
- a service which generates the subject's key pair and distributes the private key to the subject;
- a service which prepares the subject's secure-signature-creation device (SSCD) and device enabling codes and distributes the SSCD to the registered subject.

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

The following diagram illustrates the interrelationship between the services.

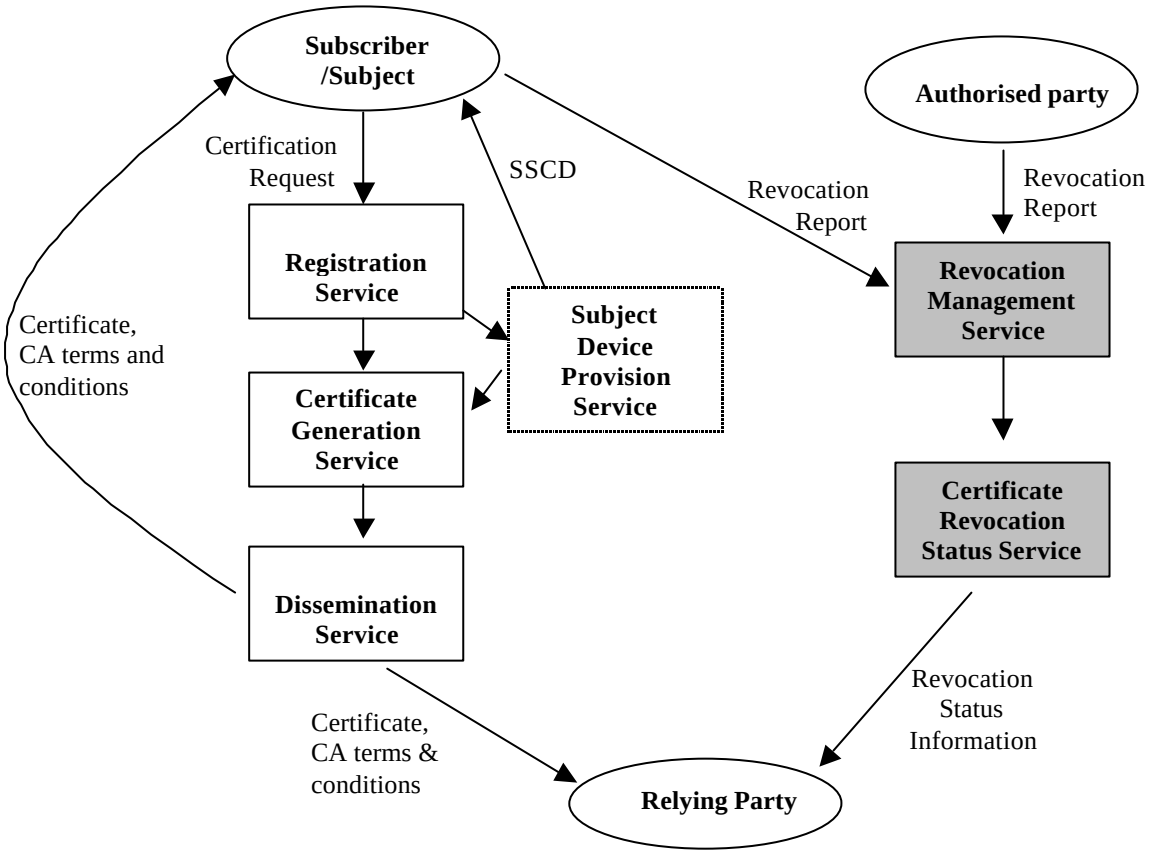

Figure 3: Illustration of subdivision of certification services used in the present document

3.4.3 Certificate policy and certification practice statement

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

3.4.3.1 Purpose

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

The present document specifies certificate policies to meet the requirements for qualified certificates as laid down in annexes I and II of the Directive [1]. CAs specify in certification practice statements how these requirements are met.

3.4.3.2 Level of specificity

A certificate policy is a less specific document than a certification practice statement. A certification practice statement is a more detailed description of the terms and conditions as well as business and operational practices of a certification authority in issuing and otherwise managing certificates. A certification practice statement defines how a specific certification authority meets the technical, organizational and procedural requirements identified in a certificate policy.

NOTE: Even lower-level documents may be appropriate for a CA detailing the specific procedures necessary to complete the practices identified in the certification practice statement. This lower-level documentation is generally regarded as an internal operational procedure documents, which may define specific tasks

and responsibilities within an organization. While this lower-level documentation may be used in the daily operation of the CA and reviewed by those doing a process review, due to its internal nature this level of documentation is considered private and proprietary and therefore beyond the scope of the present document. For example, the policy may require secure management of the private key(s), the practices may describe the dual-control, secure storage practices, while the operational procedures may describe the detailed procedures with locations, access lists and access procedures.

3.4.3.3 Approach

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

3.4.3.4 Other CA Statements

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

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

3.4.4 Subscriber and subject

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

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

In the case of certificates issued to individual for their own use the subscriber and subject can be the same entity.

In other cases, such as certificates issued to employees the subscriber and subject are different. The subscriber would be, for example, the employer. The subject would be the employee.

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

3.5 Introduction to qualified certificate policies

3.5.1 Overview

A certificate policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" [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 specifies two qualified certificate policies:

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

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.

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

Clause 8 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 IETF RFC 2527 [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.

3.5.2 Identification

The identifiers for the qualified certificate policies specified in the present document 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.

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.

3.5.3 User Community and Applicability

3.5.3.1 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;

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

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

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.

3.5.3.2 QCP Public

The certificate policy QCP Public is for certificates:

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

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

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.

3.5.4 Conformance

3.5.4.1 General

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

b) if the CA has been assessed to be conformant to the identified qualified certificate policy by a competent independent party.

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

3.5.4.2 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.

3.5.4.3 QCP Public

A conformant CA must demonstrate that:

a) it meets its obligations as defined in 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 6.2 e) and f).

3.6 Obligations and liability

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

Subject	Guidance
Indicate QCP applicability	A CA shall include an object identifier in the certificate for the QCP public + SSCD policy or for the QCP public without SSCD policy, or for any other policy, defined under the QCP framework, to which the CA claims conformance.
	Best practice
	No Stipulations.

3.6.1 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 and 5.4.3).

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

Subject	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 ETSI TS 101 456 by a third party.

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

3.6.2 Subscriber Obligations

The CA shall oblige, through agreement (see 7.3.1 h), the subscriber to ensure that the subject fulfils the following obligations:

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

Subject	Guidance
CA obliges subscriber to submit accurate and complete information	• The assessor shall 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 7.3.4);*

Subject	Guidance
Key pair usage	• The certification contract shall stipulate that the key pair is used for electronic signatures only • If applicable, the CA shall 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 subject's private key;*

Subject	Guidance
Avoid unauthorized use private key	The certification contract shall 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:*

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

Subject	Guidance
Algorithm being fit for the purpose	• Evidence shall be available that the subscriber or subject uses an algorithm and key length that are generally recognised (by experts). • The assessor shall report the precise details, as provided by the CA, of the algorithm and key length used by the subscriber.
	Best practice
	Section 3.7.2.1 defines additional Guidance on "fit for purpose."

NOTE 1: It is currently proposed that the recognition of algorithms, with associated key length, being fit for the purposes of qualified certificates is through a cryptographic advisory panel under the committee identified in article 9 of the Directive

- only the subject holds the private key once delivered to the subject.

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;*

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

Subject	Guidance
Use of an SSCD	The assessor shall 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

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

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, generate the subject's keys within the SSCD to be used for signing;

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

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

- *the subject's private key has been lost, stolen, potentially compromised; or*
- *control over the subjects private key has been lost due compromise of activation data (e.g. PIN code) or other reasons; and/or*
- *inaccuracy or changes to the certificate content, as notified to the subscriber.*

Subject	Guidance
Reasonable delay of notifying CA	The subscriber agreement shall have stipulations defining reasonable delay in notifying the CA.
	Best practice
	No Stipulations

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

3.6.3 Information for Relying Party

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 7.3.4); and

NOTE 1: Depending on CA's practices and the mechanism used to provide revocation status information, there may be a delay of up to 1 day in disseminating revocation status information.

Subject	Guidance
Period between revocation request and revocation information	For a relying party to reasonably rely on a certificate by verifying certificate status information, the period between the CA receiving a certificate revocation request and disseminating certificate status information shall not exceed 1 day.
	Best practice
	No stipulations

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 7.3.4; and

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

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.

3.6.4 Liability

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

3.7 Requirements on CA practice

3.7.1 Certification Practice Statement

The CA shall ensure that it demonstrates the reliability necessary for providing certification services

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

Subject	Guidance
Statement of the practices	The Assessor shall take notice of the following: • 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. • The assessor shall assess 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-standard for Certificate Policy and Certification Practice Statements. The ETSI TS 101 456 has included a cross-reference list in Annex D for statements to be addressed in RFC 2527. • In general, a CPS contains legal statements. A CPS is often incorporated by reference in End User contracts.

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

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*.

Subject	Guidance
CPS states the obligations of all external organizations	No Stipulations
	Best practice
	• The obligations are stated as a high level description with the objective to demonstrate reliability to the public. Detailed obligations to external organizations are confidential to the public and stated in Service Level Agreements and Service Contracts. (RFC 2527 ref: chapter 2). • The above mentioned obligations will not be specified in detail in the CPS, as the CPS will be made publicly available. A CSP acting with external organizations will conclude service provision contracts and service level agreement(s) with its contractors. A CP may be incorporated by reference in these documents.

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.*

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

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.*

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 has responsibility for ensuring the practices are properly implemented.

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

Subject	Guidance
Terms: "High level management body"; "Senior management"	No Stipulations **Best practice** • Senior management and the High Level Management Body may consist of the same persons. • A body that performs the above mentioned activities (e to g) related to approving and managing CSP practices may for example be called a Policy Management Authority (PMA) or a Policy Approval Authority (PAA). • A PMA or PAA are implemented within the CSP organization and are decision committees consisting of CA Management personnel. The implementation of these bodies allows for a drafting role (PMA) and a approving role (PAA). • In general a PMA or a PAA consists of a multidisciplinary composition, 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 and shall, following approval as in (e) above, make the revised Certification Practice Statement immediately available as required under (c) above.

3.7.2 Public Key Infrastructure – Key Management life cycle

3.7.2.1 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)).

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

Subject	Guidance
Root Key Ceremony	Evidence shall be available that the process in which CA keys are generated ('Root Key Ceremony') is under suitable control.
	Best practice
	• The root key ceremony should be described in detail in a script. In particular: - All 'security critical operations' should be literally documented (e.g. entering certain critical commands. - 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. • The (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. This is why a CSP may consider to obtain a third party opinion on the script before it will be executed.

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

- meets the requirements identified in FIPS PUB 140-1 [5] level 3 or higher; or

- meets the requirements identified in CEN Workshop Agreement 14167-2 [8]; 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	Guidance
Cryptographic Module (CM)	• Evidence shall be available that the CM is certified by a competent certification body against an evaluation report from a competent evaluation body. The certificate and the report should be available to the assessor. The certificate should either state compliance with FIPS 140-1 level 3, with CWA 14167-2 or with a suitable Protection Profile with EAL 4 level assurance. • The assessor shall verify that the CM is installed in accordance with the assumptions used under which the CM was certified.
	Best practice
	• FIPS 140-1 has been replaced by FIPS 140-2 (March 2001). • FIPS 140-1/2 deals only with the CM and does not cover the interfacing ICT systems / applications (usually based on NT or Unix and additional software). • See 3.7.4.7. • 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 certified PKI products. • Archived PIN codes should be placed in tamper-evident envelopes and stored in a safe(box) whereby each envelope in a separate safe(box) only accessible by designated individuals. Access control to these safebox must be consistent with the overall security organization.

Subject	Guidance
Initialisation Cryptographic Module (CM)	• See also Section 3.7.2.7. Evidence for all the above, shall be available. **Best practice** • We distinguish seven important processes for a CM, which might not be a complete list for all CMs: - Activation: putting the CM in a state suitable for a specific task (e.g., Initialization, Generation, Usage, Destruction). - Initialisation: setting all security parameters and tokens. - Generation: whereby all cryptographic keys are generated (based on the configuration set-up during initialization). - Usage: whereby specific cryptographic keys are used. - Backup: whereby specific cryptographic keys are backed up. - Export: whereby specific cryptographic keys are exported. - Destruction: whereby specific cryptographic keys are destroyed. • The CM should be securely sent from the manufacturer to the CA, e.g., using 'tamper evident' packaging. • The CM should be under adequate 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. • The relevant security parameters in the CM (in particular, seeding of a deterministic pseudo random number generator like Annex C of ANSI X9.17) should be adequately re-initialised by the CSP. The procedure for re-initializing should be documented in detail (i.e., including the required keying commands). • By using the appropriate internal test functions (required by FIPS 140-1/2) of the CM, the CSP must verify that the CM is properly functioning. The procedure for realizing this should be documented in detail (i.e., including the required commands).

NOTE 1: The rules of 7.2.2 (b to d) apply also to key generation even if carried out in a separate system.

c) *Certification authority key generation shall be performed using an algorithm recognized 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.*

Subject	Guidance
Key length and algorithm for CA signing key	Evidence shall be available that the choice of the algorithm and key length used by the CA 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 the CA signing key. The draft document 'Algorithms and Parameters for Secure Electronic Signatures (20011019_Algorithm_Proposal_V2.11.doc) from the EESSI 'Algorithm group' appears to become the guidance relating to this subject . • The approval on cryptographic algorithms and parameters (most notably key lengths) in 20011019_Algorithm_Proposal_V2.11.doc is only valid until 31-12-2005. • Most notably the 20011019_Algorithm_Proposal_V2.11.doc does only permit the use the SHA-1 and RIPEMD secure hashing functions (with 160 bit output), i.e., the use of the MD5 hashing function (with 128 bit output) is not permitted. • The document 20011019_Algorithm_Proposal_V2.11.doc does not give guidance for CSP that want to generate (root) CA certificates with an expiry date later than 2005. As CSPs quite often employ (root) CA certificates with a lifetime of 16-20 years, 20011019_Algorithm_Proposal_V2.11.doc does not give adequate guidance for this. • We remark that: - A CA signing key is of greater value than the individual signing key of an end user. Indeed with the CA signing key an attacker can generate any end-user certificate himself (whereby generating the end-user's private key). This fact does not necessarily imply that the key length of the CA signing key should be larger than that used by end-users, it only implies that considerations on which this key length is based should focus on the CA signing key. - Broadly speaking the choice for a certain key length depends on: 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 paper 'Selecting Cryptographic Key Sizes' from A.K. Lenstra and E.R. Verheul (Journal of Cryptology 14, pp. 255-293, Springer-Verlag, 2001) a model has been defined to select appropriate key lengths. A JavaScript program is available on www.cryptosavvy.com to assist with choosing the appropriate key lengths. • As a rule of thumb (in accordance with the above referenced paper): CA keys should preferably use SHA-1-RSA; if the CA keys need to be valid until 2012 the required key length is >= 1280 bits) if the CA keys need to be valid until 2022 the required key length is >= 2048 bits. It is not advisable to have a life span for CA keys that much larger than 20 years. • The auditor can determine which public RSA exponent *e* is used by using the (free) OpenSSL tools based on the CA certificate. • It is best if the CA refrains from using a public exponent equal to three, as there are (theoretical) cryptographical results indicating that using that exponent is less secure. Formulated differently, if the CA is neutral about this, it is best that it avoids this public exponent. It is good practice to use the public exponent equal to $2^{16}+1 = 65537$, which is actually also a default choice in many CA products.

NOTE 3: It is currently proposed that the recognition of algorithms, with associated key length, being fit for the purposes of qualified certificates is through a cryptographic advisory panel under the committee identified in article 9 of the Directive [1].

3.7.2.2 Certification authority key storage, backup and recovery

Certificate generation

The CA shall ensure that CA private keys remain confidential and maintain their integrity (see [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[5] level 3 or higher; or*
- *meets the requirements identified in CEN Workshop Agreement 14167-2 [8]; 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	Guidance
CM activation	Evidence shall be available that the CM is only activated in a sufficiently controlled environment.
	Best practice
	• See also 3.7.2.7. • Before the CM can be used it must be activated; FIPS 140-1/2 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	Guidance
Physical protection of activated CM	Evidence shall be available that the activated CM (and its peripherals like 'datakeys') has been adequately protected against unauthorised access during its lifetime (including its period at the manufacturer).
	Best practice
	• It is good practice to keep the physical location of the CM under (camera) surveillance and to declare this location as a 'no lone' zone (see above). • Entry logs to the room where the activated CM is located, must be maintained and archived. • Cases of fraud are known in the banking sector, where employees detached the link between an activated CM and the server using it and then attached the CM (still in activated mode) to a laptop, using a serial connection. By doing so, these employees were then able to decrypt messages. • Even FIPS 140-1 level 4 certified CMs (highest level of certification) can sometimes be attacked with so called chosen ciphertext/plaintext attacks. Compare the attack on the IBM 4758 Cryptographic Coprocessor www.cl.cam.ac.uk/~rnc1/descrack/ibm4758.html and the paper by James Manger (Telstra) 'A chosen ciphertext attack on RSA Optimal Encryption Padding (OAEP) as standardized in PKCS #1 V2.0', Crypto 2001 proceedings. This emphasises the necessity to declare the room where the (activated) CM is located to be a no-lone zone.

b) *When outside the signature-creation device (see (a) above) the CA private signing key shall be encrypted using an algorithm and key-length that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key part.*

Subject	Guidance
Algorithm and key-length used to encrypt CA private signing key.	Evidence shall be available that the choice of the algorithm and key length used by the CA to encrypt 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 encrypting the CA signing key. The earlier mentioned draft document 'Algorithms and Parameters for Secure Electronic Signatures (20011019_Algorithm_Proposal_V2.11.doc) from the EESSI 'Algorithm group' does not provide guidance on this subject. • It is good practice to use Triple DES with three different keys (168 bits keys). This probably provides adequate security for the next twenty years. • The CM should not allow exporting the private key under a key of size less than 90 bits; in particular the CM should not allow the private key to be exported under a Triple DES key with all three DES keys coinciding. • Additional guidance on the minimal key length of the symmetric encryption algorithm can be found on www.cryptosavvy.com. • The 20011019_Algorithm_Proposal_V2.11.doc should contain provide guidance on this subject.

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

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

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

Subject	Guidance
Security of backup copies key.	Evidence shall be available that the process in which the CA signing key is backed-up is adequately controlled, this includes the requirement that this for 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 on a test-bed, prior to execution. This is to assure that produced backups are correctly formed. - Creation of backups must be reported and archived. • The backup of the CA key is often a 'cloned' CM and 'cloned' datakeys. The security of these clones must have the same level as the operational CM and datakeys. Cloned datakeys must also be locked in different safes or safeboxes only accessible by designated individuals. Access control to these safes and safeboxes must be consistent with the overall security organization.

3.7.2.3 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 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..

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.

Subject	Guidance
Integrity and authenticity of the CA key.	Evidence shall be available that the process in which the CA certificate is distributed to relying parties adequately protects its integrity and authenticity.
	Best practice
	• The fact that a (root) CA certificate is self-signed, in fact, says nothing about its authenticity. Indeed, everybody is able to create a self-signed certificate. It is therefore good practice to employ a physical secure distribution to distribute self-signed certificates. • The self-signed certificates can be placed on a marked medium that can only be written to once (e.g., a CD-ROM or WORM) and that can provided with a mark of authenticity (e.g., a conventional signature). • It is good practice to verify the correctness of subCA certificates before handing them over to relying parties. • Publishing a SHA-1 fingerprint (hash) of a self-signed certificate in a newspaper, telephone book or even a website is good practice. The control mechanism (e.g., viewing the detail information from a browser's certificate management applet) should be described in the CP or CPS. • Proper choice of the fingerprint (hash) algorithm should probably be addressed in 20011019_Algorithm_Proposal_V2.11.doc.

3.7.2.4 Key escrow

CA and 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 annex II (j)).

3.7.2.5 Certification authority key usage

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

Certificate generation

a) CA signing key(s) used for generating certificates, as defined in clause 7.3.3, and/or issuing revocation status information, shall not be used for any other purpose.
b) The certificate signing keys shall only be used within physically secure premises.

Subject	Guidance
Proper use of CA keys.	Evidence shall be available that the CA private signing keys are not used inappropriately, e.g., a balanced log journal of the CM.
	Best practice
	• The rationale behind this is that the use of a CA private signing key should be limited to one task only, at least as far as possible. It is good practice to use a separate CA private signing key for each type of (end-user) certificate. • A CA private signing key should not be used in cryptographic services other than certificate signing and (possibly) CRL signing. For instance, a CA private signing key should not be used to establish an SSL connection. • Assurance that a CA private signing key is not used inappropriately must usually come from the (physical) control surrounding the CM, in which the CA private signing key resides. • In addition to this; the certificate associated with the private signing key must have its key usage fields set according to its function (e.g., CRLsign and Certificate Signing (keyCertSign)) and must avoid other setting key usage fields (e.g., Data Encipherment). The certificate associated with the private signing key must have its key usage fields set according to its function (e.g., CRLsign and Certificate Signing (keyCertSign)) and must avoid setting key usage fields not relating to its function (e.g., Data Encipherment). See ETSI TS 101 862, Annex A.

3.7.2.6 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 annex II (g) and annex II (f)).

In particular:

Certificate generation

a) *all copies of the CA private signing keys shall be:*

- *destroyed such that the private keys cannot be retrieved; or*
- *retained in a manner such that they are protected against being put back into use.*

Subject	Guidance
Destruction of signing CA keys	• Evidence shall be available that the process (including procedures and training) is in which CA keys are destroyed is sufficiently controlled. • Evidence shall be available that all previous CA keys (including its copies and related tokens) are destroyed.
	Best practice
	• Destruction of the signing CA keys: - The actual operations should be 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 must be documented. It must be clear what (signed) assurance these persons are actually giving - All components (e.g., the 'datakeys') related to the signing key need to be involved in the destruction process. - The actual destruction should be reported and archived. • It is good practice to physically destroy the datakeys or smartcards related to the destroyed signing key, after they have been destroyed logically. That is, not to use the datakeys or smartcards twice.

3.7.2.7 Life cycle management of cryptographic hardware used to sign certificates

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

Certificate generation

In particular the CA shall ensure that:

a) certificate 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	Guidance
Security of CM during its lifetime.	• Evidence (including records of security-related actions) shall be available that the CM (and its peripherals like 'datakeys') is and has been adequately protected against unauthorised access during its lifetime. • Evidence shall be available that: - the CM was adequately initialized and tested before used in production; - the CM is adequately tested periodically while in production. - the CM was adequately destroyed at end of its life-cycle.
	Best practice
	• It is good industry practice to designate 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. • A CM must only be activated (in either user or Crypto officer mode) when required. Installation, initialization, generation, usage, and destruction or management of CMs is performed in the presence of no less than two designated employees. • There should be appropriate controls for the reparation of CMs at the manufacturer (if at all applicable). See point 3.7.2.1. • All important events (to be formally determined) relating to the CM should be reported and archived

3.7.2.8 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.

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.

NOTE: It is currently proposed that the recognition of algorithms, with associated key length, being fit for the purposes of qualified certificates is through a cryptographic advisory panel under the committee identified in article 9 of the Directive.

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 subscriber or subject in a manner such that the secrecy of the key is not compromised and on delivery only the subject has access to its private key.

Subject	Guidance
Algorithm and key-length used for CA-generated subject keys.	Evidence shall be available that the choice of the algorithm and key length used by the CA is based on an adequate assessment/research in the field of cryptography.
	Best practice
	Guidance relating to user cryptographic algorithms and key lengths can be found in the document 20011019_Algorithm_Proposal_V2.11.doc, which in fact contains minimal requirements.

3.7.2.9 Secure-signature-creation device preparation

The CA shall ensure that if it issues SSCD this is carried out securely (see annex III).

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

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 and delivery 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	Guidance
Secure handling of SSCDs	No stipulations
	Best practice

	• Compare CEN/ISSS WS/E-Sign N 136:
	  - Private signing key for end-user must either be generated in a SSCD of type 1 and sent to the actual SSCD of type 2 or 3 over a trusted channel or must be 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) must not be 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.
	• The simplest solution (with respect to security) is to require that the SSCD and/or activation data is to be handed over to the end-user by the CSP. The end-user is then typically also given the required software/hardware. This also follows the way conventional passports are currently issued (cf. the Dutch Paspoort Wet).
	• It is good practice in the banking industry (creditcards) to send the SCCD by registered mail whereby the recipient is required to authenticate himself with a national ID card; the activation data (PIN code) is sent by separate mail in a neutral envelope.
	• A combination of both mentioned solutions can consist of handing the activation code at the end-user's registration at the registration facility and sending the SSCD by registered mail whereby the recipient is required to authenticate himself with a national ID card.

3.7.3 Public key infrastructure - Certificate Management life cycle

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

In particular:

Registration

NOTE 1: When registering, a subscriber is identified as a person with specific attributes. The specific attributes may indicate, for example, an association within an organization possibly with a role.

Subject	Guidance
Term: "Specific attributes"	The assessor shall interpret the term "specific attributes" as follows: • Specific attributes are the properties, in addition to name, surname etc, that can be used to uniquely identify the subscriber.
	Best practice
	Reference material: EESI Electronic Signature Formats (TS 101 733), section 7.3: Roles and Signer attributes.

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 7.3.4 (see 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	Guidance
Term: "Durable means of communication"	See 3.7.3.4 b)
	Best practice
	No stipulations

Subject	Guidance
Term: "Readily understandable language"	The assessor shall 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.

NOTE 2: A model PKI disclosure statement, which may be used as the basis of such a communication is given in annex B.

Subject	Guidance
Term: "PKI Disclosure Statement (PDS)"	No stipulations. **Best practice** A PDS is a supplementary instrument to a CP/CPS that discloses critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS. In case a PDS is used, the assessor will 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 section 7.3.1 a

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

Subject	Guidance
Term: "by appropriate means in accordance with national law"	In order to comply with "appropriate means", the assessor shall 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 is a legal identification document as specified by the relevant national law. In the Netherlands, this is Wet op de identificatieplicht (Wet van 9 december 1993, tot aanwijzing van documenten dienende ter vaststelling van de identiteit van personen alsmede aanwijzing van enige gevallen waarin de identiteit van personen aan de hand van deze documenten kan worden vastgesteld). • For specific legal issues: *see* chapter 6 of ETSI TS 101 456

NOTE 3: An example of evidence checked indirectly against a physical person is documentation presented for registration which was acquired as the result of an application requiring physical presence.

Subject	Guidance
Checking the evidence of the identity	The assessor shall investigate in which manner the evidence of the identity is checked: • 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. The assessor shall investigate whether: • The process of Evidence checked Indirectly provides equivalent assurance to evidence checked directly (requiring physical presence at the registration facility). • The submitted evidence of indirect 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.
	Best practice
	No stipulations.

NOTE 4: Attribute certificates are outside the scope of the current 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);*
- *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.*

NOTE 5: The place should be given in accordance to national conventions for registering births.

NOTE 6: The CA is liable as regards the accuracy "of all information contained in the certificate"

Subject	Guidance
The CA is liable…	No stipulations.
	Best practice
	For specific legal issues: *see* chapter 6 of ETSI TS 101 456

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.*

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

g) The CA shall record all the information used to verify the subject's identity, including any reference number on the documentation used for verification, and any limitations on its validity.

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

- *agreement to the subscriber's obligations (see 6.2);*

- *if required by the CA, agreement to use a SSCD;*

Subject	Guidance
Term: "Record"	The assessor shall investigate whether the CA has archived (physically and/or electronically) the signed agreements.
	Best practice
	No stipulations.

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), j)), subject device provision (see clause 7.4.11 items m), n) and any subsequent revocation (see clause 7.4.11 o)), and 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 consents to the publication of the certificate;*

- *confirmation that the information held in the certificate is being correct.*

NOTE 8: The subscriber may agree to different aspects of this agreement during different stages of registration. For example, agreement that the information held in the certificate is correct may be carried out subsequent to other aspects of the agreement.

Subject	Guidance
Consent to keeping of a record	The assessor shall investigate whether the user agreement includes the *users consent:* • of keeping a record of registration information • of passing this information to third parties • of publishing the certificate
	Best practice
	No stipulations.

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.

i) The records identified above shall be retained for at 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.

j) 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.

NOTE 11: In order for the CA to obtain the assurance that the private key is really placed in a SSCD, the certificate request process may also ensure that the key pair has effectively been generated by a SSCD.

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

3.7.3.2 Certificate renewal, rekey and update

The CA shall ensure that requests for certificates issued to a subject who has already previously 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 annex II (g)).

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.

In particular:

Registration

a) The CA shall check 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 7.3.1 a), b) and h);

c) If any information has changed, this is verified, recorded, agreed to by the subscriber in accordance with 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 intended lifetime and no indications exist that the subject's private key has been compromised.

Subject	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 section 3.7.2.
	Best practice
	No stipulations.

3.7.3.3 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 and II (g) of the Directive [1].

NOTE: A standard format for qualified certificates meeting the requirements of annex I of the Directive is defined in.

b) 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.

c) if the CA generated the subject's 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 7.2.9) is securely passed to the registered subscriber or subject.*

d) 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).

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

Subject	Guidance
Registration data exchange between distributed CA components	The assessor shall investigate whether the exchange of registration data is adequately secured, by: • Checking whether the communication between the PKI(CA) components and between subscriber and the CA system is protected to ensure integrity and confidentiality (investigate security functionalities) • Checking whether the CA System maintains files in which the communication events are logged.
	Best practice
	No stipulations.

f) 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.

3.7.3.4 Dissemination of Terms and Conditions

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties (see 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 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 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 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 7.3.1) is retained;*
- *the period of time which CA event logs (see 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.

Subject	Guidance
Term: durable means of communication	The assessor shall 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 (archival period in the Netherlands is seven years).
	Best practice
	No stipulations.

NOTE: 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.

3.7.3.5 Certificate dissemination

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties (see Directive annexII (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;

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

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

3.7.3.6 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 annex II (b)).

In particular:

Revocation management

a) The CA shall document as part of its certificate practice statement (see 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;
- 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.

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.

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 1: 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 authority designated by the CA.*

Subject	Guidance
Publication interval	The assessor shall 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 hrs). There is no prescription for the time of issuance of the CRL.
	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.

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 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.

Subject	Guidance
Availability of revocation management services and certificate status information	The assessor shall 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 shall check the existence of contracts with third parties/delegates as to whether the CA has enforced the relevant obligations mentioned in ETSI TS 101456.
	Best practice
	No stipulations.

NOTE 2: Revocation status information may be provided, for example, using on-line certificate status service or through distribution of CRLs through a repository.

j) The integrity and authenticity of the status information shall be protected.
k) Revocation status information shall be publicly and internationally available.

3.7.4 CA management and operation

3.7.4.1 Security management

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

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

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

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

NOTE 1: See ISO/IEC 17799 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.

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

NOTE 2: This documentation (commonly called a system security policy) should identify 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 should describe 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.

f) 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	Guidance
Security Management	The CA shall have a documented information security management system (ISMS), available to the assessor, which at least includes or refers 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 shall formally approve the security policy and the Information Security Management System. Included in the allocated responsibilities, shall 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. There shall a management approval procedure for all documents; it should be easily determinable for the assessor that these procedures have been followed. One or more Information Security Plans (called System Security Policies in ETSI TS 101 456) 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 we refer to ISO/IEC 17799:2000. • 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:
  - value (see asset classification below),
  - threats (e.g., which are relevant), and
  - 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 can be integrated with the CPS employed by the CA. In this fashion the whole CA organization uses the same information.
- The Information Security Plan and Policy can take the form of internal webpages with attachments; due to its nature
  - version control should be adequately addressed;
  - parts of this handbook should be classified;
  - secret core information (e.g., passwords) should not be placed in an Information Security Plan.

3.7.4.2 Asset classification and management

The CA shall ensure that its assets and information receive an appropriate level of protection. (see 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	Guidance
Asset Classification	• Management of asset classification (including updating) shall be clearly assigned to a person or body within the CA. • A complete and up-to-date inventory of all relevant assets and a description of their security properties shall be readily available to the assessor; the ownership of each asset shall be clear. • The CA's main security relevant processes shall be documented and a relation with the assets used in these processes shall be made. • Each asset shall 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. • A complete and up-to-date list of all job descriptions at the CA shall be available. The role of the function within the distinguished CA business processes and assets shall be made clear. Each job shall be classified, e.g., as trusted, security-related or non-trusted.
	Best practice
	• For Asset Classification we refer to section 5 of ISO/IEC 17799:2000. • With respect to asset classification, it is good practice: - To define classifications up to the criteria CIA (Confidentiality, Integrity and Availability) in terms of High, Medium and Low. - To document a taxonomy for each of the nine possibilities. - 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, for illustrative purposes we mention: - computer rooms: keys or codes giving access to it - cabinets, safes: keys of codes giving access - computers (hardware): BIOS passwords or physical keys - computers (OS): the accounts enabled with their various security levels (administrators, specific users etc.). - CA applications: several users (master users, security officers, CRL users). - CMs: datakeys, physical keys - Datakeys: PIN codes - Etc. • 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.

3.7.4.3 Personnel security

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

In particular:

CA General

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

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.

b) 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.

c) 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. It is recommended that the job descriptions include skills and experience requirements.

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

NOTE 2: See ISO/IEC 17799 for guidance.

Registration, certificate generation, subject device provision, revocation management

e) Managerial personnel shall be employed who possess expertise in the electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment.

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

g) 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 and maintain archives and audit logs of the CA trustworthy systems.

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

i) 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.

NOTE 3: In some countries it may not be possible for CA to obtain information on past convictions. However, the employer may be able to ask the candidate to provide such information and turn down an application in case of refusal.

Subject	Guidance
Personnel Security	• The responsibility of reviewing Personnel Security shall be assigned to a person within the CA. • A complete and up-to-date inventory of all job descriptions at the CA shall be available. The role of the function within the distinguished CA business processes and assets shall be made clear. Each job shall be rubricated, e.g., as trusted, security-related or non-trusted. • There shall 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 shall be readily available to the assessor; third party employees should be clearly marked in this inventory. There shall be a clear relation between job description inventory and the staff inventory. • All CA personnel shall have signed a confidentiality statement (non-disclosure agreement). An inventory of these statements shall be readily available to the assessor. Personnel with a trusted role within the CA shall have signed an 'independence statement' (cf. f) above) indicating that they are free from conflicting interests that might prejudice the impartiality of the CA operations. An inventory of these statements shall be readily available to the assessor. Personnel with a trusted role within the CA shall submit a 'Verklaring omtrent gedrag' from their local council, prior to entrance into office. These statements shall be readily available to the assessor. The CA shall periodically (e.g., yearly) review the trustworthiness of personnel with trusted roles. (FOR INSTANCE personnel MAY fill in and sign a statement ('staat van inlichtingen') on basis of which their trustworthiness can be re-determined).
	Best practice
	• For personnel security we refer to Section 6 of BS 7799:1999-1 (ISO/IEC 17799). • It is good practice to let staff of third party contractors sign a separate a confidentiality statement (non-disclosure agreement) in addition to the confidentiality agreement covered with the third party contractor. • It is good practice to refrain from giving third party personnel trusted roles within the CA. • It is good practice 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.

3.7.4.4 Physical and environmental security

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized (see annex II f).

In particular:

CA General

a) physical access to facilities concerned with certificate generation, subject device provision, 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 and revocation management

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

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

f) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CA's physical and environmental security policy for systems concerned with certificate generation, subject device provision and revocation management services shall address the physical access control, natural 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.

g) 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 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	Guidance
Physical and environmental security	• A clear description of the physical environment of the CA shall be available to the assessor. This description shall discuss: - security zones implemented and their protection properties (preventive, repressive, detective and corrective); - the relation with the security critical assets; - which members of the CA staff have access to what zones. • Adequate protection (preventive, repressive, detective and corrective) against fire/smoke, power failures, water, storm etc. shall be implemented, based on a documented risk-analysis readily available to the assessor. • A complete and up-to-date inventory of the CA staff having access to security zones shall be available to the assessor. • Access codes to high-security zones shall be regularly changed. • The responsibility of maintaining the above description, risk-analysis and inventory shall be assigned by management 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 we refer to Section 7 of BS 7799:1999-1 (ISO/IEC 17799). Reviewing physical and environmental security at least yearly is good industry practice.

3.7.4.5 Operations management

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

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

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

Media handling and security

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

System Planning

f) 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

g) 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.

Subject	Guidance
Incident reporting and response	• A concise, documented description of incident handling shall be available to the assessor. Amongst other things, this document shall define the notion 'security incident' and should clearly assign tasks, authorities and responsibilities. • Evidence shall be available that the incident handling procedure is adequately communicated to the CA staff. • The responsibility of maintaining, updating and periodically reviewing virus protection programs shall be assigned to a person or body within the staff. • An adequate change management procedure shall be in place within the CA; the responsibility of maintaining, updating and periodically reviewing this shall be assigned to a person or body within the staff. • The CA shall proactively keep abreast of emerging, relevant security problems and related patches. In addition the CA shall be able to timely and adequately address emerging security problems. Responsibility for both tasks should be clearly defined.
	Best practice
	• Sources of emerging security problems can be staff, manufacturers, the 'hacker community', or special mailing lists. The CA can also participate in a Computer Emergency Response Team (CERT). • It is good practice to timely install security patches in a secure manner. • Without a proper definition of 'security incident', CA staff might not report 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

h) 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	Guidance
Operations procedures and responsibilities	• The responsibility of maintaining the above description, risk-analysis and inventory shall be assigned by management to a person or body within the CA. Periodically reviewing of the above description is a management task. • All security critical operations (e.g., root key generation, end-user registration, end-user certificate production, certificate revocation, CRL production etc.) shall be documented in detail in procedures, including the roles, staff, responsibilities and assets concerned. It shall clear 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.

3.7.4.6 System Access Management

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

NOTE 1: It is recommended that firewalls be configured to prevent protocols and accesses not required for the operation of the CA.

b) Sensitive data shall be protected when exchanged over networks which are not secure.

NOTE 2: Sensitive data includes registration information.

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

d) The CA shall ensure access to information and application system functions are restricted in accordance with the access control policy and that the CA system provides sufficient computer security controls for the separation of trusted roles identified in CA's practices, including the separation of security administrator and operation functions. Particularly, use of system utility programs shall be restricted and tightly controlled.

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 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.

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	Guidance
System Access Management	• The responsibility of maintaining the above description, risk-analysis and inventory shall be assigned by management to a person or body within the CA. Periodically reviewing of the above description is a management task. • The security configuration of all security relevant assets shall be based on a risk-analysis and shall be documented in detail and kept to date. Configuration documentation shall clearly indicate all preventive, repressive, detective and corrective controls. This documentation shall be available to the assessor. • Evidence shall be available to the assessor that adequate user management is implemented at the CA, at least for its security related assets. • Evidence shall be available to the assessor that adequate account policies are in place for security relevant assets, e.g., computers, operation system, applications, computer rooms, safes. • At any time an up-to-date list of all persons having access to a security related asset of the CA and their level of access shall be readily available. Historic access records shall also be available.
	Best practice
	• For adequate user management we refer to Section 9 of ISO/IEC 17799:2000. • 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 be 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.

3.7.4.7 Trustworthy Systems Deployment and Maintenance

The CA shall use trustworthy systems and products that are protected against modification (see annex II (f)).

NOTE 1: Requirements for the trustworthy systems may be ensured using, for example, systems conforming to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 or equivalent.
NOTE 2: It is recommended that the risk analysis carried out on the CA's services (see 7.4.1) should identify its critical services requiring trustworthy systems and the levels of assurance required.

In particular:

CA General

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

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

Subject	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 or equivalent it means that these systems are evaluated by the manufacturers or by the CA. The assessor shall check the implementation of the documentation regarding installation, maintenance and use. • Evidence shall be available 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. • Evidence shall be available 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
	• CWA 14167-1 or equivalent standards 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 (e.g., for Windows NT there is a tool called C2Config). Some platforms are even directly available in a 'hardened' version.

3.7.4.8 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 annex II (a)).

In particular:

CA General

CA key compromise

a) 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.

Subject	Guidance
Term: "as soon as possible"	The assessor shall review the CA's Business continuity plan and/or the disaster recovery plan. The CA's Business Continuity Plan or the disaster recovery plan shall 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 shall be in accordance with the estimated throughput-time of all the required activities.
	Best practice
	No stipulations.

Revocation status

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

- inform all subscribers, relying parties and other CAs with which it has agreements or other form of established relations of the compromise;

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

NOTE: When another CA with which a compromised CA has an agreement is informed of the compromise, any a CA certificate has been issued for the compromised CA should be revoked.

Subject	Guidance
Undertakings following CA key compromise: notification mechanisms	The assessor shall 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 0800 emergency telephone line (recorded message) or a help desk for the relevant parties.

3.7.4.9 CA termination

The CA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings (see 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 all subscribers, relying parties and other CAs with which it has agreements or other form of established relations.

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 7.3.1) and event log archives (see 7.4.11) for their respective period of time as indicated to the subscriber and relying party (see 7.3.4);

Subject	Guidance
Undertakings to transfer obligations for maintaining registration information and event log archives	The assessor shall review the documentation and contracts that prove that the CA has implemented controls and measures to facilitate the transfer of the registration information and event logs to an external organization in case of CA termination.
	Best practice
	The CA may have taken the following measures or may 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. ***Additional requirement for CA's that provide services in accordance with Dutch law:*** The Dutch Algemene Maatregel van Bestuur states that the external party mentioned above needs to be a CA issuing qualified certificates or a CA not issuing certificates and specialized in filing certificates (i.e. a CA rendering a PKI components service other than generating qualified certificates).

- 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.

Subject	Guidance
Arrangement to cover costs	The assessor shall review the documentation, contracts or other evidence that proves that the CA has made arrangements to cover the costs to fulfil the minimum requirements.
	Best practice
	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..

3.7.4.10 Compliance with Legal Requirements

The CA shall ensure compliance with legal requirements (see [1] article 8).

In particular:

CA General

a) Important records shall be protected 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 7.4.11).

Subject	Guidance
Term: important records	Important records are (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 • Certificate Status Information • Event Log archives The records which hold personal data (in accordance with applicable Data Protection Laws and regulations) need to be adequately protected in accordance with the European Directive.
	Best practice
	The assessor can inform whether the CA has conducted a Privacy Audit.

b) The CA shall ensure that the requirements of the European data protection Directive, as implemented through national legislation, are met.

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	Guidance
Term: completely protected from disclosure	• The term completely protected does not imply the requirement to provide 100% security. It implies that the CA shall implement adequate protection against disclosure of the information that is contributed to the CA. • The assessor shall review if the CA has implemented appropriate security measures and if the CA has drafted and implemented a procedure for the disclosure of information as a result of a Legal requirement.
	Best practice
	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.

3.7.4.11 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 annex II (i)).

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

Subject	Guidance
Term: Registration Information	Registration Information is all information collected by a CA from the subscriber or subject (end user) that is necessary to conduct CA operations, including but not limited to the Subject Registration Process and Certificate Generation Purposes.
	Best practice
	No stipulations.

Subject	Guidance
Term: Records	No stipulations.
	Best practice
	Records may be in paper or electronic form.

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.

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

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.

Subject	Guidance
Term: Period of time as appropriate for providing necessary legal evidence	The assessor shall interpret "the period of time as appropriate for" as a general term for recording paper and electronic data. The Dutch Wet elektronische handtekeningen and the Dutch Archiefwet prescribe a default period of the certificate validity period added with the archival period (in the Netherlands 7 years).
	Best practice
	No stipulations.

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 shall be clearly identified 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 shall be indicated to the subscriber and relying party as specified in 7.3.1 and 7.3.4.

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

NOTE 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.

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 7.3.1 h);
- any specific choices in the subscriber agreement (e.g. consent to publication of certificate);
- 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.

3.7.5 Organizational

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

In particular that:

3.7.5.1 CA general

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

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

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

Subject	Guidance
Term: legal entity	• Legal entity means a natural person, or a legal person. The assessor shall evaluate documents provided by the CA that demonstrate that the CA is a legal entity. For the Netherlands the following requirements apply: - In case of a natural person, the assessor checks that the person is legally entitled to conclude contracts; - In case of an ondernemings-rechtspersoon (ORP), the assessor checks that the ORP is registered in the trade register and does not forbid CA activities in its articles of association; - In case of a public rechtspersoon, the assessor checks relevant law and checks that CA activities are not forbidden. • Demonstration that a CA is a legal entity means that if a CA is part of a larger entity, certification shall only be granted to the entire legal entity. In such a situation, the structure of the entire legal entity may be subject to audit by the Assessor in order to pursue specific audit trails and/or review records relating to the CA. The part of the legal entity that forms the actual CA may trade under a distinctive name, which should appear on the accreditation certificate. [Ref: TTP.NL PART 3 G 4.6]
	Best practice
	No stipulations.

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

Subject	Guidance
Term: a system or systems for quality	The assessor shall review if the CA has implemented and documented a system or systems for quality and information security management.
	Best practice
	Quality 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 CA has adequate arrangements to cover liabilities arising from its operations and/or activities.

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

Subject	Guidance
Term: financial stability and resources	No stipulations.
	Best practice
	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.

g) The CA employs a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide certification services.

h) 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.

i) 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.

3.7.5.2 Certificate generation, revocation management

j) 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.

Subject	Guidance
Independence of certificate generation and revocation management.	The assessor shall review whether: • the CA can prove independence of the certificate generation and revocation activities from other organizations;
	Best practice
	• The CA has formal rules and structures for the appointment and operation of any committees which are involved in the certification process; such committees must be free from any commercial, financial and other pressures that might influence decisions; a structure where members are chosen to provide a balance of interests where no single interest predominates will be deemed to satisfy this provision. • Decisions to issue or revoke certificates may be taken by one authorized person within the CA or by more than one person, whereby either each person could take separate decisions independently of the others or the persons together could act as a committee. If decisions are taken by a committee, comprising among others representatives from one or more clients, the operational procedures of the CA should ensure that these representatives do not have a significant influence on decision making. This can for example be assured by the distribution of voting rights or some other equivalent means [ref: TTP.NL Part 3, G4.19].

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