Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3b: Certificate Policy for authenticity, confidentiality and non-repudiation certificates in Organization Services (G3) Domain

Version	4.11
Date	February 28, 2023

[OID 2.16.528.1.1003.1.2.5.4] Authenticity
[OID 2.16.528.1.1003.1.2.5.5] Confidentiality
[OID 2.16.528.1.1003.1.2.5.7] Non repudiation

Publishers imprint

Version number	4.11
Contact person	Policy Authority of PKIoverheid

Organization	Logius

Street address
Wilhelmina van Pruisenweg 52

Postal address
Postbus 96810
2509 JE DEN HAAG

T 0900-555 4555
servicecentrum@logius.nl

Contents

1. INTRODUCTION

Refer to Programme of Requirements part 3 Basic Requirements.

1.2 Document name and identification

1.2.1 Revisions

1.2.1.1 Version 3.7 to 4.0

New

None.

Modifications

- PoR requirements have been renumbered according to a new naming convention;
- The creation of a document containing the baseline and additional requirements;
- Changes to requirements can be found in the baseline and additional requirements documents respectively.

Editorial

- Editorial changes to requirements can be found in the baseline and additional requirements documents respectively. These changes have no effect on the content of the information.

1.2.1.2 Version 4.0 to 4.1

New

- Certification against ETSI TS 102 042 (effective date no later than 4 weeks after publication of PoR 4.1).

Modifications

- Requirement 6.3.2-pkio109 (effective date no later than 4 weeks after publication of PoR 4.1).

Editorial

- Small editiorial change to the following requirements:
    - Requirement 5.7.4-pkio86.

1.2.1.3 Version 4.1 to 4.2

New

- Requirement 6.3.2-pkio148 (effective date no later than 4 weeks after publication of PoR);
- Requirement 7.1-pkio150 (effective date 1 July 2016).

Modifications

- Certificate profile: changed use of subjectAltName from “prohibited toegestaan” to “optional”;
- Ban on issuance of 5 year services certificates to 3 year: removed requirements 6.3.2.-pkio109 and added 6.3.2-pkio148.

Editorial

None.

1.2.1.4 Version 4.2 to 4.3

New

- Pkio153: additional requirements on the use of qualified seals (effective date 1-7-2016);

- New policyidentifier and profile modifications for the use of qualified seals (effective date 1-7-2016);
- Addition of Issuer.organizationalIdentifier in the certificate profile (effective date 1-7-2016).

Modifications

- Description with attribute CertificatePolicies (effective date 1-7-2016);
- Removal of optional use KeyAgreement with Key Usage (effective date no later than 4 weeks after publication of PoR 4.3);
- ETSI TS 102 176-1 replaced by ETSI TS 119 312 (effective date no later than 4 weeks after publication of PoR 4.3);
- Dropped requirement pkio95 because of i.v.m. duplicate requirement in ETSI EN 319 411-1;
- Use of values in the BasicConstraints field no longer permitted in end entity certificates (effective date 1-7-2016) ;
- ETSI TS 102 042 replaced by ETSI EN 319 411-1 (effective date 1-7-2016 or when the accreditation to the certifying body has been granted with a final date of 30 June 2017);
- Requirement 7.1-pkio150 modified (removed not permitted EKU) (effective date 1-11-2016).

Editorial

- Removed references to G1 (expired) and clarified reference to G3 (domains).

1.2.1.5 Version 4.3 to 4.4

New

None.

Modifications

- Removal of requirement 5.3.2-pkio79 (effective date 1-2-2017);
- Clarification of issuer.organizationIdentifier field (effective date 1-2-2017);
- Tightening of use optional EKUs that conflict with the parent TSP CA certificate (effective date 1-2-2017).

Editorial

- Moved QCStatements from Public to Private Extensions;
- Replaced CSP (Certificate Service Provider) with TSP (Trust Service Provider) in accordance with eIDAS directive.

1.2.1.6 Version 4.4 to 4.5

New

- Mandatory English CPS (requirement 2.2-pkio3, effective date 1-10-2017);
- Mandatory yearly renewal CPS (requirement 2.2-pkio156, effective date 1-1-2017).

Modifications

- Requirement 4.9.9-pkio67 now references RFC6960 instead of RFC2560 (effective date 31-12-2016);
- Allow/require EKU emailProtection in authenticity and non-repudiation certificates in requirement 7.1-pkio149 (effective date1-4-2017);
- Change in OID 2.16.528.1.1003.1.2.5.4 to also cover OCSP responder certificates (effective date 1-7-2017);
- Mandatory use of field “NextUpdate” in OCSP responses (requirement 4.9.9-pkio71, effective date 1-7-2017).

Editorial

- Removed typos from certificate profile.

1.2.1.7 Version 4.5 to 4.6

New

None.

Modifications

- Added subject.organizationIdentifier in the certificate profile to fix an ommission (effective date directly after publication of PoR 4.6);
- Modified reference to ETSI certificate profiles (effective date directly after publication of PoR 4.6);
- Corrected subjectAltName.othername field (effective date directly after publication of PoR 4.6).

Editorial

None.

1.2.1.8 Version 4.6 to 4.7

New

- Requirement 7.1-pkio177 (effective date immediately after publication PoR 4.7);
- Requirement 3.2.3-pkio169 (effective date 4 weeks after publication of PoR 4.7).

Modifications

- Description of a number of certificate attributes replaced by reference to requirement 7.1-pkio174 (effective date 8 weeks after publication PoR 4.7);
- Reference to CWA 14 169 amended to EN 419 211 for QSCDs. This also sets requirements for the issue of QSCDs for requirements 6.1.1-pkio88, 6.1.1-pkio93, 6.1.1-pkio153, 6.2.11-pkio105, 6.4.1-pkio112 and 4.9.1-pkio52 (effective date immediately after publication PoR 4.7);
- Requirement 6.3.2-pkio148 expired and is replaced by requirement 6.3.2-pkio109 (effective date immediately after publication of PoR 4.7).

Editorial

None.

1.2.1.9 Version 4.7 to 4.8

New

- New requirement 3.2.2-pkio186 on (re)validation of organizational data (effective date immediately after publication PoR 4.8).

Modifications

- Change in requirement 7.1-pkio150 to enable usage of constraint (EKU emailProtection) in PoR (effective date immediately after publication PoR 4.8);
- Requirement 9.17-pkio140 removed (effective date immediately after publication PoR 4.8);
- Changes in serial number requirements in requirement 7.1-pkio173 (effective date August 29, 2019).

Editorial

- Changes in definition of private key in requirement 4.9.1-pkio52 (effective date immediately after publication PoR 4.8).

1.2.1.10 Version 4.8 to 4.9

New

- Introducing new additional requirement 2.2-PKIo191 for RFC 3647 compliance in PoR Part 3b (effective date after 01-04-2020).
- Created new requirement 8.1-pkio189 as an Additional Requirement for PoR Part 3b (effective date 02-17-2020).

- Created new requirement 4.9.1-pkio192 on certificate revocation as an Additional Requirement for PoR Part 3b (effective date 02-17-2020).

Modifications

- Change requirements 6.1.1-pkio89 to comply with Mozilla policy on signature encoding (effective date 01-03-2020).
- Removed PoR Part 3b from scope of additional requirement 4.9.1-pkio52 (effective date immediately after publication PoR 4.9).

Removals:

- Requirement 6.1.1-pkio87 has been deleted (effective date immediately after publication PoR 4.9).
- Requirement 2.2-pkio8 has been deleted (effective date immediately after publication PoR 4.9).

Editorial

None.

1.2.1.11 Version 4.9 to 4.10

New

- Added basic requirement 8.2-pkio199.
- Added new additional requirement 8.4-pkio195.
- Added new additional requirement 8.4-pkio200.

Modifications

- Change the description and criteria of the `subject:organizationalUnitName` attribute in the certificate profile.
- Changes to the `subject:organizationIdentifie`r attribte in the certificate profile.
- Change the description, explanation, and criterium of the `extensions:subjectAltName:otherName` attribute in the certificate profile.
- Expand the description of the `extensions:certificatePolicies` field in the certificate profile with additional ETSI 319 411 certificate policies.
- Change the `extensions:certificatePolicies:policyQualifiers:qualifier:userNotice` field criteria to "MAY" in the certificate profile.
- Replace Telecommunications Act with eDIAS in requirement 9.6.1-pkio127.

Removals

- Remove the `subject:postalAddress` attribute from the certificate profile.
- Remove the `extensions:freshestCRL` field from the certificate profile.
- Remove the `extensions:subjectInfoAccess` field from the certificate profile.
- Remove requirement 9.6.1-pkio129.

Editorial

- Editorial changes in the description and explanation of the `extensions:certificatePolicies:policyQualifiers:qualifier:userNotic`e field in the certificate profile resulting from combining change 450 with change 445.13.
- Expanded the description of the `extensions:basicConstraints` field in the certificate profile.
- Editorial changes to requirement 9.6.1-pkio127.

1.2.1.12 Version 4.10 to 4.11

New

None.

Modifications

None.

Removals

None.

Editorial

None.

1.2.2 Relevant dates

Version	Date	Description
4.0	12-2014	Ratified by the Ministry of the Interior and Kingdom Relations December 2014
4.1	07-2015	Ratified by the Ministry of the Interior and Kingdom Relations July 2015
4.2	01-2016	Ratified by the Ministry of the Interior and Kingdom Relations January 2016
4.3	07-2016	Ratified by the Ministry of the Interior and Kingdom Relations July 2016
4.4	02-2017	Ratified by the Ministry of the Interior and Kingdom Relations February 2017
4.5	07-2017	Ratified by the Ministry of the Interior and Kingdom Relations July 2017
4.6	01-2018	Ratified by the Ministry of the Interior and Kingdom Relations January 2018
4.7	01-2019	Ratified by the Ministry of the Interior and Kingdom Relations January 2019
4.8	02-2020	Ratified by the Ministry of the Interior and Kingdom Relations February 2020
4.9	02-2021	Ratified by the Ministry of the Interior and Kingdom Relations February 2021
4.10	02-2022	Ratified by the Ministry of the Interior and Kingdom Relations February 2022
4.11	02-2023	Ratified by the Ministry of the Interior and Kingdom Relations February 2023

1.3 PKI participants

1.3.1 Certification authorities

In this document the distinction is made between the term Certification Authority (CA) and Trust Service Provider. In international usage, "CA" is an umbrella term that refers to all entities authorized to issue, manage, revoke, and renew certificates. This can apply to the actual CA certificate as well as the organization. In this CP, the organization which holds a CA is refered to as a TSP. The term CA is used to refer to the infrastructure and keymaterial from which a TSP issues and signs certificates. This CP covers all certificates issued and signed by the following CAs hereinafter referred to as TSPs.

Common Name	Not Before	Not After	Serial Number	SHA256 Fingerprint
Digidentity BV PKIoverheid Organisatie Services CA – 2021 (3b)	25 Feb 2021	12 Nov 2028	27909eb5db69f40c220006f5663b6b93442fc915	827A6B205D2E73FF379286DD0B2DED5AEC7239EFE6BC8CACB03ABCCD84B95750
KPN BV PKIoverheid Organisatie Services CA - G3 (3b)	08 Dec 2016	12 Nov 2028	4895514759099277809 (0x43f05cbc60cb61f1)	f22db657a1a929841abcac52671a5cee8a7d069586af85ce16de2b05dda22252
MinIenW PKIoverheid Organisatie Services CA - G3 (3b)	16 Apr 2019	12 Nov 2028	7ac7b828ef1fddc1e3fb7d36ba49efb82288f419	394CCBBC0B3595CA0DED40072FAF98636ED021699AD2894564879165B5B5D4C9
QuoVadis PKIoverheid Organisatie Services CA - G3 (3b)	03 Nov 2016	12 Nov 2028	5414135049653221353	BECFDE124CEDD344D925CB55EDDA662D9A9C0688FA9A0870CE3DBB6DA4313E4E
UZI-register Medewerker niet op naam CA G3 (2017) (3b)	09 May 2017	12 Nov 2028	6693480468265575250	38DED3FF6827579008AF4887EB9698A3CFA927FA8ED59F06BA090FB9A63E2D77
UZI-register Medewerker niet op naam CA G3 (2019) (3b)	18 Apr 2019	12 Nov 2028	24cb50555470eb7995c7a9758d8c42bd242af0d8	972957304031234ED17679FDCB97556D6173D5F2BF0E6E66D612680CA6E77685

1.3.2 Registration authorities

Refer to Programme of Requirements part 3 Basic Requirements.

1.3.3 Subscribers

Refer to Programme of Requirements part 3 Basic Requirements.

1.3.4 Relying parties

Refer to Programme of Requirements part 3 Basic Requirements.

1.3.5 Other participants

Refer to Programme of Requirements part 3 Basic Requirements.

1.4 Certificate usage

1.4.1 Appropiate certificate uses

The use of certificates issued under this CP relates to communication from certificate holders who act on behalf of the subscriber.

[OID 2.16.528.1.1003.1.2.5.4]

Authenticity certificates, issued under this CP, can be used to identify and authenticate, by electronic means, the service that is part of the organizational entity, that is responsible for the relevant service.

Issuance of code signing certificates by means of which the integrity and authenticity of software can be safeguarded by a digital signature being placed are NOT allowed under this CP.

Under this OID OCSP responder certificates may be issued for use within the domain Organisation Services. Said certificates can be used to sign OCSP responses for use in the verification of the validity of the end user certificate. More information can be obtained in appendix A of the base requirements.

[OID 2.16.528.1.1003.1.2.5.5]

Confidentiality certificates, issued under this CP, can be used to protect the confidentiality of data that is exchanged and/or stored in an electronic format.

[OID 2.16.528.1.1003.1.2.5.7]

Seal certificates, issued under this CP, can be used to verify electronic seals.

1.4.2 Prohibited certificate uses

Refer to Programme of Requirements part 3 Basic Requirements.

1.5 Policy administration

1.5.1 Organization administering the document

The Ministry of Interior and Kingdom Relations (BZK) is responsible for this CPS. BZK has delegated this responsibility to Logius, including approval of changes of this document.

1.5.2 Contact person

Policy Authority PKIoverheid
Wilhelmina van Pruisenweg 52
Postbus 96810
2509 JE DEN HAAG
http://www.logius.nl/pkioverheid
servicecentrum@logius.nl[1]

1.5.3 Person determining CPS suitability for the policy

The Policy Authority PKIoverheid (PA) determines the suitability of CPSs published as a result of this CP.

1.5.4 CP approval procedures

The PA PKIoverheid reserves the right to amend this CP. Changes are applicable from the date that is listed in section *1.2.2. Relevant dates*. The management of Logius is responsible for following the procedures as listed in section *9.12 Amendments* and final approval of this CP.

1 mailto:servicecentrum@logius.nl

1.6 Definitions and acronyms

1.6.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”,“SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in these Requirements MUST be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Refer to Programme of Requirements part 3 Basic Requirements.

2.1 Repositories

Refer to Programme of Requirements part 3 Basic Requirements.

2.2 Publication of certification information

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  2.2-pkio191 —

Description	The CPS of the TSP MUST follow the layout according to RFC 3647. All sections and subsections as defined in RFC3647 MUST be included in the CPS. Empty passages are not allowed. If there is no further requirement or explanation from a TSP for that paragraph, the text "No stipulation" MUST be included. Additional sections may be included, as long as they come after the sections and subsections defined by RFC 3647 and therefore do not change the RFC numbering.
Comment	-

- Page:
  2.2-pkio3 —

Description	The CPS MUST be available in English. If a CPS is published in multiple languages there MUST be no substantial substantive difference between the different versions. In case of interpretation disputes related to CPS texts the English language version SHALL always be leading.
Comment	-

2.3 Time or frequency of publication

Refer to Programme of Requirements part 3 Basic Requirements.

2.4 Access controls on repositories

Refer to Programme of Requirements part 3 Basic Requirements.

3. IDENTIFICATION AND AUTHENTICATION

Refer to Programme of Requirements part 3 Basic Requirements.

3.1 Naming

Refer to Programme of Requirements part 3 Basic Requirements.

3.1.1 Types of names

Refer to Programme of Requirements part 3 Basic Requirements.

3.1.2 Need for names to be meaningful

Refer to Programme of Requirements part 3 Basic Requirements.

3.1.3 Anonymity or pseudonymity of subscribers

Refer to Programme of Requirements part 3 Basic Requirements.

3.1.4 Rules for interpreting various name forms

Refer to Programme of Requirements part 3 Basic Requirements.

3.1.5 Uniqueness of names

Refer to Programme of Requirements part 3 Basic Requirements.

3.1.6 Recognition, authentication, and role of trademarks

Refer to Programme of Requirements part 3 Basic Requirements.

3.2 Initial identity validation

Refer to Programme of Requirements part 3 Basic Requirements.

3.2.1 Method to prove possession of private key

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  3.2.1-pkio13 —

Description	The TSP is responsible for ensuring that the subscriber supplies the certificate signing request (CSR) securely. The secure delivery must take place in the following manner: • the entry of the CSR on the TSP's application developed especially for that purpose, using an SSL connection with a PKIoverheid SSL certificate or similar or; • the entry of the CSR on the HTTPS website of the TSP that uses a PKIoverheid SSL certificate or similar or; • sending the CSR by e-mail, along with a qualified electronic signature of the certificate manager that uses a PKIoverheid qualified certificate or similar or; • entering or sending a CSR in a way that is at least equivalent to the aforementioned ways.

Comment	-

3.2.2 Authentication of organization identity

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  3.2.2-pkio144 —

Description	The TSP has to verify that the name of the organization registered by the subscriber that is incorporated in the certificate is correct and complete
Comment	-

- Page:
  3.2.2-pkio186 —

Description	If an organization changes its name but the underlying registration number (e.g. HRN) remains the same, then the subscriber DOES NOT have to go through the subscription registration again. If the organization name remains the same but the underlying registration number changes, then the TSP MUST perform the subscription registration again. In both cases, the existing certificate must be withdrawn because the data in the certificate no longer conforms to the originally validated data.
Comment	-

- Page:
  3.2.2-pkio4 —

Description	The TSP has to verify that the subscriber is an existing organization.
Comment	-

3.2.3 Authentication of individual identity

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  3.2.3-pkio169 —

Description	For certificates that are suitable for signing and / or encrypting e-mail messages and which include the e-mail address of the certificate holder, the TSP will take appropriate measures to ensure that the applicant has control over the e-mail address in question OR that he / she is authorized by the holder of the e-mail address to have this e-mail address included in a certificate. The TSP MUST state clearly in its CPS which procedures have been implemented to confirm the above. In these procedures, the TSP MUST

	perform validation of the domain part (@domain.com[2]) itself. This check MUST NOT be performed by third parties.
Comment	-

- Page:
  3.2.3-pkio22 —

Description	In accordance with Dutch legislation and regulations, the TSP has to check the identity and, if applicable, specific properties of the certificate manager. Proof of identity has to be verified based on the physical appearance of the person himself, either directly or indirectly, using means by which the same certainty can be obtained as with personal presence. The proof of identity can be supplied on paper or electronically.
Comment	-

- Page:
  3.2.3-pkio24 —

Description	The identity of the certificate manager can only be established using the valid documents referred to in article 1 of the Compulsory Identification Act (Wet op de identificatieplicht). The TSP has to check the validity and authenticity of these documents.
Comment	If the personal identity of the certificate manager is verified when a certificate is requested in the Government, Companies and Organization Domains, then the identity verification of the certificate manager will be considered to have taken place under this CP.

- Page:
  3.2.3-pkio26 —

Description	The certificate manager is a person whose identity has to be established in conjunction with an organizational entity. Proof has to be submitted of: • full name, including surname, first name, initials or other first (names) (if applicable) and surname prefixes (if applicable); • date of birth and place of birth, a nationally applicable registration number, or other characteristics of the certificate manager that can be used in order to, as far as possible, distinguish this person from other persons with the same name; • proof that the certificate manager is entitled to receive a certificate for a certificate holder on behalf of the legal personality or other organizational entity.
Comment	-

3.2.4 Non-verified subscriber information

Refer to Programme of Requirements part 3 Basic Requirements.

3.2.5 Validation of authority

Refer to Programme of Requirements part 3 Basic Requirements.

2 http://domain.com

Additional requirements:

- Page:
  3.2.5-pkio30 —

Description	The TSP has to verify that: • the proof that the certificate holder is authorized to receive a certificate on behalf of the subscriber, is authentic; • the certificate manager has received permission from the subscriber to perform the actions that he has been asked to perform (if the certificate manager performs the registration process).
Comment	The "certificate manager" who takes over those actions from the certificate holder does not necessarily have to be the same person as the system administrator or personnel officer. Also the knowledge of the activation data of the key material (for example PIN) can be shared by various people if the organization of the certificate management requires that. However, it is recommended that as few people as possible have knowledge of the PIN. It also would be wise to take measures that limit access to the PIN. An example of this is placing the PIN in a safe to which only authorized persons can gain access in certain situations.

- Page:
  3.2.5-pkio33 —

Description	The agreement that the TSP enters into with the subscriber has to state that the subscriber is responsible for immediately informing the TSP of any relevant changes to the relationship between the subscriber and certificate manager and/or service. When the service no longer exists, this has to take place by means of a revocation request.
Comment	-

3.2.6 Criteria for interoperation

Refer to Programme of Requirements part 3 Basic Requirements.

3.3 Identification and authentication for re-key requests

Refer to Programme of Requirements part 3 Basic Requirements.

3.3.1 Identification and authentication for routine re-key

Refer to Programme of Requirements part 3 Basic Requirements.

3.3.2 Identification and authentication for re-key after revocation

Refer to Programme of Requirements part 3 Basic Requirements.

3.4 Identification and authentication for revocation request

Refer to Programme of Requirements part 3 Basic Requirements.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Refer to Programme of Requirements part 3 Basic Requirements.

4.1 Certificate Application

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  4.1-pkio47 —

Description	Before a services server certificate is issued, the TSP must enter into an agreement with the subscriber and receive a certificate request signed by the certificate manager. The agreement must be signed by the Authorized Representative or Representation of the subscriber.
Comment	-

4.1.1 Who can submit a certificate application

Refer to Programme of Requirements part 3 Basic Requirements.

4.1.2 Enrollment process and responsibilities

Refer to Programme of Requirements part 3 Basic Requirements.

4.2 Certificate application processing

Refer to Programme of Requirements part 3 Basic Requirements.

4.2.1 Performing identification and authentication functions

Refer to Programme of Requirements part 3 Basic Requirements.

4.2.2 Approval or rejection of certificate applications

Refer to Programme of Requirements part 3 Basic Requirements.

4.2.3 Time to process certificate applications

Refer to Programme of Requirements part 3 Basic Requirements.

4.3 Certificate issuance

Refer to Programme of Requirements part 3 Basic Requirements.

4.3.1 CA actions during certificate issuance

Refer to Programme of Requirements part 3 Basic Requirements.

4.3.2 Notification to subscriber by the CA of issuance of Certificate

Refer to Programme of Requirements part 3 Basic Requirements.

4.4 Certificate acceptance

Refer to Programme of Requirements part 3 Basic Requirements.

4.4.1 Conduct constituting certificate acceptance

Refer to Programme of Requirements part 3 Basic Requirements.

4.4.2 Publication of the certificate by the CA

Refer to Programme of Requirements part 3 Basic Requirements.

4.4.3 Notification of certificate issuance by the CA to other Entities

Refer to Programme of Requirements part 3 Basic Requirements.

4.5 Key pair and certificate usage

Refer to Programme of Requirements part 3 Basic Requirements.

4.5.1 Subscriber private key and certificate usage

Refer to Programme of Requirements part 3 Basic Requirements.

4.5.2 Relying party public key and certificate usage

Refer to Programme of Requirements part 3 Basic Requirements.

4.6 Certificate renewal

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.1 Circumstance for certificate renewal

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.2 Who may request renewal

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.3 Processing certificate renewal requests

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.4 Notification of new certificate issuance to subscriber

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.5 Conduct constituting acceptance of a renewal certificate

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.6 Publication of the renewal certificate by the CA

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.7 Notification of certificate issuance by the CA to other entities

Refer to Programme of Requirements part 3 Basic Requirements.

4.7 Certificate re-key

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.1 Circumstance for certificate re-key

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.2 Who may request certification of a new public key

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.3 Processing certificate re-keying requests

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.4 Notification of new certificate issuance to subscriber

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.6 Publication of the re-keyed certificate by the CA

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.7 Notification of certificate issuance by the CA to other entities

Refer to Programme of Requirements part 3 Basic Requirements.

4.8 Certificate modification

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.1 Circumstance for certificate modification

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.2 Who may request certificate modification

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.3 Processing certificate modification requests

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.4 Notification of new certificate issuance to subscriber

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.5 Conduct constituting acceptance of modified certificate

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.6 Publication of the modified certificate by the CA

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.7 Notification of certificate issuance by the CA to other entities

Refer to Programme of Requirements part 3 Basic Requirements.

4.9 Certificate revocation and suspension

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.1 Circumstances for revocation

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  4.9.1-pkio192 —

Description	Certificates will be revoked when: • the subscriber indicates that the original request for a certificate was not allowed and the subscriber does not grant permission retroactively; • the TSP has sufficient evidence that the subscriber's private key (associated with the corresponding certificate) has been compromised or there is a suspicion of compromise, inherent security weakness, or that the certificate has been misused in another way . A key is considered compromised in the event of unauthorized access or suspected unauthorized access to the private key, lost or presumably lost private key, SSCD, SUD or QSCD, stolen or presumably stolen key, SSCD, SUD or QSCD or destroyed key, SSCD, SUD or QSCD if applicable; • a subscriber does not fulfill his obligations as set out in this CP or the corresponding CPS of the TSP or the agreement that the TSP has with the subscriber; • the TSP is informed or otherwise becomes aware of a material change in the information contained in the certificate. An example of this is: change of the name of the certificate holder (service); • the TSP determines that the certificate has not been issued in accordance with this CP or the associated CPS of the TSP or the agreement that the TSP has with the subscriber; • the TSP determines that information in the certificate is incorrect or misleading; • the TSP ceases its activities and the CRL and OCSP services are not continued by another TSP; • the PA of PKIoverheid determines that the technical content of the certificate entails an irresponsible risk for subscribers, relying parties and third parties (e.g. browser parties); • one of the events occurs, as described in chapter 6.2 of the Mozilla Root Store Policy[3].
Comment	-

4.9.2 Who can request revocation

Refer to Programme of Requirements part 3 Basic Requirements.

3 https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

4.9.3 Procedure for revocation request

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  4.9.3-pkio57 —

Description	In any case, the TSP has to use a CRL to make the certificate status information available.
Comment	-

4.9.4 Revocation request grace period

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.5 Time within which CA must process the revocation request

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.6 Revocation checking requirement for relying parties

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.7 CRL issuance frequency (if applicable)

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  4.9.7-pkio65 —

Description	The TSP has to update and reissue the CRL for end user certificates at least once every 7 calendar days and the date of the “Next update” field may not exceed the date of the “Effective date” field by 10 calendar days.
Comment	-

4.9.8 Maximum latency for CRLs (if applicable)

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.9 On-line revocation/status checking availability

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  4.9.9-pkio66 —

Description	The revocation management services of the TSP can support the Online Certificate Status Protocol (OCSP) as an addition to the publication of CRL information. If this support is available, this has to be stated in the CPS.

Comment	If OCSP is offered the following requirements are applicable: • 1.1-pkio10 (basic requirement) • 9.5-pkio61 (basic requirement) • 9.9-pkio67 • 9.9-pkio68 • 9.5-pkio69 (basic requirement) • 9.9-pkio70 • 9.9-pkio71 • 10.2-pkio73 (basic requirement) NB: (EV) server certificates MUST use OCSP services as stipulated in ETSI EN 319 411-1 and the Baseline Requirements.

- Page:
  4.9.9-pkio67 —

Description	If the TSP supports the Online Certificate Status Protocol (OCSP), this must conform to IETF RFC 6960.
Comment	-

- Page:
  4.9.9-pkio70 —

Description	If the TSP supports OCSP, the information that is provided through OCSP has to be at least as equally up-to-date and reliable as the information that is published by means of a CRL, during the validity of the certificate that is issued and furthermore up to at least six months after the time at which the validity of the certificate has expired or, if that time is earlier, after the time at which the validity is ended by revocation.
Comment	-

- Page:
  4.9.9-pkio71 —

Description	If the TSP supports OCSP, the TSP has to update the OCSP service at least once every 4 calendar days. The maximum expiry term of the OCSP responses is 10 calendar days. In addition OCSP responses must contain the “nextUpdate” field in conformance to RFC6960.
Comment	-

4.9.10 On-line revocation checking requirements

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.11 Other forms of revocation advertisements available

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.12 Special requirements related to key compromise

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.13 Circumstances for suspension

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.14 Who can request suspension

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.15 Procedure for suspension request

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.16 Limits on suspension period

Refer to Programme of Requirements part 3 Basic Requirements.

4.10 Certificate status services

Refer to Programme of Requirements part 3 Basic Requirements.

4.10.1 Operational characteristics

Refer to Programme of Requirements part 3 Basic Requirements.

4.10.2 Service availability

Refer to Programme of Requirements part 3 Basic Requirements.

4.10.3 Optional features

Refer to Programme of Requirements part 3 Basic Requirements.

4.11 End of subscription

Refer to Programme of Requirements part 3 Basic Requirements.

4.12 Key escrow and recovery

Refer to Programme of Requirements part 3 Basic Requirements.

4.12.1 Key escrow and recovery policy and practices

Refer to Programme of Requirements part 3 Basic Requirements.

4.12.2 Session key encapsulation and recovery policy and practices

Refer to Programme of Requirements part 3 Basic Requirements.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Refer to Programme of Requirements part 3 Basic Requirements.

5.1 Physical controls

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.1 Site location and construction

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.2 Physical access

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.3 Power and air conditioning

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.4 Water exposures

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.5 Fire prevention and protection

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.6 Media storage

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.7 Waste disposal

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.8 Off-site backup

Refer to Programme of Requirements part 3 Basic Requirements.

5.2 Procedural controls

Refer to Programme of Requirements part 3 Basic Requirements.

5.2.1 Trusted roles

Refer to Programme of Requirements part 3 Basic Requirements.

5.2.2 Number of persons required per task

Refer to Programme of Requirements part 3 Basic Requirements.

5.2.3 Identification and authentication for each role

Refer to Programme of Requirements part 3 Basic Requirements.

5.2.4 Roles requiring separation of duties

Refer to Programme of Requirements part 3 Basic Requirements.

5.3 Personnel controls

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.1 Qualifications, experience, and clearance requirements

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.2 Background check procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.3 Training requirements

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.4 Retraining frequency and requirements

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.5 Job rotation frequency and sequence

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.6 Sanctions for unauthorized actions

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.7 Independent contractor requirements

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.8 Documentation supplied to personnel

Refer to Programme of Requirements part 3 Basic Requirements.

5.4 Audit logging procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.1 Types of events recorded

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  5.4.1-pkio80 —

Description	Logging has to take place on at least:
	• Routers, firewalls and network system components;
	• Database activities and events;
	• Transactions;
	• Operating systems;
	• Access control systems;
	• Mail servers.
	
	At the very least, the TSP has to log the following events:
	• CA key life cycle management;
	• Certificate life cycle management;
	• Threats and risks such as:
	  • Successful and unsuccessful attacks on the PKI system;
	  • Activities of staff on the PKI system;
	  • Reading, writing and deleting data;
	  • Profile changes (Access Management);
	  • System failure, hardware failure and other abnormalities;
	  • Firewall and router activities;
	  • Entering and leaving the CA space.
	
	At the very least, the log files have to register the following:
	• Source addresses (IP addresses if available);
	• Destination addresses (IP addresses if available);
	• Time and date;
	• User IDs (if available);
	• Name of the incident;
	• Description of the incident.

Comment	Based on a risk analysis the TSP determines which data it should save.

5.4.2 Frequency of processing log

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.3 Retention period for audit log

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.4 Protection of audit log

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.5 Audit log backup procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.6 Audit collection system (internal vs. external)

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.7 Notification to event-causing subject

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.8 Vulnerability assessments

Refer to Programme of Requirements part 3 Basic Requirements.

5.5 Records archival

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.1 Types of records archived

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  5.5.1-pkio82 —

Description	The TSP MUST archive all information used to verify the identity of the subscriber, certificate manager and applicants of revocation requests. This information includes reference numbers of the documentation used for verification, including limitations concerning the validity.
Comment	-

5.5.2 Retention period for archive

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.3 Protection of archive

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.4 Archive backup procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.5 Requirements for time-stamping of records

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.6 Archive collection system (internal or external)

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.7 Procedures to obtain and verify archive information

Refer to Programme of Requirements part 3 Basic Requirements.

5.6 Key changeover

Refer to Programme of Requirements part 3 Basic Requirements.

5.7 Compromise and disaster recovery

Refer to Programme of Requirements part 3 Basic Requirements.

5.7.1 Incident and compromise handling procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.7.2 Computing resources, software, and_or data are corrupted

Refer to Programme of Requirements part 3 Basic Requirements.

5.7.3 Entity private key compromise procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.7.4 Business continuity capabilities after a disaster

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  5.7.4-pkio86 —

Description	The TSP has to draw up a business continuity plan (BCP) for, at the very least, the core services dissemination service, revocation management service and revocation status service, the aim being, in the event of a security breach or emergency, to inform, reasonably protect and to continue the TSP services for subscribers, relying parties and third parties (including browser parties). The TSP has to test, assess and update the BCP annually. At the very least, the BCP has to describe the following processes: • Requirements relating to entry into force; • Emergency procedure/fall-back procedure; • Requirements relating to restarting TSP services; • Maintenance schedule and test plan that cover the annual testing, assessment and update of the BCP; • Provisions in respect of highlighting the importance of business continuity; • Tasks, responsibilities and competences of the involved agents; • Intended Recovery Time or Recovery Time Objective (RTO); • Recording the frequency of back-ups of critical business information and software; • Recording the distance of the fall-back facility to the TSP's main site; and • Recording the procedures for securing the facility during the period following a security breach or emergency and for the organization of a secure environment at the main site or fall-back facility.
Comment	-

5.8 CA or RA termination

Refer to Programme of Requirements part 3 Basic Requirements.

6. TECHNICAL SECURITY CONTROLS

Refer to Programme of Requirements part 3 Basic Requirements.

6.1 Key pair generation and installation

Refer to Programme of Requirements part 3 Basic Requirements.

6.1.1 Key pair generation

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  6.1.1-pkio153 —

Description	Subject key generation of a qualified digital seal certificate for the use of mass automated signing of standardised data is allowed in ETSI 319 411-2. ETSI does not stipulate the applicable security requirements. Subject key generation within PKIoverheid is possible under the following conditions: The contract between the TSP and the subscriber contains an assertion that the subscriber will generate, store and use the private key on a qualified device for electronic signatures – such as a HSM – which meets the requirements of {7} CWA 14169 Secure signature-creation devices or EN 419 211 for Qualified signature-creation devices "EAL 4+" or equivalent security criteria such as FIPS 140-2 level 3. The subscriber shall hand over evidence to this effect with the certificate request by submitting the certification of the secure device and, if applicable, a screenshot of the settings of the secure device on FIPS140-2 level 3. • The contract between the TSP and the subscriber contains an assertion in which the subscriber states that the private key (and associated activation data, such as a PIN code) related to the public key is generated in the qualified device and is kept secret and protected in future. The subscriber shall hand over evidence to this effect of the PKI ceremony script which is used during the implementation of the qualified device for electronic signatures and the generation of the key pair. • The TSP is present during the PKI ceremony for the commissioning of the qualified device for electronic signatures and the generation of the key pair. This enables the TSP to check the effectiveness of the security measures. • During registration the Subscriber submits a written statement of demonstrably satisfying the requirements and/or conditions placed either on the use of the qualified device for electronic signatures, or by the certification of the device on the environment in which it is administrated and the administration itself. • The Subscriber submits a written statement that the certificate holder has explicitly mandated the system administrators of the qualified device for electronic signatures for the administration and that access to this device is always subject to dual control.
Comment	If the de TSP generates the key pair and the certificate and distributes these to the subscriber on a secure device it is not necessary to be present at the ceremony.

- Page: 6.1.1-pkio88 —

Description	The keys of certificate holders (or data for creating electronic signatures) have to be generated using a device that fulfils the requirements mentioned in EN 419 211 for QSCD's or CWA 14169 for SSCD's (transitional permission regime) "Secure signature-creation devices "EAL 4+"" or comparable security criteria.
Comment	-

- Page:
  6.1.1-pkio89 —

Description	The algorithm and length of the cryptographic keys that the TSP uses to generate the keys of certificate holders must meet the requirements set in the list of cryptographic algorithms and key lengths, as defined in ETSI TS 119 312. In addition, the TSP must also follow the requirements described in Chapters 5.1 and 5.1.1 of the most current Mozilla Root Store Policy. The use of RSA-PSS is permitted, but is not recommended.
Comment	Although ETSI TS 119 312 outlines the recommended algorithms and key lengths, these are compulsory within the PKI for the government. Requests relating to the use of other algorithms have to be submitted, along with the reasoning behind this, to the PA of the PKI for the government.

- Page:
  6.1.1-pkio92 —

Description	A TSP within PKIoverheid is not allowed to issue code signing certificates.
Comment	-

- Page:
  6.1.1-pkio93 —

Description	Instead of the TSP generating the keys, the certificate manager MAY generate the keys of the services authenticity and encryption certificates in a SUD using PKCS#10 to deliver the CSR to the TSP for signing, under the following conditions: • The agreement between the TSP and the subscriber stipulates that the certificate manager generates, saves and uses the private key on a secure device that conforms to the requirements of CWA 14169 for a Secure signature-creation devices or EN 419 211 for Qualified signature-creation devices "EAL 4+" or comparable security criteria. With the request the subscriber must prove that the secure device used for key generation conforms to CWA 14169 for a Secure signature-creation devices or EN 419 211 for Qualified signature-creation devices EAL 4+"" or comparable security criteria. The TSP must then verify that the SUD in question conforms (comparable to "The subscriber MUST prove that the organization may use this name.") • On registration the certificate manager must at least produce a written statement that measures have been taken in the environment of the system that generates/contains the keys. The measures must be of such quality that is practically impossible to steal or copy the keys unnoticed. The agreement between the subscriber and the TSP must stipulate that the TSP has the right to perform an audit on the measures taken (conform 6.2.11-pkio107) • The agreement between the subscriber and the TSP must contain the following condition. The subscriber must declare that the private key (and the corresponding access information such as a PIN code), relating to the public key in het SUD in question has, in an appropriate manner, been generated under the control of the certificate manager and will be kept secret and protected in the future.
Comment	-

6.1.2 Private key delivery to subscriber

Refer to Programme of Requirements part 3 Basic Requirements.

6.1.3 Public key delivery to certificate issuer

Refer to Programme of Requirements part 3 Basic Requirements.

6.1.4 CA public key delivery to relying parties

Refer to Programme of Requirements part 3 Basic Requirements.

6.1.5 Key sizes

Refer to Programme of Requirements part 3 Basic Requirements.

6.1.6 Public key parameters generation and quality checking

Refer to Programme of Requirements part 3 Basic Requirements.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Refer to Programme of Requirements part 3 Basic Requirements.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.1 Cryptographic module standards and controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.2 Private key (n out of m) multi-person control

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.3 Private key escrow

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  6.2.3-pkio100 —

Description	The TSP has to describe in the CPS which parties can have access to the private key of the confidentiality certificate held in Escrow and under which conditions.
Comment	-

- Page:
  6.2.3-pkio99 —

Description	The authorized persons who can gain access to the private key of the confidentiality certificate held in Escrow by the TSP (if applicable), have to identify themselves using the valid documents listed in article 1 of the Compulsory Identification Act (Wet op de identificatieplicht), or a valid qualified certificate (limited to a PKIoverheid signature certificate or equivalent).
Comment	-

6.2.4 Private key backup

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.5 Private key archival

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.6 Private key transfer into or from a cryptographic module

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.7 Private key storage on cryptographic module

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.8 Method of activating private key

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.9 Method of deactivating private key

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.10 Method of destroying private key

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.11 Cryptographic Module Rating

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  6.2.11-pkio105 —

Description	Instead of demonstrating compliance with CWA 14169 (for SSCD's or SUD's) or EN 419 211 (for QSCD's), TSPs can issue or recommend SSCDs, SUDs or QSCDs that are certified in line with a different protection profile against the Common Criteria (ISO/IEC 15408) at level EAL4+ or that have a comparable security level. This has to be established by a test laboratory that is accredited for performing Common Criteria evaluations.
Comment	-

- Page:
  6.2.11-pkio125 —

Description	Secure devices issued or recommended by the TSP for storage of keys (SUDs) have to fulfil the requirements laid down in document CWA 14169 "Secure signature-creation devices "EAL 4+""
Comment	-

6.3 Other aspects of key pair management

Refer to Programme of Requirements part 3 Basic Requirements.

6.3.1 Public key archival

Refer to Programme of Requirements part 3 Basic Requirements.

6.3.2 Certificate operational periods and key pair usage periods

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  6.3.2-pkio109 —

Description	Private keys that are used by a certificate holder and issued under the responsibility of this CP must not be used for more than five years. The certificates, which are issued under the responsibility of this CP, must not be valid for more than five years.
Comment	-

6.4 Activation data

Refer to Programme of Requirements part 3 Basic Requirements.

6.4.1 Activation data generation and installation

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  6.4.1-pkio112 —

Description	The TSP attaches activation data to the use of a SUD, SSCD or QSCD, to protect the private keys of the certificate holders.
Comment	The requirements that the activation data (for example the PIN code) have to fulfil can be determined by the TSPs themselves based on, for example, a risk analysis. Requirements that could be considered are the length of the PIN code and use of special characters.

- Page:
  6.4.1-pkio113 —

Description	An unlocking code can only be used if the TSP can guarantee that, at the very least, the security requirements are fulfilled that are laid down in respect of the use of the activation data.
Comment	-

6.4.2 Activation data protection

Refer to Programme of Requirements part 3 Basic Requirements.

6.4.3 Other aspects of activation data

Refer to Programme of Requirements part 3 Basic Requirements.

6.5 Computer security controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.5.1 Specific computer security technical requirements

Refer to Programme of Requirements part 3 Basic Requirements.

6.5.2 Computer security rating

Refer to Programme of Requirements part 3 Basic Requirements.

6.6 Life cycle technical controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.6.1 System development controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.6.2 Security management controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.6.3 Life cycle security controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.7 Network security controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.8 Time-stamping

Refer to Programme of Requirements part 3 Basic Requirements.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Refer to Programme of Requirements part 3 Basic Requirements.

7.1 Certificate profile

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  7.1-pkio150 —

Description	The certificate extension Extended Key Usage MUST be present, MUST NOT be marked “critical”, and MUST contain at least the following KeyPurposIds: For a services authentication certificate: • client Authentication =1.3.6.1.5.5.7.3.2 • document Signing =1.3.6.1.4.1.311.10.3.12 • emailProtection =1.3.6.1.5.5.7.3.4 For a services confidentiality certificate: • Encrypting File System =1.3.6.1.4.1.311.10.3.4 • emailProtection = 1.3.6.1.5.5.7.3.4 For a seal certificate • document Signing =1.3.6.1.4.1.311.10.3.12 • emailProtection = 1.3.6.1.5.5.7.3.4 The KeyPurposeId id-kp-serverAuth MUST NOT be present, the KeyPurposeId id-kp-codeSigning MUST NOT be present, the KeyPurposeId AnyextendedKeyusage MUST NOT be present and any KeyPurposeId solely intended to identify a service based on its FQDN MUST NOT be present. Specifically for G2 certificates any other KeyPurposeId defined in an open or accepted standard corresponding to the key usage as indicated by the KeyUsage extension MAY be present. In the G3 and following generations this extension MAY NOT be present. The above should take into account the EKUs included in the issuing TSP CA. If the issuing TSP CA is not provided with the mandatory EKUs stated above, these MAY NOT be included in the end-user certificate.
Comment	-

- Page:
  7.1-pkio173 —

Description	The serial number of all end-user certificates must meet the following requirements: a. The value of the serial number MUST NOT be 0 (zero); b. The value of the serial number MUST NOT be negative; c. The value of the serial number MUST be unique within the population of end-user certificates issued under an issuing TSP CA; d. The serial number MUST have a minimum length of 96 bits (12 octets); e. The value of the serial number MUST contain at least 64 bits of unpredictable random data; f. Said random data MUST be generated by a Cryptographically Secure Pseudorandom Number Generator (CSPRNG); g. The serial number MUST NOT be longer than 160 bits (20 octets).

Comment	-

7.1.1 Version number(s)

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.2 Certificate extensions

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.3 Algorithm object identifiers

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.4 Name forms

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.5 Name constraints

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.6 Certificate policy object identifier

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.7 Usage of Policy Constraints extension

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.8 Policy qualifiers syntax and semantics

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.9 Processing semantics for the critical Certificate Policies extension

Refer to Programme of Requirements part 3 Basic Requirements.

7.2 CRL profile

Refer to Programme of Requirements part 3 Basic Requirements.

7.2.1 Version number(s)

Refer to Programme of Requirements part 3 Basic Requirements.

7.2.2 CRL and CRL entry extensions

Refer to Programme of Requirements part 3 Basic Requirements.

7.3 OCSP profile

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  7.3-pkio123 —

Description	If the TSP supports the Online Certificate Status Protocol (OCSP), the TSP has to use OCSP certificates and responses in accordance with the requirements laid down in this respect in appendix A of the Basic Requirements, "CRL and OCSP certificate Profiles for certificate status information ".
Comment	-

7.3.1 Version number(s)

Refer to Programme of Requirements part 3 Basic Requirements.

7.3.2 OCSP extensions

Refer to Programme of Requirements part 3 Basic Requirements.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Refer to Programme of Requirements part 3 Basic Requirements.

8.1 Frequency or circumstances of assessment

Refer to Programme of Requirements part 3 Basic Requirements.

8.2 Identity/qualifications of assessor

Refer to Programme of Requirements part 3 Basic Requirements.

8.3 Assessors relationship to assessed entity

Refer to Programme of Requirements part 3 Basic Requirements.

8.4 Topics covered by assessment

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  8.4-pkio195 —

Description	In addition to this PoR, issuing certificates SHALL undergo an audit in accordance with the following schemes: a. ETSI EN 319 411-1 with policy NCP+ (ETSI CP OID 0.4.0.2042.1.2, mandating usage of SSCDs) for authenticity and confidentiality certificates, and b. ETSI EN 319 411-2 with policy QCP-l-qscd (ETSI CP OID 0.4.0.194112.1.3, mandating usage of SSCDs) for non-repudiation certificates (eIDAS eSeals), and c. CA/Browser Forum Network and Certificate System Security Requirements.
Comment	-

- Page:
  8.4-pkio200 —

Description	If the TSP issues or intends to issue qualified certificates under PKIoverheid, the following additional requirements SHALL apply: a. the audit report states that the TSP meets the eIDAS (910/2014) regulation requirements, and b. the issuing certificate with which the TSP wants to issue qualified certificates is on the Trusted Services List (TSL) of Agentschap Telecom (AT).
Comment	-

8.5 Actions taken as a result of deficiency

Refer to Programme of Requirements part 3 Basic Requirements.

8.6 Communication of results

Refer to Programme of Requirements part 3 Basic Requirements.

9. OTHER BUSINESS AND LEGAL MATTERS

Refer to Programme of Requirements part 3 Basic Requirements.

9.1 Fees

Refer to Programme of Requirements part 3 Basic Requirements.

9.1.1 Certificate issuance or renewal fees

Refer to Programme of Requirements part 3 Basic Requirements.

9.1.2 Certificate access fees

Refer to Programme of Requirements part 3 Basic Requirements.

9.1.3 Revocation or status information access fees

Refer to Programme of Requirements part 3 Basic Requirements.

9.1.4 Fees for other services

Refer to Programme of Requirements part 3 Basic Requirements.

9.1.5 Refund policy

Refer to Programme of Requirements part 3 Basic Requirements.

9.2 Financial responsibility

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  9.2-pkio124 —

Description	By means, for example, of insurance or its financial position, the TSP has to be able to cover third party recovery based on the types of liability mentioned in article 6:196b of the Civil Code (that relate to both direct and indirect damage) up to at least EUR 1,000,000 per annum.
Comment	The third party recovery described above is based on a maximum number of certificates to be issued of 100,000 for each TSP, which is in line with the current situation. When TSPs are going to issue more certificates, it will be determined whether a suitable, higher, recoverableness will be required.

9.2.1 Insurance coverage

Refer to Programme of Requirements part 3 Basic Requirements.

9.2.2 Other assets

Refer to Programme of Requirements part 3 Basic Requirements.

9.2.3 Insurance or warranty coverage for end-entities

Refer to Programme of Requirements part 3 Basic Requirements.

9.3 Confidentiality of business information

Refer to Programme of Requirements part 3 Basic Requirements.

9.3.1 Scope of confidential information

Refer to Programme of Requirements part 3 Basic Requirements.

9.3.2 Information not within the scope of confidential information

Refer to Programme of Requirements part 3 Basic Requirements.

9.3.3 Responsibility to protect confidential information

Refer to Programme of Requirements part 3 Basic Requirements.

9.4 Privacy of personal information

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.1 Privacy plan

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.2 Information treated as private

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.3 Information not deemed private

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.4 Responsibility to protect private information

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.5 Notice and consent to use private information

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.6 Disclosure pursuant to judicial or administrative process

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.7 Other information disclosure circumstances

Refer to Programme of Requirements part 3 Basic Requirements.

9.5 Intellectual property rights

Refer to Programme of Requirements part 3 Basic Requirements.

9.6 Representations and warranties

Refer to Programme of Requirements part 3 Basic Requirements.

9.6.1 CA representations and warranties

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  9.6.1-pkio132 —

Description	The TSP excludes all liability for damages if the certificate is not used in accordance with the certificate use described in paragraph 1.4.
Comment	-

9.6.2 RA representations and warranties

Refer to Programme of Requirements part 3 Basic Requirements.

9.6.3 Subscriber representations and warranties

Refer to Programme of Requirements part 3 Basic Requirements.

9.6.4 Relying party representations and warranties

Refer to Programme of Requirements part 3 Basic Requirements.

9.6.5 Representations and warranties of other participants

Refer to Programme of Requirements part 3 Basic Requirements.

9.7 Disclaimers of warranties

Refer to Programme of Requirements part 3 Basic Requirements.

9.8 Limitations of liability

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

- Page:
  9.8-pkio133 —

Description	Within the scope of certificates as mentioned in paragraph 1.4 in this CP the TSP is not allowed to place restrictions on the use of certificates.
Comment	-

9.9 Indemnities

Refer to Programme of Requirements part 3 Basic Requirements.

9.10 Term and termination

Refer to Programme of Requirements part 3 Basic Requirements.

9.10.1 Term

Refer to Programme of Requirements part 3 Basic Requirements.

9.10.2 Termination

Refer to Programme of Requirements part 3 Basic Requirements.

9.10.3 Effect of termination and survival

Refer to Programme of Requirements part 3 Basic Requirements.

9.11 Individual notices and communications with participants

Refer to Programme of Requirements part 3 Basic Requirements.

9.12 Amendments

Refer to Programme of Requirements part 3 Basic Requirements.

9.12.1 Procedure for amendment

Refer to Programme of Requirements part 3 Basic Requirements.

9.12.2 Notification mechanism and period

Refer to Programme of Requirements part 3 Basic Requirements.

9.12.3 Circumstances under which OID must be changed

Refer to Programme of Requirements part 3 Basic Requirements.

9.13 Dispute resolution provisions

Refer to Programme of Requirements part 3 Basic Requirements.

9.14 Governing law

Refer to Programme of Requirements part 3 Basic Requirements.

9.15 Compliance with applicable law

Refer to Programme of Requirements part 3 Basic Requirements.

9.16 Miscellaneous provisions

Refer to Programme of Requirements part 3 Basic Requirements.

9.16.1 Entire agreement

Refer to Programme of Requirements part 3 Basic Requirements.

9.16.2 Assignment

Refer to Programme of Requirements part 3 Basic Requirements.

9.16.3 Severability

Refer to Programme of Requirements part 3 Basic Requirements.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Refer to Programme of Requirements part 3 Basic Requirements.

9.16.5 Force Majeure

Refer to Programme of Requirements part 3 Basic Requirements.

9.17 Other provisions

Refer to Programme of Requirements part 3 Basic Requirements.

If by judicial decision one or more provisions of this CP are declared to be invalid or not applicable, this does not affect the validity and applicability of all other provisions.

Appendix A: Certificate Attributes

Profile of services certificates for the Organization Services domain.

Criteria

When defining the fields and attributes within a certificate, the following codes are used:

- V : Compulsory; indicates that the attribute is compulsory and MUST be used in the certificate.
- O : Optional; indicates that the attribute is optional and MAY be used in the certificate.
- A : Advised against; indicates that the attribute is advised against and SHOULD NOT be used in the certificate.
- N: Is NOT ALLOWED.

It is not allowed to use fields that are not specified in the certificate profiles.

For the extensions, fields/attributes are used that, in accordance with international standards, are critical, are marked in the 'Critical' column with 'yes' to show that the relevant attribute MUST be checked using a process by means of which a certificate is evaluated. Other fields/attributes are shown with 'no'.

Services certificates for authenticity and confidentiality

Basic attributes

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Version	V	MUST be set at 2 (X.509v3).	RFC 5280	Integer	Describes the version of the certificate, the value 2 stands for X.509 version 3.
SerialNumber	V	A serial number that MUST uniquely identify the certificate within the publishing CA domain.	RFC 5280	Integer	All end user certificates have to contain at least 8 bytes of unpredictable random data in the certificate's serial number (SerialNumber).
Signature	V	MUST be created on the algorithm, as stipulated by the PA.	RFC 5280, ETSI TS 102176	OID	MUST be the same as the field signatureAlgorithm. For certificates under the G2 and G3 root certificate, only sha-256WithRSAEncryption is allowed.
Issuer	V	MUST contain a Distinguished Name (DN). The field has the following attributes:	PKIo, RFC3739, ETSI TS 102280		Attributes other than those mentioned below MUST NOT be used.
Issuer.countryName	V	See requirement 7.1-pkio174	ETSI TS101862, X520, ISO 3166	Printable String	
Issuer.OrganizationName	V	See requirement 7.1-pkio174	ETSI TS 102280	UTF8String	
Issuer.organizationalUnitName	O	See requirement 7.1-pkio174	ETSI TS 102280	UTF8String	

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Issuer.serialNumber	O	See requirement 7.1-pkio174	RFC 3739	Printable String	
Issuer.commonName	V	See requirement 7.1-pkio174	PKIo, RFC 3739	UTF8String	The commonName attribute MUST NOT be needed to identify the issuing government body (no part of the Distinguished Name, requirement from RFC 3739)
Issuer.organizationIdentifier	V/N	The organizationIdentifier field contains an identification of the issuing CA. This field MUST be present when the subject.organizationIdentifier field is present in the TSP certificate and MUST NOT be present when this field is not part of the corresponding TSP certificate.	EN 319 412-1	String	The syntax of the identification string is specified in paragraph 5.1.4 van ETSI EN 319 412-1 and contains: • 3 character legal person identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).
Validity	V	MUST define the period of validity of the certificate according to RFC 5280.	RFC 5280	UTCTime	MUST include the start and end date for validity of the certificate in accordance with the applicable policy laid down in the CPS.
Subject	V	The attributes that are used to describe the subject (service) MUST mention the subject in a unique way and include information about the subscriber organization. The field has the following attributes:	PKIo, RFC3739, ETSI TS 102 280		MUST contain a Distinguished Name (DN). Attributes other than those mentioned below MUST NOT be used.
Subject.countryName	V	complete C with two-letter country code in accordance with ISO 3166-1. If an official alpha-2 code is missing, the TSP MAY use the user-assigned code XX.	RFC 3739, X520, ISO 3166, PKIo	PrintableString	The country code that is used in Subject.countryName MUST correspond with the subscriber's address in accordance with the accepted document or registry.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.commonName	V	Name that identifies the service. In services certificates this field is compulsory	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	Incorporated in the subject.commonname is the function of an organizational entity or the name by which the device or system is known.
Subject.organizationName	V	The full name of the subscriber's organization in accordance with the accepted document or Basic Registry.	PKIo	UTF8String	The subscriber organization is the organization with which the TSP has entered into an agreement and on behalf of which the certificate holder (service) communicates or acts.
Subject.organizationIdentifier	V	The value of the `subject:organizationIdentifier` field SHALL contain EITHER: • an identifier conforming to the semantics for legal person identifiers set forth in Section 5.1.4 of ETSI standard EN 319 412-1, or • an OIN/HRN number.	EN 319 412-1	String	TSPs wanting to use a register for legal person identifiers which could qualify as a "national scheme" as described in ETSI standard EN 319 412-1 Section 5.1.4 can apply at Logius for a two-character encoding identifying the relevant source. These encodings will be added to the PKIo CPS. OIN/HRN identifiers adhering to the "national scheme" clause in Section 5.1.4 of ETSI standard EN 319 412-1 are preferred from a standards perspective. This will however mean many governmental systems have to be altered, making this not a likely scenario for the forseeable future.
Subject.organizationalUnitName	A	Usage of the `subject:organizationalUnitName` field is discouraged. When used the value of the `subject:organizationalUnitName` field MUST specify the name of an organizational entity, the validation of which SHALL be described in the CPS of the TSP. This value MUST NOT resemble functional roles or titles.	PKIo		Usage of the `subject:organizationalUnitName` field is discouraged because it is inherently impossible to verify through independent sources with the exception of sub-OINs in the OIN register.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.stateOrProvinceName	A	The use is advised against. If present, this field MUST contain the province in which the subscriber is established in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the province MUST correspond with the address of the subscriber in accordance with the accepted document or registry.
Subject.localityName	A	The use is advised against. If present, this field MUST contain the location of the subscriber in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the location MUST correspond with the address of the subscriber in accordance with the accepted document or registry.
Subject.serialNumber	O	The TSP is responsible for safeguarding the uniqueness of the subject (service). The Subject.serialNumber MUST be used to identify the subject uniquely. The use of 20 positions is only allowed for OIN and HRN after additional arrangements with Logius.	RFC 3739, X 520, PKIo	Printable String	The number is determined by the TSP and/or the government. The number can differ for each domain and can be used for several applications.
subjectPublicKeyInfo	V	Contains, among other things, the public key.	ETSI TS 102 280, RFC 3279		Contains the public key, identifies the algorithm with which the key can be used.

Standard extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityKeyIdentifier	V	No	The algorithm to generate the AuthorityKey MUST be created on an algorithm determined by the PA.	ETSI TS 102 280, RFC 5280	BitString	The value MUST contain the SHA-1 hash from the authorityKey (public key of the TSP/CA).
SubjectKeyIdentifier	V	No	The algorithm to generate the subjectKey MUST be created on an algorithm determined by the PA.	RFC 5280	BitString	The value MUST contain the SHA-1 hash from the subjectKey (public key of the certificate holder).
KeyUsage	V	Yes	The attribute extension specifies the intended purpose of the key incorporated in the certificate. In the PKI for the government, for each certificate type various bits are incorporated in the keyUsage extension. In authenticity certificates the digitalSignature bit MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this. In confidentiality certificates, keyEncipherment and dataEncipherment bits MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this. In seal certificates the nonRepudiation bit MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this.	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
CertificatePolicies	V	No	MUST contain the OID of the Certificate Policy (CP) and the URI of the Certification Practice Statement (CPS), and MAY contain a user notice. The TSP SHOULD use UTF8String in the `userNotice` field, but MAY use IA5String. ALL certificates issued with their private key residing on an SSCD (qualified or not) SHOULD contain the ETSI NCP+ OID [0.4.0.2042.1.2]; those issued with their private key NOT residing on an SSCD (qualified or not) SHOULD contain the ETSI NCP OID [0.4.0.2042.1.1]. Certificates issued as EU qualified certificates to natural persons with their private key residing in a QSCD, SHOULD contain an additional ETSI QCP-l-qscd OID [0.4.0.194112.1.3], or an additional ETSI QCP-l OID of [0.4.0.194112.1.1] when their private key does not reside on a QSCD.	RFC 3739	OID, String, UTF8String or IA5String	An overview of all Certificate Policy OIDs can be found in the document "PKIoverheid registered OIDs". For the Organization Services domain the OIDs are: • Authenticity: 2.16.528.1.1003.1.2.5.4 • Non-repudiation (eSeal): 2.16.528.1.1003.1.2.5.7 • Confidentiality: 2.16.528.1.1003.1.2.5.5 Reference to the paragraph numbers of the PoR in the user notice is advised against because the persistency of this cannot be guaranteed (unlike the OID number of the CP).
SubjectAltName	O	No	MAY be used and given a worldwide unique number that identifies the service.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
SubjectAltName.otherName	O		MAY contain an `extensions:subjectAltName` extension with one or more `otherName` attributes in its `extValue` field. An `otherName` attribute is an object consisting out of a sequence of a `type-id` field and a `value` field. Each `otherName` attribute SHALL contain a `value` to uniquely identify the subject for which the other permitted subject attributes do not qualify. The `type-id` field of an `otherName` attribute SHALL contain one of the following OIDs: • *Microsoft User Principal Name* (MSUPN) [1.3.6.1.4.1.311.20.2.3], or • *IA5String* [1.3.6.1.4.1.1466.115.121.1.26] but MAY also be [2.5.5.5], or • *Permanent Identifier* [1.3.6.1.5.5.7.8.3] (described in RFC 4043), or • *PKIo-arc OID* which can be specifically assigned by the PKIo PA for this purpose (should be described in the PKIo-arc OID document). The `value` field related to `otherName` attribute type *Microsoft User Principal Name* (MSUPN): 1. SHALL be encoded in UTF8, and	PKIo	See description.	Normally, `otherName` attribute type *Microsoft User Principal Name* (MSUPN) is used for *Single Sign-On* (SSO) purposes.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			2. SHALL use syntax '<Subscriber number>@<TSP OID>'. The value field related to otherName attribute *IA5String*: 1. SHALL be encoded in ISO 646 (IA5), and 2. SHALL use syntax '<TSP OID>-<Subscriber number>'. The value field related to otherName attribute *Permanent Identifier* contains a PermanentIdentifier object, consisting out of a sequence of an identifierValue and an assigner field. The PermanentIdentifier:identifierValue field: 1. SHALL be encoded in UTF8, and 2. SHALL use syntax '<Subscriber number>'. The PermanentIdentifier:assigner field SHALL contain OID '<TSP OID>'. The value field related to otherName attribute *PKIo-arc OID* is described in the PKIo-arc OID document. The <TSP OID> consists out of an OID arc number which: • has been assigned to the TSP by the PKIo PA specifically for this usage, expanded by a number chosen by the TSP to specify its identification mechanism, and • is documented in the TSP CPS, and			

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			• is persistent. The `<Subscriber number>` consists out of a number which: • uniquely and permanently identifies the subject within the namespace of the corresponding OID, and • numbering and/or validation mechanism is described in the TSP CPS.			
SubjectAltName.rfc822Name	A		MAY be used for the service's e-mail address, for applications that need the e-mail address in order to be able to function properly.	RFC 5280	IA5String	For PKIoverheid certificates, the use of e-mail addresses is advised against, because e-mail addresses of certificate holders often change and are susceptible to spam.
BasicConstraints	O	Yes	This field SHALL have its `cA` sub-field set to its DEFAULT value (FALSE) resulting in an encoded certificate NOT including the `cA` sub-field. The optional `pathLenConstraint` sub-field SHALL NOT be included.	RFC 5280		ITU-T Recommendation X.690 (07/2002) on ASN.1 encoding rules states in Section 5.8: "The encoding of a set value or sequence value shall not include an encoding for any component value which is equal to its default value". Stating in the description that "encoded certificates do NOT include the `cA` sub-field" therefore is redundant. However, in the past some TSPs employed CA-issuing software which did not do proper ASN.1 encoding resulting in a wrongfully included `cA` sub-field in encoded certificates. This encoding error resulted in some PKIX software rejecting these certificates. This redundant information therefore has to be regarded as a cautionary hint for TSPs to check their actual certificate encoding for these errors. Chances of this encoding bug still existing in ASN.1 encoding software are however slim since the last mention of such a bug on BugZilla is from 2016.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
CRLDistributionPoints	V	No	MUST include the URI of a CRL distribution point.	RFC 5280, ETSI TS 102 280		The reference MUST be accessible through the http or LDAP protocol. The attribute Reason MUST NOT be used, reference MUST be made to 1 CRL for all types of reasons for revocation. In addition to CRL, other types of certificate status information service MAY be supported.
ExtKeyUsage	V	No		RFC 5280	KeyPurposeId's	See requirement 7.1-pkio150

Private extension

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityInfoAccess	O	No	This attribute MUST include the URI of an OCSP responder if Online Certificate Status Protocol (OCSP) plays a role.			This field can optionally be used to reference other additional information about the TSP.
QcStatement	V/N	No	Certificates for the electronic seals MUST indicate that they are issued as qualified certificates complying with annex III of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qcs-QcCompliance* statement in this extension. Certificates for the electronic seals MUST indicate that they are issued as type of certificate complying with annex I of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qct-eseal* statement in this extension. Certificates for the electronic seals MUST indicate that the private key that is part of the public key in the certificate is saved on a qualified signature creation device (QSCD) complying with annex II of EU regulation 920/2014. This compliance is indicated by including the id-etsi-qcs-QcSSCD statement in this extension.	RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	The aforementioned QcStatement identifiers relate to the following OIDs: • id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 • id-etsi-qct-eseal { id-etsi-qcs-QcType 2 } 0.4.0.1862.1.6.2 • id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4 • id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			Certificates for the electronic signature MUST contain a reference to the location of the PKI Disclosure Statement (PDS). This URL must present in the id-etsi-qcs-QcPDS statement in this extension.			
QcStatement-2	V	No	This extension munst contain an id-etsi-qcs-SemanticsId-Legal statement. This semantics identifier indicates that the organizationalIdentifier in the subject adheres to the prescribed layout.	ETSI EN 319 412-1	OID	Said QcStatement identifiers are the following OIDs: • id-etsi-qcs-SemanticsId-Legal { id-etsi-qcs-semantics-identifiers 2 } 0.4.0.194121.1.2