Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3j: Certificate Policy for Server certificates in Server 2020 (EV G1) Domain

Version	4.10
Date	March 1, 2022

[OID 2.16.528.1.1003.1.2.5.9] Server 2020

Publishers imprint

Version number	4.10
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

1.1 Overview

Refer to Programme of Requirements part 3 Basic Requirements.

1.2 Document name and identification

1.2.1 Revisions

1.2.1.1 Version 4.8

New

- Requirement 6.3.2-pkio178 (effective date November 1, 2019);
- Requirement 4.2-pkio179 (effective date November 1, 2019);
- Requirement 9.17-pkio180 (effective date August 29, 2019);
- Requirement 7.1-pkio182 (effective date immediately after publication of the PoR 4.8);
- Requirement 8.1-pkio183 (effective date immediately after publication of the PoR 4.8);
- Requirement 3.2.2-pkio186 (effective date immediately after publication of the PoR 4.8).

Modifications

- Removal of requirement 2.2-pkio155 (effective date immediately after publication of the PoR 4.8);
- Removal of requirement 6.1.1-pkio91 (effective date immediately after publication of the PoR 4.8);
- Modified serial number requirements in requirement 7.1-pkio173 (effective date August 29, 2019);
- Removal of subjectAltName.dNSName footnote (effective date immediately after publication of the PoR 4.8);
- Removal of Subject.postaladdress from profile (effective date immediately after publication of the PoR 4.8);
- Removal of requirement 9.17-pkio140 (effective date immediately after publication of the PoR 4.8);
- Hidden requirement in certificate profile on incorporation of certificate policies in end-user certificates moved to new requirement 7.1-pkio 182 (effective date immediately after publication of the PoR 4.8);

Editorial

None.

1.2.1.2 Version 4.8 to 4.9

New

- Requirement 2.2-pkio191, the CPS of the TSP MUST follow the layout according to RFC 3647 (effective date after 01-04-2020);
- Requirement 4.9.1-pkio193, describes when certificates will be revoked (effective date 02-17-2020);
- Requirement 8.1-pkio189, if the TSP issues or intends to issue qualified certificates under PKIoverheid, the following additional requirements apply in addition to those set out in requirement 8.1-pkio187 (effective date 02-17-2020).

Modifications

None.

Editorial

- The profile Server certificates in this part, at basic attributes in the appendix the attribute Subject.stateOrProvinceName will become optional (effective date 09-01-2020);

- Requirement 7.1-pkio171, A TSP MUST limit itself to the signature algorithms as defined in chapter 5.1 (and subsections) of the Mozilla Root Store Policy. The use of RSA-PSS is permitted, but is not recommended (effective date 01-03-2020).

1.2.1.3 Version 4.9 to 4.10

New

- Added basic requirement 8.2-pkio199.
- Requirement 9.6.1-pkio127 was added as a basic requirement.
- Added new additional requirement 8.4-pkio197.

Modifications

- Removal of user notice from requirement 7.1-pkio182.
- Adjusted the maximum number of days for wich data for validation of FQDNs may be reused in requirement 3.2.5-pkio170.
- Adjusted the minimal number of SCTs in public TLS certificates from 2 to 3 in requirement 4.4.3-pkio154.
- Change the criterium for the `subject:stateOrProvinceName` attribute from V to O in certificate profile of PoR Part 3j.
- Remove specific mandatory verification methods from requirement 3.2.5-pkio146.

Removals

- Remove the `extensions:subjectAltName.iPAddress` attribute from the certificate profile.
- Remove the `subject:organizationalUnitName` 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-pkio128.

Editorial

- Expanded the description of the `extensions:basicConstraints` field in the certificate profile.

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

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 PKIoverheid Server CA 2020 (resigned)	29 Jul 2020	05 Dec 2022	13a8cbc9b35ce15b3a98ec0fbf87b3380e06b6af	37610BF756CA4C3CFA18696C4C149738E644CA9F676387EC50167365D6A45CCA
KPN PKIoverheid Server C… 2020 (resigned)	29 Jul 2020	06 Dec 2022	7498a8335021985add2945b2d159d929733bdadd	592E1A2F0A34284B0E26FCB4FED22AF859848EEE8822ADB61B42DAB47A2FFDC2
QuoVadis PKIoverheid Server CA 2020 (resigned)	29 Jul 2020	05 Dec 2022	28526a1da96593d34558b664a321caa838c15777	EB2C2A806C69FC963C4E24A5BBEA20ED4E3B86AE798730BB4EEA51BF9DE33325

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 2.16.528.1.1003.1.2.5.9]

Server certificates that are issued under this CP can be used to secure a connection between a specific client and a server that is part of the organizational entity listed as the subscriber in the relevant certificate. Certificates issued with this OID are in accordance with the then current version of the Baseline Requirements. In the case of discrepancies between this PoR and the Baseline Requirements, the latter takes precedence over this document.

[OID 2.16.528.1.1003.1.2.5.8]

Under this OID OCSP responder certificates may be issued for use within the domain Server 2020. 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.

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

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:

2.2-pkio166 —

Description	The TSP MUST describe in its CPS which validation methods for validating IP addresses and / or FQDNs it uses for inclusion in the Subject.CommonName field, the SubjectAltName.dNSName field and / or the SubjectAltName.iPAdress field with it a reference to the correct chapter number of the Baseline Requirements.
Comment	-

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	-

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

3.1 Naming

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

3.2.1 Method to prove possession of private key

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

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:

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	-

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	-

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:

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	-

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.

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.

Additional requirements:

3.2.5-pkio146 —

Description	The TSP SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified.
Comment	A High Risk Certificate Request is a Request that the TSP flags for additional scrutiny by reference to internal criteria and databases maintained by the TSP, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the TSP identifies using its own risk-mitigation criteria.

3.2.5-pkio170 —

Description	The TSP MUST check whether the FQDNs supplied by the subscriber (see definition in Part 4) or IP addresses, included in a certificate, are: • Actually in the name of the subscriber OR; • Authorized by the registered domain owner OR; • That the subscriber can show that he exercises (technical) control over the FQDN in question. This must be done for every FQDN that is included in a certificate. The TSP must limit itself to the methods as prescribed in the applicable version of the Baseline Requirements of the CABForum (chapter 3.2.2.4 for FQDNs and 3.2.2.5 for IP addresses). The foregoing also holds that "Any Other Method" from 3.2.2.5 may not be used (for both 3.2.2.4.8 and for IP addresses). The verified data may be reused in a subsequent application, provided that it is no older than 398 days. If the data is older than 398 days, the above check must be carried out again. The TSP must also keep a record of the validation method (s) used for the included FQDNs per certificate. This verification may not be outsourced by the TSP to external (sub) contractors.
Comment	-

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.

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

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

4.1 Certificate Application

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.

Additional requirements:

4.2-pkio179 —

Description	A CA must be able to replace its total population of outstanding, still valid certificates within 5 days, provided the subscriber cooperates in a timely manner.
Comment	With "cooperation by the subscriber", the PA means the provision of any and all data required by the TSP to process and deliver a certificate (request) such as domain validation and Certificate Signing Request (CSR). To ensure that a subscriber is able to provide such data in a timely manner, the TSP may, for example, take the following measures: • Setting up a customer portal that facilitates and speeds up the process; • Periodically checking (domain) validation so that data is "fresh" at the time it is needed; • (Partially) automating the certificate issuing process via an API (e.g. RFC8555).

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

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

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.

Additional requirements:

4.4.3-pkio154 —

Description	The certificate SHALL contain at least 3 SCTs from separate Certificate Transparency logs. The SCTs come from a log that is either qualified or awaiting qualification at the time of certificate issue. A qualified log is defined as a CT log that complies with Chromium's Certificate Transparency Log Policy and has been included by Chromium. SCTs have to come from at least 2 different CT log operators, AND at least one of which SHALL be Google.
Comment	-

4.5 Key pair and certificate usage

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

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

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

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

4.9.1 Circumstances for revocation

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

4.9.1-pkio193 —

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, or there is an 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 meet his obligations as set out in this CP or the corresponding CPS of the TSP or the agreement that the TSP has concluded 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 concluded 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[2]. The TSP must adhere to the revocation deadlines as stated in chapter 6.1 of the previous document.
Comment	-

4.9.2 Who can request revocation

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.3 Procedure for revocation request

Refer to Programme of Requirements part 3 Basic Requirements.

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.

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

4.9.7 CRL issuance frequency (if applicable)

Refer to Programme of Requirements part 3 Basic Requirements.

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:

4.9.9-pkio152 —

Description	If the TSP supports OCSP, the OCSP response must have a minimum validity of 8 hours and a maximum validity of 7 calendar days. The next update must be available no later than half of the validity of an OCSP response.
Comment	-

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	-

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

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

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

5.1 Physical controls

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

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

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

5.4.1 Types of events recorded

Refer to Programme of Requirements part 3 Basic Requirements.

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

5.5.1 Types of records archived

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

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

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.

5.8 CA or RA termination

Refer to Programme of Requirements part 3 Basic Requirements.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

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.

6.1.1-pkio90 —

Description	The generation of key pairs the certificate holder's key by the TSP is not allowed
Comment	-

6.1.1-pkio92 —

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

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.

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:

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	-

6.2.11-pkio107 —

Description	Instead of using a hardware-based SUD, the keys of a services certificate can be protected by software if compensating measures are taken in the system's environment that contains the keys. The compensating measures must be of such a quality that it is practically impossible to steal or copy the key unnoticed. When registering, the manager of the services certificates that uses this option for software-based storage has, at the very least, to submit a written declaration to state that compensating measures have been taken that fulfil the condition stipulated to this end. The agreement between the subscriber and TSP must state that the TSP is entitled to check the measures that have been taken.
Comment	Examples of compensating measures to be considered are a combination of physical access security, logical access security, logging and audit and segregation of functions.

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

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:

6.3.2-pkio178 —

Description	Private keys used by a certificate holder and issued under the responsibility of this CP MAY NOT be used for more than two (2) years. Certificates issued under the responsibility of this CP MAY NOT be valid for more than 397 days. In the event that a certificate is replaced following revocation under section 4.9.1.1 of the Baseline Requirements, the private key of a certificate MAY NOT be reused, except in the case of revocation under point 7 (certificate not issued in accordance with BR or CP/CPS of TSP).
Comment	-

6.4 Activation data

6.4.1 Activation data generation and installation

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

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.

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

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

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

6.7.1 Network security controls (duplicate)

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

7.1 Certificate profile

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

7.1-pkio163 —

Description	The Subject.CommonName field (if included) MUST contain a FQDN (Fully Qualified Domain Name). An FQDN MUST also appear in the SubjectAltName.DNsName field. An IP address MUST also appear in the SubjectAltName.iPAdress field. A server certificate MAY contain multiple FQDNs from different domains on condition that these domains are registered in the name of the same subscriber or is authorization by the same subscriber. This means that a TSP cannot combine FQDNs in one certificate that are both from different domains and are registered in the name of different owners. The following is NOT allowed to be included in the Subject.Commonname field, SubjectAltName.iPAdress or the SubjectAltName.DNname field • wildcard FQDNs • local domain names, • private IP addresses • internationalized domain names (IDNs) • null characters \ 0 • generic TopLevel Domain (gTLD) • Country code TopLevelDomein (ccTLD)
Comment	-

7.1-pkio171 —

Description	From ETSI TS 119 312, the TSP MUST choose from 1 of the following options for the Signature field in a certificate: • sha256WithRSAEncryption: 1.2.840.113549.1.1.11 (OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }) • ecdsa-with-SHA256: 1.2.840.10045.4.3.2 {OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }}) • sha384WithRSAEncryption : 1.2.840.113549.1.1.12 {OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 } • ecdsa-with-SHA384:1.2.840.10045.4.3.3 {OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
Comment	A TSP MUST limit itself to the signature algorithms as defined in chapter 5.1 (and subsections) of the Mozilla Root Store Policy. The use of RSA-PSS is permitted, but is not recommended.

7.1-pkio172 —

Description	The Authority Information Access field must contain the following entries: Access Method = - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1). This field must contain the URI where the OCSP responder can be found that is authorized by the issuing CA of the certificate to be checked; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2). This field must contain the URI where the certificate of the issuing CA can be found.
Comment	-

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-pkio182 —

Description	The `extensions:certificatePolicies` extension MUST contain the following fields and values: • `policyIdentifier` field with value "`2.16.528.1.1003.1.2.5.9`"; • `policyQualifiers:policyQualifierId` field with value "`id-qt 1`" [RFC5280]; • `policyQualifiers:qualifier:cPSuri` field with value the HTTP URL for the TSP's Certification Practice Statement.
Comment	Usage of the `extensions:certificatePolicies:policyQualifiers:qualifier:userNotice` field is prohibited by the CA/Browser Forum. This requirement was also in use in the now defunct PoR part 3e. The `policyIdentifier` field in part 3e had a different value: `2.16.528.1.1003.1.2.5.6`.

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

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

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

8.1 Frequency or circumstances of assessment

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

8.1-pkio183 —

Description	A TSP MUST, when requested by the PA, perform a self-assessment against the Baseline Requirements based on a template predetermined by the PA.
Comment	Mozilla requires CAs to make a comparison of their processes (via CP and CPS documents) with the BRs using a template defined by Mozilla to ensure that their processes (and practices) continue to comply with CA's Baseline Requirements / Browser Forum.

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:

8.4-pkio197 —

Description	In addition to this PoR, issuing certificates SHALL undergo an audit in accordance with the following schemes: a. ETSI EN 319 411-1 (latest published version applies) with policies NCP (ETSI CP OID 0.4.0.2042.1.1) and OVCP (ETSI CP OID 0.4.0.2042.1.7), and b. CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (latest published version applies), and c. CA/Browser Forum Network and Certificate System Security Requirements.
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.

Additional requirements:

8.6-pkio158 —

Description	The PA informs TSPs about relevant changes to the Baseline Requirements and / or the Extended Validation Guidelines. TSPs must prove that they comply with stated changes by submitting a signed statement from or on behalf of the authorized director to the PA before the effective date of the change in question. The PA provides a template for this. If a TSP cannot comply on time or does not submit a signed declaration on time, the PA reserves the right to (temporarily) suspend certificate issuance at the relevant TSP until the TSP can (demonstrably) comply with the stated change.
Comment	-

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

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:

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

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

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

9.6.1 CA representations and warranties

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

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:

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

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

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

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.

Additional requirements:

9.17-pkio180 —

Description	CAs MUST actively inform their subscribers at least once every six months that, according to the terms and conditions, certificates are revoked under the conditions of - and within the time limits of - the BRG requirements specified in 4.9.1.1.
Comment	-

Appendix A Certificate

Profile of server certificates for the Organization and Organization Services domains

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.

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'.

Server certificates 1.1

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 certificates serial number (SerialNumber).
Signature	V	See requirement 7.1-pkio171	RFC 5280, ETSI TS 119 312	OID	
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	
Issuer.serialNumber	O	See requirement 7.1-pkio174	RFC 3739	Printable String	

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
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; • 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 subscribers address in accordance with the accepted document or registry.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.commonName	A	Name that identifies the server.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	See requirement 7.1-pkio163 for requirements for the contents of this field. See requirement 3.2.5-pkio170 for validation requirements.
Subject.organizationName	V	The full name of the subscribers 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 (server) communicates or acts.
Subject.stateOrProvinceName	O	MUST include the province of the subscribers branch, in accordance with the 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	V	MUST include the location of the subscriber, in accordance with the 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
SignedCertificate-TimestampList (OID 1.3.6.1.4.1.11129.2.4.2)	V	No	The Signed Certificate Timestamp List contains one or more Signed Certificate Timestamps.	RFC 6962	OCTET STRING	See requirement 4.4.3-pkio154 for the usage of the SignedCertificateTimestampList.
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 server certificates the digitalSignature and keyEncipherment bits 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	
CertificatePolicies	V	No	See requirement 7.1-pkio182 for requirements on the contents of this field.	RFC 3739	OID, String, UTF8String or IA5String	

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
SubjectAltName	V	No	MUST be used and given a worldwide unique number that identifies the server.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MUST include a unique identifier in the dnsName attribute for server certificates. Attributes other than those mentioned below MUST NOT be used.
SubjectAltName.dNSName	V		Name that identifies the server.	RFC2818, RFC5280	IA5String	See requirement 7.1-pkio163 for requirements for the content of this field. See requirement 3.2.5-pkio170 for validation requirements.
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	Extension that indicates for which applications the certificate may be used.	RFC 5280	KeyPurposeIds	In server certificates this extension MUST be included, this extension MUST NOT be labelled “critical” and this extension MUST include the KeyPurposIds id-kp-serverAuth and id-kp-clientAuth.

Private extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityInfoAccess	V	No	See requirement 7.1-pkio172			