Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3h: Certificate Policy for Server certificates in Private Services (G1) Domain

Version	4.9
Date	July 1, 2021

[OID 2.16.528.1.1003.1.2.8.6] Server

Publishers imprint

Version number	4.9
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 4.0 to 4.1

New

None.

Modifications

None.

Editorial

- Small editorial modificatoin to the following requirements:
    - Requirement 5.7.4-pkio86.

1.2.1.2 Version 4.1 to 4.2

New

None.

Modifications

- Change in subjectAltName in certificate profile (effective date direct after publication PoR).

Editorial

None.

1.2.1.3 Version 4.2 to 4.3

New

- 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);
- Removal of requirement pkio95 due to duplicate with ETSI EN 319 411-1 (effective date immediately after publication of PoR 4.3);
- 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).

Editorial

None.

1.2.1.4 Version 4.3 to 4.4

New

None.

Modifications

- 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);
- Removed requirement 5.3.2-pkio79 (effective date 1-2-2017).

Editorial

- Modified the field "ExtKeyUsage from critical to non-critical, solving conflict between the description and the field value (effective date immediately after publication of PoR 4.4);
- Replaced CSP (Certificate Service Provider) with TSP (Trust Service Provider) in accordance with eIDAS directive.

1.2.1.5 Version 4.4 to 4.5

New

- Possibility to offer CPS in English and/or Dutch (requirement 2.2-pkio157, 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);
- Change in OID 2.16.528.1.1003.1.2.8.6 to also cover OCSP responder certificates (effective date 1-7-2017);
- Mandatory use of field "NextUpdate" in OCSP responses in requirement 4.9.9-pkio71 (effective date 1-7-2017).

Editorial

None.

1.2.1.6 Version 4.5 to 4.6

New

None.

Modifications

- Corrected subjectAltName.othername field (effective date directly after publication of PoR 4.6).

Editorial

None.

1.2.1.7 Version 4.6 to 4.7

New

- Requirement 7.1-pkio177 (effective date immediately after publication of PoR 4.7);
- Requirement 7.1-pkio165 (effective date immediately after publication of the PoR 4.7);
- Requirement 2.2-pkio168 (effective date immediately after publication of PoR 4.7);
- Requirement 3.2.5-pkio162 (effective date immediately 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 issuance of QSCDs for requirements 6.2.11-pkio105, 6.4.1-pkio112 and 4.9.1-pkio52 (effective date immediately after publication of PoR 4.7).

Editorial

None.

1.2.1.8 Version 4.7 to 4.8

New

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

Modifications

- Change in serial number requirements in requirement 7.1-pkio177 (effective date August 29, 2019);Removal of Subject.postaladdress attribute (effective date immediately after publication of PoR 4.8).

Editorial

- Replacement of ETSI TS 102 176 by ETSI TS 119 312 in requirement 6.1.1-pkio91 (effective date immediately after publication of PoR 4.8);
- Changed definition of private key in requirement 4.9.1-pkio52 (effective date immediately after publication of PoR 4.8);
- Reference in equirement 3.2.5-pkio162 (effective date immediately after publication of PoR 4.8).

1.2.1.9 Version 4.8 to 4.9

New

None.

Modifications

- Requirement 2.2-pkio8 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 2.2-pkio157 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 6.1.1-pkio87 has been removed (effective date immediately after publication PoR 4.9).

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).

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
UZI-register Private Serv… CA G1	09 Mar 2017	12 Nov 2028	5613314895991348523	BDD860EF8E87E2B2C7EBB34DD6E9E1771A3A3C5DEC850BA7080E3E2904DBD897
ZOVAR Private Server CA G1	09 Mar 2017	12 Nov 2028	3936653012735493143	FE54263BC96C2DFBAC5BE5F449CFF7F5B12B6255A7BBCF761BA979E5986E1598

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 2.16.528.1.1003.1.2.8.6]

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.

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

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 mailto:servicecentrum@logius.nl

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.

1.6 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

2.2-pkio168 —

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 theSubjectAltName.iPAdress field with a reference to the relevant chapter of the Baseline Requirements OR a reference to the number provided by the PA in the event of custom validation methods as described in requirement 3.2.5-pkio162.
Comment	-

2.2-pkio3 —

Description	The CPS shall be made available in English. In addition the TSP may issue a CPS in Dutch. There may be no substantial substantive difference between the two versions.
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

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

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

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

3.2.5-pkio146 —

Description	A TSP must verify if the subscriber is the owner of the FQDN that is incorporated in the server or EV certificate. The Baseline Requirements stipulate under 4.2.1 that additional verification activity must be undertaken for High Risk Requests. PKIoverheid understands that to mean at least the following: • A domain name of a Fortune Global 500 company • A domain name with a second level domain equal to a second level domain of the top 500 domain names worldwide and specific to the Netherlands • A domain name that appears on a known spam- and/or phishing blacklist Once it is established that the holder is an organization belonging to the global 500 or if the second level domain name is equal to the top 500 domain names, the TSP may only issue a certificate after the expressed permission of an accountable manager of the TSP who is not part of the standard approval process. If the domain name appears on a phishing blacklist a certificate may not be issued.
Comment	Largest organizations: http://fortune.com/global500/ Most used domain names: http://www.alexa.com/topsites Phishing: http://www.phishtank.com. Examples of high risk requests as described above are twitter.nl[2], account.twitter.com[3]. In case of the use of a domain authorization letter extra attention must be paid to the verification and authenticity of the domain authorization letter.

2 http://twitter.nl
3 http://account.twitter.com

3.2.5-pkio162 —

Description	If an FQDN is included in the certificate, the TSP MUST check whether the FQDNs supplied by the subscriber (see definition in Part 4), 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 it exercises (technical) control over the FQDN in question. The verified data may be reused in a subsequent application, provided that it is not older than 39 months. If the data is older than 39 months, the above check must be carried out again 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) OR; • an alternative method approved in advance by the PA. 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-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

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.

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

4.9.1-pkio52 —

Description	Certificates must be revoked when: • the subscriber states that the original request for a certificate was not allowed and the subscriber does not provide consent with retrospective force; • the TSP has sufficient proof that the subscriber's private key (that corresponds with the public key in the certificate) is compromised or if compromise is suspected, or if there is inherent security vulnerability, or if the certificate has been misused in any other way. A key is considered to be compromised in the event of unauthorized access or suspected unauthorized access to the private key, if the private key, SSCD, SUD or QSCD, is lost or suspected to be lost, if the key, SSCD, SUD or QSCD, is stolen or suspected to be stolen, or if the key or SSCD, SUD or QSCD is destroyed; • a subscriber does not fulfil its obligations outlined in this CP or the corresponding CPS of the TSP or the agreement that the TSP has entered into with the subscriber; • the TSP is informed or otherwise becomes aware of a substantial change in the information that is provided in the certificate. An example of that is: a change in the name of the certificate holder; • the TSP determines that the certificate has not been issued in line with this CP or the corresponding CPS of the TSP or the agreement that the TSP has entered into with the subscriber; • the TSP determines that information in the certificate is incorrect or misleading; • the TSP ceases its work and the CRL and OCSP services are not taken over by a different TSP. • the PA of PKIoverheid determines that the technical content of the certificate entails an irresponsible risk to subscribers, relying parties and third parties (e.g. browser parties).
Comment	In addition, certificates can be revoked as a measure to prevent or to combat an emergency. Considered to be an emergency is definitely the compromise or suspected compromise of the private key of the TSP used to sign certificates.

4.9.2 Who can request revocation

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.3 Procedure for revocation request

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)

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

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.

4.9.9-pkio67 —

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

4.9.9-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

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

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

5.5.1 Types of records archived

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

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

6.1 Key pair generation and installation

6.1.1 Key pair generation

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-pkio91 —

Description	If the TSP generates the private key for the subscriber, this MUST be supplied encrypted to the subscriber to safeguard the integrity and confidentiality of the private key. The following measures must then be taken into account: • The TSP MUST generate the private key for the subscriber in the secured environment to which the PKIoverheid PoR and the corresponding audit apply; • Once the private key has been generated for the subscriber, it MUST be stored encrypted using a strong algorithm (in accordance with the requirements of ETSI TS 119 312) within the TSP's secured environment; • When storing this key, the TSP MUST apply the P12 standard, where the privacy mode and the integrity mode are used. To this end, the TSP MAY encrypt the P12 file with a personal PKI certificate of the subscriber/certificate manager. If this is not available, the TSP MUST use a password supplied by the subscriber. This password MUST be supplied by the subscriber through the TSP's website, for which an SSL/TLS connection is used, or via a similar procedure which guarantees the same trustworthiness and security; • If a password is used to encrypt the P12, this password has to contain at least 8 positions including at least one number and two special characters; • The TSP MAY NEVER send the password that is used to encrypt/ decrypt the P12 in cleartext over a network or store it on a server. The password MUST be encrypted using a strong algorithm (in accordance with the requirements of ETSI TS 119 312); • The P12 file MUST be sent to the subscriber over an SSL/TLS secured network, or be supplied out-of-band on a data carrier (e.g. USB stick or CD-Rom). • If the P12 is supplied out-of-band, this must be additionally encrypted with a key other than the P12 file. In addition, the P12 MUST be delivered to the subscriber using a certified courier, or by a representative of the TSP in a seal bag. The courier must be certified in accordance with the requirements dictated in part 2 under paragraph 2.2 for the specific service applicable here. • If the P12 file is sent over a SSL/TLS secured network the TSP MUST ensure that the P12 file is successfully downloaded no more than once. Access to the P12 file when transferring via SSL/TLS has to be blocked after three attempts.
Comment	Best practice is that the subscriber himself generates the private key that belongs to the public key. When the TSP generates the private key belonging to the public key on behalf of the subscriber, this has to fulfil the aforementioned requirements. When generating the key, it is important to realize that not only is the P12 file encrypted, but that the access to the P12 file is secured when the transfer is made.

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

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.

6.4 Activation data

6.4.1 Activation data generation and installation

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

7.1-pkio165 —

Description	The Subject.CommonName SHOULD contain an FQDN (Fully Qualified Domain Name) or an IP address. 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 are authorized 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. If it is not possible or desirable to include an FQDN in the subject.commonName field, but the field is necessary for the server to function properly, it is allowed to use the function of an organizational entity or the name with which the service, device or system is indicated. The following is not permitted to be included in the Subject.Commonname field, SubjectAltName.iPadres 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-pkio177 —

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 SHOULD 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

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-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

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.

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

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

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

9.6.1-pkio128 —

Description	In the agreement between the TSP and the subscriber, a clause (a clause as specified in article 6:253 of the Civil Code) will be included in which the TSP champions the interests of a third party relying on the certificate. This clause addresses a liability of the TSP in accordance with article 6:196b, first up to and including third paragraph, of the Civil Code, with the proviso that: a. for "a qualified certificate specified in article 1.1, division ss Telecommunications Act": "a server certificate" is read; b. for "signatory": "certificate holder" is read; c. for "creation of electronic signatures": "verification of authenticity features and creating encrypted data" is read; d. For "verification of electronic signatures": "deciphering authentication features and encrypted data" is read.
Comment	-

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

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.

Appendix A: Certificate Profile

Profile of server certificates for the Private 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'.

Server certificates – Private Services Domain

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	This certificate MUST contain at least a 2048 bit RSA key.
Issuer	V	MUST contain a Distinguished Name (DN). The field contains 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; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); • 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.
Subject.commonName	A	Name that identifies the server.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	See requirement 7.1-pkio165 for requirements for the content of this field See requirement 3.2.5-pkio162 for validation

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
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 / server) communicates or acts.
Subject.organizationalUnitName	O	Optional specification of an organizational entity. This attribute MUST NOT include a function indication or similar.	PKIo		This attribute MAY appear several times. The field MUST contain a valid name of an organizational entity of the subscriber in accordance with an accepted document or registry.
Subject.stateOrProvinceName	O	The use of this attribute is advised against. If present it MUST include the province of the subscriber's 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	A	The use of this attribute is advised against. If present it 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
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, keyEncipherment and keyAgreement 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	MUST contain the OID of the certificate policy (CP), the URI of the certification practice statement (CPS), and a user notice. The applicable PKI for the government OID scheme is described in the CP. The TSP SHOULD use UTF8String in the userNotice, but MAY use IA5String.	RFC 3739	OID, String, UTF8String or IA5String	Reference to the paragraph numbers of the PoR/CP in the user notice is advised against because the persistency of this cannot be guaranteed (unlike the OID number of the CP).

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
SubjectAltName	V	No	MUST be used and given a worldwide unique identifier that identifies the server.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		It is preferred to use FQDNs as a unique identifier. When using FQDNs these are incorporated in the dnsName field. If it is not possible or preferable to use a FQDN as a unique identifier the otherName field MUST be used. Attributes other than those mentioned below MUST NOT be used.
SubjectAltName.dNSName ⓘ This field/attribute has to be included in certificates that are issued as from 1-7-2011	V/O		Name that identifies the server.	RFC2818, RFC5280	IA5String	See requirement 7.1-pkio165 for requirements for the content of this field. See requirement 3.2.5-pkio162 for validation requirements .
SubjectAltName.iPAddress	O	No	Contains a public IP address	RFC 5280, RFC 791, RFC 2460	Octet string	See requirement 7.1-pkio165 for requirements for the content of this field. See requirement 3.2.5-pkio162 for validation requirements for the data entered in this field.
SubjectAltName.otherName	V/O		When the otherName field is used it contains a unique number that identifies the subject (service).	PKIo	IA5String, Microsoft UPN, IBM Principal-Name of Permanent-Identifier	Contains the OID of the TSP and a number, separated by a period or hyphen ('-'), that uniquely and persistently identifies the subject (service). It is recommended to use an existing registration number from the backoffice systems in combination with a code for the organization. In combination with the TSP OID number this identifier is globally unique. This number MUST be persistent.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
BasicConstraints	O	Yes	The "CA" field MUST be omitted (default value is then "FALSE").	RFC 5280		A (Dutch language) browser can then be seen: Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen ("Subjecttype = End Entity", "Path length constraint = None")
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 application the certificate can be used.	RFC 5280	KeyPurposeId's	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.
FreshestCRL	O	No	MUST contain the URI of a Delta CRL distribution point, if Delta CRLs are used.	RFC 5280, PKIo		Delta-CRLs are an optional extension. In order to fulfil the requirements of PKIoverheid a TSP MUST also publish full CRLs at the required release frequency.

Private extensions

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.
SubjectInfoAccess	O	No		RFC 5280	OID, Generalname	This field can be used to reference additional information about the subject.