Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3f: Certificate Policy for Extended Validation certificates in EV (G1) Domain

Version	4.9
Date	July 1, 2021

[OID 2.16.528.1.1003.1.2.7] Extended Validation policy

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 3.7 to 4.0

New

- Requirement 2.2-pkio9;
- Requirement 4.5.2-pkio145;
- Requirement 5.2.4-pkio77.

Modifications

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

Editorial

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

1.2.1.2 Version 4.0 to 4.1

New

- Requirement 3.2.5-pkio146 (effective date no later than 31-12-2015).

Modifications

- Requirement 3.2.5-pkio35;
- The following requirements have been deleted:
    - Requirement 3.2.0-pkio12;
    - Requirement 3.2.2-pkio15 (combined with requirement 3.2.3-pkio23 under new requirement 3.2.2-pkio147);
    - Requirement 3.2.2-pkio17;
    - Requirement 3.2.2-pkio18;
    - Requirement 3.2.2-pkio19;
    - Requirement 3.2.2-pkio20;
    - Requirement 3.2.3-pkio23 (combined with requirement 3.2.3-pkio23 under new requirement 3.2.2-pkio147);
    - Requirement 3.2.3-pkio25;
    - Requirement 3.2.3-pkio28;
    - Requirement 4.4.1-pkio50;
    - Requirement 4.9.3-pkio59;
    - Requirement 9.6.1-pkio130.
- Ban on the use of SubjectAltName.otherName (effective date no later than 4 weeks after publication of PoR 4.1).

Editorial

- Small editorial modification to the following requirement:
    - Requirement 3.2.3-pkio27.

1.2.1.3 Version 4.1 to 4.2

New

- Requirement 7.1-pkio152 (effective date 1 July 2016).

Modifications

- Addition of OID to Certificate Profiles (effective date 1 April 2016).

Editorial

None.

1.2.1.4 Version 4.2 to 4.3

New

- Addition of qualified website certificates (effective date 1-7-2016);
- Addition of issuer.organizationalIdentifier in the certificate profile (effective date 1-7-2016).

Modifications

- Description with attribute CertificatePolicies (effective date 1-7-2016);
- 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);
- Use of values in BasicConstraints field no longer permitted in end entity certificates (effective date 1-7-2016);
- ETSI TS 102 176-1 replaced by ETSI TS 119 312 (effective date no later than 4 weeks after publication of PoR 4.3).

Editorial

None.

1.2.1.5 Version 4.3 to 4.4

New

- Added requirement 4.4.3-pkio154 and modified certificate profile accordingly (mandatory use of Certificate Transparency, effective date 1-7-2017).

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).

Editorial

- Replaced CSP (Certificate Service Provider) with TSP (Trust Service Provider) in accordance with eIDAS directive.

1.2.1.6 Version 4.4 to 4.5

New

- Mandatory English CPS (requirement 2.2-pkio3, effective date 1-10-2017);
- Mandatory yearly renewal CPS (requirement 2.2-pkio156, effective date 1-1-2017);
- Mandatory mention Baseline Requirements domain validation method (2.2-pkio155).

Modifications

- Change in OID 2.16.528.1.1003.1.2.2.7 to also cover OCSP responder certificates (effective date 1-7-2017);
- Mandatory use of field “NextUpdate” in OCSP responses (requirement 4.9.9-pkio71, effective date 1-7-2017).

Editorial

- Moved QCStatement from public to private extensions;
- Modified URL CPS PA.

1.2.1.7 Version 4.5 to 4.6

New

- Requirement 4.8-pkio158 (effective date 1-9-2017, emergency change).

Modifications

- Changes in certificate profile under keyUsage and subjectAltName (effective date directly after publication of PoR 4.6);
- Prohibition of use of an email address in a server certificate under the fields subject.altName.rfc822Name and ExtKeyUsage (effective date no later than 4 weeks after publication of PoR 4.6).

Editorial

None.

1.2.1.8 Version 4.6 to 4.7

New

- Requirement 7.1-pkio171 (effective date immediately after publication of the PoR 4.7);
- Requirement 7.1-pkio172 (effective date date 8 weeks after publication of PoR 4.7);
- Requirement 7.1-pkio173 (effective date immediately after publication of PoR 4.7);
- Requirement 7.1-pkio164 (effective date immediately after publication of the PoR 4.7);
- Requirement 3.2.5-pkio161 (effective date immediately after publication of PoR 4.7).

Modifications

- Explicit statement that the TSP must comply with the BRG Chapter 1.4 (effective date immediately after publication PoR 4.7);
- Requirement 4.8-pkio158 transferred to requirement 8.6-pkio158 (effective date immediately after publication PoR 4.7);
- Declared Netsec integrally applicable (effective date immediately after publication of PoR 4.7);
- Requirement 2.2-pkio9 has expired (effective date immediately after publication of PoR 4.7);
- Description of a number of certificate attributes replaced by reference to requirement 7.1-pkio174 (effective date immediately after publication of PoR 4.7);
- Requirement 6.1.1-pkio90 clarification on generation of certificates (effective date immediately after publication of PoR 4.7).

Editorial

- Text of requirement 6.1.1-pkio90 has been amended to better reflect the requirement. (effective date immediately after publication of PoR 4.7).

1.2.1.9 Version 4.7 to 4.8

New

- Requirement 6.3.2-pkio178 on changed validity of certificates (effective date November 1, 2019);
- Requirement 4.2-pkio179 on maximum renewal period (effective date November 1, 2019);
- Requirement 9.17-pkio180 on informing subscribers on revocation periods (effective date August 29, 2019);
- Moved CertificatePolicies text from profile to this new requirement 7.1-pkio182 (effective date immediately after publication of the PoR 4.8);
- Requirement 8.1-pkio183 on BR self-assesment (effective date immediately after publication of the PoR 4.8);

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

Modifications

- Requirement 2.2-pkio155 removed (effective date immediately after publication of the PoR 4.8);
- Requirement 4.5.2-pkio145 removed (effective date immediately after publication of the PoR 4.8);
- Requirement 6.1.1-pkio91 removed (effective date immediately after publication of the PoR 4.8);
- Change of serial number requirements in requirement 7.1-pkio173 (effective date August 29, 2019);
- Removed footnote from subjectAltName.dNSName attribute (effective date immediately after publication of the PoR 4.8);
- Removed Subject.postaladdress attribute from profile (effective date immediately after publication of the PoR 4.8);
- Requirement 9.17-pkio140 removed (effective date immediately after publication of the PoR 4.8);
- Moved hidden requirement on inclusion of certificatepolicies (OID) in an end-user certificate to new requirement 7.1-pkio 182 (effective date immediately after publication of the PoR 4.8).

Editorial

- Reference in requirement 3.2.5-pkio170 (effective date immediately after publication of the PoR 4.8).

1.2.1.10 Version 4.8 to 4.9

New

- Requirement 8.1-pkio188, Contrary to what is stated in requirement 8.1-pkio187 sub 1, a TSP can choose to undergo an audit against "Webtrust for Certification Authorities - Extended Validation". The certification must take place against the current version at the time of the commencement of the audit period (effective date after 02-17-2020);
- 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).

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).

1.2.2 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
No content found.

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 2.16.528.1.1003.1.2.7]

EV SSL certificates that are issued under this CP, can be used to safeguard a connection between a specific client and a server, via the TLS/SSL protocol, that is part of the organizational entity that is 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 and the Extended Validation Guidelines. In the case of discrepancies between this PoR and the Baseline Requirements and / or the EV guidelines, the BRG and/or EVCG prevails.

Under this OID OCSP responder certificates may be issued for use within the domain Organisation Extended Validation (EV). 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-pkio167 —

Description	The TSP MUST describe in its CPS which validation methods for validating FQDNs it uses for inclusion in the Subject.CommonName field and the SubjectAltName.dNSName field including a reference to the relevant chapter 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 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-pkio147 —

Description	The TSP has to verify that the subscriber is an existing and legal organization, and who the Authorised Representative (or Representation) of the subscriber is. As evidence that it is an existing and legal organization and of the correctness and existence of the Authorised Representative (or Representation) registered by the subscriber, the TSP has to request and verify at least the following supporting documents: • For government organizations, a recently certified excerpt (no more than 1 month old) from the Chamber of Commerce's Trade Register or a law, deed of incorporation or a general governmental decree. If registration in the Trade Register has nog yet taken place, a copy of the corresponding page from the most recent version of the Staatsalmanak where the Authorised Representative (or Representation) is mentioned; • For bodies governed by private law with and without a legal personality with a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register where the Authorised Representative (or Representation) is mentioned. The TSP must verify if the Organization and Authorised Representative appear on the latest EU list of prohibited terrorists and terrorist organizations, published by the European Council These lists can be found on the web page: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001E0931:NL:NOT These are decisions concerning updating the list of people, groups and entities referred to in articles 2, 3 and 4 of Common Position 2001/931/GBVB concerning the use of specific measures to combat terrorism. The TSP must not issue EV SSL certificates to an organization or its Authorized Representative that appears on this list.
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	-

3.2.3 Authentication of individual identity

3.2.3-pkio27 —

Description	To detail the provisions in 3.2.3- pkio22, the identity of the certificate manager can only be established using the valid documents referred to in article 1 of the Compulsory Identification Act. The TSP has to check the validity and authenticity of these documents. The TSP must also establish whether the certificate manager appears on the latest EU list of prohibited terrorists and terrorist organizations: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:028:0057:0059:EN:PDF The TSP may not issue an EV SSL certificate to an organization or its certificate manager that is included on this list.
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.

3.2.5-pkio161 —

Description	The TSP MUST check that 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. 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). The TSP must also adhere to the requirements in the EV Guidelines (EVCG) chapter 11. The verified data may be reused in a subsequent application, provided that it is not older than 13 months. If the data is older than 13 months, 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).

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

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-pkio48 —

Description	Before issuing an EV SSL certificate, the TSP has to have received a fully completed application, signed by the certificate manager on behalf of the subscriber. The application must contain the following information:
	• the name of the organization;
	• the domain name (FQDN);
	• Chamber of Commerce number or Government Identification Number;
	• subscriber's address consisting of:
	  • street name and house number;
	  • town or city;
	  • province;
	  • country;
	  • postcode;
	  • general telephone number.
	• certificate manager's name.

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-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.

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.

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

Content by label

There is no content with the specified labels

4.9.6 Revocation checking requirement for relying parties

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.7 CRL issuance frequency (if applicable)

Refer to Programme of Requirements part 3 Basic Requirements.

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-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	-

4.9.10 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

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

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

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.

6.3 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

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.

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-pkio164 —

Description	The Subject.CommonName field MUST contain a FQDN (Fully Qualified Domain Name). An FQDN MUST also appear in the SubjectAltName.DNsName field. An Extended Validation certificate MAY contain several FQDNs. Every FQDN MUST fall under the same main domain. (e.g., www.logius.nl[4], application.logius.nl[5], secure.logius.nl[6] etc.). The following is NOT permitted to include in the Subject.Commonname field 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 }

4 http://www.logius.nl
5 http://application.logius.nl
6 http://secure.logius.nl

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	-

7.1.1 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

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.

8.1-pkio188 —

Description	Contrary to what is stated in requirement 8.1-pkio187 sub 1, a TSP can choose to undergo an audit against "Webtrust for Certification Authorities - Extended Validation". The certification must take place against the current version at the time of the commencement of the audit period.
Comment	-

8.1-pkio189 —

Description	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: a. The TSP must be certified against ETSI EN 319 411-2 b. The certification must be done by a CB that is accredited in accordance with the ETSI EN 319 403 scheme by an accreditation body within the meaning of Article 4 of Regulation (EC) No 765/2008 c. The certification must take place against the most recent version of ETSI EN 319 411-2 d. In addition, the report must state that the TSP meets the eIDAS (910/2014) regulation requirements. e. The TSP is registered with AT. The CA with which the TSP wants to issue qualified certificates MUST be on the Trusted List (TSL) at AT before issuance of qualified certificates can start.
Comment	-

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

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

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	-

9.6.2 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

Content by label

There is no content with the specified labels

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

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

Profile of Extended Validation certificates of the EV root certificate

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'.

Extended Validation SSL Certificates

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	See requirement 7.1-pkio173.	RFC 5280	Integer	
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 attributes listed below:	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 necessary to identify the issuing government body (no part of the Distinguished Name, requirement from RFC 3739)
Issuer.organizationIdentifier	V/N	The organizationIdentifier field contains an identification of the issuing CA. This field MUST be present when the subject.organizationIdentifier field is present in the TSP certificate and MUST NOT be present when this field is not part of the corresponding TSP certificate.	EN 319 412-1	String	The syntax of the identification string is specified in paragraph 5.1.4 van ETSI EN 319 412-1 and contains: • 3 character legal person identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).
Validity	V	MUST define the period of validity of the certificate according to RFC 5280.	RFC 5280	UTCTime	MUST include the start and end date for validity of the certificate in accordance with the applicable policy laid down in the EV 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.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.businessCategory	V	MUST include one of the following values: 2.5.4.15 = Private Organization 2.5.4.15 = Government Entity 2.5.4.15 = Business Entity 2.5.4.15 = Non-Commercial Entity	PKIo		• Private Organization applies to organizations governed by private law with a legal personality; • Government Entity applies to government organizations; • Business Entity applies to organizations governed by private law without a legal personality; Formal collaborative ventures between companies also fall under this category; • Non-Commercial Entity applies in international organizations that do not belong to one country or government (e.g. the NATO (http://www.nato.int) or the United Nations (http://www.un.int)). NO PKIoverheid EV SSL certificates MAY be issued to these types of organizations.
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-pkio164 for requirements for the content of this field See requirement 3.2.5-pkio161 for validation requirements
Subject.organizationName	V	MUST include the full name of the subscriber organization in accordance with the accepted document (State Almanac) or Basic Registry (Trade Register).	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. The TSP MAY modify the full name of the subscriber organization if this has more than 64 positions. The TSP MUST consult the subscriber about this. The modification MUST take place in such a way that the relying parties do not think that they are dealing with a different organization. If this type of modification is not possible, then TSP MAY NOT issue the EV SSL certificate.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.organizationalUnitName	O/V	Optional specification of an organizational entity. This attribute MUST NOT include a function indication or similar. Compulsory labelling of a government organization.	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. Only in those cases in which a government organization entity is not yet listed in the Trade Register, in this field the TSP MUST include the words “government organization”.
Subject.stateOrProvinceName	O	MUST include the province of the subscriber's branch, in accordance with the accepted document (State Almanac) or Basic registry (Trade Register).	PKIo, RFC 3739	UTF8String	
Subject.localityName	V	MUST include the subscriber's location in accordance with the accepted document (State Almanac) or Basic registry (Trade Register).	PKIo, RFC 3739	UTF8String	.
Subject:jurisdictionOfIncorporationCountryName	V	Fixed value: 1.3.6.1.4.1.311.60.2.1.3 = NL	RFC 5280, ISO 3166	OID	
Subject.serialNumber	V	The TSP is responsible for safeguarding the uniqueness of the subject (service). The Subject.serialNumber MUST be used to identify the subject uniquely.	RFC 3739, X 520, PKIo	Printable String	The Chamber of Commerce number MUST be included in this field. In those cases where an organizational entity within the government is not yet listed in the Trade Register the TSP MUST determine the number itself with which the uniqueness of the subject (service) is safeguarded. The TSP MUST then also include in the field Subject.organizationalUnitName the word “government organisation”.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
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	In EV SSL certificates the digitalSignature and keyEncipherment bits MUST be incorporated and marked as critical. Another keyUsage MUST NOT be combined with this.	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	
CertificatePolicies	V/O	No	MUST include the OID of this EV certificate policy (CP) and the EV OID of the CA/B forum. When the certificate is also issued as Qualified Web Certificate the QCP-w policy id MUST be included. policyIdentifier • EV policy identifier policyQualifiers:policyQualifierId • id-qt 1 [RFC 5280] policyQualifiers:qualifier:cPSuri • HTTP URL of the Certification Practice Statement of the PA of PKIoverheid In EV SSL certificates, the HTTP URL of the certification practice statement (CPS) of the TSP MUST be incorporated policyQualifiers:qualifier:cPSuri	RFC 3739 RFC 5280	OID, String, UTF8String or IA5 String	The following OIDs apply: • 2.16.528.1.1003.1.2.7 and • 2.23.140.1.1 This OID MUST be included in EV SSL certificates and in EV subordinate CA certificates that are issued under an EV TSP CA certificate. The QCP-w policy OID is 0.4.0.194112.1.4 The HTTP URL of the EV Certification Practice Statement of the PA of PKIoverheid is: https://cps.pkioverheid.nl

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			• HTTP URL of the Certification Practice Statement of the TSP In EV SSL certificates a user notice MUST be incorporated. The TSP SHOULD use UTF8String in the userNotice, but MAY use IA5String.			
SubjectAltName	V	No	MUST be used and given a worldwide unique number that identifies the service.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MUST include a unique identifier in the dNSName or iPAddress attribute. 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-pkio164 for requirements for the content of this field. See requirement 3.2.5-pkio161 for validation.
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.
BasicConstraints	O	Yes	The "CA" field must be omitted (default value is then "FALSE").	RFC 5280		In a (Dutch language) browser, the following will be visable: Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen ("Subjecttype = End Entity", "Restriction for the path length = None")
CRLDistributionPoints	V	No	MUST include the HTTP URI of a CRL distribution point.	RFC 5280, ETSI TS 102 280		

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
ExtKeyUsage	V	No	Extension that indicates for which applications the certificate can be used.	RFC 5280	KeyPurposeId's	In EV SSL certificates, the attributes id-kp-serverAuth (Verification of the server) and id-kp-clientAuth (Client verification) MUST be included.
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	V	No	See requirement 7.1-pkio172			
SubjectInfoAccess	O	No		RFC 5280	OID, Generalname	This field can be used to reference additional information about the subject.
QcStatement	V/N	No	Qualified Web Certificates MUST indicate that they are issued as qualified certificates complying with annex IV of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qcs-QcCompliance* statement in this extension. Qualified Web Certificates MUST indicate that they are issued as type of certificate complying with annex IV of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qct-web* statement in this extension. Qualified Web Certificates MAY indicate that the private key that is part of the public key in the certificate is saved on a qualified signature creation device (QSCD) complying with annex II of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qcs-QcSSCD* statement in this extension. If a QSCD is used this statement MUST be included.	RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	The aforementioned QcStatement identifiers relate to the following OIDs: • id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 • id-etsi-qct-web { id-etsi-qcs-QcType 3 } 0.4.0.1862.1.6.3 • id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4 • id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			Qualified Web Certificates MUST contain a reference to the location of the PKI Disclosure Statement (PDS). This URL must present in the *id-etsi-qcs-QcPDS* statement in this extension.			