



## Programme of Requirements part 3c: Certificate Policy for certificates in Citizen (G3) Domain

Version            4.10  
Date                March 1, 2022

[OID 2.16.528.1.1003.1.2.3.1] Authenticity  
[OID 2.16.528.1.1003.1.2.3.2] Non repudiation  
[OID 2.16.528.1.1003.1.2.3.3] Confidentiality

## Publishers imprint

Version number 4.10  
Contact person Policy Authority of PKIoverheid

Organization Logius

*Street address*

Wilhelmina van Pruisenweg 52

*Postal address*

Postbus 96810  
2509 JE DEN HAAG

T 0900-555 4555  
servicecentrum@logius.nl

## Contents

<b>1. INTRODUCTION</b>	<b>10</b>
<i>1.1 Overview</i>	10
<i>1.2 Document name and identification</i>	10
1.2.1 Revisions	10
1.2.1.1 Version 3.7 to 4.0	10
1.2.1.2 Version 4.0 to 4.1	10
1.2.1.3 Version 4.1 to 4.2	10
1.2.1.4 Version 4.2 to 4.3	10
1.2.1.5 Version 4.3 to 4.4	11
1.2.1.6 Version 4.4 to 4.5	11
1.2.1.7 Version 4.5 to 4.6	11
1.2.1.8 Version 4.6 to 4.7	12
1.2.1.9 Version 4.7 to 4.8	12
1.2.1.10 Version 4.8 to 4.9	12
1.2.1.11 Version 4.9 to 4.10	13
1.2.2 Relevant dates	13
<i>1.3 PKI participants</i>	14
1.3.1 Certification authorities	14
1.3.2 Registration authorities	14
1.3.3 Subscribers	15
1.3.4 Relying parties	15
1.3.5 Other participants	15
<i>1.4 Certificate usage</i>	15
1.4.1 Appropriate certificate uses	15
1.4.2 Prohibited certificate uses	15
<i>1.5 Policy administration</i>	15
1.5.1 Organization administering the document	16
1.5.2 Contact person	16
1.5.3 Person determining CPS suitability for the policy	16
1.5.4 CP approval procedures	16
<i>1.6 Definitions and acronyms</i>	16
1.6.1 Conventions	16
<b>2. PUBLICATION AND REPOSITORY RESPONSIBILITIES</b>	<b>17</b>
<i>2.1 Repositories</i>	17
<i>2.2 Publication of certification information</i>	17
<i>2.3 Time or frequency of publication</i>	17

2.4 Access controls on repositories .....	17
<b>3. IDENTIFICATION AND AUTHENTICATION .....</b>	<b>18</b>
3.1 Naming .....	18
3.1.1 Types of names.....	18
3.1.2 Need for names to be meaningful.....	18
3.1.3 Anonymity or pseudonymity of subscribers .....	18
3.1.4 Rules for interpreting various name forms .....	18
3.1.5 Uniqueness of names.....	18
3.1.6 Recognition, authentication, and role of trademarks.....	18
3.2 Initial identity validation .....	18
3.2.1 Method to prove possession of private key.....	18
3.2.2 Authentication of organization identity .....	18
3.2.3 Authentication of individual identity .....	18
3.2.4 Non-verified subscriber information .....	19
3.2.5 Validation of authority.....	19
3.2.6 Criteria for interoperation .....	19
3.3 Identification and authentication for re-key requests.....	19
3.3.1 Identification and authentication for routine re-key.....	19
3.3.2 Identification and authentication for re-key after revocation.....	19
3.4 Identification and authentication for revocation request .....	19
<b>4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....</b>	<b>20</b>
4.1 Certificate Application.....	20
4.1.1 Who can submit a certificate application.....	20
4.1.2 Enrollment process and responsibilities .....	20
4.2 Certificate application processing .....	20
4.2.1 Performing identification and authentication functions .....	20
4.2.2 Approval or rejection of certificate applications.....	20
4.2.3 Time to process certificate applications .....	20
4.3 Certificate issuance .....	20
4.3.1 CA actions during certificate issuance.....	20
4.3.2 Notification to subscriber by the CA of issuance of Certificate .....	20
4.4 Certificate acceptance.....	20
4.4.1 Conduct constituting certificate acceptance.....	20
4.4.2 Publication of the certificate by the CA .....	20
4.4.3 Notification of certificate issuance by the CA to other Entities .....	20
4.5 Key pair and certificate usage.....	20
4.5.1 Subscriber private key and certificate usage .....	20
4.5.2 Relying party public key and certificate usage .....	21
4.6 Certificate renewal .....	21
4.6.1 Circumstance for certificate renewal .....	21
4.6.2 Who may request renewal .....	21
4.6.3 Processing certificate renewal requests .....	21

4.6.4	Notification of new certificate issuance to subscriber .....	21
4.6.5	Conduct constituting acceptance of a renewal certificate .....	21
4.6.6	Publication of the renewal certificate by the CA .....	21
4.6.7	Notification of certificate issuance by the CA to other entities .....	21
4.7	<i>Certificate re-key</i> .....	21
4.7.1	Circumstance for certificate re-key .....	21
4.7.2	Who may request certification of a new public key .....	21
4.7.3	Processing certificate re-keying requests .....	21
4.7.4	Notification of new certificate issuance to subscriber .....	21
4.7.5	Conduct constituting acceptance of a re-keyed certificate .....	21
4.7.6	Publication of the re-keyed certificate by the CA .....	22
4.7.7	Notification of certificate issuance by the CA to other entities .....	22
4.8	<i>Certificate modification</i> .....	22
4.8.1	Circumstance for certificate modification .....	22
4.8.2	Who may request certificate modification .....	22
4.8.3	Processing certificate modification requests .....	22
4.8.4	Notification of new certificate issuance to subscriber .....	22
4.8.5	Conduct constituting acceptance of modified certificate .....	22
4.8.6	Publication of the modified certificate by the CA .....	22
4.8.7	Notification of certificate issuance by the CA to other entities .....	22
4.9	<i>Certificate revocation and suspension</i> .....	22
4.9.1	Circumstances for revocation .....	22
4.9.2	Who can request revocation.....	23
4.9.3	Procedure for revocation request .....	23
4.9.4	Revocation request grace period.....	23
4.9.5	Time within which CA must process the revocation request .....	24
4.9.6	Revocation checking requirement for relying parties.....	24
4.9.7	CRL issuance frequency (if applicable).....	24
4.9.8	Maximum latency for CRLs (if applicable) .....	24
4.9.9	On-line revocation/status checking availability .....	24
4.9.10	On-line revocation checking requirements.....	25
4.9.11	Other forms of revocation advertisements available.....	25
4.9.12	Special requirements related to key compromise .....	25
4.9.13	Circumstances for suspension .....	25
4.9.14	Who can request suspension .....	25
4.9.15	Procedure for suspension request .....	25
4.9.16	Limits on suspension period .....	26
4.10	<i>Certificate status services</i> .....	26
4.10.1	Operational characteristics.....	26
4.10.2	Service availability .....	26
4.10.3	Optional features.....	26
4.11	<i>End of subscription</i> .....	26
4.12	<i>Key escrow and recovery</i> .....	26
4.12.1	Key escrow and recovery policy and practices.....	26
4.12.2	Session key encapsulation and recovery policy and practices .....	26

**5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS ..... 27**

*5.1 Physical controls ..... 27*

5.1.1 Site location and construction ..... 27

5.1.2 Physical access ..... 27

5.1.3 Power and air conditioning..... 27

5.1.4 Water exposures ..... 27

5.1.5 Fire prevention and protection ..... 27

5.1.6 Media storage ..... 27

5.1.7 Waste disposal..... 27

5.1.8 Off-site backup ..... 27

*5.2 Procedural controls..... 27*

5.2.1 Trusted roles ..... 27

5.2.2 Number of persons required per task ..... 27

5.2.3 Identification and authentication for each role ..... 27

5.2.4 Roles requiring separation of duties ..... 27

*5.3 Personnel controls..... 28*

5.3.1 Qualifications, experience, and clearance requirements ..... 28

5.3.2 Background check procedures..... 28

5.3.3 Training requirements ..... 28

5.3.4 Retraining frequency and requirements ..... 28

5.3.5 Job rotation frequency and sequence ..... 28

5.3.6 Sanctions for unauthorized actions ..... 28

5.3.7 Independent contractor requirements ..... 28

5.3.8 Documentation supplied to personnel..... 28

*5.4 Audit logging procedures..... 28*

5.4.1 Types of events recorded..... 28

5.4.2 Frequency of processing log..... 29

5.4.3 Retention period for audit log ..... 29

5.4.4 Protection of audit log ..... 29

5.4.5 Audit log backup procedures ..... 29

5.4.6 Audit collection system (internal vs. external) ..... 29

5.4.7 Notification to event-causing subject..... 29

5.4.8 Vulnerability assessments..... 30

*5.5 Records archival ..... 30*

5.5.1 Types of records archived ..... 30

5.5.2 Retention period for archive..... 30

5.5.3 Protection of archive..... 30

5.5.4 Archive backup procedures ..... 30

5.5.5 Requirements for time-stamping of records ..... 30

5.5.6 Archive collection system (internal or external) ..... 30

5.5.7 Procedures to obtain and verify archive information ..... 30

*5.6 Key changeover..... 30*

*5.7 Compromise and disaster recovery..... 30*

5.7.1 Incident and compromise handling procedures ..... 30

5.7.2 Computing resources, software, and\_or data are corrupted..... 30

5.7.3 Entity private key compromise procedures .....	30
5.7.4 Business continuity capabilities after a disaster .....	30
5.8 CA or RA termination.....	31
<b>6. TECHNICAL SECURITY CONTROLS.....</b>	<b>32</b>
6.1 Key pair generation and installation.....	32
6.1.1 Key pair generation .....	32
6.1.2 Private key delivery to subscriber .....	32
6.1.3 Public key delivery to certificate issuer .....	33
6.1.4 CA public key delivery to relying parties .....	33
6.1.5 Key sizes.....	33
6.1.6 Public key parameters generation and quality checking .....	33
6.1.7 Key usage purposes (as per X.509 v3 key usage field) .....	33
6.2 Private Key Protection and Cryptographic Module Engineering Controls.....	33
6.2.1 Cryptographic module standards and controls .....	33
6.2.2 Private key (n out of m) multi-person control .....	33
6.2.3 Private key escrow .....	33
6.2.4 Private key backup .....	33
6.2.5 Private key archival .....	34
6.2.6 Private key transfer into or from a cryptographic module .....	34
6.2.7 Private key storage on cryptographic module .....	34
6.2.8 Method of activating private key.....	34
6.2.9 Method of deactivating private key .....	34
6.2.10 Method of destroying private key.....	34
6.2.11 Cryptographic Module Rating.....	34
6.3 Other aspects of key pair management.....	35
6.3.1 Public key archival.....	35
6.3.2 Certificate operational periods and key pair usage periods .....	35
6.4 Activation data .....	35
6.4.1 Activation data generation and installation.....	35
6.4.2 Activation data protection.....	36
6.4.3 Other aspects of activation data .....	36
6.5 Computer security controls.....	36
6.5.1 Specific computer security technical requirements .....	36
6.5.2 Computer security rating.....	36
6.6 Life cycle technical controls .....	36
6.6.1 System development controls .....	36
6.6.2 Security management controls.....	36
6.6.3 Life cycle security controls.....	36
6.7 Network security controls.....	36
6.7.1 Network security controls (duplicate) .....	36
6.8 Time-stamping .....	37
<b>7. CERTIFICATE, CRL, AND OCSP PROFILES .....</b>	<b>38</b>

<i>7.1 Certificate profile</i> .....	38
7.1.1 Version number(s).....	39
7.1.2 Certificate extensions .....	39
7.1.3 Algorithm object identifiers.....	39
7.1.4 Name forms .....	39
7.1.5 Name constraints .....	39
7.1.6 Certificate policy object identifier.....	39
7.1.7 Usage of Policy Constraints extension.....	39
7.1.8 Policy qualifiers syntax and semantics.....	39
7.1.9 Processing semantics for the critical Certificate Policies extension .....	39
<i>7.2 CRL profile</i> .....	40
7.2.1 Version number(s).....	40
7.2.2 CRL and CRL entry extensions.....	40
<i>7.3 OCSP profile</i> .....	40
7.3.1 Version number(s).....	40
7.3.2 OCSP extensions .....	40
<b>8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS</b> .....	<b>41</b>
<i>8.1 Frequency or circumstances of assessment</i> .....	41
<i>8.2 Identity/qualifications of assessor</i> .....	41
<i>8.3 Assessors relationship to assessed entity</i> .....	41
<i>8.4 Topics covered by assessment</i> .....	41
<i>8.5 Actions taken as a result of deficiency</i> .....	41
<i>8.6 Communication of results</i> .....	41
<b>9. OTHER BUSINESS AND LEGAL MATTERS</b> .....	<b>42</b>
<i>9.1 Fees</i> .....	42
9.1.1 Certificate issuance or renewal fees .....	42
9.1.2 Certificate access fees.....	42
9.1.3 Revocation or status information access fees .....	42
9.1.4 Fees for other services .....	42
9.1.5 Refund policy .....	42
<i>9.2 Financial responsibility</i> .....	42
9.2.1 Insurance coverage .....	42
9.2.2 Other assets .....	42
9.2.3 Insurance or warranty coverage for end-entities .....	42
<i>9.3 Confidentiality of business information</i> .....	43
9.3.1 Scope of confidential information.....	43
9.3.2 Information not within the scope of confidential information.....	43
9.3.3 Responsibility to protect confidential information .....	43
<i>9.4 Privacy of personal information</i> .....	43
9.4.1 Privacy plan.....	43
9.4.2 Information treated as private .....	43



9.4.3 Information not deemed private .....	43
9.4.4 Responsibility to protect private information .....	43
9.4.5 Notice and consent to use private information .....	43
9.4.6 Disclosure pursuant to judicial or administrative process.....	43
9.4.7 Other information disclosure circumstances .....	43
<i>9.5 Intellectual property rights .....</i>	<i>43</i>
<i>9.6 Representations and warranties .....</i>	<i>43</i>
9.6.1 CA representations and warranties .....	43
9.6.2 RA representations and warranties .....	44
9.6.3 Subscriber representations and warranties.....	44
9.6.4 Relying party representations and warranties .....	44
9.6.5 Representations and warranties of other participants .....	44
<i>9.7 Disclaimers of warranties .....</i>	<i>44</i>
<i>9.8 Limitations of liability .....</i>	<i>44</i>
<i>9.9 Indemnities.....</i>	<i>44</i>
<i>9.10 Term and termination .....</i>	<i>45</i>
9.10.1 Term.....	45
9.10.2 Termination .....	45
9.10.3 Effect of termination and survival .....	45
<i>9.11 Individual notices and communications with participants .....</i>	<i>45</i>
<i>9.12 Amendments .....</i>	<i>45</i>
9.12.1 Procedure for amendment .....	45
9.12.2 Notification mechanism and period .....	45
9.12.3 Circumstances under which OID must be changed .....	45
<i>9.13 Dispute resolution provisions .....</i>	<i>45</i>
<i>9.14 Governing law.....</i>	<i>45</i>
<i>9.15 Compliance with applicable law .....</i>	<i>45</i>
<i>9.16 Miscellaneous provisions .....</i>	<i>45</i>
9.16.1 Entire agreement .....	45
9.16.2 Assignment .....	45
9.16.3 Severability .....	45
9.16.4 Enforcement (attorneys' fees and waiver of rights) .....	46
9.16.5 Force Majeure .....	46
<i>9.17 Other provisions.....</i>	<i>46</i>
<b>Appendix A: Certificate Profiles.....</b>	<b>47</b>
<i>Citizen certificates .....</i>	<i>48</i>

## 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*

None.

*Modifications*

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

*Editorial*

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

##### 1.2.1.2 Version 4.0 to 4.1

*New*

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

*Modifications*

None.

*Editorial*

- Small editorial modifications to the following requirements:
  - 3.1.3-pkio11;
  - 5.7.4-pkio86;
  - 9.6.1-pkio131.

##### 1.2.1.3 Version 4.1 to 4.2

*New*

- Requirement 7.1-pkio149 (effective date July 1, 2016).

*Modifications*

None.

*Editorial*

None.

##### 1.2.1.4 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);
- Mandatory QcStatement in qualified certificate (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);
- 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 June 30, 2017).

#### *Editorial*

- Removed references to G1 Root (expired).

#### 1.2.1.5 Version 4.3 to 4.4

##### *New*

None.

##### *Modifications*

- Removal of requirement 5.3.2-pkio79 (effective date 1-2-2017);
- Clarification of issuer.organizationIdentifier field (effective date 1-2-2017);
- Tightening of use optional EKUs that conflict with the parent TSP CA certificate (effective date 1-2-2017);
- Prohibition use of QCStatement with authenticity and confidentiality certificate (equalization of parts a, c & I, 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).

##### *Modifications*

- Requirement 4.9.9-pkio67 now references RFC6960 instead of RFC2560 (effective date 31-12-2016);
- Allow/require EKU emailProtection in authenticity and non-repudiation certificates in requirement 7.1-pkio149 (effective date 1-4-2017);
- Change in OID 2.16.528.1.1003.1.2.3.1 to also cover OCSP responder certificates (effective date 1-7-2017);
- Mandatory use of field "NextUpdate" in OCSP responses (requirement 4.9.9-pkio71, effective date 1-7-2017).

##### *Editorial*

- Removed typos from certificate profile.

#### 1.2.1.7 Version 4.5 to 4.6

##### *New*

None.

##### *Modifications*

- Modified reference to ETSI certificate profiles (effective date directly after publication of PoR 4.6);
- Certificate profile, removed exception subject.surName and subject.givenName (effective date directly after publication of PoR 4.6);
- Corrected subjectAltName.othername field (effective date directly after publication of PoR 4.6).

*Editorial*

None.

#### 1.2.1.8 Version 4.6 to 4.7

*New*

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

*Modifications*

- Description of a number of certificate attributes replaced by reference to requirement 7.1-pkio174 (effective date 8 weeks after publication PoR 4.7);
- Reference to CWA 14 169 amended to EN 419 211 for QSCDs. This also sets requirements for the issue of QSCDs for requirements 6.1.1-pkio88, 6.2.11-pkio104, 6.2.11-pkio105, 6.2.11-pkio106, 6.4.1-pkio112 and 4.9.1-pkio52 (effective date immediately after publication PoR 4.7).

*Editorial*

None.

#### 1.2.1.9 Version 4.7 to 4.8

*New*

None.

*Modifications*

- 9.17-pkio139 vervallen (effective date immediately after publication PoR 4.8);
- 7.1-pkio173 aanpassing serienummer eisen (effective date August 29, 2019).

*Editorial*

- 6.1.2-pkio94 verwijzing naar ETSI TS 101 456 7.2.8.d aangepast naar 411-1 (effective date immediately after publication PoR 4.8);
- 4.9.1-pkio52 definitie privé sleutel (effective date immediately after publication PoR 4.8);
- 4.9.9-pkio68 aanpassing verwijzing (effective date immediately after publication PoR 4.8).

#### 1.2.1.10 Version 4.8 to 4.9

*New*

- Requirement 2.2-pkio191, the CPS of the TSP MUST follow the layout according to RFC 3647 (effective date after 01-04-2020).
- 4.9.1-pkio192, describes when certificates will be revoked (effective date 02-17-2020).
- 8.1-pkio189, if the TSP issues or intends to issue qualified certificates under PKIoverheid, the following additional requirements apply in addition to those set out in requirement 8.1-pkio187 (effective date 02-17-2020).

*Modifications*

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

*Removals*

- Requirement 2.2-pkio7 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).
- Requirement 6.2.3-pkio101 has been removed (effective date immediately after publication PoR 4.9).

*Editorial*

None.

1.2.1.11 Version 4.9 to 4.10

*New*

- Added basic requirement 8.2-pkio199.
- Added new additional requirement 8.4-pkio194.
- Added new additional requirement 8.4-pkio200.

*Modifications*

- Change the criterium for the `subject:surname` attribute from O to V in the certificate profile.
- Change the criterium for the `subject:givenName` attribute from V/O to V in the certificate profile.
- Change the description, explanation, and criterium of the `extensions:subjectAltName:otherName` attribute in the certificate profile.
- Expand the description of the `extensions:certificatePolicies` field in the certificate profile with additional ETSI 319 411 certificate policies.
- Change the `extensions:certificatePolicies:policyQualifiers:qualifier:userNotice` field criteria to "MAY" in the certificate profile.
- Replace Telecommunications Act with eDIAS in requirement 9.6.1-pkio127.

*Removals*

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

*Editorial*

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

1.2.2 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 referred 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
Cleverbase ID PKIoverheid Burger CA – G3 (2018)	 25 Jan 2018	 12 Nov 2028	6711424399121577698 (0x5d23c4eeae87f6e2)	5C80E569FCEE93F15A2BC0 435102B26A04F5AA1EC991 2C13A05881C1AAD502D2
Cleverbase ID PKIoverheid Burger CA – G3 (2019)	 17 Apr 2019	 12 Nov 2028	7796d55e296d01ccf50cedb 3707b0dd842695535	DE0A92E5435B613208DC4 35ECC7158BF28F420A93E0 A91D5965972053F523549
Digidentity BV PKIoverheid Burger CA - 2021	 25 Feb 2021	 12 Nov 2028	f24b00c8f2953175ec1b78bb 699eac58759b13	9C64E24D2CAAA8DD45EF9 9BA62277CEEE6005C66362 4514B8C770E2D075BB611
QuoVadis PKIoverheid Burger CA – 2021	 25 Feb 2021	 12 Nov 2028	4959c844fba7140010f2aade 5d3b4c2ad87af018	3AC3DB2C474FC34FE8011 C5A01F622824C6F8B11076 F56192AC701DAE3D70534

#### 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 Appropriate certificate uses*

The use of certificates issued under this CP relates to communication of certificate holders who act in a private capacity.

#### *[OID 2.16.528.1.1003.1.2.3.1]*

Authenticity certificates, that are issued under this CP, can be used for reliable electronic identification and authentication of persons. This concerns both the mutual identification of people and identification between people and computerized devices.

Authenticity certificates that are issued under this CP cannot be used to identify people in cases where the law requires that the identity of persons may only be established using the document referred to in the Compulsory Identification Act (Wet op de identificatieplicht).

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

#### *[OID 2.16.528.1.1003.1.2.3.2]*

Signature certificates, that are issued under this CP, can be used to verify electronic signatures, that have "the same legal consequences as a handwritten signature", as specified in article 15a, first and second paragraphs, in Title 1 of Book 3 of the Civil Code (Burgerlijk Wetboek) under section 1A and are qualified certificates as referred to in article 1.1, paragraph ss of the Telecommunications Act (Telecomwet).

#### *[OID 2.16.528.1.1003.1.2.3.3]*

Confidentiality certificates, issued under this CP, can be used to protect the confidentiality of data that is exchanged and/or stored in electronic form. This concerns both the mutual exchange between people and exchange between people and computerized devices.

### *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](mailto:servicecentrum@logius.nl)<sup>1</sup>

#### *1.5.3 Person determining CPS suitability for the policy*

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

#### *1.5.4 CP approval procedures*

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

### **1.6 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.

---

<sup>1</sup> <mailto:servicecentrum@logius.nl>



## 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

### 2.1 Repositories

Refer to Programme of Requirements part 3 Basic Requirements.

### 2.2 Publication of certification information

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

#### 2.2-pkio191 —

<b>Description</b>	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.
<b>Comment</b>	-

#### 2.2-pkio3 —

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

### 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.

Additional requirements:

##### 3.1.3-pkio11 —

<b>Description</b>	Pseudonyms MUST NOT be used in certificates.
<b>Comment</b>	-

##### 3.1.4 Rules for interpreting various name forms

Refer to Programme of Requirements part 3 Basic Requirements.

##### 3.1.5 Uniqueness of names

Refer to Programme of Requirements part 3 Basic Requirements.

##### 3.1.6 Recognition, authentication, and role of trademarks

Refer to Programme of Requirements part 3 Basic Requirements.

#### 3.2 Initial identity validation

##### 3.2.1 Method to prove possession of private key

Refer to Programme of Requirements part 3 Basic Requirements.

##### 3.2.2 Authentication of organization identity

Refer to Programme of Requirements part 3 Basic Requirements.

##### 3.2.3 Authentication of individual identity


Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

##### 3.2.3-pkio169 —

<b>Description</b>	For certificates that are suitable for signing and / or encrypting e-mail messages and which include the e-mail address of the certificate holder, the TSP will take appropriate measures to ensure that the applicant has control over the e-mail
--------------------	--

	address in question OR that he / she is authorized by the holder of the e-mail address to have this e-mail address included in a certificate. The TSP MUST state clearly in its CPS which procedures have been implemented to confirm the above. In these procedures, the TSP MUST perform validation of the domain part (@domain.com <sup>2</sup> ) itself. This check MUST NOT be performed by third parties.
<b>Comment</b>	-

 3.2.3-pkio21 —

<b>Description</b>	When issuing certificates to natural persons the TSP has to verify that the full name used by the certificate holder that is incorporated in the certificate is correct and complete, including the surname, first forename, initials or other forename(s) (if applicable) and surname prefixes (if applicable).
<b>Comment</b>	-

*3.2.4 Non-verified subscriber information*

Refer to Programme of Requirements part 3 Basic Requirements.

*3.2.5 Validation of authority*

Refer to Programme of Requirements part 3 Basic Requirements.

*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.

---

<sup>2</sup> <http://domain.com>

## 4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

### 4.1 Certificate Application

#### 4.1.1 *Who can submit a certificate application*

Refer to Programme of Requirements part 3 Basic Requirements.

#### 4.1.2 *Enrollment process and responsibilities*

Refer to Programme of Requirements part 3 Basic Requirements.

### 4.2 Certificate application processing

#### 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.

Additional requirements:

 4.9.1-pkio192 —

<b>Description</b>	<p>Certificates will be revoked when:</p> <ul style="list-style-type: none"> <li>• the subscriber indicates that the original request for a certificate was not allowed and the subscriber does not grant permission retroactively;</li> <li>• the TSP has sufficient evidence that the subscriber's private key (associated with the corresponding certificate) has been compromised or there is a suspicion of compromise, inherent security weakness, or that the certificate has been misused in another way . A key is considered compromised in the event of unauthorized access or suspected unauthorized access to the private key, lost or presumably lost private key, SSCD, SUD or QSCD, stolen or presumably stolen key, SSCD, SUD or QSCD or destroyed key, SSCD, SUD or QSCD if applicable;</li> <li>• a subscriber does not fulfill his obligations as set out in this CP or the corresponding CPS of the TSP or the agreement that the TSP has with the subscriber;</li> <li>• the TSP is informed or otherwise becomes aware of a material change in the information contained in the certificate. An example of this is: change of the name of the certificate holder (service);</li> <li>• the TSP determines that the certificate has not been issued in accordance with this CP or the associated CPS of the TSP or the agreement that the TSP has with the subscriber;</li> <li>• the TSP determines that information in the certificate is incorrect or misleading;</li> <li>• the TSP ceases its activities and the CRL and OCSP services are not continued by another TSP;</li> <li>• the PA of PKIoverheid determines that the technical content of the certificate entails an irresponsible risk for subscribers, relying parties and third parties (e.g. browser parties);</li> <li>• one of the events occurs, as described in chapter 6.2 of the <a href="#">Mozilla Root Store Policy</a><sup>3</sup>.</li> </ul>
<b>Comment</b>	-

#### 4.9.2 Who can request revocation

Refer to Programme of Requirements part 3 Basic Requirements.

#### 4.9.3 Procedure for revocation request

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

#### 4.9.3-pki057 –

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

#### 4.9.4 Revocation request grace period

Refer to Programme of Requirements part 3 Basic Requirements.

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

4.9.5 Time within which CA must process the revocation request

Refer to Programme of Requirements part 3 Basic Requirements.


4.9.6 Revocation checking requirement for relying parties

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.7 CRL issuance frequency (if applicable)

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

 4.9.7-pkio65 —

<b>Description</b>	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.
<b>Comment</b>	-


4.9.8 Maximum latency for CRLs (if applicable)

Refer to Programme of Requirements part 3 Basic Requirements.


4.9.9 On-line revocation/status checking availability

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:


 4.9.9-pkio66 —

<b>Description</b>	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.
<b>Comment</b>	<p>If OCSP is offered the following requirements are applicable:</p> <ul style="list-style-type: none"> <li>• 1.1-pkio10 (basic requirement)</li> <li>• 9.5-pkio61 (basic requirement)</li> <li>• 9.9-pkio67</li> <li>• 9.9-pkio68</li> <li>• 9.5-pkio69 (basic requirement)</li> <li>• 9.9-pkio70</li> <li>• 9.9-pkio71</li> <li>• 10.2-pkio73 (basic requirement)</li> </ul> <p>NB: (EV) server certificates MUST use OCSP services as stipulated in ETSI EN 319 411-1 and the Baseline Requirements.</p>


 4.9.9-pkio67 —

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




 4.9.9-pkio68 —

<b>Description</b>	To detail the provisions of IETF RFC 6960, OCSP responses have to be signed digitally by either: <ul style="list-style-type: none"> <li>• the private (CA) key with which the certificate is signed of which the status is requested, or;</li> <li>• a responder appointed by the TSP which holds an OCSP Signing certificate issued for this purpose by the TSP, or;</li> <li>• a responder that holds an OCSP Signing certificate that falls under the hierarchy of the PKI for the government.</li> </ul>
<b>Comment</b>	-

 4.9.9-pkio70 —

<b>Description</b>	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.
<b>Comment</b>	-

 4.9.9-pkio71 —

<b>Description</b>	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.
<b>Comment</b>	-

*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.

Additional requirements:

 5.4.1-pkio80 —

<b>Description</b>	<p>Logging has to take place on at least:</p> <ul style="list-style-type: none"> <li>• Routers, firewalls and network system components;</li> <li>• Database activities and events;</li> <li>• Transactions;</li> <li>• Operating systems;</li> <li>• Access control systems;</li> <li>• Mail servers.</li> </ul> <p>At the very least, the TSP has to log the following events:</p> <ul style="list-style-type: none"> <li>• CA key life cycle management;</li> <li>• Certificate life cycle management;</li> <li>• Threats and risks such as:             <ul style="list-style-type: none"> <li>• Successful and unsuccessful attacks on the PKI system;</li> <li>• Activities of staff on the PKI system;</li> <li>• Reading, writing and deleting data;</li> <li>• Profile changes (Access Management);</li> <li>• System failure, hardware failure and other abnormalities;</li> <li>• Firewall and router activities;</li> <li>• Entering and leaving the CA space.</li> </ul> </li> </ul> <p>At the very least, the log files have to register the following:</p> <ul style="list-style-type: none"> <li>• Source addresses (IP addresses if available);</li> <li>• Destination addresses (IP addresses if available);</li> <li>• Time and date;</li> <li>• User IDs (if available);</li> <li>• Name of the incident;</li> <li>• Description of the incident.</li> </ul>
<b>Comment</b>	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*

Refer to Programme of Requirements part 3 Basic Requirements.

#### *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.

Additional requirements:

 5.7.4-pkio86 —

<p><b>Description</b></p>	<p>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:</p> <ul style="list-style-type: none"> <li>• Requirements relating to entry into force;</li> <li>• Emergency procedure/fall-back procedure;</li> <li>• Requirements relating to restarting TSP services;</li> <li>• Maintenance schedule and test plan that cover the annual testing, assessment and update of the BCP;</li> <li>• Provisions in respect of highlighting the importance of business continuity;</li> <li>• Tasks, responsibilities and competences of the involved agents;</li> <li>• Intended Recovery Time or Recovery Time Objective (RTO);</li> <li>• Recording the frequency of back-ups of critical business information and software;</li> <li>• Recording the distance of the fall-back facility to the TSP's main site; and</li> <li>• 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.</li> </ul>
<p><b>Comment</b></p>	<p>-</p>

**5.8 CA or RA termination**

Refer to Programme of Requirements part 3 Basic Requirements.

## 6. TECHNICAL SECURITY CONTROLS

### 6.1 Key pair generation and installation

#### 6.1.1 Key pair generation

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

##### 6.1.1-pkio88 –

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

##### 6.1.1-pkio89 –

<b>Description</b>	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.
<b>Comment</b>	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.

#### 6.1.2 Private key delivery to subscriber

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

##### 6.1.2-pkio94 –

<b>Description</b>	[OID 2.16.528.1.1003.1.2.2.2 and 2.16.528.1.1003.1.2.5.2], [OID 2.16.528.1.1003.1.2.2.1 and 2.16.528.1.1003.1.2.5.1] and [OID 2.16.528.1.1003.1.2.3.2 and 2.16.528.1.1003.1.2.3.1].  The certificate holder's private key has to be delivered to the certificate holder, if required through the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the certificate holder, the private key can be maintained under the certificate holder's sole control.
<b>Comment</b>	This text corresponds with ETSI EN 319 411-1 SDP 6.3.3-09, but has been integrated because this requirement only applies to signature and authenticity certificates.



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.

Additional requirements:

 6.2.3-pkio100 –

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

 6.2.3-pkio99 –

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

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.

Additional requirements:

Refer to Programme of Requirements part 3 Basic Requirements.


6.2.10 Method of destroying private key

Refer to Programme of Requirements part 3 Basic Requirements.


6.2.11 Cryptographic Module Rating

Refer to Programme of Requirements part 3 Basic Requirements.


Additional requirements:

 6.2.11-pkio104 —

<b>Description</b>	Secure devices issued or recommended by the TSP for creating electronic signatures (SSCDs or QSCDs) have to fulfil the requirements laid down in document CWA 14169 "Secure signature-creation devices or EN 419 211 for Qualified signature-creation devices "EAL 4+" and the requirements outlined in or pursuant to the Electronic Signatures Decree article 5, parts a, b, c and d.
<b>Comment</b>	The use of different types of secure devices, such as a smartcard or a USB key, is allowed. The condition is that the SSCD or QSCD meets the substantive requirements as specified in 6.2.11-pkio104, 6.2.11-pkio105 and 6.2.11-pkio106.

 6.2.11-pkio105 —

<b>Description</b>	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.
<b>Comment</b>	-

 6.2.11-pkio106 —

<b>Description</b>	The concurrence of SSCDs or QSCDs with the requirements outlined in PKIo requirement no. 6.2.11-pkio104 has to have been ratified by a government body appointed to inspect the secure devices, for the creation of electronic signatures in accordance with the Dutch Telecommunications Act (TW) article 18.17, third paragraph. In this respect, also see the Ruling on Electronic Signatures, articles 4 and 5.
<b>Comment</b>	-

### 6.3 Other aspects of key pair management

#### 6.3.1 Public key archival

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

##### 6.3.1-pkio108 —

<b>Description</b>	[OID 2.16.528.1.1003.1.2.2.2, 2.16.528.1.1003.1.2.5.2 and 2.16.528.1.1003.1.2.3.2]  The signature certificate has to be saved during the term of validity and furthermore during a period of at least seven years after the date on which the validity of the certificate expired.
<b>Comment</b>	The Electronic Signature Regulation article 2, paragraph 1i stipulates a term of seven years. No further provisions apply to the authenticity certificate and the confidentiality certificate in relation to archiving public keys.

#### 6.3.2 Certificate operational periods and key pair usage periods

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

##### 6.3.2-pkio109 —

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

### 6.4 Activation data


#### 6.4.1 Activation data generation and installation

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

##### 6.4.1-pkio112 —

<b>Description</b>	The TSP attaches activation data to the use of a SUD, SSCD or QSCD, to protect the private keys of the certificate holders.
<b>Comment</b>	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 –

<b>Description</b>	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.
<b>Comment</b>	-

*6.4.2 Activation data protection*

Refer to Programme of Requirements part 3 Basic Requirements.

*6.4.3 Other aspects of activation data*

Refer to Programme of Requirements part 3 Basic Requirements.

**6.5 Computer security controls**

*6.5.1 Specific computer security technical requirements*

Refer to Programme of Requirements part 3 Basic Requirements.

*6.5.2 Computer security rating*

Refer to Programme of Requirements part 3 Basic Requirements.

**6.6 Life cycle technical controls**

*6.6.1 System development controls*

Refer to Programme of Requirements part 3 Basic Requirements.

*6.6.2 Security management controls*

Refer to Programme of Requirements part 3 Basic Requirements.

*6.6.3 Life cycle security controls*

Refer to Programme of Requirements part 3 Basic Requirements.

**6.7 Network security controls**

*6.7.1 Network security controls (duplicate)*

Refer to Programme of Requirements part 3 Basic Requirements.

## **6.8 Time-stamping**

Refer to Programme of Requirements part 3 Basic Requirements.

## 7. CERTIFICATE, CRL, AND OCSP PROFILES

### 7.1 Certificate profile

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

#### 7.1-pkio149 —

<b>Description</b>	<p>The certificate extension Extended Key Usage MUST be present, MUST NOT be marked "critical", and MUST contain at least the following KeyPurposIds:</p> <p>For an authenticity certificate:  client Authentication =1.3.6.1.5.5.7.3.2  document Signing =1.3.6.1.4.1.311.10.3.12  emailProtection = 1.3.6.1.5.5.7.3.4</p> <p>For a signature certificate:  document Signing =1.3.6.1.4.1.311.10.3.12  emailProtection = 1.3.6.1.5.5.7.3.4  (mandatory for G3, optional for G2)</p> <p>For an confidentiality certificate:  emailProtection =1.3.6.1.5.5.7.3.4  Encrypting File System =1.3.6.1.4.1.311.10.3.4</p> <p>The KeyPurposeId id-kp-serverAuth MUST NOT be present and the KeyPurposeId id-kp-codeSigning MUST NOT be present.</p> <p>Specifically for G2 certificates any other KeyPurposeId defined in an open or accepted standard corresponding to the key usage as indicated by the KeyUsage extension MAY be present. In the G3 and following generations this extension MAY NOT be present.</p> <p>The above should take into account the EKUs included in the issuing TSP CA. If the issuing TSP CA is not provided with the mandatory EKUs stated above, these MAY NOT be included in the end-user certificate.</p>
<b>Comment</b>	-

#### 7.1-pkio173 —

<b>Description</b>	<p>The serial number of all end-user certificates must meet the following requirements:</p> <ul style="list-style-type: none"> <li>a. The value of the serial number MUST NOT be 0 (zero);</li> <li>b. The value of the serial number MUST NOT be negative;</li> <li>c. The value of the serial number MUST be unique within the population of end-user certificates issued under an issuing TSP CA;</li> <li>d. The serial number MUST have a minimum length of 96 bits (12 octets);</li> <li>e. The value of the serial number MUST contain at least 64 bits of unpredictable random data;</li> <li>f. Said random data MUST be generated by a Cryptographically Secure Pseudorandom Number Generator (CSPRNG);</li> <li>g. The serial number MUST NOT be longer than 160 bits (20 octets).</li> </ul>
<b>Comment</b>	-

*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

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

### 7.3-pkio123 —

<b>Description</b>	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".
<b>Comment</b>	-

### 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.

Additional requirements:

#### 8.4-pkio194 —

<b>Description</b>	In addition to this PoR, issuing certificates SHALL undergo an audit in accordance with the following schemes: <ul style="list-style-type: none"> <li>a. ETSI EN 319 411-1 with policy NCP+ (ETSI CP OID 0.4.0.2042.1.2, mandating usage of SSCDs) for authenticity and confidentiality certificates, and</li> <li>b. ETSI EN 319 411-2 with policy QCP-n-qscd (ETSI CP OID 0.4.0.194112.1.2, mandating usage of SSCDs) for non-repudiation certificates (eIDAS eSignatures), and</li> <li>c. CA/Browser Forum Network and Certificate System Security Requirements.</li> </ul>
<b>Comment</b>	-

#### 8.4-pkio200 —

<b>Description</b>	If the TSP issues or intends to issue qualified certificates under PKIoverheid, the following additional requirements SHALL apply: <ul style="list-style-type: none"> <li>a. the audit report states that the TSP meets the eIDAS (910/2014) regulation requirements, and</li> <li>b. the issuing certificate with which the TSP wants to issue qualified certificates is on the Trusted Services List (TSL) of Agentschap Telecom (AT).</li> </ul>
<b>Comment</b>	-

### 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

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

#### 9.2-pkio124 —

<b>Description</b>	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.
<b>Comment</b>	The third party recovery described above is based on a maximum number of certificates to be issued of 100,000 for each TSP, which is in line with the current situation. When TSPs are going to issue more certificates, it will be determined whether a suitable, higher, recoverableness will be required.

#### 9.2.1 Insurance coverage

Refer to Programme of Requirements part 3 Basic Requirements.

#### 9.2.2 Other assets

Refer to Programme of Requirements part 3 Basic Requirements.

#### 9.2.3 Insurance or warranty coverage for end-entities

Refer to Programme of Requirements part 3 Basic Requirements.

### **9.3 Confidentiality of business information**

#### *9.3.1 Scope of confidential information*

Refer to Programme of Requirements part 3 Basic Requirements.

#### *9.3.2 Information not within the scope of confidential information*

Refer to Programme of Requirements part 3 Basic Requirements.

#### *9.3.3 Responsibility to protect confidential information*

Refer to Programme of Requirements part 3 Basic Requirements.

### **9.4 Privacy of personal information**

#### *9.4.1 Privacy plan*

Refer to Programme of Requirements part 3 Basic Requirements.

#### *9.4.2 Information treated as private*

Refer to Programme of Requirements part 3 Basic Requirements.

#### *9.4.3 Information not deemed private*

Refer to Programme of Requirements part 3 Basic Requirements.

#### *9.4.4 Responsibility to protect private information*

Refer to Programme of Requirements part 3 Basic Requirements.

#### *9.4.5 Notice and consent to use private information*

Refer to Programme of Requirements part 3 Basic Requirements.

#### *9.4.6 Disclosure pursuant to judicial or administrative process*

Refer to Programme of Requirements part 3 Basic Requirements.

#### *9.4.7 Other information disclosure circumstances*

Refer to Programme of Requirements part 3 Basic Requirements.

### **9.5 Intellectual property rights**


Refer to Programme of Requirements part 3 Basic Requirements.

### **9.6 Representations and warranties**

#### *9.6.1 CA representations and warranties*

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

 9.6.1-pkio131 —

<b>Description</b>	The TSP can include in a non-repudiation certificate restrictions with regard to the use of the certificate, provided that the restrictions are clear to third parties. The TSP is not liable for losses that results from the use of a signature certificate that is contrary to the provisions in accordance with the previous sentence listed therein.
<b>Comment</b>	This article is based on Civil Code art. 196b, paragraph 3

 9.6.1-pkio132 —

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

*9.6.2 RA representations and warranties*

Refer to Programme of Requirements part 3 Basic Requirements.

*9.6.3 Subscriber representations and warranties*

Refer to Programme of Requirements part 3 Basic Requirements.

*9.6.4 Relying party representations and warranties*

Refer to Programme of Requirements part 3 Basic Requirements.

*9.6.5 Representations and warranties of other participants*

Refer to Programme of Requirements part 3 Basic Requirements.

**9.7 Disclaimers of warranties**

Refer to Programme of Requirements part 3 Basic Requirements.

**9.8 Limitations of liability**

Refer to Programme of Requirements part 3 Basic Requirements.

Additional requirements:

 9.8-pkio133 —

<b>Description</b>	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.
<b>Comment</b>	-

**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 Profiles

Profile of the certificate for the Citizen 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'.

## Citizen certificates

### Basic attributes

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Version	V	MUST be set at 2 (X.509v3).	RFC5280	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.	RFC5280	Integer	All end user certificates have to contain at least 8 bytes of unpredictable random data in the certificates serial number (SerialNumber).
Signature	V	MUST be created on the algorithm, as stipulated by the PA.	RFC5280, ETSI TS 102176	OID	MUST be the same as the field signatureAlgorithm. For certificates under the G2 and G3 root certificate, only sha-256WithRSAEncryption is allowed.
Issuer	V	MUST contain a Distinguished Name (DN). The field has the following attributes:	PKIo, RFC3739, ETSI TS 102280		Attributes other than those mentioned below MUST NOT be used.
Issuer.countryName	V	See requirements 7.1-pkio174	ETSI TS101862, X520, ISO 3166	Printable String	
Issuer.OrganizationName	V	See requirements 7.1-pkio174	ETSI TS 102280	UTF8String	
Issuer. organizationalUnitName	O	See requirements 7.1-pkio174	ETSI TS 102280: 5.2.4	UTF8String	



Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Issuer.serialNumber	O	See requirements 7.1-pkio174	RFC 3739	Printable String	
Issuer.commonName	V	See requirements 7.1-pkio174	PKIo, RFC 3739	UTF8String	The commonName attribute MUST NOT be necessary in order to identify the issuing government body (no part of the Distinguished Name, requirement from RFC 3739)
Issuer.organizationIdentifier	V/N	The organizationalIdentifier field contains an identification of the issuing CA. This field MUST be present when the field subject.organizationIdentifier is present in the TSP certificate and MUST NOT be present when this field is not present in the 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: <ul style="list-style-type: none"> <li>• 3 character legal person identity type reference;</li> <li>• 2 character ISO 3166 [2] country code;</li> <li>• hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and</li> <li>• identifier (according to country and identity type reference).</li> </ul>
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 (end user) MUST mention the subject in a unique manner. The field has the following attributes:	PKIo, RFC3739, ETSI TS 102 280		MUST contain a Distinguished Name (DN). Attributes other than those mentioned below MUST NOT be used.
Subject.countryName	V	complete C with two-letter country code in accordance with ISO 3166-1. If an official alpha-2 code is missing, the TSP MAY use the user-assigned code XX.	RFC 3739, X520, ISO 3166, PKIo	PrintableString	The country code that is used in Subject.countryName MUST correspond with the subscribers address in accordance with the accepted document or registry.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.commonName	V	The commonName attribute MUST be entered in accordance with the Naming Convention Subject.commonName paragraph shown above.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	The contents of this field MUST correspond with the name given in the GBA. The Compulsory Identification Act document or other evidence (excerpt from the population register) can be used to demonstrate this. The use of commas as punctuation in the commonName is advised against due to possible technical conflicts when processing the certificate.
Subject.Surname	V	A correct reproduction of the element of the name laid down in the CN. Based on the Compulsory Identification Act document.	RFC 3739	UTF8String	This field MUST show the subjects surname including surname prefixes correctly as shown on the Compulsory Identification Act document.
Subject.givenName	V/O	A correct reproduction of the element of the name laid down in the CN. Based on the Compulsory Identification Act document.	RFC 3739	UTF8String	This field MUST show the subjects first name(s) correctly as shown on the Compulsory Identification Act document.
Subject.stateOrProvinceName	A	The use is advised against. If present, this field MUST contain the province of the certificate holders branch in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the province MUST correspond with the certificate holders address in accordance with the GBA. The certificate holder will have to submit recent proof of his address.
Subject.localityName	A	The use is advised against. If present, this field MUST contain the location of the certificate holder in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the domicile MUST correspond with the certificate holders address in accordance with the GBA. The certificate holder will have to submit recent proof of his address.
Subject.serialNumber	V	Number to be determined by the TSP. The combination of CommonName, OrganizationName and Serialnumber MUST be unique within the context of the TSP.	RFC 3739, X 520, PKIo	Printable String	The serialnumber is intended to distinguish between subjects with the same commonName and the same OrganizationName.  To avoid susceptibilities a serial Number attribute MUST be allocated to every subject.

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	<p>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.</p> <p>In authenticity certificates the digitalSignature bit MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this.</p> <p>In confidentiality certificates, keyEncipherment and dataEncipherment bits MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this.</p> <p>In certificates for the electronic signature the non-repudiation bit MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this.</p>	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
CertificatePolicies	V	No	<p>MUST contain the OID of the Certificate Policy (CP) and the URI of the Certification Practice Statement (CPS), and MAY contain a user notice. The TSP SHOULD use UTF8String in the userNotice field, but MAY use IA5String.</p> <p>ALL certificates issued with their private key residing on an SSCD (qualified or not) SHOULD contain the ETSI NCP+ OID [0.4.0.2042.1.2]; those issued with their private key NOT residing on an SSCD (qualified or not) SHOULD contain the ETSI NCP OID [0.4.0.2042.1.1].</p> <p>Certificates issued as EU qualified certificates to natural persons with their private key residing in a QSCD, SHOULD contain an additional ETSI QCP-n-qscd OID [0.4.0.194112.1.2], or an additional ETSI QCP-n OID of [0.4.0.194112.1.0] when their private key does not reside on a QSCD.</p>	RFC 3739	OID, String, UTF8String or IA5String	<p>An overview of all Certificate Policy OIDs can be found in the document "PKIoverheid registered OIDs".</p> <p>For the Citizen domain the OIDs are:</p> <ul style="list-style-type: none"> <li>• Authenticity: 2.16.528.1.1003.1.2.3.1</li> <li>• Non-repudiation (eSignatures): 2.16.528.1.1003.1.2.3.2</li> <li>• Confidentiality: 2.16.528.1.1003.1.2.3.3</li> </ul> <p>Reference to the paragraph numbers of the PoR in the user notice is advised against because the persistency of this cannot be guaranteed (unlike the OID number of the CP).</p>
SubjectAltName	V	No	MUST be used and given a personal worldwide unique identification number.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MUST include a unique identifier in the othername attribute. Attributes other than those mentioned below MUST NOT be used.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
SubjectAltName.otherName	O		<p>MAY contain an extensions:subjectAltName extension with one or more otherName attributes in its extValue field.</p> <p>An otherName attribute is an object consisting out of a sequence of a type-id field and a value field. Each otherName attribute SHALL contain a value to uniquely identify the subject for which the other permitted subject attributes do not qualify.</p> <p>The type-id field of an otherName attribute SHALL contain one of the following OIDs:</p> <ul style="list-style-type: none"> <li>• <i>Microsoft User Principal Name (MSUPN)</i> [1.3.6.1.4.1.311.20.2.3], or</li> <li>• <i>IA5String</i> [1.3.6.1.4.1.1466.115.121.1.26] but MAY also be [2.5.5.5], or</li> <li>• <i>Permanent Identifier</i> [1.3.6.1.5.5.7.8.3] (described in RFC 4043), or</li> <li>• <i>PKIo-arc OID</i> which can be specifically assigned by the PKIo PA for this purpose (should be described in the PKIo-arc OID document).</li> </ul> <p>The value field related to otherName attribute type <i>Microsoft User Principal Name (MSUPN)</i>:</p> <ol style="list-style-type: none"> <li>1. SHALL be encoded in UTF8, and</li> <li>2. SHALL use syntax '&lt;Subscriber number&gt;@&lt;TSP OID&gt;'.</li> </ol> <p>The value field related to otherName attribute <i>IA5String</i>:</p> <ol style="list-style-type: none"> <li>1. SHALL be encoded in ISO 646 (IA5), and</li> </ol>	PKIo	See description.	Normally, otherName attribute type <i>Microsoft User Principal Name (MSUPN)</i> is used for <i>Single Sign-On (SSO)</i> purposes.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			<p>2. SHALL use syntax '&lt;TSP OID&gt;-&lt;Subscriber number&gt;'.                      The value field related to otherName attribute <i>Permanent Identifier</i> contains a PermanentIdentifier object, consisting out of a sequence of an identifierValue and an assigner field.</p> <p>The PermanentIdentifier:identifierValue field:</p> <ol style="list-style-type: none"> <li>1. SHALL be encoded in UTF8, and</li> <li>2. SHALL use syntax '&lt;Subscriber number&gt;'.</li> </ol> <p>The PermanentIdentifier:assigner field SHALL contain OID '&lt;TSP OID&gt;'.</p> <p>The value field related to otherName attribute <i>PKIo-arc OID</i> is described in the PKIo-arc OID document.</p> <p>The &lt;TSP OID&gt; consists out of an OID arc number which:</p> <ul style="list-style-type: none"> <li>• has been assigned to the TSP by the PKIo PA specifically for this usage, expanded by a number chosen by the TSP to specify its identification mechanism, and</li> <li>• is documented in the TSP CPS, and</li> <li>• is persistent.</li> </ul> <p>The &lt;Subscriber number&gt; consists out of a number which:</p> <ul style="list-style-type: none"> <li>• uniquely and permanently identifies the subject within the namespace of the corresponding OID, and</li> <li>• numbering and/or validation mechanism is described in the TSP CPS.</li> </ul>			

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
SubjectAltName.rfc822Name	A		MAY be used for the certificate holders e-mail address, for applications that need the e-mail address to be able to function properly.	RFC 5280	IA5String	<p>For PKIoverheid certificates, the use of e-mail addresses is advised against, because e-mail addresses of certificate holders often change and are susceptible to spam.</p> <p>If the e-mail address is included in the certificate, the TSP MUST:</p> <ul style="list-style-type: none"> <li>• have the subscriber sign for approval, and;</li> <li>• check whether the email address belongs to the subscriber and that the subscriber has access to the email address (for example by performing a challenge response).</li> </ul>
BasicConstraints	O	Yes	This field SHALL have its cA sub-field set to its DEFAULT value (FALSE) resulting in an encoded certificate NOT including the cA sub-field. The optional pathLenConstraint sub-field SHALL NOT be included.	RFC 5280		<p>ITU-T Recommendation X.690 (07/2002) on ASN.1 encoding rules states in Section 5.8: "The encoding of a set value or sequence value shall not include an encoding for any component value which is equal to its default value". Stating in the description that "encoded certificates do NOT include the cA sub-field" therefore is redundant. However, in the past some TSPs employed CA-issuing software which did not do proper ASN.1 encoding resulting in a wrongfully included cA sub-field in encoded certificates. This encoding error resulted in some PKIX software rejecting these certificates. This redundant information therefore has to be regarded as a cautionary hint for TSPs to check their actual certificate encoding for these errors. Chances of this encoding bug still existing in ASN.1 encoding software are however slim since the last mention of such a bug on BugZilla is from 2016.</p>



Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
CRLDistributionPoints	V	No	MUST include the URI of a CRL distribution point.	RFC 5280, ETSI TS 102 280		The reference MUST be accessible through the http or LDAP protocol. The attribute Reason MUST NOT be used, reference MUST be made to 1 CRL for all types of reasons for revocation. In addition to CRL, other types of certificate status information service MAY be supported.
ExtKeyUsage	V	No		RFC 5280		See requirement 7.1-pkio149

**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.
QcStatement	V/N	No	<p>Certificates for the electronic signature MUST indicate that they are issued as qualified certificates complying with annex I of EU regulation 920/2014. This compliance is indicated by including the <i>id-etsi-qcs-QcCompliance</i> statement in this extension.</p> <p>Certificates for the electronic signature MUST indicate that they are issued as type of certificate complying with annex I of EU regulation 920/2014. This compliance is indicated by including the <i>id-etsi-qct-esign</i> statement in this extension.</p> <p>Certificates for the electronic signature MUST indicate that the private key that is part of the public key in the certificate is saved on a qualified signature creation device (QSCD) complying with annex II of EU regulation 920/2014. This compliance is indicated by including the <i>id-etsi-qcs-QcSSCD</i> statement in this extension.</p> <p>Certificates for the electronic signature MUST contain a reference to the location of the PKI Disclosure Statement (PDS). This URL must present in the <i>id-etsi-qcs-QcPDS</i> statement in this extension.</p>	RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	<p>The aforementioned QcStatement identifiers relate to the following OIDs:</p> <ul style="list-style-type: none"> <li>id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1</li> <li>id-etsi-qct-esign { id-etsi-qcs-QcType 1 } 0.4.0.1862.1.6.1</li> <li>id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4</li> <li>id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5</li> </ul>

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			The certificates for authenticity and the certificates for confidentiality MUST NOT use this extention.			