



Programme of Requirements part 3i: Certificate Policy for certificates in Private Persons (G1) Domain

Version 4.9
Date July 1, 2021

[OID 2.16.528.1.1003.1.2.8.1] Authenticity
[OID 2.16.528.1.1003.1.2.8.2] Non repudiation
[OID 2.16.528.1.1003.1.2.8.3] Confidentiality

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	11
<i>1.1 Overview</i>	<i>11</i>
<i>1.2 Document name and identification</i>	<i>11</i>
1.2.1 Revisions	11
1.2.1.1 Version 4.0 to 4.1.....	11
1.2.1.2 Version 4.1 to 4.2.....	11
1.2.1.3 Version 4.2 to 4.3.....	11
1.2.1.4 Version 4.3 to 4.4.....	12
1.2.1.5 Version 4.4 to 4.5.....	12
1.2.1.6 Version 4.5 to 4.6.....	12
1.2.1.7 Version 4.6 to 4.7.....	12
1.2.1.8 Version 4.7 to 4.8.....	13
1.2.1.9 Version 4.8 to 4.9.....	13
1.2.2 Relevant dates.....	13
<i>1.3 PKI participants</i>	<i>14</i>
1.3.1 Certification authorities	14
1.3.2 Registration authorities	15
1.3.3 Subscribers	15
1.3.4 Relying parties.....	15
1.3.5 Other participants	15
<i>1.4 Certificate usage</i>	<i>15</i>
1.4.1 Appropriate certificate uses	15
1.4.2 Prohibited certificate uses.....	15
<i>1.5 Policy administration</i>	<i>15</i>
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>	<i>16</i>
1.6.1 Conventions	16
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	17
<i>2.1 Repositories</i>	<i>17</i>
<i>2.2 Publication of certification information</i>	<i>17</i>
<i>2.3 Time or frequency of publication</i>	<i>17</i>
<i>2.4 Access controls on repositories</i>	<i>17</i>

3. IDENTIFICATION AND AUTHENTICATION	18
<i>3.1 Naming</i>	<i>18</i>
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
<i>3.2 Initial identity validation</i>	<i>18</i>
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	19
3.2.4 Non-verified subscriber information	19
3.2.5 Validation of authority.....	19
3.2.6 Criteria for interoperation	21
<i>3.3 Identification and authentication for re-key requests.....</i>	<i>21</i>
3.3.1 Identification and authentication for routine re-key.....	21
3.3.2 Identification and authentication for re-key after revocation.....	21
<i>3.4 Identification and authentication for revocation request</i>	<i>22</i>
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	23
<i>4.1 Certificate Application.....</i>	<i>23</i>
4.1.1 Who can submit a certificate application.....	23
4.1.2 Enrollment process and responsibilities	23
<i>4.2 Certificate application processing</i>	<i>23</i>
4.2.1 Performing identification and authentication functions	23
4.2.2 Approval or rejection of certificate applications.....	23
4.2.3 Time to process certificate applications	23
<i>4.3 Certificate issuance</i>	<i>23</i>
4.3.1 CA actions during certificate issuance.....	23
4.3.2 Notification to subscriber by the CA of issuance of Certificate	23
<i>4.4 Certificate acceptance.....</i>	<i>23</i>
4.4.1 Conduct constituting certificate acceptance.....	23
4.4.2 Publication of the certificate by the CA	23
4.4.3 Notification of certificate issuance by the CA to other Entities	23
<i>4.5 Key pair and certificate usage.....</i>	<i>23</i>
4.5.1 Subscriber private key and certificate usage	23
4.5.2 Relying party public key and certificate usage	24
<i>4.6 Certificate renewal</i>	<i>24</i>
4.6.1 Circumstance for certificate renewal	24
4.6.2 Who may request renewal	24
4.6.3 Processing certificate renewal requests	24
4.6.4 Notification of new certificate issuance to subscriber	24

4.6.5	Conduct constituting acceptance of a renewal certificate	24
4.6.6	Publication of the renewal certificate by the CA	24
4.6.7	Notification of certificate issuance by the CA to other entities	24
<i>4.7</i>	<i>Certificate re-key</i>	<i>24</i>
4.7.1	Circumstance for certificate re-key	24
4.7.2	Who may request certification of a new public key	24
4.7.3	Processing certificate re-keying requests	24
4.7.4	Notification of new certificate issuance to subscriber	24
4.7.5	Conduct constituting acceptance of a re-keyed certificate	24
4.7.6	Publication of the re-keyed certificate by the CA	25
4.7.7	Notification of certificate issuance by the CA to other entities	25
<i>4.8</i>	<i>Certificate modification</i>	<i>25</i>
4.8.1	Circumstance for certificate modification	25
4.8.2	Who may request certificate modification	25
4.8.3	Processing certificate modification requests	25
4.8.4	Notification of new certificate issuance to subscriber	25
4.8.5	Conduct constituting acceptance of modified certificate	25
4.8.6	Publication of the modified certificate by the CA	25
4.8.7	Notification of certificate issuance by the CA to other entities	25
<i>4.9</i>	<i>Certificate revocation and suspension</i>	<i>25</i>
4.9.1	Circumstances for revocation	25
4.9.2	Who can request revocation.....	26
4.9.3	Procedure for revocation request.....	26
4.9.4	Revocation request grace period.....	26
4.9.5	Time within which CA must process the revocation request	26
4.9.6	Revocation checking requirement for relying parties.....	27
4.9.7	CRL issuance frequency (if applicable).....	27
4.9.8	Maximum latency for CRLs (if applicable)	27
4.9.9	On-line revocation/status checking availability	27
4.9.10	On-line revocation checking requirements.....	28
4.9.11	Other forms of revocation advertisements available.....	28
4.9.12	Special requirements related to key compromise	28
4.9.13	Circumstances for suspension	28
4.9.14	Who can request suspension	28
4.9.15	Procedure for suspension request	28
4.9.16	Limits on suspension period	28
<i>4.10</i>	<i>Certificate status services.....</i>	<i>28</i>
4.10.1	Operational characteristics.....	28
4.10.2	Service availability	29
4.10.3	Optional features.....	29
<i>4.11</i>	<i>End of subscription</i>	<i>29</i>
<i>4.12</i>	<i>Key escrow and recovery.....</i>	<i>29</i>
4.12.1	Key escrow and recovery policy and practices.....	29
4.12.2	Session key encapsulation and recovery policy and practices	29
5.	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	30

<i>5.1 Physical controls</i>	30
5.1.1 Site location and construction	30
5.1.2 Physical access	30
5.1.3 Power and air conditioning.....	30
5.1.4 Water exposures	30
5.1.5 Fire prevention and protection	30
5.1.6 Media storage.....	30
5.1.7 Waste disposal.....	30
5.1.8 Off-site backup	30
<i>5.2 Procedural controls</i>	30
5.2.1 Trusted roles	30
5.2.2 Number of persons required per task	30
5.2.3 Identification and authentication for each role	30
5.2.4 Roles requiring separation of duties	30
<i>5.3 Personnel controls</i>	31
5.3.1 Qualifications, experience, and clearance requirements	31
5.3.2 Background check procedures.....	31
5.3.3 Training requirements	31
5.3.4 Retraining frequency and requirements	31
5.3.5 Job rotation frequency and sequence	31
5.3.6 Sanctions for unauthorized actions	31
5.3.7 Independent contractor requirements	31
5.3.8 Documentation supplied to personnel.....	31
<i>5.4 Audit logging procedures</i>	31
5.4.1 Types of events recorded.....	31
5.4.2 Frequency of processing log.....	32
5.4.3 Retention period for audit log.....	32
5.4.4 Protection of audit log	32
5.4.5 Audit log backup procedures	32
5.4.6 Audit collection system (internal vs. external)	32
5.4.7 Notification to event-causing subject.....	32
5.4.8 Vulnerability assessments.....	33
<i>5.5 Records archival</i>	33
5.5.1 Types of records archived	33
5.5.2 Retention period for archive.....	33
5.5.3 Protection of archive.....	33
5.5.4 Archive backup procedures	33
5.5.5 Requirements for time-stamping of records	33
5.5.6 Archive collection system (internal or external)	33
5.5.7 Procedures to obtain and verify archive information	33
<i>5.6 Key changeover</i>	33
<i>5.7 Compromise and disaster recovery</i>	33
5.7.1 Incident and compromise handling procedures	33
5.7.2 Computing resources, software, and_or data are corrupted.....	33
5.7.3 Entity private key compromise procedures.....	34
5.7.4 Business continuity capabilities after a disaster	34

5.8 CA or RA termination.....	34
6. TECHNICAL SECURITY CONTROLS.....	35
6.1 Key pair generation and installation.....	35
6.1.1 Key pair generation	35
6.1.2 Private key delivery to subscriber	35
6.1.3 Public key delivery to certificate issuer	35
6.1.4 CA public key delivery to relying parties	35
6.1.5 Key sizes.....	36
6.1.6 Public key parameters generation and quality checking	36
6.1.7 Key usage purposes (as per X.509 v3 key usage field)	36
6.2 Private Key Protection and Cryptographic Module Engineering Controls.....	36
6.2.1 Cryptographic module standards and controls	36
6.2.2 Private key (n out of m) multi-person control	36
6.2.3 Private key escrow	36
6.2.4 Private key backup	36
6.2.5 Private key archival	36
6.2.6 Private key transfer into or from a cryptographic module	36
6.2.7 Private key storage on cryptographic module	36
6.2.8 Method of activating private key.....	37
6.2.9 Method of deactivating private key	37
6.2.10 Method of destroying private key.....	37
6.2.11 Cryptographic Module Rating.....	37
6.3 Other aspects of key pair management.....	37
6.3.1 Public key archival.....	37
6.3.2 Certificate operational periods and key pair usage periods	38
6.4 Activation data	38
6.4.1 Activation data generation and installation	38
6.4.2 Activation data protection.....	38
6.4.3 Other aspects of activation data	38
6.5 Computer security controls.....	39
6.5.1 Specific computer security technical requirements	39
6.5.2 Computer security rating.....	39
6.6 Life cycle technical controls	39
6.6.1 System development controls	39
6.6.2 Security management controls.....	39
6.6.3 Life cycle security controls.....	39
6.7 Network security controls.....	39
6.7.1 Network security controls (duplicate)	39
6.8 Time-stamping	39
7. CERTIFICATE, CRL, AND OCSP PROFILES	40
7.1 Certificate profile	40
7.1.1 Version number(s).....	41

7.1.2 Certificate extensions	41
7.1.3 Algorithm object identifiers.....	41
7.1.4 Name forms	41
7.1.5 Name constraints	41
7.1.6 Certificate policy object identifier.....	41
7.1.7 Usage of Policy Constraints extension.....	41
7.1.8 Policy qualifiers syntax and semantics.....	41
7.1.9 Processing semantics for the critical Certificate Policies extension	41
<i>7.2 CRL profile</i>	<i>41</i>
7.2.1 Version number(s).....	41
7.2.2 CRL and CRL entry extensions.....	42
<i>7.3 OCSP profile.....</i>	<i>42</i>
7.3.1 Version number(s).....	42
7.3.2 OCSP extensions	42
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	43
<i>8.1 Frequency or circumstances of assessment.....</i>	<i>43</i>
<i>8.2 Identity/qualifications of assessor</i>	<i>43</i>
<i>8.3 Assessors relationship to assessed entity</i>	<i>43</i>
<i>8.4 Topics covered by assessment</i>	<i>43</i>
<i>8.5 Actions taken as a result of deficiency.....</i>	<i>43</i>
<i>8.6 Communication of results.....</i>	<i>43</i>
9. OTHER BUSINESS AND LEGAL MATTERS	44
<i>9.1 Fees.....</i>	<i>44</i>
9.1.1 Certificate issuance or renewal fees	44
9.1.2 Certificate access fees.....	44
9.1.3 Revocation or status information access fees	44
9.1.4 Fees for other services	44
9.1.5 Refund policy	44
<i>9.2 Financial responsibility.....</i>	<i>44</i>
9.2.1 Insurance coverage	44
9.2.2 Other assets	44
9.2.3 Insurance or warranty coverage for end-entities	44
<i>9.3 Confidentiality of business information</i>	<i>44</i>
9.3.1 Scope of confidential information.....	44
9.3.2 Information not within the scope of confidential information.....	45
9.3.3 Responsibility to protect confidential information	45
<i>9.4 Privacy of personal information</i>	<i>45</i>
9.4.1 Privacy plan.....	45
9.4.2 Information treated as private	45
9.4.3 Information not deemed private	45
9.4.4 Responsibility to protect private information	45
9.4.5 Notice and consent to use private information	45

9.4.6 Disclosure pursuant to judicial or administrative process.....	45
9.4.7 Other information disclosure circumstances	45
<i>9.5 Intellectual property rights</i>	<i>45</i>
<i>9.6 Representations and warranties</i>	<i>45</i>
9.6.1 CA representations and warranties	45
9.6.2 RA representations and warranties	46
9.6.3 Subscriber representations and warranties.....	46
9.6.4 Relying party representations and warranties	46
9.6.5 Representations and warranties of other participants	46
<i>9.7 Disclaimers of warranties</i>	<i>46</i>
<i>9.8 Limitations of liability</i>	<i>47</i>
<i>9.9 Indemnities.....</i>	<i>47</i>
<i>9.10 Term and termination</i>	<i>47</i>
9.10.1 Term.....	47
9.10.2 Termination	47
9.10.3 Effect of termination and survival	47
<i>9.11 Individual notices and communications with participants</i>	<i>47</i>
<i>9.12 Amendments</i>	<i>47</i>
9.12.1 Procedure for amendment	47
9.12.2 Notification mechanism and period	47
9.12.3 Circumstances under which OID must be changed	47
<i>9.13 Dispute resolution provisions</i>	<i>47</i>
<i>9.14 Governing law.....</i>	<i>47</i>
<i>9.15 Compliance with applicable law</i>	<i>47</i>
<i>9.16 Miscellaneous provisions</i>	<i>48</i>
9.16.1 Entire agreement	48
9.16.2 Assignment	48
9.16.3 Severability	48
9.16.4 Enforcement (attorneys' fees and waiver of rights)	48
9.16.5 Force Majeure	48
<i>9.17 Other provisions.....</i>	<i>48</i>
Appendix A: Certificate Profile	49
<i>Personal certificates – Private Persons Domain</i>	<i>50</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 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 changes to the following requirements:
 - 3.1.3-pkio11;
 - 3.2.5-pkio32;
 - 5.7.4-pkio86;
 - 9.6.1-pkio131.

1.2.1.2 Version 4.1 to 4.2

New

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

Modifications

None.

Editorial

None.

1.2.1.3 Version 4.2 to 4.3

New

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

Modifications

- Description with attribute CertificatePolicies (effective date 1-7-2016);
- Removal optional use KeyAgreement with Key Usage (effective date no later than 4 weeks after publication of PoR 4.3);
- Mandatory QcStatement 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 BasicConstraints field no longer permitted in end entity certificates (effective date 1-7-2016);
- ETSI TS 102 042 replaced by ETSI EN 319 411-1 (effective date 1-7-2016 or when the accreditation to the certifying body has been granted with a final date of 30 June 2017).

Editorial

None.

1.2.1.4 Version 4.3 to 4.4

New

None.

Modifications

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

Editorial

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

1.2.1.5 Version 4.4 to 4.5

New

- Possibility to offer CPS in English and/or Dutch (requirement 2.2-pkio157, effective date 1-10-2017).

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 2.16.528.1.1003.1.2.8.1 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 references to the public G1 root from the certificate profile, modified text to private G1 root.

1.2.1.6 Version 4.5 to 4.6

New

None.

Modifications

- Modified reference to ETSI certificate profiles (effective date directly after publication of PoR 4.6);
- Corrected subjectAltName.othername field (effective date directly after publication of PoR 4.6).

Editorial

None.

1.2.1.7 Version 4.6 to 4.7

New

- Requirement 3.2.5-pkio160, list of limitative professions transferred (from PoR part 4) (effective date immediately after publication of PoR 4.7);
- Requirement 7.1-pkio177 (effective date immediately after publication of PoR 4.7).

Modifications

- Authentic proof for practicing a recognized profession merged in requirement 3.2.5-pki29 (effective date immediately after publication of PoR 4.7);
- Limitative list of professions updated, "municipal" tax bailiff (effective date immediately after publication of PoR 4.7);
- Description of a number of certificate attributes replaced by reference to requirement 7.1-pki174 (effective date 8 weeks after publication of 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-pki88, 6.2.11-pki104, 6.2.11-pki105, 6.2.11-pki106, 6.4.1-pki112 and 4.9.1-pki52 (effective date immediately after publication PoR 4.7).

Editorial

None.

1.2.1.8 Version 4.7 to 4.8

New

- Requirement 3.2.2-pki186 on (re)validation of organizational data (effective date immediately after publication of PoR 4.8).

Modifications

- Change in serial number requirements in requirement 7.1-pki177 (effective date August 29, 2019);
- Requirement 9.17-pki139 removed (effective date immediately after publication of PoR 4.8).

Editorial

- Reference to ETSI TS 101 456 7.2.8.d changed to 411-1 in requirement 6.1.2-pki94 (effective date immediately after publication of PoR 4.8);
- Changed definition of private key in requirement 4.9.1-pki52 (effective date immediately after publication of PoR 4.8);
- Changed reference in requirement 4.9.9-pki68 (effective date immediately after publication of PoR 4.8).

1.2.1.9 Version 4.8 to 4.9

New

- Requirement 8.1-pki189, 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-pki187 (effective date 02-17-2020).

Modifications

- Requirement 2.2-pki157 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 6.1.1-pki87 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 6.2.3-pki101 has been removed (effective date immediately after publication PoR 4.9).

Editorial

- Changed in the certificate profiles the criteria and description for basic attribute "subject.title" from O to V/N (effective date 02-12-2021).

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
QuoVadis PKIoverheid Private Personen CA - G1	 03 Nov 2016	 12 Nov 2028	6291493416790648338	A5F7150BC358D1498BFDD 8EB39732362DCB6A903F5 7451B930363BDFAF835BA 4

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 from certificate holders who act on behalf of the subscriber.

[OID 2.16.528.1.1003.1.2.8.1]

Authenticity certificates, which are issued under this CP, can be used to reliably identify and authenticate persons, organizations and resources electronically. This concerns both the mutual identification of people and identification between people and computerized devices.

Under this OID OSCP responder certificates may be issued for use within the domain Private Persons. Said certificates can be used to sign OSCP 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 2.16.528.1.1003.1.2.8.2]

Signature certificates, which are issued under this CP, can be used to verify electronic signatures, that have "the same legal consequences as a handwritten signature", as stated in article 15a, first and second paragraphs, in Title 1 of Book 3 of the Dutch 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 2.16.528.1.1003.1.2.8.3]

Confidentiality certificates, which are issued under this CP, can be used to protect the confidentiality of data that is exchanged and/or stored in an 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.nl¹

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.


¹ <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

 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

3.1.3-pkio11 —

Description	Pseudonyms MUST NOT be used in certificates.
Comment	-

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

3.2.2-pkio14 —

Description	When issuing organization-linked certificates the TSP has to verify that the subscriber is an existing organization.
Comment	-


3.2.2-pkio16 —

Description	In terms of organization-linked certificates, the TSP has to verify that the name of the organization registered by the subscriber that is incorporated in the certificate is correct and complete.
Comment	-

 3.2.2-pkio186 —

Description	<p>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.</p> <p>In both cases, the existing certificate must be withdrawn because the data in the certificate no longer conforms to the originally validated data.</p>
Comment	-

3.2.3 Authentication of individual identity


 3.2.3-pkio21 —

Description	<p>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).</p>
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-pkio160 —

Description	<p>The restrictive list of recognized professions for which professional certificates can be issued is as follows:</p> <ul style="list-style-type: none"> • Accountant-Administratieconsulent (Accountant-Administration Officer); • Advocaat (Lawyer); • Octrooigemachtigde (Patent Agent); • Registerloods (Marine pilot); • Those who have been entered into a register as meant in article 3 of the Professions in the individual healthcare Act (Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)); • Those who practice a profession of which the education is mandated through article 34, section 1 and article 36a of the Professions in the individual healthcare Act (Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)); • Notaris (Civil Law Notary); • Kandidaat notaris (Junior Civil Law Notary); • Toegevoegd Notaris (Added Notary); • Gerechtsdeurwaarder (Court Bailiff); • Waarnemend gerechtsdeurwaarder (Acting Court Bailiff); • Toegevoegd gerechtsdeurwaarder (Additional Court Bailiff); • Kandidaat gerechtsdeurwaarder (Junior Court Bailiff); • Registeraccountant (Registered Accountant); • Dierenarts (Veterinary Surgeon); • Zeevarende (Seafarer); • (Hoofd)bewaarder ((Head) Registrar); • Gemandateerd bewaarder Mandated Registrar; • Technisch Medewerker schepen (Ships Technician); • Inspecteur Scheepsregistraties (Ship Registration Inspector); • Belastingdeurwaarder (Government-appointed Tax Bailiff); • Rijksdeurwaarder (Government Bailiff); • Gemeentelijk Belastingdeurwaarder (Municipal Tax Bailiff).
Comment	-

 3.2.5-pkio29 —

Description	<p>In terms of organization-linked certificate holders, the TSP has to check that:</p> <ul style="list-style-type: none"> • the proof that the certificate holder, authorized to receive a certificate on behalf of the subscriber, is authentic; • the name and identity markers mentioned in this proof correspond with the certificate holder's identity established under 3.2.3-pkio21. <p>In terms of profession-linked certificate holders, the TSP has to check that:</p> <ul style="list-style-type: none"> • the proof, that the certificate holder is authorised to practise the recognized profession, is authentic; • the name and identity markers mentioned in this proof correspond with the certificate holder's identity established under 3.2.3-pkio21.
--------------------	---

Comment	<p>Only considered to be authentic proof for practising a recognized profession is:</p> <ul style="list-style-type: none"> a. either a valid proof of registration in a (professional) register recognized by the relevant professional group, to which disciplinary rules stipulated by law apply; b. or an appointment by a Minister; c. or valid proof (e.g. a permit) that the legal requirements in relation to practising a profession, are fulfilled. d. or an appointment by a municipal official or mayor (only in case of municipal tax bailiff). <p>Understood to be meant by valid proof is proof that has not expired or that has not (temporarily or provisionally) been revoked.</p> <p>PoR requirement 3.2.5-pkio160 contains a limitative list of the professions referred to under a, b, and c.</p> <p>In the reference matrix in appendix B there is a reference to all requirements that relate to paragraph 3.2.3.</p>
----------------	---

 3.2.5-pkio32 —

Description	<p>Subscriber is a legal personality (organization-linked certificates):</p> <p>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 that have been made to the relationship between the subscriber and the certificate holder, by means of a revocation request. Relevant changes can, in this respect, for instance be termination of employment and suspension.</p> <p>Subscriber is a natural person (occupation-linked certificates):</p> <p>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 that have been made by means of a revocation request. A relevant change in this respect is, in any case, no longer having legal proof as outlined in 3.2.5-pkio29.</p>
Comment	-

3.2.6 Criteria for interoperation

Refer to Programme of Requirements part 3 Basic Requirements.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Refer to Programme of Requirements part 3 Basic Requirements.

3.3.2 Identification and authentication for re-key after revocation

Refer to Programme of Requirements part 3 Basic Requirements.

3.4 Identification and authentication for revocation request

Refer to Programme of Requirements part 3 Basic Requirements.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 *Who can submit a certificate application*

Refer to Programme of Requirements part 3 Basic Requirements.

4.1.2 *Enrollment process and responsibilities*

Refer to Programme of Requirements part 3 Basic Requirements.

4.2 Certificate application processing

4.2.1 *Performing identification and authentication functions*

Refer to Programme of Requirements part 3 Basic Requirements.

4.2.2 *Approval or rejection of certificate applications*

Refer to Programme of Requirements part 3 Basic Requirements.

4.2.3 *Time to process certificate applications*

Refer to Programme of Requirements part 3 Basic Requirements.

4.3 Certificate issuance

4.3.1 *CA actions during certificate issuance*

Refer to Programme of Requirements part 3 Basic Requirements.

4.3.2 *Notification to subscriber by the CA of issuance of Certificate*

Refer to Programme of Requirements part 3 Basic Requirements.

4.4 Certificate acceptance

4.4.1 *Conduct constituting certificate acceptance*

Refer to Programme of Requirements part 3 Basic Requirements.

4.4.2 *Publication of the certificate by the CA*

Refer to Programme of Requirements part 3 Basic Requirements.

4.4.3 *Notification of certificate issuance by the CA to other Entities*

Refer to Programme of Requirements part 3 Basic Requirements.

4.5 Key pair and certificate usage

4.5.1 *Subscriber private key and certificate usage*

Refer to Programme of Requirements part 3 Basic Requirements.

4.5.2 Relying party public key and certificate usage

Refer to Programme of Requirements part 3 Basic Requirements.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.2 Who may request renewal

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.3 Processing certificate renewal requests

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.4 Notification of new certificate issuance to subscriber

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.5 Conduct constituting acceptance of a renewal certificate

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.6 Publication of the renewal certificate by the CA

Refer to Programme of Requirements part 3 Basic Requirements.

4.6.7 Notification of certificate issuance by the CA to other entities

Refer to Programme of Requirements part 3 Basic Requirements.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.2 Who may request certification of a new public key

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.3 Processing certificate re-keying requests

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.4 Notification of new certificate issuance to subscriber

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.6 Publication of the re-keyed certificate by the CA

Refer to Programme of Requirements part 3 Basic Requirements.

4.7.7 Notification of certificate issuance by the CA to other entities

Refer to Programme of Requirements part 3 Basic Requirements.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.2 Who may request certificate modification

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.3 Processing certificate modification requests

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.4 Notification of new certificate issuance to subscriber

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.5 Conduct constituting acceptance of modified certificate

Refer to Programme of Requirements part 3 Basic Requirements.

4.8.6 Publication of the modified certificate by the CA


Refer to Programme of Requirements part 3 Basic Requirements.

4.8.7 Notification of certificate issuance by the CA to other entities

Refer to Programme of Requirements part 3 Basic Requirements.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

 4.9.1-pkio52 —

Description	<p>Certificates must be revoked when:</p> <ul style="list-style-type: none"> • the subscriber states that the original request for a certificate was not allowed and the subscriber does not provide consent with retrospective force; • the TSP has sufficient proof that the subscriber's private key (that corresponds with the public key in the certificate) is compromised or if compromise is suspected, or if there is inherent security vulnerability, or if the certificate has been misused in any other way. A key is considered to be compromised in the event of unauthorized access or suspected unauthorized access to the private key, if the private key, SSCD, SUD or QSCD, is lost or suspected to be lost, if the key, SSCD, SUD or QSCD, is stolen or suspected to be stolen, or if the key or SSCD, SUD or QSCD is destroyed; • a subscriber does not fulfil its obligations outlined in this CP or the corresponding CPS of the TSP or the agreement that the TSP has entered into with the subscriber; • the TSP is informed or otherwise becomes aware of a substantial change in the information that is provided in the certificate. An example of that is: a change in the name of the certificate holder; • the TSP determines that the certificate has not been issued in line with this CP or the corresponding CPS of the TSP or the agreement that the TSP has entered into with the subscriber; • the TSP determines that information in the certificate is incorrect or misleading; • the TSP ceases its work and the CRL and OCSP services are not taken over by a different TSP. • the PA of PKIoverheid determines that the technical content of the certificate entails an irresponsible risk to subscribers, relying parties and third parties (e.g. browser parties).
Comment	<p>In addition, certificates can be revoked as a measure to prevent or to combat an emergency. Considered to be an emergency is definitely the compromise or suspected compromise of the private key of the TSP used to sign certificates.</p>

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

4.9.4 Revocation request grace period

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.5 Time within which CA must process the revocation request

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.6 Revocation checking requirement for relying parties

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.7 CRL issuance frequency (if applicable)

4.9.7-pkio65 —

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

4.9.8 Maximum latency for CRLs (if applicable)

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.9 On-line revocation/status checking availability

4.9.9-pkio66 —

Description	The revocation management services of the TSP can support the Online Certificate Status Protocol (OCSP) as an addition to the publication of CRL information. If this support is available, this has to be stated in the CPS.
Comment	<p>If OCSP is offered the following requirements are applicable:</p> <ul style="list-style-type: none"> • 1.1-pkio10 (basic requirement) • 9.5-pkio61 (basic requirement) • 9.9-pkio67 • 9.9-pkio68 • 9.5-pkio69 (basic requirement) • 9.9-pkio70 • 9.9-pkio71 • 10.2-pkio73 (basic requirement) <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 —

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


4.9.9-pkio68 —

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

Comment	-
----------------	---

 4.9.9-pkio70 –

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

 4.9.9-pkio71 –

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

4.9.10 On-line revocation checking requirements

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.11 Other forms of revocation advertisements available

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.12 Special requirements related to key compromise

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.13 Circumstances for suspension

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.14 Who can request suspension

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.15 Procedure for suspension request

Refer to Programme of Requirements part 3 Basic Requirements.

4.9.16 Limits on suspension period

Refer to Programme of Requirements part 3 Basic Requirements.

4.10 Certificate status services

4.10.1 Operational characteristics

Refer to Programme of Requirements part 3 Basic Requirements.

4.10.2 Service availability

Refer to Programme of Requirements part 3 Basic Requirements.

4.10.3 Optional features

Refer to Programme of Requirements part 3 Basic Requirements.

4.11 End of subscription

Refer to Programme of Requirements part 3 Basic Requirements.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Refer to Programme of Requirements part 3 Basic Requirements.

4.12.2 Session key encapsulation and recovery policy and practices

Refer to Programme of Requirements part 3 Basic Requirements.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 *Site location and construction*

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.2 *Physical access*

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.3 *Power and air conditioning*

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.4 *Water exposures*

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.5 *Fire prevention and protection*

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.6 *Media storage*

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.7 *Waste disposal*

Refer to Programme of Requirements part 3 Basic Requirements.

5.1.8 *Off-site backup*

Refer to Programme of Requirements part 3 Basic Requirements.

5.2 Procedural controls

5.2.1 *Trusted roles*

Refer to Programme of Requirements part 3 Basic Requirements.

5.2.2 *Number of persons required per task*

Refer to Programme of Requirements part 3 Basic Requirements.

5.2.3 *Identification and authentication for each role*

Refer to Programme of Requirements part 3 Basic Requirements.

5.2.4 *Roles requiring separation of duties*

Refer to Programme of Requirements part 3 Basic Requirements.

5.3 Personnel controls

5.3.1 *Qualifications, experience, and clearance requirements*

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.2 *Background check procedures*

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.3 *Training requirements*

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.4 *Retraining frequency and requirements*

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.5 *Job rotation frequency and sequence*

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.6 *Sanctions for unauthorized actions*

Refer to Programme of Requirements part 3 Basic Requirements.

5.3.7 *Independent contractor requirements*


Refer to Programme of Requirements part 3 Basic Requirements.

5.3.8 *Documentation supplied to personnel*

Refer to Programme of Requirements part 3 Basic Requirements.

5.4 Audit logging procedures

5.4.1 *Types of events recorded*

 5.4.1-pki080 —

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

5.4.2 Frequency of processing log

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.3 Retention period for audit log

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.4 Protection of audit log

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.5 Audit log backup procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.6 Audit collection system (internal vs. external)

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.7 Notification to event-causing subject

Refer to Programme of Requirements part 3 Basic Requirements.

5.4.8 Vulnerability assessments

Refer to Programme of Requirements part 3 Basic Requirements.

5.5 Records archival

5.5.1 Types of records archived

5.5.1-pkio82 —

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

5.5.2 Retention period for archive

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.3 Protection of archive

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.4 Archive backup procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.5 Requirements for time-stamping of records

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.6 Archive collection system (internal or external)

Refer to Programme of Requirements part 3 Basic Requirements.

5.5.7 Procedures to obtain and verify archive information

Refer to Programme of Requirements part 3 Basic Requirements.

5.6 Key changeover

Refer to Programme of Requirements part 3 Basic Requirements.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.7.2 Computing resources, software, and_or data are corrupted

Refer to Programme of Requirements part 3 Basic Requirements.

5.7.3 Entity private key compromise procedures

Refer to Programme of Requirements part 3 Basic Requirements.

5.7.4 Business continuity capabilities after a disaster

5.7.4-pkio86 —

Description	<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"> • Requirements relating to entry into force; • Emergency procedure/fall-back procedure; • Requirements relating to restarting TSP services; • Maintenance schedule and test plan that cover the annual testing, assessment and update of the BCP; • Provisions in respect of highlighting the importance of business continuity; • Tasks, responsibilities and competences of the involved agents; • Intended Recovery Time or Recovery Time Objective (RTO); • Recording the frequency of back-ups of critical business information and software; • Recording the distance of the fall-back facility to the TSP's main site; and • Recording the procedures for securing the facility during the period following a security breach or emergency and for the organization of a secure environment at the main site or fall-back facility.
Comment	-

5.8 CA or RA termination

Refer to Programme of Requirements part 3 Basic Requirements.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1-pkio88 —

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

6.1.1-pkio89 —

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

6.1.2 Private key delivery to subscriber

6.1.2-pkio94 —

Description	[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.
Comment	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

6.2.3-pkio100 —

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

6.2.3-pkio99 —

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

6.2.4 Private key backup

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.5 Private key archival

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.6 Private key transfer into or from a cryptographic module

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.7 Private key storage on cryptographic module

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.8 Method of activating private key

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.9 Method of deactivating private key

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.10 Method of destroying private key

Refer to Programme of Requirements part 3 Basic Requirements.

6.2.11 Cryptographic Module Rating

6.2.11-pkio104 —

Description	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.
Comment	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 —

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

6.2.11-pkio106 —

Description	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.
Comment	-

6.3 Other aspects of key pair management

6.3.1 Public key archival

6.3.1-pkio108 —

Description	[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.
Comment	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

6.3.2-pkio109 –

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

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.1-pkio112 –

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

6.4.1-pkio113 –

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

6.4.2 Activation data protection

Refer to Programme of Requirements part 3 Basic Requirements.

6.4.3 Other aspects of activation data

Refer to Programme of Requirements part 3 Basic Requirements.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Refer to Programme of Requirements part 3 Basic Requirements.

6.5.2 Computer security rating

Refer to Programme of Requirements part 3 Basic Requirements.

6.6 Life cycle technical controls

6.6.1 System development controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.6.2 Security management controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.6.3 Life cycle security controls

Refer to Programme of Requirements part 3 Basic Requirements.

6.7 Network security controls

6.7.1 Network security controls (duplicate)

Refer to Programme of Requirements part 3 Basic Requirements.

6.8 Time-stamping

Refer to Programme of Requirements part 3 Basic Requirements.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1-pkio149 —

Description	<p>The certificate extension Extended Key Usage MUST be present, MUST NOT be marked "critical", and MUST contain at least the following KeyPurposeIds:</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>
Comment	-

7.1-pkio177 —

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

7.1.1 Version number(s)

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.2 Certificate extensions

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.3 Algorithm object identifiers

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.4 Name forms

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.5 Name constraints

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.6 Certificate policy object identifier

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.7 Usage of Policy Constraints extension

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.8 Policy qualifiers syntax and semantics

Refer to Programme of Requirements part 3 Basic Requirements.

7.1.9 Processing semantics for the critical Certificate Policies extension

Refer to Programme of Requirements part 3 Basic Requirements.

7.2 CRL profile

7.2.1 Version number(s)

Refer to Programme of Requirements part 3 Basic Requirements.

7.2.2 CRL and CRL entry extensions

Refer to Programme of Requirements part 3 Basic Requirements.

7.3 OCSP profile

 7.3-pkio123 —

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

9

7.3.1 Version number(s)

Refer to Programme of Requirements part 3 Basic Requirements.

7.3.2 OCSP extensions

Refer to Programme of Requirements part 3 Basic Requirements.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

Refer to Programme of Requirements part 3 Basic Requirements.

8.2 Identity/qualifications of assessor

Refer to Programme of Requirements part 3 Basic Requirements.

8.3 Assessors relationship to assessed entity

Refer to Programme of Requirements part 3 Basic Requirements.

8.4 Topics covered by assessment

Refer to Programme of Requirements part 3 Basic Requirements.

8.5 Actions taken as a result of deficiency

Refer to Programme of Requirements part 3 Basic Requirements.

8.6 Communication of results

Refer to Programme of Requirements part 3 Basic Requirements.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Refer to Programme of Requirements part 3 Basic Requirements.

9.1.2 Certificate access fees

Refer to Programme of Requirements part 3 Basic Requirements.

9.1.3 Revocation or status information access fees

Refer to Programme of Requirements part 3 Basic Requirements.


9.1.4 Fees for other services

Refer to Programme of Requirements part 3 Basic Requirements.

9.1.5 Refund policy

Refer to Programme of Requirements part 3 Basic Requirements.

9.2 Financial responsibility

 9.2-pkio124 —

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

9.2.1 Insurance coverage

Refer to Programme of Requirements part 3 Basic Requirements.

9.2.2 Other assets

Refer to Programme of Requirements part 3 Basic Requirements.

9.2.3 Insurance or warranty coverage for end-entities

Refer to Programme of Requirements part 3 Basic Requirements.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Refer to Programme of Requirements part 3 Basic Requirements.

9.3.2 Information not within the scope of confidential information

Refer to Programme of Requirements part 3 Basic Requirements.

9.3.3 Responsibility to protect confidential information

Refer to Programme of Requirements part 3 Basic Requirements.

9.4 Privacy of personal information

9.4.1 Privacy plan

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.2 Information treated as private

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.3 Information not deemed private

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.4 Responsibility to protect private information

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.5 Notice and consent to use private information

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.6 Disclosure pursuant to judicial or administrative process

Refer to Programme of Requirements part 3 Basic Requirements.

9.4.7 Other information disclosure circumstances

Refer to Programme of Requirements part 3 Basic Requirements.

9.5 Intellectual property rights

Refer to Programme of Requirements part 3 Basic Requirements.


9.6 Representations and warranties

9.6.1 CA representations and warranties


9.6.1-pkio127 —

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: <ul style="list-style-type: none">a. for "a qualified certificate specified in article 1.1, division ss Telecommunications Act": "an authenticity certificate" is read;b. for "signatory": "certificate holder" is read;c. for "electronic signatures": "authenticity properties" is read.
-------------	---


Comment	-
----------------	---

 9.6.1-pkio129 —

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: <ol style="list-style-type: none"> a. for "a qualified certificate specified in article 1.1, division ss Telecommunications Act": "a confidentiality certificate" is read; b. for "signatory": "certificate holder" is read; c. for "creation of electronic signatures": "creation of encrypted data" is read; d. For "verification of electronic signatures": "decoding of encrypted data" is read.
Comment	-

 9.6.1-pkio131 —

Description	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.
Comment	This article is based on Civil Code art. 196b, paragraph 3

 9.6.1-pkio132 —

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

9.6.2 RA representations and warranties

Refer to Programme of Requirements part 3 Basic Requirements.

9.6.3 Subscriber representations and warranties

Refer to Programme of Requirements part 3 Basic Requirements.

9.6.4 Relying party representations and warranties

Refer to Programme of Requirements part 3 Basic Requirements.

9.6.5 Representations and warranties of other participants

Refer to Programme of Requirements part 3 Basic Requirements.

9.7 Disclaimers of warranties

Refer to Programme of Requirements part 3 Basic Requirements.

9.8 Limitations of liability

☰ 9.8-pkio133 —

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

9.9 Indemnities

Refer to Programme of Requirements part 3 Basic Requirements.

9.10 Term and termination

9.10.1 Term

Refer to Programme of Requirements part 3 Basic Requirements.

9.10.2 Termination

Refer to Programme of Requirements part 3 Basic Requirements.

9.10.3 Effect of termination and survival

Refer to Programme of Requirements part 3 Basic Requirements.

9.11 Individual notices and communications with participants

Refer to Programme of Requirements part 3 Basic Requirements.

9.12 Amendments

9.12.1 Procedure for amendment

Refer to Programme of Requirements part 3 Basic Requirements.

9.12.2 Notification mechanism and period

Refer to Programme of Requirements part 3 Basic Requirements.

9.12.3 Circumstances under which OID must be changed

Refer to Programme of Requirements part 3 Basic Requirements.

9.13 Dispute resolution provisions

Refer to Programme of Requirements part 3 Basic Requirements.

9.14 Governing law

Refer to Programme of Requirements part 3 Basic Requirements.

9.15 Compliance with applicable law

Refer to Programme of Requirements part 3 Basic Requirements.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Refer to Programme of Requirements part 3 Basic Requirements.

9.16.2 Assignment

Refer to Programme of Requirements part 3 Basic Requirements.

9.16.3 Severability

Refer to Programme of Requirements part 3 Basic Requirements.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Refer to Programme of Requirements part 3 Basic Requirements.

9.16.5 Force Majeure

Refer to Programme of Requirements part 3 Basic Requirements.

9.17 Other provisions

Refer to Programme of Requirements part 3 Basic Requirements.

Appendix A: Certificate Profile

Profile of the personal certificates for the Private Persons 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'.

Naming convention Subject.commonName

The following requirements apply to the CommonName of the Subject field. The main principle is that the TSP is responsible for correct entry of the CommonName. For a correct implementation this entails that the TSP has to be able to check each part that is entered. The CommonName has the following format^[1]:

[aristocratic designation] [**Full first forename OR nickname**] [*initials other forenames OR full other forenames*] [surname prefixes + surname partner '-'] [aristocratic title] [**surname prefixes + surname at birth**]

whereby:

text in bold = compulsory part

Italic = compulsory part, style in accordance with Compulsory Identification Act document or presented Local Council Personal Records Database extract

normal = optional part; if present, the style has to be the same as the Compulsory Identification Act document or the presented Local Council Personal Records Database extract

In principle, the TSP decides whether or not optional parts are allowed. If it prefers, the TSP can leave the choice for an option to the subscriber or the party requesting the certificate. If the CommonName becomes too long for the number of characters that are allowed, optional parts have to be omitted (starting with the replacement of other forenames by initials from the last to the first position) until the name fits in the maximum field length.

^[1] The presented order is not compulsory, the surname can also be given first followed by forenames/initials.

Personal certificates – Private Persons Domain

Basic attributes

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Version	V	MUST be set at 2 (X.509v3).	RFC 5280	Integer	Describes the version of the certificate, the value 2 stands for X.509 version 3.
SerialNumber	V	A serial number that MUST uniquely identify the certificate within the publishing CA domain.	RFC 5280	Integer	All end user certificates have to contain at least 8 bytes of unpredictable random data in the certificate's serial number (SerialNumber).
Signature	V	MUST be set on the algorithm, as stipulated by the PA.	RFC 5280, ETSI TS 102176	OID	For certificates issued under this PoR part only sha-256WithRSAEncryption is allowed.
Issuer	V	MUST contain a Distinguished Name (DN). The field has the following attributes	PKIo, RFC3739, ETSI TS 102280		Attributes other than those mentioned below MUST NOT be used.
Issuer.countryName	V	See requirement 7.1-pkio174	ETSI TS101862, X520, ISO 3166	Printable String	
Issuer.OrganizationName	V	See requirement 7.1-pkio174	ETSI TS 102280	UTF8String	
Issuer. organizationalUnitName	O	See requirement 7.1-pkio174	ETSI TS 102280: 5.2.4	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 in order 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: <ul style="list-style-type: none"> • 3 character legal person identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).
Validity	V	MUST define the period of validity of the certificate according to RFC 5280.	RFC 5280	UTCTime	MUST include the start and end date for validity of the certificate in accordance with the applicable policy laid down in the CPS.
subject	V	The attributes that are used to describe the subject (end user) MUST mention the subject in a unique manner and include information about the subscriber. 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	Printable String	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	V	The commonName attribute MUST be entered in accordance with the paragraph <i>Naming convention Subject.commonName</i> above.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	See the naming convention of Subject.commonName.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.Surname	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	The use of this field is mandatory from 1-2-2017 onwards. This field MUST show the subject's 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	The use of this field is mandatory from 1-2-2017 onwards. This field MUST show the subject's first name(s) correctly as shown on the Compulsory Identification Act document.
Subject.organizationName	V	Full name of the subscriber in accordance with the accepted document or Basic Registry	PKIo	UTF8String	The subscriber is the entity with which the TSP has entered into an agreement and on behalf of which or pursuant to which the certificate holder acts when using the certificate.
Subject.organizationalUnitName	O	Optional specification of an organizational entity. This attribute MUST NOT include a function indication or similar.	PKIo		This attribute MAY appear several times in organization-linked certificate holders. The field MUST contain a valid name of an organizational entity of the subscriber in accordance with an accepted document or registry. In occupational-linked certificate holders, this attribute MUST NOT be incorporated.
Subject.stateOrProvinceName	A	The use is advised against. If present, this field MUST contain the province in which the subscriber is established in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the province MUST correspond with the address of the subscriber in accordance with the accepted document or registry.
Subject.localityName	A	The use is advised against. If present, this field MUST contain the location of the subscriber in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the location MUST correspond with the address of the subscriber in accordance with the accepted document or registry.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.postalAddress	A	The use is advised against. If present, this field MUST contain the postal address of the subscriber in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	The address MUST correspond with the address of the subscriber in accordance with the accepted document or registry.
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.
Subject.title	V/N	MUST contain value from limitative list of professions in PoR requirement 3.2.5-pkio160.	ETSI TS 102 280, RFC 3739, RFC 5280		This field SHALL only be used in certificates of the 'professional certificate' type.
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 critical. Another keyUsage MUST NOT be combined with this.</p> <p>In confidentiality certificates, keyEncipherment and dataEncipherment bits MUST be incorporated and marked as critical. 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 critical. 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	MUST contain the OID of the certificate policy (CP), the URI of the certification practice statement (CPS), and a user notice. The applicable PKI for the government OID scheme is described in the CP. The TSP SHOULD use UTF8String in the userNotice, but MAY use IA5String.	RFC 3739	OID, String, UTF8String or IA5String	Reference to the paragraph numbers of the PoR/CP in the user notice is advised against because the persistency of this cannot be guaranteed (unlike the OID number of the CP). If this concerns a profession-linked certificate, it is preferable to make a note of the fact in the user notice that the certificate holder is acting in the capacity of his/her profession.
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	V		<p>MUST be used containing a unique identification number that identifies the certificate holder.</p> <p>An additional othername entry MAY be included in the authentication certificate for use with SSO (Single Sign On).</p>	PKIo	IA5String, Microsoft UPN, IBM Principal-Name, Kerberos PrincipalName or Permanent-Identifier	<p>Includes an <i>OID</i> of the TSP awarded by PKIoverheid to the TSP and a <i>number</i> that is unique within the namespace of that <i>OID</i> that permanently identifies the subject, in one of the following ways:</p> <ol style="list-style-type: none"> 1. MS UPN: <i>[number]</i>@<i>[OID]</i> 2. MS UPN: <i>[OID]</i>.<i>[number]</i> 3. IA5String: <i>[OID]</i>-<i>[number]</i> 4. Permanent Identifier: Identifiervalue = <i>[number]</i> Assigner = <i>[OID]</i> <p>Alternative 1. is also suitable for SSO. If a second othername for SSO is given in the certificate, the SSO othername MUST be given first in the SubjectAltName, before the PKIoverheid format othername described above, in order to ensure the proper operation of the SSO mechanism. It is recommended that an existing registration number from back office systems is used, such as a staff number in combination with a code for the organization. In combination with the TSP <i>OID</i>, this identifier is internationally unique. This number MUST be persistent.</p>

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
SubjectAltName.rfc822Name	A		MAY be used for the certificate holder's e-mail address, for applications that need the e-mail address to be able to function properly.	RFC 5280	IA5String	<p>For PKIoverheid certificates in the Government/Companies and Organization domains, the use of e-mail addresses is advised again, because e-mail addresses of certificate holders often change and furthermore are privacy sensitive (spam).</p> <p>If the e-mail address is included in the certificate, the TSP MUST:</p> <ul style="list-style-type: none"> • have the subscriber sign his/her approval for these and; • check that the e-mail address belongs to the subscriber's domain, or; • check that the e-mail address belongs to the subscriber (e.g. the professional) and that this person has access to the e-mail address (for example by performing a challenge response).
subjectDirectoryAttributes	O	No		RFC 5280; RFC 3739		The use of this extension is allowed. These attributes MAY NOT contain personal data that can impair the subject's privacy.
BasicConstraints	O	Yes	The "CA" field MUST be omitted (default value is then "FALSE").	RFC 5280		<p>A (Dutch language) browser can then be seen:</p> <p>"Subjecttype = Eidentiteit", "Beperking voor padlengte = Geen" ("Subject type = End Entity", "Path length constraint = None")</p>
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.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
ExtKeyUsage	V	No		RFC 5280	KeyPurposeId's	See requirement 7.1-pkio149.
FreshestCRL	O	No	MUST contain the URI of a Delta CRL distribution point, if Delta CRLs are used.	RFC 5280, PKIo		Delta-CRLs are an optional extension. In order to fulfil the requirements of PKIoverheid a TSP MUST also publish full CRLs at the required release frequency.

Private extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityInfoAccess	O	No	This attribute MUST include the URI of an OCSP responder if Online Certificate Status Protocol (OCSP) plays a role.			This field can optionally be used to reference other additional information about the TSP.
SubjectInfoAccess	O	No		RFC 5280	OID, Generalname	This field can be used to reference additional information about the subject, provided that the information that is offered does not infringe the privacy of the subject.
BiometricInfo	O	No	Contains the hash of a biometric template and optionally a URI that references a file with the biometric template itself.	RFC 3739		
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>	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"> • id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 • id-etsi-qct-esign { id-etsi-qcs-QcType 1 } 0.4.0.1862.1.6.1 • 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
			<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 (QSSCD) complying with annex II of EU regulation 920/2014I. 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> <p>The certificates for authenticity and the certificates for confidentiality MUST NOT use this extension.</p>			

