



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

TRIALcertificates for PKIoverheid

Version	5.1.1
Date	September 1, 2021

Publisher's imprint

Version number 5.1.1
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	12
1.1 Overview	12
1.2 Document name and identification	12
1.2.1 Revisions	13
1.2.2 Relevant dates	14
1.3 PKI participants	15
1.3.1 Certification authorities	15
1.3.2 Registration authorities	15
1.3.3 Subscribers	15
1.3.4 Relying parties	16
1.3.5 Other participants	16
1.4 Certificate usage	16
1.4.1 Appropriate certificate uses	16
1.4.2 Prohibited certificate uses	17
1.5 Policy administration	17
1.5.1 Organization administering the document	17
1.5.2 Contact person	17
1.5.3 Person determining CPS suitability for the policy	17
1.5.4 CP approval procedures	17
1.6 Definitions and acronyms	17
1.6.1 Conventions	17
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	18
2.1 Repositories	18
2.1-tpkio2	18
2.2 Publication of certification information	18
2.2-tpkio12	18
2.2-tpkio13	18
2.3 Time or frequency of publication	18
2.4 Access controls on repositories	18
2.4-tpkio14	18
3. IDENTIFICATION AND AUTHENTICATION	19
3.1 Naming	19
3.1.1 Types of names	19
3.1.2 Need for names to be meaningful	19
3.1.3 Anonymity or pseudonymity of subscribers	19
3.1.4 Rules for interpreting various name forms	19
3.1.5 Uniqueness of names	19
3.1.6 Recognition, authentication, and role of trademarks	19

3.2 Initial identity validation	19
3.2.1 Method to prove possession of private key	19
3.2.2 Authentication of organization identity	20
3.2.3 Authentication of individual identity	20
3.2.4 Non-verified subscriber information	21
3.2.5 Validation of authority	22
3.2.6 Criteria for interoperation	22
3.3 Identification and authentication for re-key requests.....	22
3.3.1 Identification and authentication for routine re-key	22
3.3.2 Identification and authentication for re-key after revocation.....	23
3.4 Identification and authentication for revocation request	23
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	24
4.1 Certificate Application.....	24
4.1-tpkio9	24
4.1.1 Who can submit a certificate application	24
4.1.2 Enrollment process and responsibilities	24
4.2 Certificate application processing	24
4.2.1 Performing identification and authentication functions	24
4.2.2 Approval or rejection of certificate applications.....	24
4.2.3 Time to process certificate applications	24
4.3 Certificate issuance	24
4.3.1 CA actions during certificate issuance.....	24
4.3.2 Notification to subscriber by the CA of issuance of Certificate	25
4.4 Certificate acceptance.....	25
4.4.1 Conduct constituting certificate acceptance.....	25
4.4.2 Publication of the certificate by the CA	25
4.4.3 Notification of certificate issuance by the CA to other Entities	25
4.5 Key pair and certificate usage	25
4.5.1 Subscriber private key and certificate usage	25
4.5.2 Relying party public key and certificate usage	25
4.6 Certificate renewal	25
4.6.1 Circumstance for certificate renewal	25
4.6.2 Who may request renewal	25
4.6.3 Processing certificate renewal requests	25
4.6.4 Notification of new certificate issuance to subscriber	25
4.6.5 Conduct constituting acceptance of a renewal certificate.....	25
4.6.6 Publication of the renewal certificate by the CA	25
4.6.7 Notification of certificate issuance by the CA to other entities	26
4.7 Certificate re-key	26
4.7.1 Circumstance for certificate re-key	26
4.7.2 Who may request certification of a new public key	26
4.7.3 Processing certificate re-keying requests	26
4.7.4 Notification of new certificate issuance to subscriber	26
4.7.5 Conduct constituting acceptance of a re-keyed certificate	26

4.7.6 Publication of the re-keyed certificate by the CA	26
4.7.7 Notification of certificate issuance by the CA to other entities	26
4.8 Certificate modification	26
4.8.1 Circumstance for certificate modification	27
4.8.2 Who may request certificate modification	27
4.8.3 Processing certificate modification requests	27
4.8.4 Notification of new certificate issuance to subscriber	27
4.8.5 Conduct constituting acceptance of modified certificate	27
4.8.6 Publication of the modified certificate by the CA	27
4.8.7 Notification of certificate issuance by the CA to other entities	27
4.9 Certificate revocation and suspension	27
4.9.1 Circumstances for revocation	27
4.9.2 Who can request revocation.....	27
4.9.3 Procedure for revocation request	27
4.9.4 Revocation request grace period.....	27
4.9.5 Time within which CA must process the revocation request	27
4.9.6 Revocation checking requirement for relying parties.....	27
4.9.7 CRL issuance frequency (if applicable).....	28
4.9.8 Maximum latency for CRLs (if applicable)	28
4.9.9 On-line revocation/status checking availability	28
4.9.10 On-line revocation checking requirements.....	29
4.9.11 Other forms of revocation advertisements available.....	29
4.9.12 Special requirements related to key compromise	29
4.9.13 Circumstances for suspension	29
4.9.14 Who can request suspension	29
4.9.15 Procedure for suspension request	29
4.9.16 Limits on suspension period	29
4.10 Certificate status services.....	29
4.10.1 Operational characteristics.....	29
4.10.2 Service availability	30
4.11 End of subscription	30
4.12 Key escrow and recovery.....	30
4.12.1 Key escrow and recovery policy and practices.....	30
4.12.2 Session key encapsulation and recovery policy and practices	30
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	31
5.1 Physical controls	31
5.1-tpkio29	31
5.1.1 Site location and construction	31
5.1.2 Physical access	31
5.1.3 Power and air conditioning.....	31
5.1.4 Water exposures	31
5.1.5 Fire prevention and protection	31
5.1.6 Media storage	31
5.1.7 Waste disposal.....	31
5.1.8 Off-site backup	31

<i>5.2 Procedural controls</i>	31
5.2-tpkio30	31
5.2.1 Trusted roles	32
5.2.2 Number of persons required per task	32
5.2.3 Identification and authentication for each role	32
5.2.4 Roles requiring separation of duties PKIoverheid.....	32
<i>5.3 Personnel controls</i>	32
5.3-tpkio31	32
5.3.1 Qualifications, experience, and clearance requirements	32
5.3.2 Background check procedures.....	32
5.3.3 Training requirements	32
5.3.4 Retraining frequency and requirements	32
5.3.5 Job rotation frequency and sequence	32
5.3.6 Sanctions for unauthorized actions	32
5.3.7 Independent contractor requirements	32
5.3.8 Documentation supplied to personnel.....	32
<i>5.4 Audit logging procedures</i>	33
5.4.1 Types of events recorded.....	33
5.4.2 Frequency of processing log.....	33
5.4.3 Retention period for audit log.....	33
5.4.4 Protection of audit log	33
5.4.5 Audit log backup procedures	33
5.4.6 Audit collection system (internal vs. external)	33
5.4.7 Notification to event-causing subject.....	33
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)	34
5.5.7 Procedures to obtain and verify archive information	34
<i>5.6 Key changeover</i>	34
<i>5.7 Compromise and disaster recovery</i>	34
5.7.1 Incident and compromise handling procedures	34
5.7.2 Computing resources, software, and_or data are corrupted.....	34
5.7.3 Entity private key compromise procedures	34
5.7.4 Business continuity capabilities after a disaster	34
<i>5.8 CA or RA termination</i>	34
6. TECHNICAL SECURITY CONTROLS	35
<i>6.1 Key pair generation and installation</i>	<i>35</i>
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.....	35
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-tpkio36	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	37
6.4 Activation data	37
6.4.1 Activation data generation and installation.....	37
6.4.2 Activation data protection.....	37
6.4.3 Other aspects of activation data	37
6.5 Computer security controls.....	38
6.5-tpkio41	38
6.5.1 Specific computer security technical requirements	38
6.5.2 Computer security rating.....	38
6.6 Life cycle technical controls	38
6.6.1 System development controls	38
6.6.2 Security management controls.....	38
6.6.3 Life cycle security controls.....	38
6.7 Network security controls.....	38
6.7-tpkio42	38
6.8 Time-stamping	38
7. CERTIFICATE, CRL, AND OCSP PROFILES	39
7.1 Certificate profile	39
7.1-tpkio44	39
7.1-tpkio45	39
7.1-tpkio47	39
7.1-tpkio67	39
7.1-tpkio68	40
7.1-tpkio81	40

7.1.1 Version number(s).....	40
7.1.2 Certificate extensions	40
7.1.3 Algorithm object identifiers.....	44
7.1.4 Name forms	45
7.1.5 Name constraints	51
7.1.6 Certificate policy object identifier.....	51
7.1.7 Usage of Policy Constraints extension.....	52
7.1.8 Policy qualifiers syntax and semantics.....	52
7.1.9 Processing semantics for the critical Certificate Policies extension	52
7.2 CRL profile	53
7.2-tpkio96	53
7.2-tpkio98	53
7.2-tpkio99	53
7.2.1 Version number(s).....	53
7.2.2 CRL and CRL entry extensions.....	53
7.3 OCSP profile.....	56
7.3-tpkio111.....	56
7.3.1 Version number(s).....	56
7.3.2 OCSP extensions	56
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	58
8.1 <i>Frequency or circumstances of assessment</i>	58
8.2 <i>Identity/qualifications of assessor</i>	58
8.3 <i>Assessor's relationship to assessed entity</i>	58
8.4 <i>Topics covered by assessment</i>	58
8.5 <i>Actions taken as a result of deficiency</i>	58
8.6 <i>Communication of results</i>	58
9. OTHER BUSINESS AND LEGAL MATTERS	59
9.1 <i>Fees</i>	59
9.1.1 Certificate issuance or renewal fees	59
9.1.2 Certificate access fees.....	59
9.1.3 Revocation or status information access fees	59
9.1.4 Fees for other services.....	59
9.1.5 Refund policy	59
9.2 <i>Financial responsibility</i>	59
9.2.1 Insurance coverage	59
9.2.2 Other assets	59
9.2.3 Insurance or warranty coverage for end-entities	59
9.3 <i>Confidentiality of business information</i>	59
9.3.1 Scope of confidential information.....	59
9.3.2 Information not within the scope of confidential information.....	59
9.3.3 Responsibility to protect confidential information	59
9.4 <i>Privacy of personal information</i>	60

9.4.1 Privacy plan.....	60
9.4.2 Information treated as private	60
9.4.3 Information not deemed private	60
9.4.4 Responsibility to protect private information	60
9.4.5 Notice and consent to use private information	60
9.4.6 Disclosure pursuant to judicial or administrative process.....	60
9.4.7 Other information disclosure circumstances	60
<i>9.5 Intellectual property rights</i>	<i>60</i>
<i>9.6 Representations and warranties</i>	<i>60</i>
9.6.1 CA representations and warranties	60
9.6.2 RA representations and warranties	60
9.6.3 Subscriber representations and warranties.....	60
9.6.4 Relying party representations and warranties	60
9.6.5 Representations and warranties of other participants	60
<i>9.7 Disclaimers of warranties</i>	<i>61</i>
9.7-tpkio97	61
<i>9.8 Limitations of liability</i>	<i>61</i>
<i>9.9 Indemnities.....</i>	<i>61</i>
<i>9.10 Term and termination</i>	<i>61</i>
9.10.1 Term.....	61
9.10.2 Termination	61
9.10.3 Effect of termination and survival	61
<i>9.11 Individual notices and communications with participants</i>	<i>61</i>
<i>9.12 Amendments</i>	<i>61</i>
9.12.1 Procedure for amendment	61
9.12.2 Notification mechanism and period	61
9.12.3 Circumstances under which OID must be changed	61
<i>9.13 Dispute resolution provisions</i>	<i>62</i>
<i>9.14 Governing law.....</i>	<i>62</i>
<i>9.15 Compliance with applicable law</i>	<i>62</i>
<i>9.16 Miscellaneous provisions</i>	<i>62</i>
9.16.1 Entire agreement	62
9.16.2 Assignment	62
9.16.3 Severability	62
9.16.4 Enforcement (attorneys' fees and waiver of rights)	62
9.16.5 Force Majeure	62
<i>9.17 Other provisions.....</i>	<i>62</i>
Appendix A: Requirements (CP) for personal authentication certificates (OID	
2.16.528.1.1003.1.2.9.1)	63
<i>Requirements in this CP for OID 2.16.528.1.1003.1.2.9.1</i>	<i>63</i>

Appendix B: Requirements (CP) for personal signature certificates (OID 2.16.528.1.1003.1.2.9.2) 66
Requirements in this CP for OID 2.16.528.1.1003.1.2.9.2 66

Appendix C: Requirements (CP) for personal encryption certificates (OID 2.16.528.1.1003.1.2.9.3) 69
Requirements in this CP for OID 2.16.528.1.1003.1.2.9.3 69

Appendix D: Requirements (CP) for services authentication certificates (OID 2.16.528.1.1003.1.2.9.4) 72
Requirements in this CP for OID 2.16.528.1.1003.1.2.9.4 72

Appendix E: Requirements (CP) for services encryption certificates (OID 2.16.528.1.1003.1.2.9.5) 75
Requirements in this CP for OID 2.16.528.1.1003.1.2.9.5 75

Appendix F: Requirements (CP) for services signature certificates (OID 2.16.528.1.1003.1.2.9.10) 78
Requirements in this CP for OID 2.16.528.1.1003.1.2.9.10 78

Appendix G: Requirements (CP) for server certificates (OID 2.16.528.1.1003.1.2.9.6) 81
Requirements in this CP for OID 2.16.528.1.1003.1.2.9.6 81

1. INTRODUCTION

1.1 Overview

The PKIoverheid TRIAL (G3) hierarchy (PKIoverheid TRIAL) has been established by the Policy Authority PKIoverheid to enable TSPs and subscribers to deploy non-production (test) PKIoverheid certificates in testing or staging environments with the intent to test the suitability of their systems with (new types of) PKIoverheid certificates. This document is issued by the PA PKIoverheid to define the policies that Trust Service Providers operating in this PKI are required to adhere to.

For more information about general PKIoverheid concepts, please refer to Part 1 of the Programme of Requirements which can be found on <https://www.logius.nl/english/pkioverheid>.

1.2 Document name and identification



This document is the Policy Authority PKIoverheid TRIAL Certificate Policy ("CP"). It sets forth the policy requirements that the PA PKIoverheid imposes on Trust Service Providers (TSPs) which are part of the PKIoverheid TRIAL (G3) hierarchy.


The following Policy identifiers are reserved for use by TSPs as a means of asserting compliance with specific requirements imposed by this CP:

OID	CP
2.16.528.1.1003.1.2.9.1	Identifies TRIAL personal authenticity certificates within the PKIoverheid TRIAL Organization Person domain, that contains the public key for identification and authentication.
2.16.528.1.1003.1.2.9.2	Identifies TRIAL personal signature certificate within the PKIoverheid TRIAL Organization Person domain, that contains the public key for the qualified electronic signature/non repudiation.
2.16.528.1.1003.1.2.9.3	Identifies TRIAL personal confidentiality certificate within the PKIoverheid TRIAL Organization Person domain, that contains the public key for confidentiality.
2.16.528.1.1003.1.2.9.4	Identifies TRIAL services authenticity certificates within the PKIoverheid TRIAL Organization Services domain, that contains the public key for identification and authentication.
2.16.528.1.1003.1.2.9.5	Identifies TRIAL services confidentiality certificate within the PKIoverheid TRIAL Organization Services domain, that contains the public key for confidentiality.
2.16.528.1.1003.1.2.9.6	Identifies TRIAL Server certificates within the PKIoverheid TRIAL Organization Services domain (formerly known as TRIAL Type 1 Server Certificates).
2.16.528.1.1003.1.2.9.6.1	Identifies TRIAL Server type 2 certificates [DEPRECATED].
2.16.528.1.1003.1.2.9.6.2	Identifies TRIAL Server type 3 certificates [DEPRECATED].
2.16.528.1.1003.1.2.9.10	Identifies TRIAL services signature certificates within the PKIoverheid TRIAL Organization Services domain, that contains the public key for the qualified electronic signature/non repudiation. Also known as <i>eSeals</i> .


⚠ Signature certificates (2.16.528.1.1003.1.2.9.2 and 2.16.1.1003.1.2.9.10) are designed to match the production certificates certificate profile as closely as possible. However, due to the fact that TRIAL certificates are not meant to be used in a production environment, they **MUST NOT** assert specific profile extensions marking them as a qualified certificates as meant in regulation 910/2014 (eIDAS).

1.2.1 Revisions

Version	Date	Remarks
5.0	 10-mrt-2020	Major revision of the original PKIoverheid TEST PvE v2.0 from 2012
5.1	 27-aug-2020	<ul style="list-style-type: none"> - Fixing writing errors. - Fixing incorrect or missing references. - Fixing incorrect requirements. - Adding the requirements: 7.1.4-tpkio117, 7.1.4-tpkio118, 7.1.4-tpkio119 7.1.4-tpkio120, 7.1.4-tpkio121

Version	Date	Remarks
5.1.1	 1-sep-2021	<p>Change T001: Set life-time of all certificates to 1 year, deprecating different server certificate types. Existing requirement: Requirement 6.3.2-tpkio37 became applicable to all TRIAL certificate types. Repealed: Requirement 6.3.2-tpkio38, Requirement 6.3.2-tpkio39, Requirement 6.3.2-tpkio40, Requirement 7.1.6-tpkio91, Requirement 7.1.6-tpkio92.</p> <p>Change T002: Revised Certificate Profiles. In TRIAL PoR 5.1 some Certificate Profile fields were missing due to typos in labels of individual requirements resulting in omissions in the automatically generated Appendices. These typos will now be fixed. Existing requirement: Yes, Appendices A through G Modifications: Added to Appendix A: 7.1.2-tpkio46, 7.1.2-tpkio48, 7.1.2-tpkio49, 7.1.2-tpkio59, 7.1.2-tpkio60, 7.1.2-tpkio64, 7.1.2-tpkio65, 7.1.2-tpkio82, 7.2-tpkio96. Added to Appendix B: 7.1.2-tpkio46, 7.1.2-tpkio48, 7.1.2-tpkio49, 7.1.2-tpkio52, 7.1.2-tpkio53, 7.1.2-tpkio54, 7.1.2-tpkio59, 7.1.2-tpkio60, 7.1.2-tpkio64, 7.1.2-tpkio65, 7.1.2-tpkio82. Added to Appendix C: 7.1.2-tpkio46, 7.1.2-tpkio49, 7.1.2-tpkio59, 7.1.2-tpkio60, 7.1.2-tpkio64, 7.1.2-tpkio65, 7.1.2-tpkio82. Added to Appendix D: 7.1.2-tpkio46, 7.1.2-tpkio49, 7.1.2-tpkio59, 7.1.2-tpkio60, 7.1.2-tpkio82. Added to Appendix E: 7.1.2-tpkio46, 7.1.2-tpkio49, 7.1.2-tpkio59, 7.1.2-tpkio60, 7.1.2-tpkio82. Added to Appendix F: 7.1.2-tpkio49, 7.1.2-tpkio59, 7.1.2-tpkio60, 7.1.2-tpkio82, 7.1.4-tpkio77, 7.1.4-tpkio120. Added to Appendix G: 7.1.2-tpkio46, 7.1.2-tpkio49, 7.1.2-tpkio59, 7.1.2-tpkio82.</p> <p>Change T003: QcStatement is missing from TRIAL Organization Person certificates. This needs to be fixed. New requirement: 7.1.2-tpkio124. Added requirement 7.1.2-tpkio124 which describes the qcStatements for TRIAL Organization Person certificates.</p> <p>Change T004: Limit the number of extensions:subjectAltName:dNSName entries to 10. Existing requirement: 7.1.4-tpkio83 Modifications: In 7.1.4-tpkio83 Limit the number of extensions:subjectAltName:dNSName entries to 10.</p>

1.2.2 Relevant dates

No stipulation as of  10-mrt-2020 . This section will be updated as new versions of this CP are published.

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 (TSP). 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
KPN BV TRIAL PKIoverheid Organisatie Persoon CA - G3	📅 27 Feb 2020	📅 13 Nov 2028	6ffacdc0a5703f42a69225e6435c321a5e067c8c	B9E46607FD6D60B41515C8547371DABC657668AD49BCB55233E4029515902D9C
KPN BV TRIAL PKIoverheid Organisatie Server CA - G3	📅 27 Feb 2020	📅 13 Nov 2028	0e56cfba4c0be27956a9cb9ff96d9c875dbec219	0AA8CF081D7E32689E5AB720F964C41E9D221ECC564614846918719CEE3A1494
KPN BV TRIAL PKIoverheid Organisatie Services CA - G3	📅 27 Feb 2020	📅 13 Nov 2028	5be7d94d47baebe34148dba0385ab3008555b703	8B7E375390BD4177B557720524E759F7715592808E325B936E03CBCAF6785E26
QuoVadis TRIAL PKIoverheid Organisatie Persoon CA - G3	📅 27 Feb 2020	📅 13 Nov 2028	622df11ef3c0d88da5728919a613a1ae139fdc98	466FB468F253F648ADDAFC0244BEF84598FFD6EF568DC62AA33A3F2D05A6E2ED
QuoVadis TRIAL PKIoverheid Organisatie Server CA - G3	📅 27 Feb 2020	📅 13 Nov 2028	42756ba0989b586bdb4237d6a02c66e950c416d4	F00147847367A2CA056F46C2608DC1973F2D4824D83E66F29421A52D81D79465
QuoVadis TRIAL PKIoverheid Organisatie Services CA - G3	📅 27 Feb 2020	📅 13 Nov 2028	26a7225f0aaaa0364e0dc7aabdf80f6a411c011e	9E409C65474692A4DD85811490933AD2473966B096BEF9804C96B36934DEA35C

1.3.2 Registration authorities

Registration Authorities (RAs) are entities that approve and authenticate requests to obtain, renew, or revoke certificates. RA tasks within PKIoverheid are as follows:

- Identify and authenticate subscribers
- Verify that subscribers are authorized to request or revoke certificates
- Approving individuals, entities, and/or devices that are to be included in a certificate.

After performing the tasks listed above they will authorize and/or request a TSP to issue, renew, or revoke a certificate.

1.3.3 Subscribers

Subscribers within the PKIoverheid TRIAL hierarchy are defined as organizations or individuals (working for organizations) to whom a TSP has issued (a) PKIoverheid TRIAL certificate(s). Before issuance of the first certificate the subscriber has to agree to a Subscriber agreement supplied by the TSP. Requirements for this subscriber agreement are listed in relevant sections of this CP.

1.3.4 Relying parties

Relying parties are all parties which that can encounter and or process a PKIoverheid TRIAL certificate. Relying parties should be aware of the purpose of the PKIoverheid TRIAL certificates (see also section [1.1 Overview](#)) and as such MUST NOT make decisions based on the (perceived) trustworthiness of a PKIoverheid TRIAL certificate.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

1.4.1-tpkio3

Description	<p>Certificates issued within the PKIoverheid TRIAL hierarchy SHALL only be used for testing purposes.</p> <p>Testing purposes for Server/SSL certificates are as follows (please not that this is not an exhaustive list):</p> <ul style="list-style-type: none"> • Usage of subscriber SSL certificates by the TSP for own (internal) testing • Usage of subscriber SSL certificates to test an non-production application or website to test system behaviour when encountering PKIoverheid certificates • Testing the process of generating keypairs and CSRs and implementing the final PKIoverheid TRIAL certificate <p>In case of doubt if an use case is deemed to be for "testing purposes" a TSP SHALL contact the PA to seek permission for issuance of PKIoverheid TRIAL certificates.</p> <p>If the certificates are to be used by a TSP for internal testing the requirements in sections 2, 3.2.2, 3.2.3, 3.2.4, and 4.1 will not be applicable to the TSP.</p> <p>TSPs are allowed to issue PKIoverheid TRIAL certificates to third parties (e.g. external subscribers) for testing. In that case The TPS MUST adhere to all requirements listed in this CP.</p>
Comment	-

1.4.1-tpkio33

Description	<p>Certificates issued within the PKIoverheid TRIAL hierarchy SHALL only be used for testing purposes.</p> <p>Testing purposes for Personal certificates and Services certificates are as follows (please not that this is also not an exhaustive list):</p> <ul style="list-style-type: none"> • Usage of subscriber Personal/Services certificates by the TSP for own (internal) testing • Usage of subscriber Personal/Services certificates to test a non-production application to test the process of implementing PKIoverheid personal/services certificates in workflows etc.
--------------------	---

Comment	<p>In case of doubt if an use case is deemed to be for "testing purposes" a TSP SHALL contact the PA to seek permission for issuance of PKIoverheid TRIAL certificates.</p> <p>If the certificates are to be used by a TSP for internal testing the requirements in sections 2, 3.2.2, 3.2.3, 3.2.4, and 4.1 will not be applicable to the TSP.</p> <p>TSPs are allowed to issue PKIoverheid TRIAL certificates to third parties (e.g. external subscribers) for testing. In that case The TPS MUST adhere to all requirements listed in this CP.</p>
----------------	---

1.4.2 Prohibited certificate uses

No stipulation.

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

See part 4 of the PoR PKIoverheid which can be found on <https://www.logius.nl/english/pkioverheid>

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

2.1-tpkio2

Description	A TSP MUST establish and maintain a repository where information as listed in section 2.2 Publication of certification information is available. The repository could either be maintained by the TSP itself or maintenance can be delegated to a third party.
Comment	-

2.2 Publication of certification information

2.2-tpkio12

Description	A TSP MUST make the issuing CA or issuing CAs which she uses for issuing end-user PKIoverheid TRIAL certificates available to download for subscribers and relying parties.
Comment	-

2.2-tpkio13

Description	A TSP MUST make available the location of the CRLs and the OCSP responders in the repository on a publicly available web page.
Comment	-

2.3 Time or frequency of publication

No stipulation.

2.4 Access controls on repositories

2.4-tpkio14

Description	The repository MUST be publicly available.
Comment	-

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

To indicate that this hierarchy is intended for test purposed only, the words TRIAL and/or TEST are used in several subject and/or issuer attributes. See [7. CERTIFICATE, CRL, AND OCSP PROFILES](#) of this CP for more information.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

3.2.1-tpkio6

Description	<p>The TSP is responsible for ensuring that the subscriber supplies the certificate signing request (CSR) securely. The secure delivery must take place in the following manner:</p> <ul style="list-style-type: none"> • the entry of the CSR on the TSP's application developed especially for that purpose, using an SSL connection with a PKIoverheid SSL certificate or similar or; • the entry of the CSR on the HTTPS website of the TSP that uses a PKIoverheid SSL certificate or similar or; • sending the CSR by e-mail, along with a qualified electronic signature of the certificate manager that uses a PKIoverheid qualified certificate or similar or; • entering or sending a CSR in a way that is at least equivalent to the aforementioned ways.
--------------------	--

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

3.2.2 Authentication of organization identity

3.2.2-tpkio5

Description	At initial registration TSP MUST verify that the subscriber is an existing organization.
Comment	-

3.2.2-tpkio15

Description	The TSP MUST 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-tpkio16

Description	Before a services server certificate is issued, the TSP MUST enter into an agreement with the subscriber and receive a certificate request signed by the certificate manager. The agreement must be signed by the Authorized Representative or Representation of the subscriber.
Comment	-

3.2.2-tpkio17

Description	When entering into an agreement with the subscriber, the TSP SHALL request a copy of the identification document of the legal representative of the subscriber (see also 3.2.2-tpkio16). This is for identification purposes. The identity of the legal representative can only be established using the valid documents referred to in article 1 of the Compulsory Identification Act (Wet op de identificatieplicht). The TSP MUST check the validity and authenticity of these documents.
Comment	-

3.2.3 Authentication of individual identity

3.2.3-tpkio4

Description	When a TSP issues PKIoverheid TRIAL certificates for use in testing within the TSP's organization there is no need for identity validation.
Comment	-

3.2.3-tpkio7

Description	If an OIN is included in a certificate (in the subject.serialnumber attribute) a TSP MUST check the autorisation of the applicant to use the OIN in accordance with the requirements laid down in the agreement between the State of the Netherlands and the TSP.
Comment	-

3.2.3-tpkio19

Description	In accordance with Dutch legislation and regulations, the TSP MUST check the identity and, if applicable, specific properties of the certificate manager. Proof of identity has to be verified based on the physical appearance of the person himself, either directly or indirectly, using means by which the same certainty can be obtained as with personal presence. The proof of identity can be supplied on paper or electronically.
Comment	-

3.2.3-tpkio20

Description	The identity of the certificate manager can only be established using the valid documents referred to in article 1 of the Compulsory Identification Act (Wet op de identificatieplicht). The TSP MUST check the validity and authenticity of these documents. If the personal identity of the certificate manager has already been verified for under another (production) CP of PKIoverheid then the demands of this requirement are deemed to have been satisfied.
Comment	-

3.2.4 *Non-verified subscriber information*

No stipulation.

3.2.5 Validation of authority

3.2.5-tpkio8

Description	<p>When a FQDN is included in the certificate, the TSP MUST check whether the FQDNs supplied by the subscriber (see definition in Part 4), included in a certificate, are:</p> <ul style="list-style-type: none"> • Actually in the name of the subscriber OR; • Authorized by the registered domain owner OR; • That the subscriber can show that it exercises (technical) control over the FQDN in question. <p>The verified data MAY be reused in a subsequent application, provided that it is not older than 39 months. If the data is older than 39 months, the above check must be carried out again. This must be done for every FQDN that is included in a certificate.</p> <p>The TSP MUST limit itself to:</p> <ul style="list-style-type: none"> • the methods as prescribed in the applicable version of the Baseline Requirements of the CABForum (chapter 3.2.2.4) OR; • an alternative method approved in advance by the PA.
Comment	-

3.2.5-tpkio18

Description	<p>The TSP MUST check that the evidence supplied by the subscriber that certificate holder is authorized to receive certificates is genuine and that the certificate manager has been authorized by the subscriber to execute the necessary actions (in cases in which the certificate manager handles the registration process).</p>
Comment	<p>The Certificate Manager who acts on behalf of the certificate holder does not necessarily have to be a system administrator or an HR-consultant. It is up to the subscriber to appoint a suitable person for the role (if needed).</p>

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

No stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1-tpkio9

Description	The TSP MUST include in the terms of use that the subscriber will only use a test certificate for testing purposes.
Comment	-

4.1.1 Who can submit a certificate application

No stipulation.

4.1.2 Enrollment process and responsibilities

No stipulation.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

No stipulation.

4.2.2 Approval or rejection of certificate applications

No stipulation.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

4.3.1-tpkio10

Description	Only TSPs who have been admitted to the production hierarchy of PKIoverheid MAY issue PKIoverheid TRIAL certificates to third parties.
Comment	Aspiring TSPs SHALL NOT issue PKIoverheid TRIAL certificates to third parties. An aspiring TSP MUST ask the Policy Authority PKIoverheid for written permission to issue PKIoverheid TRIAL certificates for internal testing. For the purposes of this CP "internal testing" is defined as being in use within the same legal entity as the TSP.

4.3.2 Notification to subscriber by the CA of issuance of Certificate

No stipulation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other Entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

No stipulation.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

4.7.1-tpkio21

Description	A TSP SHALL NOT issue certificates for which the key pair has been used for a previous expired or revoked certificate.
Comment	-

4.7.1-tpkio22

Description	A TSP MAY reuse a keypair once when issuing a certificate when the previous certificate has expired. A TSP SHALL NOT issue a certificate using a keypair which has been previously in a certificate issued by the TSP that has been revoked.
Comment	-

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

No stipulation.

4.9.2 Who can request revocation

No stipulation.

4.9.3 Procedure for revocation request

No stipulation.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

No stipulation.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

4.9.7 CRL issuance frequency (if applicable)

4.9.7-tpkio1

Description	A TSP MUST use CRLs to provide certificate status information to relying parties. A TSP MUST use 1 CRL for all types of reasons for revocation per issuing CA.
Comment	-

4.9.8 Maximum latency for CRLs (if applicable)

No stipulation.

4.9.9 On-line revocation/status checking availability

4.9.9-tpkio3

Description	A TSP MUST use OCSP to provide certificate status information. OCSP responses MUST conform to RFC6960 and MUST either: <ol style="list-style-type: none"> 1. Be signed by the CA that issued the certificates whose revocation status is being checked, OR 2. Be signed by an OCSP Responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked. If a TSP implements the latter option then the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.
Comment	-

4.9.9-tpkio24

Description	A TSP MAY use OCSP to provide certificate status information.
Comment	If OCSP is used, OCSP responses MUST conform to RFC6960 and MUST either: <ol style="list-style-type: none"> 1. Be signed by the CA that issued the certificates whose revocation status is being checked, OR 2. Be signed by an OCSP Responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked. If a TSP implements the latter option then the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.9-tpkio26

Description	A TSP MUST NOT use or make use of precomputed OCSP responses.
Comment	-

4.9.10 On-line revocation checking requirements

4.9.10-tpkio25

Description	If a TSP support OCSP, it SHALL support an OCSP capability using the GET method for certificates issued in accordance with this CP.
Comment	-

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements related to key compromise

No stipulation.

4.9.13 Circumstances for suspension

4.9.13-tpkio27

Description	A TSP MUST NOT support certificate suspension.
Comment	-

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

4.10.1-tpkio28

Description	A TSP MUST keep revoked certificates on a CRL for at least 6 months after the date listed in the notAfter field of a certificate.
Comment	-

4.10.2 Service availability

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1-tpkio29

Description	A TSP SHALL take all appropriate measures concerning Physical Controls based on a risk analysis in which applicable risks have been taken into account.
Comment	-

5.1.1 Site location and construction

No stipulation.

5.1.2 Physical access

No stipulation.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

5.2-tpkio30

Description	A TSP SHALL take all appropriate measures concerning Procedural Controls based on a risk analysis in which applicable risks have been taken into account.
Comment	-

5.2.1 Trusted roles

No stipulation.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

No stipulation.

5.2.4 Roles requiring separation of duties PKIoverheid

No stipulation.

5.3 Personnel controls

5.3-tpkio31

Description	A TSP SHALL take all appropriate measures concerning Personnel Controls based on a risk analysis in which applicable risks have been taken into account.
Comment	-

5.3.1 Qualifications, experience, and clearance requirements

No stipulation.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No stipulation.

5.4 Audit logging procedures

5.4.1 Types of events recorded

No stipulation.

5.4.2 Frequency of processing log

No stipulation.

5.4.3 Retention period for audit log

No stipulation.

5.4.4 Protection of audit log

No stipulation.

5.4.5 Audit log backup procedures

No stipulation.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

No stipulation.

5.5.2 Retention period for archive

No stipulation.

5.5.3 Protection of archive

No stipulation.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

No stipulation.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

No stipulation.

5.7.2 Computing resources, software, and_or data are corrupted

No stipulation.

5.7.3 Entity private key compromise procedures

No stipulation.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA termination

No stipulation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1-tpkio32

Description	The TSP SHALL reject a certificate request if the requested Public Key does not meet the requirements as listed in sections 6.1.5 Key sizes and 6.1.6 Public key parameters generation and quality checking or if it has a known weak Private Key.
Comment	-

6.1.1-tpkio35

Description	A TSP SHALL NOT generate key pairs for server certificates.
Comment	-

6.1.2 Private key delivery to subscriber

No stipulation.

6.1.3 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to relying parties

See [2.2-tpkio12](#).

6.1.5 Key sizes

6.1.5-tpkio34

Description	Certificates issued to end-users MUST meet the following requirements for algorithm type and key size:
Comment	-

Type	Permitted Values
Digest algorithm	SHA-256 or SHA-384

Minimum RSA modulus size (bits)	2048
ECC curve	P-256 or P-384

6.1.6 Public key parameters generation and quality checking

No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

No stipulation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2-tpkio36

Description	A TSP SHALL take all appropriate measures concerning protection of the signing key of a PKIoverheid TRIAL TSP CA (issuing CA) based on a risk analysis in which applicable risks have been taken into account.
Comment	-

6.2.1 Cryptographic module standards and controls

No stipulation.

6.2.2 Private key (n out of m) multi-person control

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

No stipulation.

6.2.5 Private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

No stipulation.

6.2.8 Method of activating private key

No stipulation.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

6.3.2-tpkio37

Description	Private keys that are used by a certificate holder and issued under the requirements of this CP MUST NOT be used for more than 397 days. The certificates, which are issued under the requirements of this CP, MUST NOT be valid for more than 397 days as well.
Comment	-

6.4 Activation data

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5-tpkio41

Description	A TSP SHALL take all appropriate measures concerning Computer Security Controls based on a risk analysis in which applicable risks have been taken into account.
Comment	-

6.5.1 Specific computer security technical requirements

No stipulation.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

6.7-tpkio42

Description	A TSP SHALL take all appropriate measures concerning Network Security Controls based on a risk analysis in which applicable risks have been taken into account.
Comment	-

6.8 Time-stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1-tpkio44

Description	The TSP SHALL meet the technical requirements set forth in Section 2.2 Publication of certification information , Section 6.1.5 Key sizes and Section 6.1.6 Public key parameters generation and quality checking .
Comment	-

7.1-tpkio45

Description	<p>A Serial Number MUST be included in a certificate. The serial number of a PKIoverheid certificate issued by A TSP MUST comply with the following requirements:</p> <ol style="list-style-type: none"> 1. The value of the serial number MUST NOT be 0 (zero) 2. The value of the serial number MUST NOT be negative 3. The value of the serial number MUST be unique for each certificate issued by a given TSP CA 4. The serial number SHALL have a minimum length of 96 bits (12 octets) 5. The serial number SHALL contain at least 64 bits of random data 6. The random data SHOULD be generated by a CSPRNG (Cryptographically Secure Pseudorandom Number Generator). 7. The serial number MUST NOT be longer than 160 bits (20 octets).
Comment	-

7.1-tpkio47

Description	A TSP MUST only include certificate fields and extensions in a PKIoverheid TRIAL end-user certificate that explicitly listed in section 7.1 Certificate profile .
Comment	-

7.1-tpkio67

Description	The Signature field MUST be included and it's content MUST be set to match the requirements as described in section 6.1.5-tpkio34 .
Comment	-

7.1-tpkio68

Description	A TSP MUST include the Validity field as indicated in RFC5280 section 4.1.2.5. The values used in this field MUST be set as not to exceed the maximum validity period as defined in section 6.3.2 Certificate operational periods and key pair usage periods .
Comment	-

7.1-tpkio81

Description	The subjectPublicKeyInfo field MUST be included in het certificate. Requirements on the key size and algoritms allowed are specified in sections 6.1.5 Key sizes and 7.1.3 Algorithm object identifiers .
Comment	-

7.1.1 Version number(s)

7.1.1-tpkio43

Description	Certificates issued by TSPs operating within the PKIOverheid framework MUST be of type X.509 v3.
Comment	-

7.1.2 Certificate extensions

7.1.2-tpkio46

Description	The Validity field MUST be set in accordance with both RFC5280 and the requirements puth forth in section 6.3.2 of this CP regarding certificate lifespan.
Comment	-

7.1.2-tpkio48

Description	A TSP MUST include the KeyUsage field in a PKIOverheid TRIAL certificate under this CP. This field must be marked as Critical and MUST only contains the digitalSignature and keyEncipherment bits.
Comment	-

7.1.2-tpkio49

Description	The field SubjectKeyIdentifier MUST be included in a PKIOverheid TRIAL certificate. The field MUST be set in accordance with RFC5280.
--------------------	---

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

7.1.2-tpkio50

Description	A TSP MUST include the KeyUsage field in a PKIoverheid TRIAL certificate under this CP. This field must be marked as Critical and MUST only contains the digitalSignature bit.
Comment	-

7.1.2-tpkio51

Description	A TSP MUST include the KeyUsage field in a PKIoverheid TRIAL certificate under this CP. This field must be marked as Critical and MUST only contain the keyEncipherment and dataEncipherment bits.
Comment	-

7.1.2-tpkio52

Description	A TSP MUST include the KeyUsage field in a PKIoverheid TRIAL certificate under this CP. This field must be marked as Critical and MUST only contain the nonRepudiation bit.
Comment	-

7.1.2-tpkio53

Description	A TSP MAY include the BasicConstraints extension. If included, the cA boolean MUST be an empty value. The pathLenConstraint MUST NOT be used.
Comment	-

7.1.2-tpkio54

Description	A TSP MUST include the CRLDistributionPoints. The extension MUST NOT be marked critical, and it MUST contain the HTTP URL or LDAP location of the CA's CRL service. The attribute Reason MUST NOT be used.
Comment	-

7.1.2-tpkio55

Description	A TSP MUST include the extension ExtendedKeyUsage. This extension MUST NOT be marked as critical and MUST include the KeyPurposdeIDs id-kp-serverAuth (RFC5280) en ad-kp-clientAuth (RFC5280).
--------------------	--

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

7.1.2-tpkio56

Description	A TSP MUST include the extension ExtendedKeyUsage. This extension MUST NOT be marked as critical and MUST include the KeyPurposeIDs id-kp-clientAuth (RFC5280), id-kp-emailProtection (RFC5280) and document Signing (OID 1.3.6.1.4.1.311.10.3.12).
Comment	-

7.1.2-tpkio57

Description	A TSP MUST include the extension ExtendedKeyUsage. This extension MUST NOT be marked as critical and MUST include the KeyPurposeIDs id-kp-emailProtection (RFC5280) and document Signing (OID 1.3.6.1.4.1.311.10.3.12).
Comment	-

7.1.2-tpkio58

Description	A TSP MUST include the extension ExtendedKeyUsage. This extension MUST NOT be marked as critical and MUST include the KeyPurposeIDs id-kp-emailProtection (RFC5280) and Encryption File System (OID 1.3.6.1.4.1.311.10.3.4).
Comment	-

7.1.2-tpkio59

Description	A TSP MAY include the FreshestCRL extension. If included, it MUST NOT be marked critical. In order to fulfill the requirements of PKIoverheid a TSP MUST also publish full CRLs.
Comment	-

7.1.2-tpkio60

Description	A TSP MAY include the authorityInformationAccess extension to be used to reference other additional information about the TSP . IT MUST NOT be marked as critical. If the TSP supports OCSP, this extension MUST include the URI of an OCSP responder.
Comment	-

7.1.2-tpkio61

Description	A TSP MUST include the authorityInformationAccess extension. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It MUST also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).
Comment	-

7.1.2-tpkio64

Description	A TSP MAY include the subjectDirectoryAttributes field. If included, it MUST NOT be marked at critical. The TSP SHALL NOT include personal information that can hurt the privacy of the subject
Comment	-

7.1.2-tpkio65

Description	A TSP MAY include the BiometricInfo extension. If included, it MUST NOT be marked as critical, MUST contain a hash of a biometric template and MAY contain an URI to refer to a file containing the biometric template itself.
Comment	-

7.1.2-tpkio66

Description	A TSP MUST include the qcStatement-2 extension as defined in RFC3739 section 3.6.2.1. The extension MUST NOT be marked as critical and MUST include the semanticsidentifier id-etsi-qcs-SemanticsId-Legal as defined in ETSI TS 119 412-1 section 5.1.3. Contrary to section 5.1.3, a TSP SHALL only use the prefix NTR. Any other prefix, if offered by ETSI TS 119 412-1 MUST NOT be used.
Comment	-

7.1.2-tpkio82

Description	The field AuthorityKeyIdentifier MUST be included in a PKIoverheid TRIAL certificate. The field MUST be set in accordance with RFC5280.
Comment	-

7.1.2-tpkio115

Description	A TSP MAY include the Subject.GivenName field. When included this field MUST contain a correct reproduction of the element of the name laid down in the CN, based on the Compulsory Identification Act document.
--------------------	--

Comment	This field MUST show the subject's given name correctly, as shown on the Compulsory Identification Act document.
----------------	--

7.1.2-tpkio116

Description	<p>A TSP MAY include the Subject.SurName field. When included this field MUST contain a correct reproduction of the element of the name laid down in the CN, based on the Compulsory Identification Act document.</p> <p>This field MUST show the subject's surname including surname prefixes correctly, as shown on the Compulsory Identification Act document.</p>
Comment	

7.1.2-tpkio124

Description	<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>
Comment	<p>The aforementioned QcStatement identifiers relate to the following OIDs:</p> <ul style="list-style-type: none"> • <i>id-etsi-qcs-QcCompliance</i> { <i>id-etsi-qcs</i> 1 } (or 0.4.0.1862.1.1) • <i>id-etsi-qct-esign</i> { <i>id-etsi-qcs-QcType</i> 1 } (or 0.4.0.1862.1.6.1) • <i>id-etsi-qcs-QcSSCD</i> { <i>id-etsi-qcs</i> 4 } (or 0.4.0.1862.1.4) • <i>id-etsi-qcs-QcPDS</i> { <i>id-etsi-qcs</i> 5 } (or 0.4.0.1862.1.5)

7.1.3 Algorithm object identifiers

7.1.3-tpkio62

Description	TSPs MUST only use the key sizes and signature algorithms defined in requirements 6.1.5-tpkio34 .
Comment	-

7.1.4 Name forms

7.1.4-tpkio63

Description	The Issuer field MUST be included. It MUST contain a Distinguished Name which MUST match the Subject DN of the Issuing CA to support name chaining as specified in RFC 5280, Section 4.1.2.4.
Comment	-

7.1.4-tpkio68

Description	The Subject Field MUST be included. Subject attributes MUST NOT contain only metadata such as `', `-', and ` ` (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.
Comment	-

7.1.4-tpkio69

Description	<p>The subject.commonName attribute MUST be included. It MUST contain the following information:</p> <p>[aristocratic designation] [Full first forename OR nickname] [initials other forenames OR full other forenames] [surname prefixes + surname partner '-'] [aristocratic title] [<i>surname prefixes + surname at birth</i>]</p> <p>whereby:</p> <p>text in bold = compulsory part</p> <p><i>Italic</i> = compulsory part, style in accordance with Compulsory Identification Act document</p> <p>normal = optional part;</p> <p>It also MUST include the word "TRIAL" after the initial subject information to indicate that it is a TRIAL certificate and is to be used for testing purposes only.</p>
Comment	-

7.1.4-tpkio70

Description	The subject.commonName attribute MUST be included. It MUST include a name that identifies the service (e.g. the function of an organizational entity or the name by which the device or system is known). It also MUST include the word "TRIAL" after the initial subject information to indicate that it is a TRIAL certificate and is to be used for testing purposes only.
Comment	-

7.1.4-tpkio71

<p>Description</p>	<p>The subject.commonName attribute SHOULD NOT be included. If included, it SHOULD contain either a FQDN (Fully Qualified Domain Name) or an IP address. An FQDN must also appear in the SubjectAltName.DNsName field. An IP address MUST also appear in the SubjectAltName.iPAddress field.</p> <p>If it is not possible or desirable to include an FQDN in the subject.commonName field, but the field is necessary for the server to function properly, a TSP MAY choose to include the function of an organizational entity or the name with which the service, device or system is indicated.</p> <p>A server certificate MAY contain multiple FQDNs from different domains on condition that these domains are registered in the name of the same subscriber or are under authorization by the same subscriber. This means that a TSP cannot combine FQDNs in one certificate that are both from different domains and are registered in the name of different owners. The following is NOT allowed to be included in the Subject.Commonname field, SubjectAltName.iPAddress or the SubjectAltName.DNname field</p> <ul style="list-style-type: none"> • wildcard FQDNs; • local domain names; • private IP addresses; • internationalized domain names (IDNs); • null characters \0-generic TopLevel Domain (gTLD); • Country code TopLevelDomein (ccTLD).
<p>Comment</p>	<p>-</p>

7.1.4-tpkio72

<p>Description</p>	<p>The following values MUST NOT be included in the Subject.Commonname field, SubjectAltName.iPAdres or the SubjectAltName.DNname field:</p> <ul style="list-style-type: none"> • wildcard FQDNs • local domain names • private IP addresses • internationalized domain names (IDNs) • null characters \0 • generic TopLevel Domain (gTLD) • Country code TopLevelDomein (ccTLD)
<p>Comment</p>	<p>-</p>

7.1.4-tpkio73

Description	The Subject.countryName attribute MUST be included in a certificate. It MUST contain a 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.
Comment	-

7.1.4-tpkio74

Description	The Subject.organizationName attribute MUST be included in a certificate. It MUST contain the full organization name of the subscriber as supplied by the subscriber during registration. It also MUST include the word "TRIAL" after the initial subject information to indicate that it is a TRIAL certificate and is to be used for testing purposes only.
Comment	-

7.1.4-tpkio75

Description	The Subject.organizationalUnitName MUST be included in a certificate. It MUST contain the text "only to be used for testing purposes". Additional instances of this attribute MAY be included in a certificate if needed. If so included, it MUST NOT contain a function indication or similar and MUST contain a valid name of an organisational entity of the subscriber in accordance with an accepted document or registry.
Comment	-

7.1.4-tpkio76

Description	The Subject.stateOrProvinceName attribute MAY be included in a certificate. If included, it MUST include the province or state in which the subscriber is registered according to the accepted document or registry.
Comment	-

7.1.4-tpkio77

Description	The Subject.localityName attribute MAY be included in a certificate. If included IT MUST include the location of the subscriber, in accordance with the accepted document or registry.
Comment	-

7.1.4-tpkio78

Description	The Subject.postalAddress and Subject.postalCode attributes MUST NOT be included in a certificate.
Comment	-

7.1.4-tpkio79

Description	The Subject.serialNumber MUST be included in a certificate. It MUST contain a number which can be determined by the TSP. The combination of CommonName, OrganizationName and Serialnumber MUST be unique within the context of the TSP. To avoid susceptibilities a serial Number attribute MUST be allocated to every subject.
Comment	-

7.1.4-tpkio80

Description	The Subject.serialNumber MAY be included in a certificate. If included, It MUST contain a number generated by the TSP so that the combination of CommonName, OrganizationName and Serialnumber is unique within the context of the TSP, or MUST contain an OIN/HRN. The TSP SHALL only use 20 position serial numbers for OIN/HRN and only after additional arrangements have been made with Logius.
Comment	-

7.1.4-tpkio83

Description	<p>Certificates SHALL contain the <code>extensions:subjectAltName</code> extension with at least one instance of the <code>dnsName</code> attribute in its <code>extValue</code> field.</p> <p>Each <code>dnsName</code> attribute SHALL contain a Fully-Qualified Domain Name (FQDN).</p> <p>The FQDN SHALL:</p> <ul style="list-style-type: none"> • be in the "preferred name syntax", as specified in RFC5280, and • be owned or controlled by the Subject and to be associated with the Subject's server which MAY be owned and operated by the Subject or another entity (e.g., a hosting service), the verification of which is described in Section 3.2.5. <p>Additionally, the FQDN SHALL NOT:</p> <ul style="list-style-type: none"> • contain a wildcard, and/or • be an Internal Name. <p>The total number of instances of the <code>dnsName</code> attribute in a single certificate SHALL NOT:</p> <ul style="list-style-type: none"> • exceed 10 when these instances consist of just one Base Domain Name and sub-domains thereof, or • exceed 5 when these instances consist of mixed Base Domain Names.
Comment	Further details and requirements for the Othername attribute are listed under 7.1.4-tpkio85

7.1.4-tpkio84

Description	The subjectAltName field MUST be included in a certificate. Each entry MUST be a Othername attribute.
Comment	Further details and requirements for the Othername attribute are listed under 7.1.4-tpkio85

7.1.4-tpkio85

Description	<p>If a certificate contains a subject.Altname.OtherName field, it MUST include an OID of the TSP assigned by the PA to the TSP, as well as a number that is unique within the namespace of that OID that permanently identifies the subject, in one of the following ways:</p> <ol style="list-style-type: none"> 1. MS UPN: <i>(number)@(OID)</i> 2. MS UPN (OID).<i>(number)</i> 3. IA5String: <i>(OID)-(number)</i> 4. <i>Permanent Identifier:Identifiervalue = numberAssigner = OID</i> <p>The chosen number MUST be persistent.</p>
Comment	It is recommended that an existing registration number from back office systems is used, in combination with a code for the organization. In combination with the TSP OID, this identifier is internationally unique.

7.1.4-tpkio117

Description	The SubjectAltName.rfc822Name attribute MAY be included. If included it is to be used for the e-mail address of the certificate holder, for applications that need the e-mail address to function properly.
Comment	-

7.1.4-tpkio118

Description	The SubjectAltName.rfc822Name attribute MAY be included. If included it is to be used for the e-mail address of the service, for applications that need the e-mail address to function properly.
Comment	-

7.1.4-tpkio119

Description	<p>The SubjectAltName.otherName attribute MUST be included. It MUST be used containing a unique identification number that identifies the certificate holder. In addition, in the authentication certificate, an 'othername' MAY be included for use with Single Sign On (SSO).</p> <p>The field must contain one of the following strings: IA5String, Microsoft UPN, IBM Principal-Name, Kerberos PrincipalName or Permanent-Identifier.</p>
Comment	<ol style="list-style-type: none"> 1. MS UPN: [number]@[OID] 2. MS UPN: [OID].[number] 3. IA5String: [OID]-[number] 4. Permanent Identifier: Identifiervalue = [number]Assigner = [OID]

7.1.4-tpkio120

Description	<p>The Subject.organizationIdentifier attribute MUST be included. The organizationIdentifierfield contains an identification of the subject.</p>
Comment	<p>The type is string and the syntax of the identification string is specified in paragraph 5.1.4 of ETSI EN 319 412-1 and contains:</p> <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).

7.1.4-tpkio121

Description	<p>The Subject.serialNumber attribute MAY be included. If included the TSP is responsible for safeguarding the uniqueness of the subject (service). The Subject.serialNumber MUST be used to identify the subject uniquely. The use of 20 positions is only allowed for OIN and HRN after additional arrangements with Logius.</p>
Comment	<p>The type is Printable String and the number is determined by the TSP and/or the government. The number can differ for each domain and can be used for several applications.</p>

7.1.4-tpkio122

Description	<p>The Subject.Surname attribute MUST be included when it is included in the Compulsory Identification Act document. A correct reproduction of the element of the name laid down in the CN. Based on the Compulsory Identification Act document. It MUST be in the UTF8String Format.</p>
Comment	<p>This field MUST show the subject's surname including surname prefixes correctly, as shown on the Compulsory Identification Act document.</p>

7.1.4-tpkio123

Description	The Subject.givenName attribute MUST be included when it is included in the Compulsory Identification Act document. A correct reproduction of the element of the name laid down in the CN. Based on the Compulsory Identification Act document. It MUST be in the UTF8String Format.
Comment	This field MUST show the subject's given name correctly, as shown on the Compulsory Identification Act document.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

7.1.6-tpkio11

Description	The Certificatepolicies extension MUST be included, MUST NOT be marked as critical, and MUST contain the policyIdentifier 2.1.6.528.1.1003.1.2.9.1 ({joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1) nederlandse-overheid(1003) pki-voor-de-overheid(1) cp(2).test(9).authenticiteitpersoon(1)})
Comment	-

7.1.6-tpkio86

Description	The Certificatepolicies extension MUST be included, MUST NOT be marked as critical, and MUST contain the policyIdentifier 2.1.6.528.1.1003.1.2.9.2 ({joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1) nederlandse-overheid(1003) pki-voor-de-overheid(1) cp(2).test(9).onweerlegbaarheid(2)})
Comment	-

7.1.6-tpkio87

Description	The Certificatepolicies extension MUST be included, MUST NOT be marked as critical, and MUST contain the policyIdentifier 2.1.6.528.1.1003.1.2.9.3 ({joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1) nederlandse-overheid(1003) pki-voor-de-overheid(1) cp(2).test(9).vertrouwelijkheid(3)})
Comment	-

7.1.6-tpkio88

Description	The Certificatepolicies extension MUST be included, MUST NOT be marked as critical, and MUST contain the policyIdentifier 2.1.6.528.1.1003.1.2.9.4 ({joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1) nederlandse-overheid(1003) pki-voor-de-overheid(1) cp(2).test(9).authenticiteit-services(4)})
--------------------	--

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

7.1.6-tpkio89

Description	The Certificatepolicies extension MUST be included, MUST NOT be marked as critical, and MUST contain the policyIdentifier 2.1.6.528.1.1003.1.2.9.5 ({joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1) nederlandse-overheid(1003) pki-voor-de-overheid(1) cp(2).test(9).vertrouwelijkheid-services(5)}
Comment	-

7.1.6-tpkio90

Description	The Certificatepolicies extension MUST be included, MUST NOT be marked as critical, and MUST contain the policyIdentifier 2.1.6.528.1.1003.1.2.9.6 ({joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1) nederlandse-overheid(1003) pki-voor-de-overheid(1) cp(2).test(9).server(6)}
Comment	-

7.1.6-tpkio93

Description	The Certificatepolicies extension MUST be included, MUST NOT be marked as critical, and MUST contain the policyIdentifier 2.1.6.528.1.1003.1.2.9.10 ({joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1) nederlandse-overheid(1003) pki-voor-de-overheid(1) cp(2).test(9).onweerlegbaarheid-services(10)}
Comment	-

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

7.1.8-tpkio94

Description	A user notice qualifier MUST be included in the certificatePolicies extension and MUST contain an explicitText field. The explicitText field MUST mention the testing nature of the PKIoverheid TRIAL certificate and MAY include further disclaimers by the TSP as indicated in section 1.3.4 Relying parties .
Comment	-

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2-tpkio96

Description	Requirements 7.1-tpkio67 and 7.1.4-tpkio63 MUST be adhered to by the TSP for the CRL profile.
Comment	-

7.2-tpkio98

Description	The ThisUpdate and NextUpdate fields MUST be included in a CRL. If this CP imposed requirements on TSPs for the maximum validity of an CRL in section 4.10 Certificate status services a TSP MUST set the values of these fields accordingly.
Comment	-

7.2-tpkio99

Description	The revokedCertificates field MUST be included in a CRL. It MUST include the date and time of revocation and serialNumber of the revoked certificates. If there are no revoked certificates, this field MUST NOT be present.
Comment	-

7.2.1 Version number(s)

No stipulation.

7.2.1-tpkio95

Description	CRLs issued by TSPs MUST be version 2.
Comment	-

7.2.2 CRL and CRL entry extensions

No stipulation.

7.2.2-tpkio100

Description	The authorityKeyIdentifier field MAY be included. If included, it MUST NOT be marked as critical and MUST include the SHA-1 hash from authorityKey (public key of the TSP/CA).
Comment	-

7.2.2-tpkio102

Description	The IssuerAltName field SHOULD NOT be included in a CRL. If included, it MUST NOT be set as critical and MUST include a DNS name, IP address or URI. A RFC822 name MUST NOT be used.
Comment	-

7.2.2-tpkio103

Description	The CRLNumber extension MUST be included in a CRL. It MUST NOT be marked critical and it MUST contain an incremental number that provides support when determining the order of CRLs.
Comment	-

7.2.2-tpkio104

Description	The DeltaCRLIndicator extension MAY be included in a CRL to mark it als a Delta CRL. If included, it MUST be marked as critical and contain the number of the baseCRL it updates.
Comment	-

7.2.2-tpkio105

Description	The issuingDistributionPoint extension MAY be included in a CRL. If included, it MUST be marked as critical and MUST conform to the specifications and requirements as defined by RFC5280 section 5.2.5
Comment	-

7.2.2-tpkio106

Description	The FreshestCRL extension MAY be included in a full CRL. IT MUST NOT be included in a Delta CRL. If included, it MUST NOT be marked as critical and MUST contain the URI of a Delta CRL distribution point.
Comment	-

7.2.2-tpkio107

Description	The authorityInfoAccess extension MAY be included in a CRL. If included, it MUST NOT be marked as critical. and MUST conform to section 5.2.7 of RFC5280.
Comment	-

7.2.2-tpkio108

Description	The reasonCode extension MAY be included in a CRL. If included, it MUST NOT be marked as critical and MUST contain a valid reason for revocation per RFC 5280 section 5.3.1. If no reason is given, this extension MUST be omitted.
Comment	-

7.2.2-tpkio109

Description	The invalidityDate attribute MAY be included in a CRL entry. If included, it MUST NOT be marked as critical and MUST indicate the date and time on which the certificate was suspected to have been compromised or otherwise made invalid if it precedes the date and time on which the TSP processed the revocation.
Comment	-

7.2.2-tpkio110

Description	The certificate Issuer extension SHOULD NOT be included in a CRL. If included, it MUST be marked as critical and MUST be used to identify the original issuer of the certificate.
Comment	-

7.3 OCSP profile

7.3-tpkio111

Description	<p>The following requirements MUST be adhered to by a TSP with regards to the OCSP profile:</p> <ul style="list-style-type: none"> • 7.1-tpkio44 • 7.1-tpkio45 • 7.1-tpkio67 • 7.1-tpkio68 • 7.1-tpkio81 • 7.1.1-tpkio43 • 7.1.2-tpkio50 • 7.1.2-tpkio54 • 7.1.3-tpkio62 • 7.1.4-tpkio63 • 7.1.4-tpkio68 • 7.1.4-tpkio70 • 7.1.4-tpkio73 • 7.1.4-tpkio74 • 7.1.4-tpkio75 • 7.1.4-tpkio76 • 7.1.4-tpkio77 • 7.1.4-tpkio78 • 7.1.6-tpkio88 • 7.1.8-tpkio94
Comment	-

7.3.1 Version number(s)

7.3.2 OCSP extensions

No stipulation.

7.3.2-tpkio112

Description	<p>When issuing an OCSP signing certificate, a TSP MUST include the extension ExtendedKeyUsage. This extension MUST be marked as critical and MUST include the KeyPurposeID id-kp-OCSPSigning.</p>
Comment	-

7.3.2-tpkio113

Description	When issuing an OCSP signing certificate, a TSP MUST include the extension ocspNoCheck. This extension SHOULD NOT be marked critical. The value of the extension MUST be NULL
Comment	-

7.3.2-tpkio114

Description	When issuing an OCSP signing certificate, a TSP MAY include the extension ocspNoCheck. If included, this extension SHOULD NOT be marked critical and the value of the extension MUST be NULL.
Comment	-

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The PKIoverheid TRIAL hierarchy is designed and built upon the principle of "best effort" to emulate the technical aspects and requirements of PKIoverheid production certificates within the environment of a TSP's internal organization or a subscriber's staging environment. As such, no specific external or internal audit requirements are applicable to TSP's operating under this CP.

8.1 Frequency or circumstances of assessment

No stipulation.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

No stipulation.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

No stipulation.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

See [1.3.4 Relying parties](#)

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

9.7-tpkio97

Description	In the agreement between the TSP and the subscriber a clause MUST be included in which the TSP disclaims all warranties regarding the perceived trustworthiness and availability of PKIoverheid TRIAL certificates or it's associated revocation checking mechanisms.
Comment	-

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

The change procedure for the PoR of the PKIoverheid is incorporated in PKIoverheid's Certificate PracticeStatement. The CPS can be obtained in an electronic format on the PA's website: <https://cps.pkioverheid.nl>

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

Dutch law is applicable to the CPs of PKIoverheid.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.


9.16.5 Force Majeure

No stipulation.






























9.17 Other provisions

No stipulation.

Appendix A: Requirements (CP) for personal authentication certificates (OID 2.16.528.1.1003.1.2.9.1)

 This Appendix is only a list of requirements for which explicit requirements have been defined in this CP. This Appendix is only provides for the benefit of TSPs for an overview per certificate type.


Requirements in this CP for OID 2.16.528.1.1003.1.2.9.1

-  1.4.1-tpkio33
-  2.1-tpkio2
-  2.2-tpkio12
-  2.2-tpkio13
-  2.4-tpkio14
-  3.2.2-tpkio15
-  3.2.2-tpkio17
-  3.2.2-tpkio5
-  3.2.3-tpkio19
-  3.2.3-tpkio20
-  3.2.3-tpkio4
-  4.1-tpkio9
-  4.10.1-tpkio28
-  4.3.1-tpkio10
-  4.7.1-tpkio21
-  4.9.10-tpkio25
-  4.9.13-tpkio27
-  4.9.7-tpkio1
-  4.9.9-tpkio24
-  5.1-tpkio29
-  5.2-tpkio30
-  5.3-tpkio31
-  6.1.1-tpkio32
-  6.1.5-tpkio34
-  6.2-tpkio36
-  6.3.2-tpkio37
-  6.5-tpkio41
-  6.7-tpkio42
-  7.1-tpkio44
-  7.1-tpkio45
-  7.1-tpkio47































-  7.1-tpkio67
-  7.1-tpkio68
-  7.1-tpkio81
-  7.1.1-tpkio43
-  7.1.2-tpkio115
-  7.1.2-tpkio116
-  7.1.2-tpkio46
-  7.1.2-tpkio48
-  7.1.2-tpkio49
-  7.1.2-tpkio50
-  7.1.2-tpkio53
-  7.1.2-tpkio54
-  7.1.2-tpkio56
-  7.1.2-tpkio59
-  7.1.2-tpkio60
-  7.1.2-tpkio64
-  7.1.2-tpkio65
-  7.1.2-tpkio82
-  7.1.3-tpkio62
-  7.1.4-tpkio117
-  7.1.4-tpkio119
-  7.1.4-tpkio122
-  7.1.4-tpkio123
-  7.1.4-tpkio63
-  7.1.4-tpkio68
-  7.1.4-tpkio69
-  7.1.4-tpkio73
-  7.1.4-tpkio74
-  7.1.4-tpkio75
-  7.1.4-tpkio76
-  7.1.4-tpkio77
-  7.1.4-tpkio78
-  7.1.4-tpkio79
-  7.1.4-tpkio84
-  7.1.4-tpkio85
-  7.1.6-tpkio11
-  7.1.8-tpkio94

-  7.2-tpkio96
-  7.2-tpkio98
-  7.2-tpkio99
-  7.2.1-tpkio95
-  7.2.2-tpkio100
-  7.2.2-tpkio102
-  7.2.2-tpkio103
-  7.2.2-tpkio104
-  7.2.2-tpkio105
-  7.2.2-tpkio106
-  7.2.2-tpkio107
-  7.2.2-tpkio108
-  7.2.2-tpkio109
-  7.2.2-tpkio110
-  7.3.2-tpkio112
-  7.3.2-tpkio114
-  9.7-tpkio97

Appendix B: Requirements (CP) for personal signature certificates (OID 2.16.528.1.1003.1.2.9.2)

 This Appendix is only a list of requirements for which explicit requirements have been defined in this CP. This Appendix is only provides for the benefit of TSPs for an overview per certificate type.


Requirements in this CP for OID 2.16.528.1.1003.1.2.9.2

-  1.4.1-tpkio33
-  2.1-tpkio2
-  2.2-tpkio12
-  2.2-tpkio13
-  2.4-tpkio14
-  3.2.2-tpkio15
-  3.2.2-tpkio17
-  3.2.2-tpkio5
-  3.2.3-tpkio19
-  3.2.3-tpkio20
-  3.2.3-tpkio4
-  4.1-tpkio9
-  4.10.1-tpkio28
-  4.3.1-tpkio10
-  4.7.1-tpkio21
-  4.9.10-tpkio25
-  4.9.13-tpkio27
-  4.9.7-tpkio1
-  4.9.9-tpkio24
-  5.1-tpkio29
-  5.2-tpkio30
-  5.3-tpkio31
-  6.1.1-tpkio32
-  6.1.5-tpkio34
-  6.2-tpkio36
-  6.3.2-tpkio37
-  6.5-tpkio41
-  6.7-tpkio42
-  7.1-tpkio44
-  7.1-tpkio45
-  7.1-tpkio47



























-  7.1-tpkio67
-  7.1-tpkio68
-  7.1-tpkio81
-  7.1.1-tpkio43
-  7.1.2-tpkio115
-  7.1.2-tpkio116
-  7.1.2-tpkio124
-  7.1.2-tpkio46
-  7.1.2-tpkio48
-  7.1.2-tpkio49
-  7.1.2-tpkio52
-  7.1.2-tpkio53
-  7.1.2-tpkio54
-  7.1.2-tpkio57
-  7.1.2-tpkio59
-  7.1.2-tpkio60
-  7.1.2-tpkio64
-  7.1.2-tpkio65
-  7.1.2-tpkio82
-  7.1.3-tpkio62
-  7.1.4-tpkio117
-  7.1.4-tpkio119
-  7.1.4-tpkio122
-  7.1.4-tpkio123
-  7.1.4-tpkio63
-  7.1.4-tpkio68
-  7.1.4-tpkio69
-  7.1.4-tpkio73
-  7.1.4-tpkio74
-  7.1.4-tpkio75
-  7.1.4-tpkio76
-  7.1.4-tpkio77
-  7.1.4-tpkio78
-  7.1.4-tpkio79
-  7.1.4-tpkio84
-  7.1.4-tpkio85
-  7.1.6-tpkio86

-  7.1.8-tpkio94
-  7.2-tpkio96
-  7.2-tpkio98
-  7.2-tpkio99
-  7.2.1-tpkio95
-  7.2.2-tpkio100
-  7.2.2-tpkio102
-  7.2.2-tpkio103
-  7.2.2-tpkio104
-  7.2.2-tpkio105
-  7.2.2-tpkio106
-  7.2.2-tpkio107
-  7.2.2-tpkio108
-  7.2.2-tpkio109
-  7.2.2-tpkio110
-  7.3.2-tpkio112
-  7.3.2-tpkio114
-  9.7-tpkio97

Appendix C: Requirements (CP) for personal encryption certificates (OID 2.16.528.1.1003.1.2.9.3)

 This Appendix is only a list of requirements for which explicit requirements have been defined in this CP. This Appendix is only provides for the benefit of TSPs for an overview per certificate type.


Requirements in this CP for OID 2.16.528.1.1003.1.2.9.3

-  1.4.1-tpkio33
-  2.1-tpkio2
-  2.2-tpkio12
-  2.2-tpkio13
-  2.4-tpkio14
-  3.2.2-tpkio15
-  3.2.2-tpkio17
-  3.2.2-tpkio5
-  3.2.3-tpkio19
-  3.2.3-tpkio20
-  3.2.3-tpkio4
-  4.1-tpkio9
-  4.10.1-tpkio28
-  4.3.1-tpkio10
-  4.7.1-tpkio21
-  4.9.10-tpkio25
-  4.9.13-tpkio27
-  4.9.7-tpkio1
-  4.9.9-tpkio24
-  5.1-tpkio29
-  5.2-tpkio30
-  5.3-tpkio31
-  6.1.1-tpkio32
-  6.1.5-tpkio34
-  6.2-tpkio36
-  6.3.2-tpkio37
-  6.5-tpkio41
-  6.7-tpkio42
-  7.1-tpkio44
-  7.1-tpkio45
-  7.1-tpkio47
































-  7.1-tpkio67
-  7.1-tpkio68
-  7.1-tpkio81
-  7.1.1-tpkio43
-  7.1.2-tpkio115
-  7.1.2-tpkio116
-  7.1.2-tpkio46
-  7.1.2-tpkio49
-  7.1.2-tpkio51
-  7.1.2-tpkio53
-  7.1.2-tpkio54
-  7.1.2-tpkio58
-  7.1.2-tpkio59
-  7.1.2-tpkio60
-  7.1.2-tpkio64
-  7.1.2-tpkio65
-  7.1.2-tpkio82
-  7.1.3-tpkio62
-  7.1.4-tpkio117
-  7.1.4-tpkio119
-  7.1.4-tpkio122
-  7.1.4-tpkio123
-  7.1.4-tpkio63
-  7.1.4-tpkio68
-  7.1.4-tpkio69
-  7.1.4-tpkio73
-  7.1.4-tpkio74
-  7.1.4-tpkio75
-  7.1.4-tpkio76
-  7.1.4-tpkio77
-  7.1.4-tpkio78
-  7.1.4-tpkio79
-  7.1.4-tpkio84
-  7.1.4-tpkio85
-  7.1.6-tpkio87
-  7.1.8-tpkio94
-  7.2-tpkio96

-  7.2-tpkio98
-  7.2-tpkio99
-  7.2.1-tpkio95
-  7.2.2-tpkio100
-  7.2.2-tpkio102
-  7.2.2-tpkio103
-  7.2.2-tpkio104
-  7.2.2-tpkio105
-  7.2.2-tpkio106
-  7.2.2-tpkio107
-  7.2.2-tpkio108
-  7.2.2-tpkio109
-  7.2.2-tpkio110
-  7.3.2-tpkio112
-  7.3.2-tpkio114
-  9.7-tpkio97

Appendix D: Requirements (CP) for services authentication certificates (OID 2.16.528.1.1003.1.2.9.4)

 This Appendix is only a list of requirements for which explicit requirements have been defined in this CP. This Appendix is only provides for the benefit of TSPs for an overview per certificate type.


Requirements in this CP for OID 2.16.528.1.1003.1.2.9.4

-  1.4.1-tpkio33
-  2.1-tpkio2
-  2.2-tpkio12
-  2.2-tpkio13
-  2.4-tpkio14
-  3.2.2-tpkio15
-  3.2.2-tpkio17
-  3.2.2-tpkio5
-  3.2.3-tpkio19
-  3.2.3-tpkio20
-  3.2.3-tpkio4
-  3.2.5-tpkio18
-  4.1-tpkio9
-  4.10.1-tpkio28
-  4.3.1-tpkio10
-  4.7.1-tpkio21
-  4.9.10-tpkio25
-  4.9.13-tpkio27
-  4.9.7-tpkio1
-  4.9.9-tpkio24
-  5.1-tpkio29
-  5.2-tpkio30
-  5.3-tpkio31
-  6.1.1-tpkio32
-  6.1.5-tpkio34
-  6.2-tpkio36
-  6.3.2-tpkio37
-  6.5-tpkio41
-  6.7-tpkio42
-  7.1-tpkio44
-  7.1-tpkio45































-  7.1-tpkio47
-  7.1-tpkio67
-  7.1-tpkio68
-  7.1-tpkio81
-  7.1.1-tpkio43
-  7.1.2-tpkio46
-  7.1.2-tpkio49
-  7.1.2-tpkio50
-  7.1.2-tpkio53
-  7.1.2-tpkio54
-  7.1.2-tpkio56
-  7.1.2-tpkio59
-  7.1.2-tpkio60
-  7.1.2-tpkio82
-  7.1.3-tpkio62
-  7.1.4-tpkio118
-  7.1.4-tpkio119
-  7.1.4-tpkio120
-  7.1.4-tpkio121
-  7.1.4-tpkio63
-  7.1.4-tpkio68
-  7.1.4-tpkio70
-  7.1.4-tpkio73
-  7.1.4-tpkio74
-  7.1.4-tpkio75
-  7.1.4-tpkio76
-  7.1.4-tpkio77
-  7.1.4-tpkio78
-  7.1.4-tpkio84
-  7.1.4-tpkio85
-  7.1.6-tpkio88
-  7.1.8-tpkio94
-  7.2-tpkio96
-  7.2-tpkio98
-  7.2-tpkio99
-  7.2.1-tpkio95
-  7.2.2-tpkio100

-  7.2.2-tpkio102
-  7.2.2-tpkio103
-  7.2.2-tpkio104
-  7.2.2-tpkio105
-  7.2.2-tpkio106
-  7.2.2-tpkio107
-  7.2.2-tpkio108
-  7.2.2-tpkio109
-  7.2.2-tpkio110
-  7.3.2-tpkio112
-  7.3.2-tpkio114
-  9.7-tpkio97

Appendix E: Requirements (CP) for services encryption certificates (OID 2.16.528.1.1003.1.2.9.5)

 This Appendix is only a list of requirements for which explicit requirements have been defined in this CP. This Appendix is only provides for the benefit of TSPs for an overview per certificate type.


Requirements in this CP for OID 2.16.528.1.1003.1.2.9.5

-  1.4.1-tpkio33
-  2.1-tpkio2
-  2.2-tpkio12
-  2.2-tpkio13
-  2.4-tpkio14
-  3.2.2-tpkio15
-  3.2.2-tpkio17
-  3.2.2-tpkio5
-  3.2.3-tpkio19
-  3.2.3-tpkio20
-  3.2.3-tpkio4
-  3.2.5-tpkio18
-  4.1-tpkio9
-  4.10.1-tpkio28
-  4.3.1-tpkio10
-  4.7.1-tpkio21
-  4.9.10-tpkio25
-  4.9.13-tpkio27
-  4.9.7-tpkio1
-  4.9.9-tpkio24
-  5.1-tpkio29
-  5.2-tpkio30
-  5.3-tpkio31
-  6.1.1-tpkio32
-  6.1.5-tpkio34
-  6.2-tpkio36
-  6.3.2-tpkio37
-  6.5-tpkio41
-  6.7-tpkio42
-  7.1-tpkio44
-  7.1-tpkio45




























-  7.1-tpkio47
-  7.1-tpkio67
-  7.1-tpkio68
-  7.1-tpkio81
-  7.1.1-tpkio43
-  7.1.2-tpkio46
-  7.1.2-tpkio49
-  7.1.2-tpkio53
-  7.1.2-tpkio54
-  7.1.2-tpkio58
-  7.1.2-tpkio59
-  7.1.2-tpkio60
-  7.1.2-tpkio82
-  7.1.3-tpkio62
-  7.1.4-tpkio118
-  7.1.4-tpkio119
-  7.1.4-tpkio120
-  7.1.4-tpkio121
-  7.1.4-tpkio63
-  7.1.4-tpkio68
-  7.1.4-tpkio70
-  7.1.4-tpkio73
-  7.1.4-tpkio74
-  7.1.4-tpkio75
-  7.1.4-tpkio76
-  7.1.4-tpkio77
-  7.1.4-tpkio78
-  7.1.4-tpkio84
-  7.1.4-tpkio85
-  7.1.6-tpkio89
-  7.1.8-tpkio94
-  7.2-tpkio96
-  7.2-tpkio98
-  7.2-tpkio99
-  7.2.1-tpkio95
-  7.2.2-tpkio100
-  7.2.2-tpkio102

-  7.2.2-tpkio103
-  7.2.2-tpkio104
-  7.2.2-tpkio105
-  7.2.2-tpkio106
-  7.2.2-tpkio107
-  7.2.2-tpkio108
-  7.2.2-tpkio109
-  7.2.2-tpkio110
-  7.3.2-tpkio112
-  7.3.2-tpkio114
-  9.7-tpkio97

Appendix F: Requirements (CP) for services signature certificates (OID 2.16.528.1.1003.1.2.9.10)

 This Appendix is only a list of requirements for which explicit requirements have been defined in this CP. This Appendix is only provides for the benefit of TSPs for an overview per certificate type.


Requirements in this CP for OID 2.16.528.1.1003.1.2.9.10

-  1.4.1-tpkio33
-  2.1-tpkio2
-  2.2-tpkio12
-  2.2-tpkio13
-  2.4-tpkio14
-  3.2.2-tpkio15
-  3.2.2-tpkio17
-  3.2.2-tpkio5
-  3.2.3-tpkio19
-  3.2.3-tpkio20
-  3.2.3-tpkio4
-  3.2.5-tpkio18
-  4.1-tpkio9
-  4.10.1-tpkio28
-  4.3.1-tpkio10
-  4.9.10-tpkio25
-  4.9.13-tpkio27
-  4.9.7-tpkio1
-  4.9.9-tpkio24
-  5.1-tpkio29
-  5.2-tpkio30
-  5.3-tpkio31
-  6.1.1-tpkio32
-  6.1.5-tpkio34
-  6.2-tpkio36
-  6.3.2-tpkio37
-  6.5-tpkio41
-  6.7-tpkio42
-  7.1-tpkio44
-  7.1-tpkio45
-  7.1-tpkio47

-  7.1-tpkio67
-  7.1-tpkio68
-  7.1-tpkio81
-  7.1.1-tpkio43
-  7.1.2-tpkio49
-  7.1.2-tpkio52
-  7.1.2-tpkio53
-  7.1.2-tpkio54
-  7.1.2-tpkio57
-  7.1.2-tpkio59
-  7.1.2-tpkio60
-  7.1.2-tpkio66
-  7.1.2-tpkio82
-  7.1.3-tpkio62
-  7.1.4-tpkio120
-  7.1.4-tpkio63
-  7.1.4-tpkio68
-  7.1.4-tpkio70
-  7.1.4-tpkio73
-  7.1.4-tpkio74
-  7.1.4-tpkio75
-  7.1.4-tpkio76
-  7.1.4-tpkio77
-  7.1.4-tpkio78
-  7.1.4-tpkio84
-  7.1.4-tpkio85
-  7.1.6-tpkio93
-  7.1.8-tpkio94
-  7.2-tpkio96
-  7.2-tpkio98
-  7.2-tpkio99
-  7.2.1-tpkio95
-  7.2.2-tpkio100
-  7.2.2-tpkio102
-  7.2.2-tpkio103
-  7.2.2-tpkio104
-  7.2.2-tpkio105

-  7.2.2-tpkio106
-  7.2.2-tpkio107
-  7.2.2-tpkio108
-  7.2.2-tpkio109
-  7.2.2-tpkio110
-  7.3.2-tpkio112
-  7.3.2-tpkio114
-  9.7-tpkio97

Appendix G: Requirements (CP) for server certificates (OID 2.16.528.1.1003.1.2.9.6)

 This Appendix is only a list of requirements for which explicit requirements have been defined in this CP. This Appendix is only provides for the benefit of TSPs for an overview per certificate type.

Requirements in this CP for OID 2.16.528.1.1003.1.2.9.6

-  1.4.1-tpkio3
-  2.1-tpkio2
-  2.2-tpkio12
-  2.2-tpkio13
-  2.4-tpkio14
-  3.2.1-tpkio6
-  3.2.2-tpkio15
-  3.2.2-tpkio16
-  3.2.2-tpkio17
-  3.2.2-tpkio5
-  3.2.3-tpkio19
-  3.2.3-tpkio20
-  3.2.3-tpkio4
-  3.2.3-tpkio7
-  3.2.5-tpkio8
-  4.1-tpkio9
-  4.10.1-tpkio28
-  4.3.1-tpkio10
-  4.7.1-tpkio22
-  4.9.10-tpkio25
-  4.9.13-tpkio27
-  4.9.7-tpkio1
-  4.9.9-tpkio26
-  4.9.9-tpkio3
-  5.1-tpkio29
-  5.2-tpkio30
-  5.3-tpkio31
-  6.1.1-tpkio32
-  6.1.1-tpkio35
-  6.1.5-tpkio34
-  6.2-tpkio36

-  6.3.2-tpkio37
-  6.5-tpkio41
-  6.7-tpkio42
-  7.1-tpkio44
-  7.1-tpkio45
-  7.1-tpkio47
-  7.1-tpkio67
-  7.1-tpkio68
-  7.1-tpkio81
-  7.1.1-tpkio43
-  7.1.2-tpkio46
-  7.1.2-tpkio48
-  7.1.2-tpkio49
-  7.1.2-tpkio53
-  7.1.2-tpkio54
-  7.1.2-tpkio55
-  7.1.2-tpkio59
-  7.1.2-tpkio61
-  7.1.2-tpkio82
-  7.1.3-tpkio62
-  7.1.4-tpkio63
-  7.1.4-tpkio68
-  7.1.4-tpkio71
-  7.1.4-tpkio72
-  7.1.4-tpkio73
-  7.1.4-tpkio74
-  7.1.4-tpkio75
-  7.1.4-tpkio76
-  7.1.4-tpkio77
-  7.1.4-tpkio78
-  7.1.4-tpkio80
-  7.1.4-tpkio83
-  7.1.4-tpkio85
-  7.1.6-tpkio90
-  7.1.8-tpkio94
-  7.2-tpkio96
-  7.2-tpkio98

-  7.2-tpkio99
-  7.2.1-tpkio95
-  7.2.2-tpkio100
-  7.2.2-tpkio102
-  7.2.2-tpkio103
-  7.2.2-tpkio104
-  7.2.2-tpkio105
-  7.2.2-tpkio106
-  7.2.2-tpkio107
-  7.2.2-tpkio108
-  7.2.2-tpkio109
-  7.2.2-tpkio110
-  7.3.2-tpkio112
-  7.3.2-tpkio113
-  9.7-tpkio97