Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3: Basic Requirements PKIoverheid

Version	4.11
Date	February 28, 2023

Publishers imprint

Version number	4.11
Contact person	Policy Authority of PKIoverheid

Organization	Logius

Street address
Wilhelmina van Pruisenweg 52

Postal address
Postbus 96810
2509 JE DEN HAAG

T 0900-555 4555
servicecentrum@logius.nl

Contents

1 INTRODUCTION

1.1 Overview

This is part 3 Additional Requirements of the Programme of Requirements (PoR) of the PKI for the government and is called the Additional Requirements PKIoverheid. Set out in the PoR are the standards for the PKI for the government. This section of part 3 relates to the additional requirements laid down for the services of a Trust Service Provider (TSP) within the PKI for the government. Within the PKI for the government, a distinction is made between various domains. These additional requirements relate to all types of certificate issued under these domains, whereby the distinction is made in the corresponding PoR parts.

A detailed explanation regarding the background and structure of the PKI for the government, as well as the cohesion between the various parts within the PoR is included in part 1 of the PoR.

1.1.1 Design of the Certificate Policies

Part 3 of the Programme of Requirements of PKIoverheid consitis of the following elements:

- *Part 3 Basic Requirements:* The basic requirements are applicable to all Certificate Policies in part 3 of the Programme of Requirements;
- *Part 3 Additional Requirements:* Contains all additional requirements that are applicable to one or more CPs, but not all CPs;
- *Part 3 Reference matrix PKIoverheid and ETSI:* An overview of PKIoverheid requirements with a reference to the applicable ETSI norm(s);
- *Part 3a through 3j:* The Certificate Policies for the different PKIoverheid certificates. These CP's govern the issueance of end entity certificates under the regular root, the private root and the Extended Validation root. These root certificates are broken down into different versions or generations.

The CPs in part 3 of the PoR are structured as follows:

- *Part 3a:* Personal certificates in the Organization domain;
- *Part 3b:* Services authentication and encryption certificates in the Organization domain;
- *Part 3c:* Personal certificates in the Citizen domain;
- *Part 3d:* Services certificates in the Autonomous Devices domain;
- *Part 3e:* Website and server certificates in the Organization domain;
- *Part 3f:* Extended Validation certificates under the Extended Validation root;
- *Part 3g:* Services authentication and encryption certificates in the Private Services domain;
- *Part 3h:* Server certificates in the Private Services domain;
- *Part 3i:* Personal certificates in the Private Services domain;
- *Part 3j:* Organization Validation certificates under the Extended Validation root.

All PKIoverheid requirements have a unique and persistant number which also contains a reference to RFC 3647. Furthermore, each PKIoverheid requirement can have a relation with one or more ETSI requirements for the issuance of PKI certificates. In a separate Excel tabsheet in the OoA template "Referentiematrix PKIoverheid and ETSI" this relationship is listed, aiding in interpreting the PKIoverheid requirements in the context of the ETSI requirements.

The PKIoverheid requirements are divided into the *Basic Requirements* and the *Additonal Requirements*. The *Basic Requirements* are applicable to all CPs. Additionally, each CP contains references to the *Additional Requirments* that are applicable to that specific CP. The CPs do not contain reference to the *Basic Requirements* or relevant ETSI standard, as these are automatically applicable.

To comply with a specific CP the applicable ETSI standard, the *Basic Requirements* and part of the *Additional Requirements* of PKIoverheid must be met.

Incorporated in chapters 2 to 9 inclusive are the specific PKIoverheid requirements. The table below shows the structure within which all PKIoverheid requirements (PKIo requirement) are specified individually.

Requirement	Unique number of the PKIo requirement. In each paragraph, consecutive numbering is used for the PKIo requirements. In combination with the RFC 3647 paragraph number, this forms a unique label for the PKIo requirement.
Description	Description of the PKIo requirement that applies to this domain of the PKI for the government.
Comment	To provide a better understanding of the context in which the requirement has to be placed a comment has been added to a number of PKIo requirements.

1.2 Document name and identification

1.2.1 Revisions

1.2.1.1 Version 3.7 to 4.0

New

None.

Modifications

- PoR requirements have been renumbered according to a new naming convention;
- The creation of a document containing the basic and additional requirements;
- Requirement 3.3.1-pkio45;
- Requirement 6.5.1-pkio116;
- Requirement 4.5.2-pkio52.

Editorial

None.

1.2.1.2 Version 4.0 to 4.1

New

None.

Modifications

- Requirement 6.7.1-pkio120 (effective date no later than 01-09-2015).

Editorial

- Small editiorial changes to the following requirements:
  - 2.2-pkio5;
  - 5.3-pkio78;
  - 6.2.5-pkio103;
  - 6.7.1-pkio118;
  - 6.7.1-pkio119;
  - 6.7.1-pkio120;
  - 9.12.2-pkio136.

1.2.1.3 Version 4.1 to 4.2

New

None.

Modifications

- Requirement 7.1-pkio121 (effective date on publication of the PoR).

Editorial

None.

1.2.1.4 Version 4.2 to 4.3

New

None.

Modifications

- Changed references from ETSI TS 102 042 to ETSI EN 319 411-1. In addition updated all reference to paragraph numbers in the relevant ETSI standards;
- Converted all references to ETSI TS 102 176-1 to ETSI TS 119 312 (effective date 4 weeks after publication of the PoR).

Editorial

None.

1.2.1.5 Version 4.3 to 4.4

New

None.

Modifications

- Changed CRL profile to include modified fields in the certificate profile surrounding OrganizationalIdentifier (effective date 1-2-2017).

Editorial

- Changed reference to the CPS (old URL no longer exists) under heading 9.12;
- Changed reference to OCSP profile to correct PoR.

1.2.1.6 Version 4.4 to 4.5

New

None.

Modifications

- Changed reference to RFC6960 instead of. RFC2560 (effective date 31-12-2017);
- Modification of Policy ID in OCSP certificate profile (effective date 1-7-2017);
- Requirement 2.2-pkio3 is now an additional requirement (effective date 1-10-2017).

Editorial

- Changed Certification Service Provider to Trust Service Provider in paragraph 1.1;
- Changed X509v3 to X509v2 for CRL's in the CRL profile;
- Vermelding Wet Elektronische Handtekeningen verwijderd (vervallen).

1.2.1.7 Version 4.5 to 4.6

New

- Requirement 4.8-pkio159 (effective date 1-9-2017, urgency change).

Modifications

- Requirement 5.7.1-pkio85 (effective date directly after publication of the PoR);

- Requirement 5.7.1-pkio84 (effective date directly after publication of the PoR);
- Requirement 6.5.1-pkio114 (effective date 1-5-2018).

Editorial

None.

1.2.1.8 Version 4.6 to 4.7

New

- Requirement 7.1-pkio174 (effective date 8 weeks after publication of the PoR).

Modifications

- Requirement 4.8-pkio159 transferred to requirement 8.1-pkio159 (effective date immediately after publication of the PoR);
- Adjustment of reference to ETSI requirements, applicable for requirement 3.3.1-pkio36 and requirement 3.3.2-pkio46 (effective date immediately after publication of the PoR);
- Requirement 6.6.1-pkio117 reference to EN 419 211 for QSCDs. (effective date immediately after publication of the PoR).

Editorial

- The reference to the ETSI requirements that deal with the same topic as the PKIoverheid requirement has been moved to an additional tab in the OoA template.

1.2.1.9 Version 4.7 to 4.8

New

- 5.7.1-pkio181 (effective date immediately after publication of the PoR);
- 6.7.1-pkio185 separate requirement for securing web applications (effective date immediately after publication of the PoR);
- 9.17-pkio184 reporting on number of certificates issued (effective date immediately after publication of the PoR).

Modifications

- Reference to IETF RFC 2560 changed to IETF RFC 6960 in requirement 4.9.9-pkio69 (effective date immediately after publication of the PoR);
- Change in requirement 6.7.1-pkio118 on patch management arrangements (effective date immediately after publication of the PoR);
- 5.5.2-pkio83 (effective date immediately after publication of the PoR).

Editorial

- 6.5.1-pkio116 (effective date immediately after publication of the PoR);
- Split requirement 5.7.1-pkio85 rewritten original and new requirement 5.7.1-pkio 181 (effective date immediately after publication of the PoR);
- 4.9.9-pkio69 reference (effective date immediately after publication of the PoR);
- 2.2-pkio156 replaced AND by OR (effective date immediately after publication of the PoR).

1.2.1.10 Version 4.8 to 4.9

New

- Requirement 8.1-pkio187, in case the TSP issues or wants to issue non-qualified certificates within PKIoverheid (effective date 02-17-2020);
- Requirement 9.17-pkio190, this requirement only applies if a TSP deploys CAs that are not technically contrained as described in chapter 5.3.1 in the Mozilla Root Store Policy (effective date 02-17-2020).

Modifications

None.

Deletions

- Requirement 4.9.3-pkio54 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 4.9.5-pkio63 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 4.9.5-pkio64 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 5.2-pkio75 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 6.1.1-pkio87 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 6.1.7-pkio97 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 6.6.1-pkio117 has been removed (effective date immediately after publication PoR 4.9);
- Requirement 9.12.2-pkio137 has been removed (effective date immediately after publication PoR 4.9).

Editorial

None.

1.2.1.11 Version 4.9 to 4.10

New

- Move requirement 9.6.1-pkio127 from PoR Part 3 Additional Requirements to PoR Part 3 Basic Requirements.
- Added basic requirement 8.2-pkio199.

Modifications

- Remove references to the Dutch language in requirement 2.2-pkio3.

Removals

- Remove requirement 2.2-pkio6.
- Remove the extensions:freshestCRL field from the CRL and OCSP profiles.
- Remove the extensions:subjectInfoAccess field from the CRL profile.

Editorial

None.

1.2.1.12 Version 4.10 to 4.11

New

None.

Modifications

None.

Removals

None.

Editorial

None.

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
4.10	02-2022	Ratified by the Ministry of the Interior and Kingdom Relations February 2022
4.11	02-2023	Ratified by the Ministry of the Interior and Kingdom Relations February 2023

1.3 PKI participants

1.3.1 Certification authorities

In this document the distinction is made between the term Certification Authority (CA) and Trust Service Provider. In international usage, "CA" is an umbrella term that refers to all entities authorized

to issue, manage, revoke, and renew certificates. This can apply to the actual CA certificate as well as the organization. In this CP, the organization which holds a CA is refered to as a TSP. The term CA is used to refer to the infrastructure and keymaterial from which a TSP issues and signs certificates.

All TSPs issuing PKIo certificates are mentioned in the relevant parts of the PoR 3a through 3j.

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 authorizated 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 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

No stipulation.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The use of certificates issued under this CP relates to communication of certificate holders who act on behalf of the subscriber.

[OID 2.16.528.1.1003.1.2.5.1]

Authenticity certificates, that 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 OCSP responder certificates may be issued for use within the domain Organisation Person. Said certificates can be used to sign OCSP responses for use in the verification of the validity of the end user certificate. More information can be obtained in appendix A of the base requirements.

[OID 2.16.528.1.1003.1.2.5.2]

Signature certificates, that are issued under this CP, can be used to verify electronic signatures, that have "the same legal consequences as a handwritten signature", as 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 2.16.528.1.1003.1.2.5.3]

Confidentiality certificates, that 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.nl[1]

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 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

No stipulation.

2.1 Repositories

- Page:
  2.1-pkio1 —

Description	The maximum period of time within which the availability of the dissemination service has to be restored is set at 24 hours.
Comment	-

- Page:
  2.1-pkio2 —

Description	There MUST be an electronic repository where the information referred to in [2.2] is published. This repository can be managed by the TSP or by an independent organization.
Comment	The information that has to be published is included in ETSI TS 101 456. The relevant articles in which the information is specified can be found in the reference matrix in appendix B.

2.2 Publication of certification information

- Page:
  2.2-pkio156 —

Description	The CPS (or CPSs) must be reviewed or renewed yearly. The TSP must demonstrate a renewal by incrementing the CPS's version number and adding a date to the CPS's change log, even if no actual changes have been made.
Comment	-

- Page:
  2.2-pkio5 —

Description	The TSP has to include the OIDs of the CPs that are used in the CPS.
Comment	-

2.3 Time or frequency of publication

No stipulation.

2.4 Access controls on repositories

No stipulation.

3. IDENTIFICATION AND AUTHENTICATION

No stipulation.

3.1 Naming

No stipulation.

3.1.1 Types of names

- Page:
  3.1.1-pkio10 —

Description	The TSP has to fulfil the requirements laid down for name formats in the Certificate, CRL and OCSP profiles.
Comment	Included in appendix A of the Basic Requirements are the CRL and OCSP profiles. The PoR part for a certain type of certificate contains the certificate profile in appendix A.

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

No stipulation.

3.2.1 Method to prove possession of private key

No stipulation.

3.2.2 Authentication of organization identity

No stipulation.

3.2.3 Authentication of individual identity

No stipulation.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

No stipulation.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

No stipulation.

3.3.1 Identification and authentication for routine re-key

- Page:
  3.3.1-pkio36 —

Description	ETSI EN 319 411-1 GEN-6.3.6-10 is only allowed for encryption certificates. For all other types of PKIoverheid certificates a re-key MUST take place when renewing a certificate.
Comment	ETSI EN 319 411-1 GEN-6.3.6-10 states under which conditions recertification of the keys of encryption certificates is permitted. The requirement means that certificates CANNOT be renewed without a re-key for the authenticity, signature and server certificates.

- Page:
  3.3.1-pkio45 —

Description	Before certificates are renewed, it must be checked that both requirement 3.1.1-pkio and all requirements stated under [3.1] and [3.2] of the CP for that type of certificate have been fulfilled.
Comment	The relevant articles in which the requirements are specified can be found in part 3 Reference matrix PKIoverheid and ETSI. When replacing a personal certificate at the end of its lifetime the qualified signature of the non-repudiation certificate can be used during registration and identification, instead of the physical presence of the certificate holder. This is subject to a number of conditions: • The non-repudiation certificate must be valid at the time of renewal; • The file must be current and complete, including a copy of a valid ID document (WID); • Subject details of the applicant of the new personal certificate are the same as the details in the valid non-repudiation certificate, e.g. organization field; • The single renewal of the certificate without physical appearance is only possible through the TSP that issued the non-repudiation certificate based on physical identification. All personal certificates under PoR parts 3a, 3c and 3i can be renewed once in this manner.

3.3.2 Identification and authentication for re-key after revocation

- Page:
  3.3.2-pkio46 —

Description	After revocation of the certificate, the relevant keys cannot be recertified. ETSI EN 319 411-1 GEN-6.3.6-10 does not apply.
Comment	-

3.4 Identification and authentication for revocation request

No stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

No stipulation.

4.1 Certificate Application

No stipulation.

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

No stipulation.

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

No stipulation.

4.3.1 CA actions during certificate issuance

No stipulation.

4.3.2 Notification to subscriber by the CA of issuance of Certificate

No stipulation.

4.4 Certificate acceptance

No stipulation.

4.4.1 Conduct constituting certificate acceptance

- Page:
  4.4.1-pkio49 —

Description	After issuance of a certificate, the certificate holder of a personal certificate or the certificate manager of the other types of certificate has to specifically confirm to the TSP the delivery of the key material that is part of the certificate.

Comment	When keys protected by software are used (see [6.2.11-pkio106 and 6.2.11-pkio107]) where the private key is generated by the certificate manager rather than the TSP, the delivery of key material is not applicable. However, the data required in 7.3.1.i and 7.3.1.m must be logged. This stipulation is applicable to CP parts E, F and H.

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

No stipulation.

4.5.1 Subscriber private key and certificate usage

No stipulation.

4.5.2 Relying party public key and certificate usage

- Page:
  4.5.2-pkio51 —

Description	The terms and conditions for users that are made available to the relying parties have to state that the relying party has to check the validity of the full chain of certificates up to the source (root certificate) that is relied on. The terms and conditions must also state that the subscriber is personally responsible for prompt replacement in the event of an approaching expiry of validity, and for emergency replacement in the event of a private key compromise and/or other types of emergencies relating to the certificate or the higher level certificates. The subscriber is expected to take adequate measures in order to safeguard the continuity of the use of certificates.
Comment	The validity of a certificate does not indicate the certificate holder's authority to perform a specific transaction on behalf of an organization or pursuant to his or her profession. The PKI for the government does not arrange authorization; a relying party has to convince itself of that in a different manner. It is advisable to inform the subscriber to take into account the “ICT beveiligingsrichtlijnen voor de transport layer security (TLS)” of the NCSC when using PKIoverheid server certificates. This advice can be obtained online via the website of the NCSC.

4.6 Certificate renewal

No stipulation.

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

No stipulation.

4.7.1 Circumstance for certificate re-key

No stipulation.

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

No stipulation.

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

No stipulation.

4.9.1 Circumstances for revocation

No stipulation.

4.9.2 Who can request revocation

- Page:
  4.9.2-pkio53 —

Description	The following parties can request revocation of an end user certificate: • the certificate manager; • the certificate holder; • the subscriber; • the TSP; any other party or person that has an interest, at the discretion of the TSP.
Comment	-

4.9.3 Procedure for revocation request

- Page:

4.9.3-pkio55 —

Description	The maximum period of time within which the availability of the revocation management services have to be restored is set at four hours.
Comment	-

- Page:
  4.9.3-pkio56 —

Description	The TSP has to record the reasons for revocation of a certificate if the revocation is initiated by the TSP.
Comment	-

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

- Page:
  4.9.5-pkio61 —

Description	The maximum delay between receiving a revocation request or revocation report and the amendment of the revocation status information that is available to all relying parties, is set at four hours.
Comment	This requirement applies to all types of certificate status information (CRL and OCSP)

4.9.6 Revocation checking requirement for relying parties

No stipulation.

4.9.7 CRL issuance frequency (if applicable)

No stipulation.

4.9.8 Maximum latency for CRLs (if applicable)

No stipulation.

4.9.9 On-line revocation/status checking availability

- Page:
  4.9.9-pkio69 —

Description	To detail the provisions in {16} IETF RFC 6960, the use of precomputed OCSP responses is not allowed.
Comment	-

4.9.10 On-line revocation checking requirements

No stipulation.

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

- Page:
  4.9.13-pkio72 —

Description	Suspension of a certificate MUST NOT be supported.
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

No stipulation.

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

- Page:
  4.10.2-pkio73 —

Description	The maximum period of time within which the availability of the revocation status information has to be restored is set at four hours.
Comment	This requirement only applies to the CRL and not to other mechanisms, such as OCSP.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

No stipulation.

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

No stipulation.

5.1 Physical controls

No stipulation.

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

- Page:
  5.2-pkio74 —

Description	The TSP has to reperform the risk analysis at least every year, or if the PA provides an instruction to that end, or the NCSC provides advice to that end. The risk analysis has to cover all PKIoverheid processes that fall under the responsibility of the TSP. Based on the risk analysis, the TSP has to develop, implement, maintain, enforce and evaluate an information security plan. This plan describes a cohesive framework of appropriate administrative, organizational, technical and physical measures and procedures with which the TSP can safeguard the availability, exclusivity and integrity of all PKIoverheid processes, requests and the information that is used to this end.

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

- Page:
  5.2.4-pkio76 —

Description	The TSP has to enforce separation of duties between at least the following roles: • Security officer The security officer is responsible for the implementation of and compliance with the stipulated security guidelines. • System auditor The system auditor fulfils a supervisory role and provides an independent opinion on the manner in which the business processes are arranged and on the manner in which the requirements relating to security are fulfilled. • Systems administrator The systems manager maintains the TSP systems, which includes installing, configuring and maintaining the systems. • TSP operators The TSP operators are responsible for the everyday operation of the TSP systems for, among other things, registration, the generation of certificates, the delivery of an SSCD to the certificate holder and revocation management.
Comment	The aforementioned job descriptions are not limitative and the TSP is free to extend the description within the requirements of segregation of functions, or to divide the functions further still, or to share these between other trusted officials.

- Page:
  5.2.4-pkio77 —

Description	The TSP has to enforce separation of duties between staff who monitor the issuance of a certificate and staff who approve the issuance of a certificate.
Comment	-

5.3 Personnel controls

- Page:
  5.3-pkio78 —

Description	Because publication of confidential information can have significant consequences (among other things, for the trustworthiness) the TSP has to make every effort to make sure that confidential information is dealt with confidentially and that it remains confidential. One important aspect is to ensure that declarations of confidentiality are signed by staff members and contracted third parties.
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

No stipulation.

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

- Page:
  5.4.3-pkio81 —

Description	The retention period of PKIo audit logs containing the required event types of all PKI systems in scope SHALL be 24 months, after which the audit log data SHALL be deleted within 1 month, including any back-up copies. The parts of these audit logs which end up as supporting evidence for incidents in ticketing software are exempt from this requirement. These incident tickets SHALL be retained at least 24 months, but SHOULD be accessible for at least 7 years. Audit logs SHALL include the event types described in Section 5.4.1 (3) of the "*Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificate*s" related to all PKI systems in scope.
Comment	The PKI systems in scope are described in Section 3 of the "*Network and Certificate System Security Requirements*" issued by the CA/Browser Forum.

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

No stipulation.

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

No stipulation.

5.7.1 Incident and compromise handling procedures

- Page:
  5.7.1-pkio181 —

Description	The PA obliges the TSP to subscribe to the NCSC security advice to be knowledgeable about dangers or events that can in threaten or influence the security of the services and/or the image of the PKI for the government.
Comment	-

- Page:
  5.7.1-pkio84 —

Description	In the event of a security breach and/or emergency the TSP has to immediately inform the PA, the NCSC, the Agentschap Telecom (AT) and the certifying body (CB). In case of the loss of privacy sensitive information the Autoriteit Persoonsgegevens (AP) must also be informed. After analysis the TSP has to keep the PA, the NCSC, AT and the CB informed about how the incident is progressing.
Comment	Understood to be meant by security breach in the PKIoverheid context is: An infringement of the TSP core services: registration service, certificate generation service, subject device provisioning service, dissemination service, revocation management service and revocation status service. This is including, but not limited to: • unauthorized elimination of a core service or rendering this core service inaccessible; • unauthorized access to a core service in order to eavesdrop on, intercept and/or change electronic messaging; • unauthorized access to a core service for unauthorized removal, amendment or alteration of computer data.

- Page:
  5.7.1-pkio85 —

Description	The TSP will inform the PA immediately about the risks, dangers or events that can in any way threaten or influence the security of the services and/or the image of the PKI for the government. This is including, but not limited to security breaches and/or emergencies relating to other PKI services performed by the TSP, which are not PKIoverheid services.
Comment	-

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

No stipulation.

6.1 Key pair generation and installation

No stipulation.

6.1.1 Key pair generation

No stipulation.

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

No stipulation.

6.1.5 Key sizes

- Page:
  6.1.5-pkio96 —

Description	The length of the certificate holders' cryptographic keys have to fulfil the requirements laid down in that respect in the list of cryptographic algorithms and key lengths as defined in ETSI TS 119 312.
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.

6.1.6 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

No stipulation.

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

- Page:
  6.2.3-pkio98 —

Description	Escrow by the TSP is not allowed for the private keys of PKIoverheid certificates, with the exception of encryption certificates.
Comment	-

6.2.4 Private key backup

- Page:
  6.2.4-pkio102 —

Description	Back-up of the certificate holders' private keys by the TSP is not allowed.
Comment	-

6.2.5 Private key archival

- Page:
  6.2.5-pkio103 —

Description	Archiving of the certificate holders' private keys by the TSP is not allowed.
Comment	-

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

No stipulation.

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

- Page:
  6.3.2-pkio110 —

Description	At the time that an end user certificate is issued, the remaining term of validity of the higher level TSP certificate has to exceed the intended term of validity of the end user certificate.
Comment	-

6.4 Activation data

No stipulation.

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

No stipulation.

6.5.1 Specific computer security technical requirements

- Page:
  6.5.1-pkio114 —

Description	The TSP has to use multi-factor authentication (e.g. smartcard with personal certificates and a personal password or biometry and a personal password) for the system or all user accounts which are used to issue or approve certificates. This is also mandatory for systems or the user accounts with which data validation takes place. The TSP may waive this measure for systems or user accounts with which data validation takes place, provided that it has implemented technical measures, as a result of which a user account can only validate certificate requests on the basis of a pre-approved list of domains or e-mail addresses.
Comment	Multi-factor authentication tokens cannot be connected permanently or semi-permanently to the system (e.g. a permanently activated smartcard). That is because this would enable certificates to be issued or approved (semi) automatically, or for non-authorized staff to issue or approve certificates.

- Page:
  6.5.1-pkio115 —

Description	The staff of external Registration Authorities (RA) or Resellers may not have access to the system or the user accounts of the TSP which enables issuance or approval of certificates. This function is restricted to authorized staff of the TSP. If an RA or a Reseller does have this access, the RA or the Reseller will be seen as part of the TSP and it/they have to comply with the PKI for the government Programme of Requirements fully and demonstrably.
Comment	-

- Page:
  6.5.1-pkio116 —

Description	The TSP SHALL prevent unauthorized access to the following core services: • registration service, • certificate generation service, • subject device provision service, • dissemination service, • revocation management service, • revocation status service. To this end, these core services are separated either • physically or logically from the non-PKI network domains, or • physically or logically from the PKI network domains that do not meet the Network Security Guidelines of the CA/B Forum, or • physically or logically from the PKI network domains that do not meet the network related PKIoverheid requirements from RFC3647 paragraph 6, “Technical Security Controls”. The TSP enforces a unique authentication for each core service mentioned above. When the physical or logical separation of the network domains described above is not feasible, the various core services must be implemented on separate network domains, where there has to be a unique authentication for each core service mentioned above. The TSP must document the organization of the network domains, at least in a graphical manner. This requirement does not apply to other environments, such as acceptance and test.
Comment	-

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

No stipulation.

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

- Page:
  6.7-pkio119 —

Description	Using an audit tool, at least each month the TSP performs a security scan on its PKIoverheid infrastructure. The TSP documents the result of every security scan and the measures that were taken in relation to this scan.
Comment	Some examples of commercial and non-commercial audit tools are GFI LanGuard, Nessus, Nmap, OpenVAS and Retina.

- Page:
  6.7.1-pkio118 —

Description	The TSP has to ensure that all PKIoverheid ICT systems relating to the registration service, certificate generation service, subject device provision service, dissemination service, revocation management service and revocation status service: • are equipped with the latest updates and; • the web application controls and filters all input by users and; • the web application codes the dynamic output and; • the web application maintains a secure session with the user and; • the web application uses a database securely.
Comment	The TSP has to use the NCSC's "Checklist beveiliging webapplicaties (Security of Web Applications Checklist)[1]" as guidance for this. In addition it is recommended that the TSP implements all other recommendations from the latest version of the white paper "Raamwerk Beveiliging Webapplicaties (The Framework for Web Application Security)" by the NCSC. **[1]** http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/factsheets/checklist-webapplicatie-beveiliging/checklist-webapplicatie-beveiliging/govcert%3AdocumentResource/govcert%3Aresource

- Page:
  6.7.1-pkio120 —

Description	At least once a year, the TSP arranges for a penetration test to be performed on the PKIoverheid internet facing environment, by an independent, experienced, and competent external supplier. In addition a TSP is obliged to arrange a pen test to be performed when substantial changes to the internet facing environment have occurred, • The assessment if substantial changes have occurred takes place by means of a documented risk analysis. • The pen test is performed by an independent, experienced, and competent pen tester. • The pen test must take place no later than one month after the release, but preferably before going to production. The TSP has to document the findings from the pen tests mentioned above and the measures that will be taken in this respect, or to arrange for these to be documented. If necessary, the PA can instruct the TSP to perform additional pen tests.
Comment	CLARIFICATION Substantial changes include: • New software; • New version of existing software, excluding patches; • Changes in infrastructuur. As guidance for the selection of suppliers, the TSP can use the recommendation in chapter 4 (“Supplier Selection”) as described in the latest version of the whitepaper entitled “Pentesten doe je zo[1]” (how to perform penetration testing) published by the NCSC. **[1]** http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/whitepapers/pentesten-doe-je-zo/pentesten-doe-je-zo/govcert%3AdocumentResource/govcert%3Aresource

- Page:
  6.7.1-pkio185 —

Description	For web application(s) related to: • the registration service, • certificate generation service, • subject device provision service, • dissemination service, • revocation management service and • revocation status service the TSP must secure the following: • That the web application checks and filters all user input and; • That the web application encodes the dynamic output and; • That the web application maintains a secure session with the user and; That the web application uses a database in a secure way.

Comment	The TSP can use the "ICT-Beveiligingsrichtlijnen voor Webapplicaties[2]" of the NCSC as guidance.

6.7.1 Network security controls (duplicate)

Content by label

There is no content with the specified labels

6.8 Time-stamping

No stipulation.

2 https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties/ICT-Beveiligingsrichtlijnen-voor-Webapplicaties-Verdieping-Printversie.pdf

7. CERTIFICATE, CRL, AND OCSP PROFILES

No stipulation.

7.1 Certificate profile

- Page:
  7.1-pkio121 —

Description	The TSP has to issue certificates in accordance with the requirements stipulated in that respect in appendix A of the applicable PoR part for that type of certificate, namely "Certificate profiles". Only those certificate elements which are mentioned in the certificate profile may be used. Usage of ny and all other elements is prohibited.
Comment	-

- Page:
  7.1-pkio174 —

Description	All elements within the Issuer field must match the corresponding Subject field of the issuing CA.
Comment	-

7.1.1 Version number(s)

No stipulation.

7.1.2 Certificate extensions

No stipulation.

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

No stipulation.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

No stipulation.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

- Page:
  7.2-pkio122 —

Description	The TSP has to issue CRLs in accordance with the requirements stipulated in that respect in appendix A of this document, "CRL and OCSP profiles".
Comment	-

7.2.1 Version number(s)

No stipulation.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

No stipulation.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

No stipulation.

8.1 Frequency or circumstances of assessment

- Page:
  8.1-pkio159 —

Description	A TSP is required for each (annual) ETSI audit: - to use the current version of the Overview of Requirements developed and made available by PA PKIoverheid OR; - use an Overview of Requirements developed by the TSP itself. This Overview of Requirement must be reviewed and approved by the PA prior to the (annual) ETSI audit for completeness. To this end, the TSP must provide the Overview of Requirements (including accompanying Statement of Applicability) to the PA prior to an audit. If one of these conditions is not met, the PA reserves the right to refuse the audit report.
Comment	- As part of this statement, the legend must state which versions of the applicable standards have been used. - The TSP must allow for processing time by the PA (maximum of 15 working days). - A copy of the reviewed Overview of Requirements will be sent to the ETSI auditor. - The Overview of Requirements is also referred to as Overview of Applicability (OoA).

8.2 Identity/qualifications of assessor

- Page:
  8.2-pkio199 —

Description	The TSP's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively SHALL possess the following qualifications and skills: a. independence from the subject of the audit, and b. the ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme, and c. employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third party attestation function, and d. accredited in accordance with the ETSI EN 319 403 scheme by an accreditation body within the meaning of Article 4 of Regulation (EC) No 765/2008, and bound by law, government regulation, or professional code of ethics.
Comment	Criteria for an Eligible Audit Scheme, if present, are described in Section 8.4 of this PoR.

8.3 Assessors 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

No stipulation.

9.1 Fees

No stipulation.

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

No stipulation.

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

No stipulation.

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

No stipulation.

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

- Page:
  9.5-pkio126 —

Description	The TSP indemnifies the subscriber in respect of claims by third parties due to violations of intellectual property rights by the TSP.
Comment	-

9.6 Representations and warranties

No stipulation.

9.6.1 CA representations and warranties

- Page:
  9.6.1-pkio127 —

Description	In the agreement between the TSP and the subscriber, a clause (as specified in Article 253 of the Civil Code, Book 6) will be included in which the TSP champions the interests of a third party relying on the certificate. This clause addresses liability of the TSP in accordance with EU Regulation No 910/2014 (eIDAS) Article 13 and applies to all certificates issued by the TSP.

Comment	-

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

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

- Page:
  9.8-pkio135 —

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 value of the transactions for which certificates can be used.
Comment	-

9.9 Indemnities

No stipulation.

9.10 Term and termination

No stipulation.

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

No stipulation.

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

- Page:
  9.12.2-pkio136 —

Description	If a published amendment of the CP can have consequences for the end users, the TSPs will announce the amendment to the subscribers and/or certificate holders registered with them in accordance with their CPS.
Comment	-

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

- Page:
  9.13-pkio138 —

Description	The complaints handling process and dispute resolution procedures applied by the TSP may not prevent proceedings being instituted with the ordinary court.
Comment	-

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

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

- Page:
  9.17-pkio184 —

Description	The TSP must provide data twice a year on the total number of issued certificates and outstanding certificates in the previous period. These figures must be supplied in the format prepared and distributed for this by the PA.
Comment	-

- Page:
  9.17-pkio190 —

Description	This requirement only applies if a TSP deploys CAs that are not technically contrained as described in chapter 5.3.1 in the Mozilla Root Store Policy. If an event occurs or threatens to occur as described in Chapter 8 of the Mozilla Root Store Policy, the TSP must: • Inform the PA of this without delay; • Not take (irreversible) actions without the approval of the PA; • Take all possible actions to (permanently) meet the requirements in Chapter 8 of the aforementioned Root Store Policy.
Comment	-

10 Appendix A: CRL and OCSP certificate Profiles for certificate status information

10.1 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.

In the extensions, fields/attributes that are critical according to the international standards are marked with 'yes' in the 'Critical' column to show that the relevant attribute MUST be checked by a process with which a certificate is evaluated. Other fields/attributes are shown with 'no'.

10.2 References

1. Guideline 1999/93/EC of the European Parliament and of the European Council of Ministers dated 13 December 1999 concerning a European framework for electronic signatures
2. ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: "Information Technology – Open Systems Interconnection – The directory: Public key and attribute certificate frameworks".
3. ITU-T Recommendation X.520 (2001) ISO/IEC 9594-6: "Information Technology – Open Systems Interconnection – The directory: Selected Attribute Types".
4. RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".
5. RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
6. RFC 3739: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".
7. OID RA management PKI overheid – OID scheme.
8. ETSI TS 101 862: "Qualified certificate profile", version 1.3.3 (2006-01).
9. ETSI TS 102 280: "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", version 1.1.1 (2004-03).
10. ETSI TS 119 312: “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”, version 1.1.1 (2014-11).
11. ISO 3166 "English country names and code elements".
12. RFC 6960: “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

10.3 Profile of the CRL

10.3.1 General requirements in relation to the CRL

- The CRLs have to fulfil the X.509v3 standard for CRLs.
- A CRL contains information about revoked certificates that fall within the current period of validity or of which the period of validity expired less than 6 months ago.

10.3.2 CRL attributes

Field / Attribute	Criteria	Description	Standard reference[1]	Type	Explanation
Version	V	MUST be set to 1 (X.509v2 CRL profile).	RFC 5280	Integer	Describes the version of the CRL profile, the value 1 stands for X.509 version 2.
Signature	V	MUST be set to the algorithm, as stipulated by the PA.	RFC 5280	OID	MUST be the same as the field signatureAlgorithm. For maximum interoperability, for certificates under the G1 root certificate, only sha-1WithRSAEncryption is allowed. For certificates under the G2 root certificate, only sha-256WithRSAEncryption is allowed.
Issuer	V	MUST contain a Distinguished Name (DN). The field has attributes as described in the following rows.	PKIo, RFC 5280		Attributes other than those mentioned below MUST NOT be used. The attributes that are used MUST be the same as the corresponding attributes in the Subject field of the TSP certificate (for validation).
Issuer.countryName	V	See requirement 7.1-pkio174	ISO3166, X.520	Printable String	

Field / Attribute	Criteria	Description	Standard reference[1]	Type	Explanation
Issuer.stateOrProvinceName	N	Is not used.	PKIo	UTF8String	-
Issuer.OrganizationName	V	see requirement 7.1-pkio174	ETSI TS 102280: 5.2.4	UTF8String	

Field / Attribute	Criteria	Description	Standard reference[1]	Type	Explanation
Issuer.organizationIdentifier	V/N	The organizationIdentifier filed contains an identification of the issuing CA. This field MUST be included in CRLs when the field subject.organizationIdentifier is part of the TSP certificate used to sign the CRL and MUST not be included in CRL's when this field is not part of the TSP certificate in question.	EN 319 412-1	UFF8String	The syntax of the identificatiestring is specified in paragraph 5.1.4 of ETSI EN 319 412-1 and contains: • 3 character legal person identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference). Permissable values for this field are the OIN or the KVK number of the TSP. The information MUST be the same as the subject.organizationIdentifier incorporated in the TSP CA certificate.
Issuer.organizationalUnitName	O	See requirement 7.1-pkio174	ETSI TS 102280: 5.2.4	UTF8String	

Field / Attribute	Criteria	Description	Standard reference[1]	Type	Explanation
Issuer.localityName	N	Is not used.	PKIo	UTF8String	-
Issuer.serialNumber	O	See requirement 7.1-pkio174	RFC 3739	Printable String	
Issuer.commonName	V	See requirement 7.1-pkio174	PKIo, RFC 5280	UTF8String	The commonName attribute MUST NOT be necessary to identify the issuing authority (not part of the Distinctive Name, requirement from RFC 3739).
ThisUpdate	V	MUST indicate the date and time on which the CRL is amended.	RFC 5280	UTCTime	MUST include the issuance date of the CRL in accordance with the applicable policy set out in the CPS.
NextUpdate	V	MUST indicate the date and time of the next version of the CRL (when it can be expected).	PKIo, RFC 5280	UTCTime	This is the latest date on which an update can be expected, however an earlier update is possible. MUST be completed in accordance with the applicable policy set out in the CPS.

Field / Attribute	Criteria	Description	Standard reference[1]	Type	Explanation
revokedCertificates	V	MUST include the date and time of revocation and *serialNumber* of the revoked certificates.	RFC 5280	SerialNumbers, UTCTime	If there are no revoked certificates, the revoked certificates list MUST NOT be present.

10.3.3 Standard extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference[1]	Type	Explanation
authorityKeyIdentifier	O	No	This attribute is interesting if a TSP has more signature certificates with which a CRL could be signed (using this attribute, it can then be ascertained which public key has to be used to verify the signature of the CRL).	RFC 5280	KeyIdentifier	The value MUST include the SHA-1 hash from the authorityKey (public key of the TSP/CA).
IssuerAltName	A	No	This attribute allows alternative names to be used for the TSP (as issuer of the CRL) (the use is advised against).	RFC 5280		The DNS name, IP address and URI could potentially be entered into this field. The use of an rfc822 name (e-mail address) is NOT allowed.
CRLNumber	V	No	This attribute MUST contain an incremental number that provides support when determining the order of CRLs (the TSP provides the numbering in the CRL).	RFC 5280	Integer	
DeltaCRLIndicator	O	Yes	If 'delta CRLs' are used, a value for this attribute MUST be entered.	RFC 5280	BaseCRLNumber	Contains the number of the baseCRL of which the Delta CRL is an extension.

Field / Attribute	Criteria	Critical?	Description	Standard reference[1]	Type	Explanation
issuingDistributionPoint	O	Yes	If this extension is used, this attribute identifies the CRL distribution point. It can also contain additional information (such as a limited set of reason codes why the certificate has been revoked).	RFC 5280		If used, this field MUST fulfil the specifications in RFC 5280
FreshestCRL	O	No	This attribute is also known by the name 'Delta CRL Distribution Point'. If used it MUST contain the URI of a Delta CRL distribution point. This is never present in a Delta CRL.	RFC 5280		This field is used in complete CRLs and indicates where Delta CRL information can be found that will update the complete CRL.
authorityInfoAccess	O	No	Optional reference to the certificate of the CRL.Issuer.	RFC 5280	id-ad-caIssuers (URI)	MUST conform to § 5.2.7 of RFC 5280.
CRLReason	O	No	theCRLReason MUST indicate the most appropriate reason for revocation of the certificate, as defined in the CPS of the TSP. The field MUST NOT contain the certificateHold value.	RFC 5280	reasonCode	Explains the reason for revocation.

Field / Attribute	Criteria	Critical?	Description	Standard reference[1]	Type	Explanation
holdInstructionCode	N	No	Is not used.	RFC 5280	OID	The PKI for the government does not use the 'On hold' status.
invalidityDate	O	No	This attribute can be used to indicate a date and time on which the certificate has become compromised if it differs from the date and time on which the TSP processed the revocation.	RFC 5280	GeneralizedTime	
certificateIssuer	A	Yes	If an indirect CRL is used, this attribute MAY be used to identify the original issuer of the certificate.	RFC 5280	GeneralNames	

10.4 Profile OCSP

10.4.1 General requirements in relation to OCSP

- If the TSP supports the Online Certificate Status Protocol (OCSP), OCSP responses and OCSPSigning certificates MUST fulfil the requirements relating to this stipulated in IETF RFC 6960.
- OCSP Signing certificates MUST correspond with the X.509v3 standard for public key certificates. General requirements in relation to certificates are listed in RFC5280
- The [X.509] standard allows unlimited extension of the attributes within a certificate. In connection with interoperability requirements, this may not be used within the PKI for the government. Only attributes indicated in this appendix as Compulsory (V), Optional (O) or Advised Against (A) may be used.
- OCSP Signing certificates must fulfil the profile for services certificates set out in part 3b of the Programme of Requirements PKIoverheid, with the following exceptions:

10.4.2 OCSP Signing certificate attributes

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
Issuer	V		MUST contain a Distinguished Name (DN).	PKIo		An OCSPSigning certificate MUST be issued under the hierarchy of the PKI for the government.
KeyUsage	V	Yes	The attribute extension specifies the intended purpose of the key incorporated in the certificate. In the PKI for the government, for each certificate type various bits are incorporated in the keyUsage extension. In OCSPSigning certificates, the digitalSignature bit MUST be incorporated and the extension marked as being critical. The non-Repudiation bit MUST NOT be included.	RFC 5280, RFC 2560	BitString	

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
CertificatePolicies	V	No	MUST contain the OID of the PKIoverheid certificate policy (CP) as described alongside, the URI of the CPS, and a user notice. The OID schedule to be used in the PKI for the government is described in the CP - Services.	RFC 3739	OID, String, String	The OID for OCSP certificates (for all domains) under the G2 is: 2.16.528.1.1003.1.2.5.4. The OID for OCSP certificates under the G3 is as follows: - Organization Person: 2.16.528.1.1003.1.2.5.1 - Organization Services: 2.16.528.1.1003.1.2.5.4 - Organization Servier: 2.16.528.1.1003.1.2.5.6 - Citizen: 2.16.528.1.1003.1.2.3.1 - Autonomous Devices: 2.16.528.1.1003.1.2.6.1 The OID for OCSP certificates under the EV is 2.16.528.1.1003.1.2.7 The OID for OCSP certificates under the Private Root is as follows:

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
						- Private Services/server: 2.16.528.1.1003.1.2.8.4 - Private Persons: 2.16.528.1.1003.1.2.8.1
ExtKeyUsage	V	Yes	MUST be used with the value id-kp-OCSPSigning.	RFC 5280		
ocspNoCheck	V/O		The CA/B Forum Baseline Requirements require the use of the ocspNoCheck for publicly trusted server and EV certificates. For the other PKIoverheid certificates the use is optional.	RFC 2560		The CA/B Forum Baseline Requirements require the use of the ocspNoCheck. It is therefore not clear how browsers are to react on OCSP responder certificates without a ocspNoCheck extension. Browsers will most probably not check the status of an ocsp signing certificate without the extension.