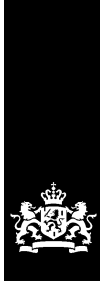

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3c: Certificate Policy - Citizen Domain

Date 28 January 2014

Authenticity	2.16.528.1.1003.1.2.3.1
Non repudiation	2.16.528.1.1003.1.2.3.2
Confidentiality	2.16.528.1.1003.1.2.3.3

Publisher's imprint

Version number 3.6
Contact person Policy Authority of PKIoverheid

Organization Logius

Street address
Wilhelmina van Pruisenweg 52

Postal address
P.O. Box 96810
2509 JE THE HAGUE

T 0900 - 555 4555
servicecentrum@logius.nl

Contents

The Policy Authority (PA) of the PKI for the government supports the Minister of the Interior and Kingdom Relations in managing the PKI for the government.

The PKI for the government is an agreements system. This system enables generic and large-scale use of the electronic signature, and it also facilitates remote identification and confidential communication.
The tasks of the PA of PKIoverheid are:

- contributing towards the development and the maintenance of the framework of standards that underlies the PKI for the government, the Programme of Requirements (PoR);
- assisting in the process of admittance by Certification Service Providers (CSPs) to the PKI for the government and preparing the administration;
- supervising and monitoring the activities of CSPs that issue certificates under the root of the PKI for the government.

The purpose of the Policy Authority is:
Enforcement of a practicable and reliable framework of standards for PKI services that provides an established level of security for the government's communication needs that is transparent to users.

Revision control

Version	**Date**	**Description**
1.0	09-11-2005	Ratified by the Ministry of the Interior and Kingdom Relations November 2005
1.1	25-01-2008	Ratified by the Ministry of the Interior and Kingdom Relations January 2008
1.2	13-01-2009	Ratified by the Ministry of the Interior and Kingdom Relations January 2009
2.0	09-10-2009	Ratified by the Ministry of the Interior and Kingdom Relations October 2009
2.1	11-01-2010	Amendments further to a change of name from GBO.Overheid to Logius
3.0	25-01-2011	Ratified by the Ministry of the Interior and Kingdom Relations January 2011
3.1	01-07-2011	Ratified by the Ministry of the Interior and Kingdom Relations June 2011
3.2	27-01-2012	Ratified by the Ministry of the Interior and Kingdom Relations January 2012
3.3	01-07-2012	Ratified by the Ministry of the Interior and Kingdom Relations June 2012
3.4	04-02-2013	Ratified by the Ministry of the Interior and Kingdom Relations January 2013

3.5	06-07-2013	Ratified by the Ministry of the Interior and Kingdom Relations July 2013
3.6	01-2014	Ratified by the Ministry of the Interior and Kingdom Relations January 2014

1 Introduction to the Certificate Policy

1.1 Overview

This is part 3c of the Programme of Requirements (PoR) for the PKI for the government and is known as the Certificate Policy (CP). Set out in the PoR are the standards for the PKI for the government. This section relates to the requirements laid down for the services of a Certification Service Provider (CSP) within the PKI for the government. Within the PKI for the government , a distinction is made between various domains. This document only relates to the personal certificates issued by a CSP in the Citizen domain.

This chapter includes a brief explanation of the CP. A more 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.

For a list of the definitions and abbreviations used in this section, please refer to part 4 of the PoR.

1.1.1 Design of the Certificate Policy

As stated in part 1 of the PoR, the requirements that form part of the CP consist of requirements [1]:

- that ensue from the Dutch legal framework in relation to the electronic signature;
- that ensue from the current version of the ETSI standard EN 319 411-2, public + SSCD (ETSI CP OID 0.14561.1);
- that are specifically drawn up by and for the PKIoverheid.

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.

RFC 3647	Reference to the paragraph from the RFC 3647 structure to which the PKIo requirement relates. RFC 3647 is a PKIX framework of the Internet Engineering Task Force (IETF) and is the de facto standard for the structure of Certificate Policies and Certification Practice Statements[2].
Number	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.
ETSI	Reference to the requirement(s) from ETSI EN 319 411-2 from which the PKIo requirement is derived or which provides further detail.
PKIo	The PKIo requirement that applies within this domain of the PKI for the government.
Comment	To provide a better understanding of the context in which the requirement has

1 *For an explanation regarding the positioning of the requirements applicable within the PKI for the government, please refer to part 1 of the PoR.*

2 *Chapters 2 to 9 inclusive only include those paragraphs from RFC 3647 to which a PKIo requirement applies.*

	to be placed a comment has been added to a number of PKIo requirements.

This CP also includes a number of provisions that are not formulated as PKIo requirements. These provisions do not make any demands on the CSPs within the PKI for the government, but do apply as a policy to the PKI for the government. This concerns provisions from paragraphs 1.1, 1.1.1, 1.1.2, 1.2, 1.3, 1.4, 1.5, 8, 9.12.1, 9.12.2, 9.14 and 9.17.

The profiles used within PKIoverheid relating to the end user certificates and certificate status information are listed in appendix A.

Based on chapters 1 to 9 inclusive, a reference matrix is included in appendix B. In accordance with the RFC 3647 structure, the matrix contains a reference to the applicable requirements within the PKI for the government. A distinction is made between requirements originating from Dutch law, requirements from ETSI EN 319 411-2 and the PKIo requirements.

1.1.2 Status

This is version 3.6 of part 3c of the PoR. The current version has been updated up to January 2013 inclusive.

The PA has devoted the utmost attention and care to the data and information incorporated in this CP. Nevertheless, it is possible that there are inaccuracies and imperfections. The PA accepts no liability for damage resulting from these inaccuracies or imperfections, nor is any liability assumed for damage caused by the use or distribution of this CP, if this CP is used for purposes other than for the use of certificates described in paragraph 1.4 of this CP.

1.2 References to this CP

Within the PKI for the government, both a structure or root based on the SHA-1 (G1) algorithm and roots based on the SHA-256 algorithm (G2 and G3) are used. Furthermorea division is made into different domains under these root certificates.

For the G1 root this division consists of the Government/Companies domains (these two domains have merged over time) and Citizen domain.
Under the G2 root there are domains for Organization, Citizen, and Autonomous Devices.
Under the G3 root domains exist for Organization Person, Organisation Services, Citizen, and Autonomous Devices.

Each CP is uniquely identified by an OID, in accordance with the following schedule.

OID	CP
2.16.528.1.1003.1.2.3.1	for the authenticity certificate, that contains the public key for identification and authentication
2.16.528.1.1003.1.2.3.2	for the signature certificate, that contains the public key for the qualified electronic signature
2.16.528.1.1003.1.2.3.3	for the confidentiality certificate that contains the public key for confidentiality

The OID is structured as follows: {joint-iso-itu-t (2). country (16). the Netherlands (528). Dutch organization (1). Dutch government (1003). PKI for the government (1). CP (2). citizen domain (3). authenticity (1)/non repudiation (2)/confidentiality (3). version number}.

If requirements only apply to one or two types of certificates, this is expressly specified by stating the Object Identifier (OID) referencing the applicable CP or CPs.

1.3 User Community

In the Government and Companies, Organization, and Organization Person domains, the distinction between subscriber and certificate holder is relevant because, in practice, the following situation is anticipated: the CSP has an agreement with the subscriber which stipulates that the CSP will issue certificates to the certificate holders to be appointed by the subscriber (for example, the subscriber's employees). In the Citizen domain, the subscriber and certificate holder are the same person. Where the subscriber is listed in the CP Citizen, this has to interpreted as certificate holder. The citizen takes on the obligations of both the subscriber and the certificate holder.

Within the Citizen domain, the user community consists of certificate holders (the citizens that use the certificates) and relying parties who act with trust in certificates of the relevant certificate holders.

The parties within the user community are subscribers, certificate holders and relying parties.

- A subscriber is a natural person who enters into an agreement with a CSP for certification of the public keys. A subscriber is also a certificate holder.
- A certificate holder is an entity, characterized in a certificate as the holder of the private key that is linked to the public key provided in the certificate.
- A relying party is every natural or legal personality who is a recipient of a certificate and who acts with a reliance on that certificate.

1.4 Certificate Usage

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

[OID 2.16.528.1.1003.1.2.3.1] Authenticity certificates, that are issued under this CP, can be used for reliable electronic identification and authentication of persons. This concerns both the mutual identification of people and identification between people and computerized devices.

[OID 2.16.528.1.1003.1.2.3.1] Authenticity certificates that are issued under this CP cannot be used to identify people in cases where the law requires that the identity of persons may only be established using the document referred to in the Compulsory Identification Act (Wet op de identificatieplicht).

[OID 2.16.528.1.1003.1.2.3.2] Signature certificates, that are issued under this CP, can be used to verify electronic signatures, that have "the same legal consequences as a handwritten signature", as specified in article 15a, first and second paragraphs, in Title 1 of Book 3 of the Civil Code (Burgerlijk Wetboek) under section 1A and are qualified certificates as referred to in article 1.1, paragraph ss of the Telecommunications Act (Telecomwet).

[OID 2.16.528.1.1003.1.2.3.3] Confidentiality certificates, issued under this CP, can be used to protect the confidentiality of data that is exchanged and/or stored in electronic form. This concerns both the mutual exchange between people and exchange between people and computerized devices.

1.5 Contact information Policy Authority

The PA is responsible for this CP. Questions relating to this CP can be put to the PA; the address can be found at: http://www.logius.nl/pkioverheid.

2 Publication and Repository Responsibilities

2.1 Electronic Repository

RFC 3647	2.1 Electronic repository
Number	1
ETSI	7.3.5.e, EN 319 411-2
PKIo	The maximum period of time within which the availability of the dissemination service has to be restored is set at 24 hours.

RFC 3647	2.1 Electronic repository
Number	2
ETSI	7.3.1.b, EN 319 411-2 6.2, EN 319 411-2 7.3.5.f, EN 319 411-2
PKIo	There MUST be an electronic repository where the information referred to in [2.2] is published. This repository can be managed by the CSP or by an independent organisation.
Comment	The information that has to be published is included in ETSI EN 319 411-2, QCP public + SSCD. The relevant articles in which the information is specified can be found in the reference matrix in appendix B.

2.2 Publication of CSP information

RFC 3647	2.2 Publication of CSP information
Number	1
ETSI	7.3.1.b, EN 319 411-2
PKIo	The CPS has to be written in Dutch.

RFC 3647	2.2 Publication of CSP information
Number	2
ETSI	5.2.b, EN 319 411-2
PKIo	The CSP has to include the OIDs of the CPs that are used in the CPS.

RFC 3647	2.2 Publication of CSP information
Number	3
ETSI	7.3.1.b, EN 319 411-2
PKIo	All information has to be available in Dutch.

RFC 3647	2.2 Publication of CSP information
Number	4
ETSI	7.3.1.a, EN 319 411-2
PKIo	The CSP has to actively inform the citizen and to state in the conditions that the authenticity certificate is not referred to in the Compulsory Identification Act (Wid) as an identity document and therefore cannot be used to identify persons in cases where the law requires that the identity of persons is established using a document referred to in the Compulsory Identification Act. The CSP has to express that the authenticity certificate cannot be used when using government services, where the law requires that the identity of persons is established using a document in the Compulsory Identification Act.

2.4 Access to Published Information

RFC 3647	2.4 Access to published information
Number	1
ETSI	6.1.c, EN 319 401
PKIo	It has to be possible for anyone to consult the CPS of a Certification Service Provider within PKIoverheid.
Comment	'Anyone' means that, in addition to the subscribers and certificate holders, every potential relying party has to be able to consult the CPS.

3 Identification and Authentication

3.1 Naming

RFC 3647	3.1.1 Types of names
Number	1
ETSI	7.3.3.a, EN 319 411-2 7.3.6.g, EN 319 411-2
PKIo	The CSP has to fulfil the requirements laid down for name formats in the Programme of Requirements, part 3 – appendix A Certificate, CRL and OCSP profiles.
Comment	Included in appendix A is an explanation of the various profiles and permitted name formats.

RFC 3647	3.1.3 Anonymity or pseudonimity of certificate holders
Number	1
ETSI	7.3.3.a, EN 319 411-2 7.3.6.g, EN 319 411-2
PKIo	Pseudonyms MUST NOT be used in certificates.

3.2 Initial Identity Validation

RFC 3647	3.2.3 Authentication of individual identity
Number	1
ETSI	7.3.1.d, EN 319 411-2
PKIo	The CSP has to verify that the full name given by the certificate holder that is incorporated in the certificate is correct and complete, including the surname, first forename, first name or other forename(s) (if applicable) and surname prefixes (if applicable).

3.3 Identification and Authentication for Re-key Requests

RFC 3647	3.3.1 Identification and authentication for routine re-key
Number	1
ETSI	7.3.2.d, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.3] 7.3.2.d applies.
Comment	7.3.2.d. states under which conditions recertification of keys is permitted.

RFC 3647	3.3.1 Identification and authentication for routine re-key
Number	2
ETSI	7.3.2.d, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.1] and [OID 2.16.528.1.1003.1.2.3.2] 7.3.2.d do not apply.
Comment	The requirement means that certificates CANNOT be renewed without a re-key for the authenticity and signature certificate.

RFC 3647	3.3.1 Identification and authentication for routine re-key
Number	3
ETSI	7.3.2.a, EN 319 411-2 7.3.2.c, EN 319 411-2
PKIo	Before certificates are renewed, it must be checked that all requirements stated under [3.1] and]3.2] have been fulfilled.
Comment	The relevant articles in which the requirements are specified can be found in the reference matrix in appendix B.

RFC 3647	3.3.2 Identification and authentication for re-key after revocation
Number	1
ETSI	7.3.2.d, EN 319 411-2
PKIo	After revocation of the certificate, the relevant keys cannot be recertified. 7.3.2.d does not apply.

4 Certificate Life-Cycle Operational Requirements

4.4 Certificate Acceptance

RFC 3647	4.4.1 Conduct constituting acceptance of certificates
Number	1
ETSI	7.3.1.i, EN 319 411-2
PKIo	After issuance of a certificate, the certificate holder has to specifically confirm to the CSP the delivery of the key material that is part of the certificate.

4.5 Key Pair and Certificate Usage

RFC 3647	4.5.2 Relying party public key and certificate usage
Number	1
ETSI	6.3.a, EN 319 411-2
PKIo	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 should not be confused with the authority of the certificate holder to perform a specific transaction on behalf of an organization. The PKI for the government does not arrange authorization; a relying party has to convince itself of that in a different manner.

4.9 Certificate Revocation and Suspension

RFC 3647	4.9.1 Circumstances for revocation
Number	1
ETSI	7.3.6.a, EN 319 411-2
PKIo-OO	Certificates must be revoked when: • the subscriber states that the original request for a certificate was not allowed and the subscriber does not provide consent with retrospective force; • the CSP has sufficient proof that the subscriber's private key (that

	corresponds with the public key in the certificate) is compromised or if compromise is suspected, or if there is inherent security vulnerability, or if the certificate has been misused in any other way. A key is considered to be compromised in the event of unauthorized access or suspected unauthorized access to the private key, if the private key or SSCD is lost or suspected to be lost, if the key or SSCD is stolen or suspected to be stolen, or if the key or SSCD is destroyed; • a subscriber does not fulfil its obligations outlined in this CP or the corresponding CPS of the CSP or the agreement that the CSP has entered into with the subscriber; • the CSP is informed or otherwise becomes aware of a substantial change in the information that is provided in the certificate. An example of that is: a change in the name of the certificate holder; • the CSP determines that the certificate has not been issued in line with this CP or the corresponding CPS of the CSP or the agreement that the CSP has entered into with the subscriber; • the CSP determines that information in the certificate is incorrect or misleading; • the CSP ceases its work and the CRL and OCSP services are not taken over by a different CSP. • The PA of PKIoverheid determines that the technical content of the certificate entails an irresponsible risk to subscribers, relying parties and third parties (e.g. browser parties).
Comment	In addition, certificates can be revoked as a measure to prevent or to combat an emergency. Considered to be an emergency is definitely the compromise or suspected compromise of the private key of the CSP used to sign certificates.

RFC 3647	4.9.2 Who can request revocation
Number	1
ETSI	7.3.6.a, EN 319 411-2
PKIo	The following parties can request revocation of an end user certificate: • the certificate holder; • the CSP; • any other party or person that has an interest, at the discretion of the CSP.
Comment	As in the Citizen domain the certificate holder is also the subscriber, the subscriber is not specifically included as a party who can make a request for revocation.

RFC 3647	4.9.3 Procedure for revocation request
Number	1
ETSI	7.3.6.a, EN 319 411-2
PKIo	The CSP is entitled to lay down additional requirements in respect of a request

	for revocation. These additional requirements have to be included in the CPS of the CSP.

RFC 3647	4.9.3 Procedure for revocation request
Number	2
ETSI	7.3.6.h, EN 319 411-2
PKIo	The maximum period of time within which the availability of the revocation management services have to be restored is set at four hours.

RFC 3647	4.9.3 Procedure for revocation request
Number	3
ETSI	7.3.6.a, EN 319 411-2
PKIo	The CSP has to record the reasons for revocation of a certificate if the revocation is initiated by the CSP.

RFC 3647	4.9.3 Procedure for revocation request
Number	4
ETSI	7.3.6.i, EN 319 411-2 (and Electronic Signature Directive article 2I paragraph 1l)
PKIo	In any case, the CSP has to use a CRL to make the certificate status information available.

RFC 3647	4.9.5 Time within which CA must process the revocation request
Number	1
ETSI	7.3.6.a, EN 319 411-2
PKIo	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)

RFC 3647	4.9.6 Revocation checking requirement for relying parties
Number	1
ETSI	6.3.a, EN 319 411-2
PKIo	An end-user who consults the certificate status information has to verify the authenticity of this information using the electronic signature with which the information has been signed and the corresponding certification path.

RFC 3647	4.9.6 Revocation checking requirement for relying parties
Number	2
ETSI	6.3.a, EN 319 411-2
PKIo	The obligation mentioned in [4.9.6-1] has to be included by the CSP in the terms and conditions for users that are made available to the relying parties.

RFC 3647	4.9.7 CRL issuance frequency
Number	1
ETSI	7.3.6, EN 319 411-2
PKIo	The CSP has to update and reissue the CRL for end user certificates at least once every 7 calendar days and the date of the " Next update" field may not exceed the date of the "Effective date" field by 10 calendar days.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	1
ETSI	7.3.6.i, EN 319 411-2
PKIo	The revocation management services of the CSP can support the Online Certificate Status Protocol (OCSP) as an addition to the publication of CRL information. If this support is available, this has to be stated in the CPS.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	2
ETSI	7.3.6.i, EN 319 411-2

PKIo	If the CSP supports the Online Certificate Status Protocol (OCSP), this must conform to IETF RFC 2560.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	3
ETSI	7.3.6.i, EN 319 411-2
PKIo	To detail the provisions of IETF RFC 2560, OCSP responses have to be signed digitally by either: • the private (CA) key with which the certificate is signed of which the status is requested, or; • a responder appointed by the CSP which holds an OCSP Signing certificate issued for this purpose by the CSP, or; • a responder that holds an OCSP Signing certificate that falls under the hierarchy of the PKI for the government.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4
ETSI	7.3.6.i, EN 319 411-2
PKIo	To detail the provisions of IETF RFC 2560, the use of the precomputed OCSP responses (precomputed responses) is not allowed.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	5
ETSI	7.3.6.i, EN 319 411-2
PKIo	If the CSP supports OCSP, the information that is provided through OCSP has to be at least as equally up-to-date and reliable as the information that is published by means of a CRL, during the validity of the certificate that is issued and furthermore up to at least six months after the time at which the validity of the certificate has expired or, if that time is earlier, after the time at which the validity is ended by revocation.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	6
ETSI	7.3.6.i, EN 319 411-2

PKIo	If the CSP supports OCSP, the CSP has to update the OCSP service at least once every 4 calendar days. The maximum expiry term of the OCSP responses is 10 calendar days.

RFC 3647	4.9.13 Circumstances for suspension
Number	1
ETSI	7.3.6.d, EN 319 411-2
PKIo	Suspension of a certificate CANNOT be supported.

4.10 Certificate Status Service

RFC 3647	4.10.2 Service availability
Number	1
ETSI	7.3.6.i, EN 319 411-2
PKIo	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.

5 Facility, Management and Operational Controls

5.2 Procedural Controls

RFC 3647	5.2. Procedural Controls
Number	1
ETSI	6.4.1.a, EN 319 401 6.4.5, EN 319 401
PKIo	The CSP 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 CSP. Based on the risk analysis, the CSP 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 CSP can safeguard the availability, exclusivity and integrity of all PKIoverheid processes, requests and the information that is used to this end.

RFC 3647	5.2. Procedural Controls
Number	2
ETSI	6.4.1.b, EN 319 401
PKIo	In addition to an audit performed by an accredited auditor, the CSP MAY perform an audit of the external suppliers of PKIoverheid core services, in order to satisfy itself that these suppliers have implemented and operationalized the relevant requirements from the PoR of PKIoverheid, in accordance with the requirements of the CSP and taking into account its business objectives, processes and infrastructure. The CSP is entirely free to choose to perform its own audit, or to arrange for this to be performed, or to use existing audit results such as those from the formal certification audits, the various internal and external audits, Third Party Notifications and (foreign) compliancy reports. The CSP is also entitled to view the underlying evidentiary material, such as audit files and other documentation including system documentation. Of course the foregoing is limited to the CSP processes, systems and infrastructure hosted by the suppliers for PKIo core services.

RFC 3647	5.2.4 Roles requiring separation of duties
Number	1

ETSI	6.4.3.d and 6.4.3.h, EN 319 401
PKIo	The CSP 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 CSP systems, which includes installing, configuring and maintaining the systems. • CSP operators The CSP operators are responsible for the everyday operation of the CSP 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 CSP 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.

RFC 3647	5.2.4 Roles requiring separation of duties
Number	2
ETSI	6.4.3.d and 6.4.3.h, EN 319 401
PKIo	The CSP has to enforce separation of duties between staff who monitor the issuance of a certificate and staff who approve the issuance of a certificate.

5.3 Personnel Controls

RFC 3647	5.3 Declaration of confidentiality
Number	1
ETSI	6.4.3.e, EN 319 401
PKIo	Because publication of confidential information can have significant consequences (among other things, for the trustworthiness) the CSP 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.

RFC 3647	5.3.2 Background checks procedure
Number	1
ETSI	6.4.3-j, EN 319 401
PKIo	Before engaging the services of someone to work on one or more PKIoverheid core services, the CSP or external supplier that performs part of this work MUST verify the identity and the security of this employee.

5.4 Audit Logging Procedures

RFC 3647	5.4.1 Types of events recorded
Number	1
ETSI	6.4.5.j, EN 319 401

PKIo	Logging has to take place on at least:
	• Routers, firewalls and network system components;
	• Database activities and events;
	• Transactions;
	• Operating systems;
	• Access control systems;
	• Mail servers.
	
	At the very least, the CSP has to log the following events:
	• CA key life cycle management;
	• Certificate life cycle management;
	• Threats and risks such as:
	  • Successful and unsuccessful attacks on the PKI system;
	  • Activities of staff on the PKI system;
	  • Reading, writing and deleting data;
	  • Profile changes (Access Management);
	  • System failure, hardware failure and other abnormalities;
	  • Firewall and router activities;
	  • Entering and leaving the CA space.
	
	At the very least, the log files have to register the following:
	• Source addresses (IP addresses if available);
	• Target addresses (IP addresses if available);
	• Time and date;
	• User IDs (if available);
	• Name of the incident;
	• Description of the incident.

Comment	Based on a risk analysis the CSP determines which data it should save.

RFC 3647	5.4.3 Retention period for audit log

Number	1
ETSI	NCP+ 6.4.11.e, EN 319 401
PKIo	The CSP has to store log files for incidents relating to: • CA key life cycle management and; • Certificate lifecycle management; These log files must be retained for 7 years and then deleted. The CSP has to store log files for incidents relating to: • Threats and risks; These log files must be retained for 18 months and then deleted. The log files have to be retained in such a way that the integrity and accessibility of the data is safeguarded.

5.5 Records Archival

RFC 3647	5.5.2 Retention period for archive
Number	1
ETSI	6.4.11.e, EN 319 401
PKIo	No PKIo requirement applies, only a comment.
Comment	At the request of the entitled party, it can be agreed that the required information is stored for longer by the CSP. This is, however, not mandatory for the CSP.

5.7 Compromise and Disaster Recovery

RFC 3647	5.7.1 Incident and compromise handling procedures.
Number	1
ETSI	7.4.8.d, EN 319 411-2
PKIo	After analysis and establishment of a security breach and/or emergency the CSP has to immediately inform the PA, the NCSC and the auditor, and has to keep the PA, the NCSC and the auditor informed about how the incident is progressing.
Comment	Understood to be meant by security breach in the PKIoverheid context is: An infringement of the CSP 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.

RFC 3647	5.7.1 Incident and compromise handling procedures.
Number	2
ETSI	7.4.8.e, EN 319 411-2
PKIo	The CSP 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 CSP, which are not PKIoverheid services.

RFC 3647	5.7.4 Business continuity capabilities after a disaster.
Number	1
ETSI	6.4.8.a, EN 319 401
PKIo	The CSP has to draw up a business continuity plan (BCP) for, at the very least, the core services dissemination service, revocation management service and revocation status service, the aim being, in the event of a security breach or emergency, to inform, reasonably protect and to continue the CSP services for subscribers, relying parties and third parties (including browser parties). The CSP has to test, assess and update the BCP annually. At the very least, the BCP has to describe the following processes: ▪ Requirements relating to entry into force; ▪ Emergency procedure/fall-back procedure; ▪ Requirements relating to restarting CSP services; ▪ Maintenance schedule and test plan that cover the annual testing, assessment and update of the BCP; ▪ Provisions in respect of highlighting the importance of business continuity; ▪ Tasks, responsibilities and competences of the involved agents; ▪ Intended Recovery Time or Recovery Time Objective (RTO); ▪ Recording the frequency of back-ups of critical business information and software; ▪ Recording the distance of the fall-back facility to the CSP's main site; and ▪ Recording the procedures for securing the facility during the period following a security breach or emergency and for the organization of a secure environment at the main site or fall-back facility.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

RFC 3647	6.1.1 Key pair generation for the CSP sub CA
Number	1
ETSI	7.2.1.c and 7.2.1.d, EN 319 411-2
PKIo	The algorithm and the length of the cryptographic that are used for generating the keys for the CSP sub CA have to fulfil the requirements laid down in that respect in the list of recommended cryptographic algorithms and key lengths as defined in ETSI TS 102 176-1.
Comment	Although ETSI TS 102 176 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.

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	2
ETSI	7.2.8.c and 7.3.1.l, EN 319 411-2
PKIo	The generation of the keys of certificate holders (or information for creating electronic signatures) has to take place using a device that fulfils the requirements mentioned in {12} CWA 14167 "Secure signature-creation devices "EAL 4+"" or similar security criteria.
Comment	In the Citizen domain the secure device has to be a smartcard that fulfils the requirements relating to the eNIK.

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	3
ETSI	7.2.8.a, EN 319 411-2
PKIo	The algorithm and the length of the cryptographic keys used by the CSP for generating keys of certificate holders has to fulfil the requirements laid down in that respect in the list of cryptographic algorithms and key lengths as defined in ETSI TS 102 176-1.
Comment	Although ETSI TS 102 176 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.

RFC 3647	6.1.2 Private key and SSCD delivery to certificate holder
Number	1
ETSI	7.2.8.d, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.2; OID 2.16.528.1.1003.1.2.3.1] The private key of the certificate holder has to be delivered to the certificate holder, if required through the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the certificate holder, the private key can be maintained under the certificate holder's sole control.
Comment	This text corresponds with QCP 7.2.8.d, but has been integrated because this requirement only applies to signature and authenticity certificates.

RFC 3647	6.1.5 Key sizes
Number	1
ETSI	7.2.8.b, EN 319 411-2
PKIo	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 102 176-1.
Comment	Although ETSI TS 102 176 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.

RFC 3647	6.1.7 Key usage purposes (as per X.509 v3 key usage field)
Number	1
ETSI	7.2.5, EN 319 411-2
PKIo	The key usage extension (key usage) in X.509 v3 certificates (RFC5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile) defines the purpose of the use of the key embodied in the certificate. The CSP has to indicate the use of keys in the certificate, in accordance with the requirements laid down in that respect in appendix A 'Certificate and CRL and OCSP profiles' of this CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

RFC 3647	6.2.3 Private key escrow of certificate holder key
Number	1
ETSI	7.2.4, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.2; OID 2.16.528.1.1003.1.2.3.1] Escrow by the CSP is not allowed for the private keys of the signature certificate and the authenticity certificate.

RFC 3647	6.2.3 Private key escrow of certificate holder key
Number	2
ETSI	7.2.4, EN 319 411-2 (ETSI TS 102 042, 7.2.4.b)
PKIo	[OID 2.16.528.1.1003.1.2.3.3] The authorized persons, who can gain access to the private key of the confidentiality certificate (if applicable) held by the CSP in Escrow, have to identify themselves using the applicable documents referred to in article 1 of the Compulsory Identification Act (Wet op de identificatieplicht), or a valid qualified certificate (restricted to the PKIoverheid signature certificate or equivalent).

RFC 3647	6.2.3 Private key escrow of certificate holder key
Number	3
ETSI	7.2.4, EN 319 411-2 (ETSI TS 102 042 7.2.4.b)
PKIo	[OID 2.16.528.1.1003.1.2.3.3] The CSP has to describe in the CPS which parties can have access to the private key of the confidentiality certificate held in Escrow and under which conditions.

RFC 3647	6.2.3 Private key escrow of certificate holder key
Number	4
ETSI	7.2.4, EN 319 411-2 (ETSI TS 102 042 , 7.2.4.b)
PKIo	[OID 2.16.528.1.1003.1.2.3.3] If the CSP keeps the private key of the confidentiality certificate in Escrow, the CSP has to guarantee that this private key is kept secret and is only made available to appropriately authorized persons.

Comment	Although this requirement corresponds with ETSI TS 102 042 , 7.2.4.b, this requirement is nevertheless positioned as a PKIo requirement in order to make sure that this forms part of the approved audit statement that the CSP has to submit.

RFC 3647	6.2.4 Private key backup of certificate holder key
Number	1
ETSI	7.2.4 and 7.2.8.e, EN 319 411-2
PKIo	Back-up of the certificate holders' private keys by the CSP is not allowed.

RFC 3647	6.2.3 Private key archival of certificate holder key
Number	1
ETSI	7.2.4 and 7.2.8.e, EN 319 411-2
PKIo	Archiving of the certificate holders' private keys by the CSP is not allowed.

RFC 3647	6.2.11 Cryptographic module rating
Number	1
ETSI	5.3.1.c, EN 319 411-2
PKIo	The secure devices issued or recommended by the CSP for creating electronic signatures (SSCDs) have to fulfil the requirements laid down in document {7} CWA 14169 "Secure signature-creation devices "EAL 4+"" and the requirements stipulated in or in accordance with the Electronic Signatures Decree article 5, parts a,b,c and d.

RFC 3647	6.2.11 Cryptographic module rating
Number	2
ETSI	5.3.1.c, EN 319 411-2
PKIo	Instead of demonstrating compliance with CWA 14169, CSPs can issue or recommend SSCDs that are certified in line with a different protection profile against the Common Criteria (ISO/IEC 15408) at level EAL4+ or that have a comparable security level. This has to be established by a test laboratory that is accredited for performing Common Criteria evaluations.

RFC 3647	6.2.11 Cryptographic module rating
Number	3
ETSI	5.3.1.c, EN 319 411-2
PKIo	The concurrence of SSCDs with the requirements outlined in PKIo requirement no. 6.2.11-1 has to have been ratified by a government body appointed to inspect the secure devices, for the creation of electronic signatures in accordance with the Dutch Telecommunications Act (TW) article 18.17, third paragraph. In this respect, also see the Ruling on Electronic Signatures, articles 4 and 5.

6.3 Other Aspects of Key Pair Management

RFC 3647	6.3.1 Public key archival
Number	1
ETSI	6.4.11.e, EN 319 401
PKIo	[OID 2.16.528.1.1003.1.2.3.2] The signature certificate has to be saved for the term of validity and furthermore, for a period of at least seven years after the date on which the validity of the certificate has expired.
Comment	The Electronic Signature Regulation article 2, paragraph 1i stipulates a term of seven years. No further provisions apply to the authenticity certificate and the confidentiality certificate in relation to archiving public keys.

RFC 3647	6.3.2 Certificate operational periods and key pair usage periods
Number	1
ETSI	7.2.6, EN 319 411-2
PKIo	Private keys that are used by a certificate holder and issued under the responsibility of this CP must not be used for more than five years. The certificates, that are issued under the responsibility of this CP, have to be valid for no more than five years.
Comment	The CSPs within the PKI for the government cannot issue certificates with a maximum term of validity of five years until the PA has provided explicit permission for this. The explicit permission is to be recorded with this article.

RFC 3647	6.3.2 Certificate operational periods and key pair usage periods
Number	2
ETSI	7.2.6, EN 319 411-2

PKIo	At the time that an end user certificate is issued, the remaining term of validity of the higher level CSP certificate has to exceed the intended term of validity of the end user certificate.

6.4 Activation data

RFC 3647	6.4.1 Activation data generation and installation
Number	1
ETSI	7.2.9.d, EN 319 411-2
PKIo	The CSP attaches activation data to the use of an SSCD, to protect the private keys of the certificate holders.
Comment	The requirements that the activation data (for example the PIN code) have to fulfil, can be determined by the CSPs themselves based on, for example, a risk analysis. Requirements that could be considered are the length of the PIN code and use of special characters.

RFC 3647	6.4.1 Activation data generation and installation
Number	2
ETSI	7.2.9.d, EN 319 411-2
PKIo	An unlocking code can only be used if the CSP can guarantee that, at the very least, the security requirements are fulfilled that are laid down in respect of the use of the activation data.

6.5 Computer Security Controls

RFC 3647	6.5.1 Specific computer security technical requirements
Number	1
ETSI	7.4.6, EN 319 411-2 6.4.6, EN 319 401
PKIo	The CSP 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 the user accounts which are used to issue or approve certificates.
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.

RFC 3647	6.5.1 Specific computer security technical requirements
Number	2
ETSI	7.4.6, EN 319 411-2 6.4.6, EN 319 401
PKIo	The staff of external Registration Authorities (RA) or Resellers may not have access to the system or the user accounts of the CSP which enables issuance or approval of certificates. This function is restricted to authorized staff of the CSP. If an RA or a Reseller does have this access, the RA or the Reseller will be seen as part of the CSP and it/they have to comply with the PKI for the government Programme of Requirements fully and demonstrably.

RFC 3647	6.5.1 Specific computer security technical requirements
Number	3
ETSI	6.4.6.a, EN 319 401
PKIo	The CSP prevents unauthorized access to the following core services: registration service, certificate generation service, subject device provision service, dissemination service, revocation management service and revocation status service. To this end, these core services are separated either physically or logically from the non-PKI network domains, or the various core services will be implemented on separate network domains, where there has to be a unique authentication for each core service. If core services use the same network domains, the CSP enforces a unique authentication for each core service. The CSP documents the organization of the network domains, at least in a graphical manner.
Comment	This requirement applies to both the production environment and the fall-back environment. This requirement does not apply to other environments, such as acceptance and test.

6.6 Life Cycle Technical Controls

RFC 3647	6.6.1 System development controls
Number	1
ETSI	6.4.7, EN 319 401 7.4.7, EN 319 411-2
PKIo	In relation to this ETSI requirement, the PKIoverheid have only formulated a comment and no specific PKIo requirement applies.
Comment	Compliance with 7.4.7. and Electronic Signature Regulation art. 2 paragraph 1c can be demonstrated by: • an audit statement from the supplier of the products, which has had an independent EDP audit performed based on CWA 14167-1; • an audit statement from an internal auditor from the CSP based on CWA

	14167-1; • an audit statement from an external auditor based on CWA 14167-1.

6.7 Network Security Controls

RFC 3647	6.7.1 Network security controls
Number	1
ETSI	6.4.6, EN 319 401 7.4.7, EN 319 411-2
PKIo	The CSP 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 CSP has to use the NCSC's "Checklist beveiliging webapplicaties (Security of Web Applications Checklist)[3]" as guidance for this. In addition it is recommended that the CSP implements all other recommendations from the latest version of the white paper "Raamwerk Beveiliging Webapplicaties (The Framework for Web Application Security)" by the NCSC.

RFC 3647	6.7.1 Network security controls
Number	2
ETSI	7.4.6, EN 319 411-2 6.4.6, EN 319 401
PKIo	Using an audit tool, at least each month the CSP performs a security scan on its PKIoverheid infrastructure. The CSP 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.

RFC 3647	6.7.1 Network security controls
Number	3

[3] http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/factsheets/checklist-webapplicatie-beveiliging/checklist-webapplicatie-beveiliging/govcert%3AdocumentResource/govcert%3Aresource

ETSI	7.4.6, EN 319 411-2 6.4.6, EN 319 401
PKIo	At least once a year, the CSP arranges for a pen test to be performed on the PKIoverheid internet facing environment, by an independent, experienced, external supplier. The CSP has to document the findings from the pen test and the measures that will be taken in this respect, or to arrange for these to be documented.
Comment	As guidance for the selection of suppliers, the CSP can use the recommendation in chapter 4 ("Supplier Selection") as described in the latest version of the whitepaper entitled "Pentesten doe je zo[4]" (how to perform penetration testing) published by the NCSC. If necessary, the PA can instruct the CSP to perform additional pen tests.

[4] *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*

7 Certificate, CRL and OSCP profiles

7.1 Certificate Profile

RFC 3647	7.1 Certificate profile
Number	1
ETSI	7.3.3.a, EN 319 411-2
PKIo	The CSP has to issue certificates in accordance with the requirements stipulated in that respect in appendix A of this document, "Certificate, CRL and OCSP profiles".

7.2 CRL Profile

RFC 3647	7.2 CRL Profile
Number	1
ETSI	7.3.6.g, EN 319 411-2
PKIo	The CSP has to issue CRLs in accordance with the requirements stipulated in that respect in appendix A of this document, "Certificate, CRL and OCSP profiles".

7.3 OCSP Profile

RFC 3647	7.3 OCSP profile
Number	1
ETSI	OCSP is not covered in ETSI.
PKIo	If the CSP supports the Online Certificate Status Protocol (OCSP), the CSP has to use OCSP certificates and responses in accordance with the requirements laid down in this respect in appendix A of this document, "Certificate, CRL and OCSP profiles".

8 Compliance Audit and Other Assessments

All subjects relating to the conformity assessment of the CSPs within the PKI for the government are covered in PoR part 2: Admittance to and Supervision within the PKI for the government.

9 Other Business and Legal Matters

9.2 Financial Responsibility

RFC 3647	9.2.1 Insurance coverage, 9.2.2 Other resources
Number	1
ETSI	6.5.c, EN 319 401
PKIo	By means, for example, of insurance or its financial position, the CSP has to be able to cover third party recovery based on the types of liability mentioned in article 6:196b of the Civil Code (that relate to both direct and indirect damage) up to at least EUR 1,000,000 per annum.
Comment	The third party recovery described above is based on a maximum number of certificates to be issued of 100,000 for each CSP, which is in line with the current situation. When CSPs are going to issue more certificates, it will be determined whether a suitable, higher, recoverableness will be required.

9.5 Intellectual Property Rights

RFC 3647	9.5 Intellectual property rights
Number	1
ETSI	ETSI does not cover a violation of intellectual property rights
PKIo	The CSP indemnifies the subscriber in respect of claims by third parties due to violations of intellectual property rights by the CSP.

9.6 Representations and Warranties

RFC 3647	9.6.1 CA Representations and Warranties by CSPs
Number	1
ETSI	6.4 and Annex A, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.1] In the agreement between the CSP and the subscriber, a clause (a clause as specified in article 6:253 of the Civil Code) will be included in which the CSP champions the interests of a third party relying on the certificate. This clause addresses a liability of the CSP in accordance with article 6:196b, first up to and including third paragraph, of the Civil Code, with the proviso that: a. for "a qualified certificate specified in article 1.1, division ss Telecommunications Act": "an authenticity certificate" is read; b. for "signatory": "certificate holder" is read; c. for "electronic signatures": "authenticity properties" is read.

RFC 3647	9.6.1 CA Representations and Warranties by CSPs
Number	2
ETSI	6.4 and Annex A, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.3] In the agreement between the CSP and the subscriber, a clause (a clause as specified in article 6:253 of the Civil Code) will be included in which the CSP champions the interests of a third party relying on the certificate. This clause addresses a liability of the CSP in accordance with article 6:196b, first up to and including third paragraph, of the Civil Code, with the proviso that: a. for "a qualified certificate specified in article 1.1, division ss Telecommunications Act": "a confidentiality certificate" is read; b. for "signatory": "certificate holder" is read; c. for "creation of electronic signatures": "creation of encrypted data" is read; d. For "verification of electronic signatures": "decoding of encrypted data" is read.

RFC 3647	9.6.1 CA Representations and Warranties by CSPs
Number	3
ETSI	6.4 and Annex A, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.2] In a signature certificate, the PA can include restrictions regarding the use of that certificate, provided that those restrictions are clear to third parties. The CSP is not liable for losses that results from the use of a signature certificate that is contrary to the provisions in accordance with the previous sentence listed therein.
Comment	This article is based on Civil Code art. 196b, paragraph 3

RFC 3647	9.6.1 CA Representations and Warranties by CSPs
Number	4
ETSI	6.4 and Annex A, EN 319 411-2
PKIo	The CSP excludes all liability for damages if the certificate is not used in accordance with the certificate use described in paragraph 1.4.

9.8 Limitations of Liability

RFC 3647	9.8 Limitations of liability
Number	1

ETSI	6.4, EN 319 411-2
PKIo	Within the scope of certificates as mentioned in paragraph 1.4 in this CP the CSP is not allowed to place restrictions on the use of certificates.

RFC 3647	9.8 Limitations of liability
Number	2
ETSI	6.4, EN 319 411-2
PKIo	Within the scope of certificates, as mentioned in paragraph 1.4 in this CP the CSP is not allowed to place restrictions on the value of the transactions for which certificates can be used.

9.12 Amendments

The change procedure for the PoR of the PKIoverheid is incorporated in PKIoverheid's Certificate Policy Statement. The CPS can be obtained in an electronic format on the PA's website:

https://www.logius.nl/producten/toegang/pkioverheid/documentatie/cps/

RFC 3647	9.12.2 Notification mechanism and period
Number	1
ETSI	This subject is not covered in ETSI.
PKIo	If a published amendment of the CP can have consequences for the end users, the CSPs will announce the amendment to the subscribers and/or certificate holders registered with them in accordance with their CPS.

RFC 3647	9.12.2 Notification mechanism and period
Number	2
ETSI	This subject is not covered in ETSI.
PKIo	The CSP has to provide the PA with information about the intention to amend the CA structure. Consider, for example, the creation of a sub-CA.

This CP and the approved amendments made to it can be obtained in an electronic format through the Internet on the PA's website. The address of this is: http://www.logius.nl/pkioverheid.

9.13 Dispute Resolution Procedures

RFC 3647	9.13 Dispute resolution provisions
Number	1
ETSI	6.5.e, EN 319 401
PKIo	The complaints handling process and dispute resolution procedures applied by the CSP may not prevent proceedings being instituted with the ordinary court.

9.14 Governing Law

Dutch law applies to this CP.

9.17 Miscellaneous provisions

RFC 3647	9.17 Miscellaneous provisions
Number	1
ETSI	This subject is not covered in ETSI, as ETSI has been specifically drafted for qualified certificates.
PKIo	The CSP has to be capable of issuing all types of personal certificates listed under [1.2].

If by judicial decision one or more provisions of this CP are declared to be invalid or not applicable, this does not affect the validity and applicability of all other provisions.

Appendix A Certificate profiles and certificate status information

Profile of the certificate for the Citizen domain

Criteria
When defining the fields and attributes within a certificate, the following codes are used:

- V : Compulsory; indicates that the attribute is compulsory and MUST be used in the certificate.
- O : Optional; indicates that the attribute is optional and MAY be used in the certificate.
- A : Advised against; indicates that the attribute is advised against and SHOULD NOT be used in the certificate.
- N : Not allowed; indicates that the use of the attribute in the PKI for the government is not allowed.

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

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 102176-1 : "Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms", version 2.0.0 (2007-11).
11. ISO 3166 "English country names and code elements".

General requirements

- End user certificates MUST correspond with the X.509v3 standard for public key certificates. General requirements in relation to certificates are listed in RFC5280, specific requirements for qualified certificates are listed in RFC 3739.

- 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, Optional or Advised Against may be used.
- The certificate for the electronic signature MUST correspond with the EESSI Qualified Certificate profile (ETSI TS 101 862). If there are any differences between TS 101 862 and RFC 3739, TS 101 862 prevails.
- Personal certificates MUST correspond with the standard ETSI TS 102 280 as far as the certificate profile is concerned. When there are differences between TS 102280 and TS 101862, RFC3739 or RFC5280, TS 102280 prevails.

Naming convention Subject.commonName
The following requirements apply to the CommonName of the Subject field. The main principle is that the CSP is responsible for correct entry of the CommonName. For a correct implementation this entails that the CSP has to be able to check each part that is entered. This means the following for parts:

A. Notation:
The notation and spelling of the parts of the CommonName have to be in accordance with the GBA registration (GBA: municipal personal records database). This can be done by consulting the Compulsory Identification Act document provided with the identification.

B. Order:
The CSP is, in principle, free to choose the order between the categories <First name(s) and/or initials>, <Surname prefixes> and <Surname>. Of course, within such a category, the order has to be maintained (on account of rule A). The use of commas as punctuation between the categories is advised against due to possible technical conflicts when processing the certificate.

C. First names in the CommonName:
The CSP is free to use either first name(s) in full or initials in the CommonName. The style of first name(s) or initials may not conflict with the Compulsory Identification Act document that is used or the GBA registration (see rule A). If when full first names are used the CommonName contains more characters than the field can cope with technically, use will be made of the replacement of the full first names by initials, starting with the last full first name, until the CommonName that is used does fit.

D. Entry of the name of partner/spouse:
1. A certificate holder is not obliged to include the partner name in PKIO certificates. In that case <Surname> only consists of the <maiden name/boy's name from the Compulsory Identification Act document that is provided>.

2. If the certificate holder does wish for his/her partner's name to be included in a PKIO certificate, then the <Surname> consists of <Name partner/spouse>-<maiden name/boy's name from the Compulsory Identification Act document that is provided>.

3. With respect to the correctness of <Name partner/spouse> the certificate holder has to show evidence. It should be noted that, as far as the entry of the status ('spouse of') is concerned, a Compulsory Identification Act document does not have to run in synchronization with the GBA registration (and this does not have to run in synchronization with the current situation). The Compulsory Identification Act document will therefore not always be adequate as evidence.

If, when the name of the partner/spouse is entered, the names jointly contain more characters than the CommonName field can hold after application of rule C, only the maiden name/boy's name listed in the Compulsory Identification Act document is reverted to.

Personal certificates

Basic attributes

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Version	V	MUST be set at 2 (X.509v3).	RFC5280	Integer	Describes the version of the certificate, the value 2 stands for X.509 version 3.
SerialNumber	V	A serial number that MUST uniquely identify the certificate within the publishing CA domain.	RFC5280	Integer	All end user certificates have to contain at least 8 bytes of unpredictable random data in the certificate's serial number (SerialNumber).
Signature	V	MUST be created on the algorithm, as stipulated by the PA.	RFC5280, ETSI TS 102176	OID	MUST be the same as the field signatureAlgorithm. For maximum interoperability only sha-1WithRSAEncryption is allowed for certificates under the G1 root certificate. As from 01-01-2011 the CSP MAY only issue certificates based on sha-1WithRSAEncryption under the G1 root certificate in very exceptional situations. This certificate MUST contain a 2048 bit RSA key. This certificate MAY only be valid until no later than 31-12-2011. For certificates under the G2 root certificate, only sha-256WithRSAEncryption is allowed.
Issuer	V	MUST contain a Distinguished Name (DN). The field has the following attributes:	PKIo, RFC3739, ETSI TS 102280		Attributes other than those mentioned below MUST NOT be used. The attributes that are used MUST be the same as the corresponding attributes in the Subject field of the CSP certificate (for validation).
Issuer.countryName	V	MUST contain the country code of the country where the issuing organization of the certificate is located.	ETSI TS101862, X520, ISO 3166	Printable String	C = NL for CSPs located in the Netherlands.
Issuer.stateOrProvinceName	N	Use is not allowed.	PKIo	UTF8String	-

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Issuer.OrganizationName	V	Full name in accordance with the accepted document or basic registry	ETSI TS 102280	UTF8String	
Issuer. organizationalUnitName	O	Optional specification of an organizational entity. This field MUST NOT include a function indication or similar. It may include, if applicable, the types of certificates that are supported.	ETSI TS 102280: 5.2.4	UTF8String	Several instances of this attribute MAY be used.
Issuer.localityName	N	Use is not allowed.	PKIo	UTF8String	-
Issuer.serialNumber	O	MUST be used in accordance with RFC 3739 if required for unambiguous naming	RFC 3739	Printable String	
Issuer.commonName	V	MUST include the name of the CA in accordance with accepted document or basic registry, optionally including the Domain indication and/or the types of certificates that are supported	PKIo, RFC 3739	UTF8String	The commonName attribute MUST NOT be necessary in order to identify the issuing government body (no part of the Distinguished Name, requirement from RFC 3739)
Validity	V	MUST define the period of validity of the certificate according to RFC 5280.	RFC 5280	UTCTime	MUST include the start and end date for validity of the certificate in accordance with the applicable policy laid down in the CPS.
subject	V	The attributes that are used to describe the subject (end user) MUST mention the subject in a unique manner. The field has the following attributes:	PKIo, RFC3739, ETSI TS 102 280		MUST contain a Distinguished Name (DN). Attributes other than those mentioned below MUST NOT be used.
Subject.countryName	V	complete C with two-letter country code in	RFC 3739, X520,	PrintableString	The country code that is used in Subject.countryName MUST correspond

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		accordance with ISO 3166-1. If an official alpha-2 code is missing, the CSP MAY use the user-assigned code XX.	ISO 3166, PKIo		with the subscriber's address in accordance with the accepted document or registry.
Subject.commonName	V	The commonName attribute MUST be entered in accordance with the Naming Convention Subject.commonName paragraph shown above.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	The contents of this field MUST correspond with the name given in the GBA. The Compulsory Identification Act document or other evidence (excerpt from the population register) can be used to demonstrate this. The use of commas as punctuation in the commonName is advised against due to possible technical conflicts when processing the certificate.
Subject.Surname	A	A correct reproduction of the element of the name laid down in the CN. Based on the Compulsory Identification Act document.	RFC 3739	UTF8String	The use of this field is advised against. If this field is used, it MUST show the subject's surname including surname prefixes correctly. The surname MUST NOT be in conflict with the information in the commonname
Subject.givenName	A	A correct reproduction of the element of the name laid down in the CN. Based on the Compulsory Identification Act document.	RFC 3739	UTF8String	The use of this field is advised against. If this field is used, it MUST show the subject's first name(s) correctly. The givenName MUST NOT conflict with the information in the commonname; the givenName may contain full first name(s), whilst the commonName contains initials.
Subject.pseudonym	N	Pseudonyms may not be used.	ETSI TS 102 280, RFC 3739, PKIo		
Subject.organizationName	N	For certificates in the Citizen domain, the use of organizationName is not allowed	PKIo	UTF8String	In the Citizen domain, the certificate holder and subscriber are one and the same and there is therefore no subscriber organization whose name can be entered in this field
Subject.organizationalUnitName	N	For certificates in the Citizen domain, the	PKIo		In the Citizen domain, the certificate holder and subscriber are one and

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		use of organizationUnitName is not allowed			the same and there is therefore no subscriber organization part whose name can be entered in this field
Subject.stateOrProvinceName	A	The use is advised against. If present, this field MUST contain the province of the certificate holder's branch in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the province MUST correspond with the certificate holder's address in accordance with the GBA. The certificate holder will have to submit recent proof of his address.
Subject.localityName	A	The use is advised against. If present, this field MUST contain the location of the certificate holder in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the domicile MUST correspond with the certificate holder's address in accordance with the GBA. The certificate holder will have to submit recent proof of his address.
Subject.postalAddress	A	The use is advised against. If present, this field MUST contain the certificate holder's postal address in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	The address MUST correspond with the certificate holder's address in accordance with the GBA. The certificate holder will have to submit recent proof of his address.
Subject.emailAddress	N	Use is not allowed.	RFC 5280	IA5String	This field MUST NOT be used in new certificates.
Subject.serialNumber	V	Number to be determined by the CSP. The combination of CommonName and Serialnumber MUST be unique within the context of the CSP.	RFC 3739, X 520, PKIo	Printable String	The serial number is intended to enable a distinction to be made between subjects with the same commonName. To avoid susceptibilities a serial Number attribute MUST be allocated to every subject.
Subject.title	N	The use of the title attribute is not allowed for certificates in the Citizen domain.	ETSI TS 102 280, RFC 3739, RFC 5280		Includes the role of a subject in the organization mentioned in the Organization attribute (RFC 3739). In the Citizen domain, the Organization attribute is not allowed and title can therefore also not be

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
					used.
subjectPublicKeyInfo	V	Contains, among other things, the public key.	ETSI TS 102 280, RFC 3279		Contains the public key, identifies the algorithm with which the key can be used.
IssuerUniqueIdentifier	N	Is not used.	RFC 5280		The use of this is not allowed (RFC 5280)
subjectUniqueIdentifier	N	Is not used.	RFC 5280		The use of this is not allowed (RFC 5280)

Standard extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityKeyIdentifier	V	No	The algorithm to generate the AuthorityKey MUST be created on an algorithm determined by the PA.	ETSI TS 102 280, RFC 5280	BitString	The value MUST contain the SHA-1 hash from the authorityKey (public key of the CSP/CA).
SubjectKeyIdentifier	V	No	The algorithm to generate the subjectKey MUST be created on an algorithm determined by the PA.	RFC 5280	BitString	The value MUST contain the SHA-1 hash from the subjectKey (public key of the certificate holder).
KeyUsage	V	Yes	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 authenticity certificates the digitalSignature bit MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this. In confidentiality certificates, keyEncipherment and dataEncipherment bits MUST be incorporated and marked as being essential. Optionally this MAY be combined with the keyAgreement bit. another keyUsage MUST NOT be combined with this.	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			In certificates for the electronic signature the non-repudiation bit MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this.			
privateKeyUsagePeriod	N		Is not used.	RFC 5280		
CertificatePolicies	V	No	MUST contain the OID of the certificate policy (CP), the URI of the certification practice statement (CPS), and a user notice. The applicable PKI for the government OID scheme is described in the CP.	RFC 3739	OID, String, String	For the Citizen domain, the OIDs are: 2.16.528.1.1003.1.2.3.1, 2.16.528.1.1003.1.2.3.2 and 2.16.528.1.1003.1.2.3.3. Reference to the paragraph numbers of the PoR/CP in the user notice is advised against because the persistency of this cannot be guaranteed (unlike the OID number of the CP).
PolicyMappings	N		Is not used.			This extension is not used in end user certificates
SubjectAltName	V	No	MUST be used and given a personal worldwide unique identification number.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MUST include a unique identifier in the othername attribute. Attributes other than those mentioned below MUST NOT be used.
SubjectAltName.otherName	V		MUST be used containing a unique identification number that identifies the certificate holder.	PKIo	IA5String, Microsoft UPN, IBM Principal-Name or Permanent-Identifier	Includes the OID of the CPS and a number that permanently and uniquely identifies the subject service, separated by a point or hyphen ('-'). It is advised that an existing registration number from the back office systems is used. In combination with the CSP's OID number, this identifier is unique throughout the world. This number MUST be persistent.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
SubjectAltName.rfc822Name	A		MAY be used for the certificate holder's e-mail address, for applications that need the e-mail address to be able to function properly.	RFC 5280	IA5String	For PKIoverheid certificates, the use of e-mail addresses is advised against, because e-mail addresses of certificate holders often change and are susceptible to spam. If the e-mail address is included in the certificate, the CSP MUST: • have the subscriber sign for approval, and; • check whether the email address belongs to the subscriber and that the subscriber has access to the email address (for example by performing a challenge response).
IssuerAltName	N		Is not used.	RFC 5280		
subjectDirectoryAttributes	N		Is not used.	RFC 5280; RFC 3739		This extension may not be used. These attributes contain personal data that can impair the privacy of the subject.
BasicConstraints	O	Yes	The "CA" field MUST be set at "FALSE", or be omitted (default value is then "FALSE").	RFC 5280		A (Dutch language) browser can then be seen: "Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen" ("Subject type = End Entity", "Path length constraint = None")
NameConstraints	N		Is not used.	RFC 5280		Is not used in end user certificates.
PolicyConstraints	N		Is not used.	RFC 5280		Is not used in end user certificates.
CRLDistributionPoints	V	No	MUST include the URI of a CRL distribution point.	RFC 5280, ETSI TS 102 280		The reference MUST be accessible through the http or LDAP protocol. The attribute Reason MUST NOT be used, reference MUST be made to 1 CRL for all types of reasons for revocation. In addition to CRL, other types of certificate status information service MAY be supported.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
ExtKeyUsage	N	No	Is not used.	RFC 5280		Is not used in certificates in the Citizen domain. This field is also called enhancedKeyUsage.
InhibitAnyPolicy	N		Is not used.	RFC 5280		Is not used in end user certificates.
FreshestCRL	O	No	MUST contain the URI of a Delta CRL distribution point, if Delta CRLs are used.	RFC 5280, PKIo		Delta-CRLs are an optional extension. In order to fulfil the requirements of PKIoverheid a CSP MUST also publish full CRLs at the required release frequency.

Private extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityInfoAccess	O	No	This attribute MUST include the URI of an OCSP responder if Online Certificate Status Protocol (OCSP) plays a role.			This field can optionally be used to reference other additional information about the CSP.
SubjectInfoAccess	O	No		RFC 5280	OID, Generalname	This field can be used to reference additional information about the subject, provided that the information that is offered does not infringe the privacy of the subject.
BiometricInfo	O	No	Contains the hash of a biometric template and optionally a URI that references a file with the biometric template itself.	RFC 3739		
QcStatement	V/N	No	Certificates for the electronic signature MUST indicate that they are issued as qualified certificates complying with annex I and annex II of the European Directive. This compliance is indicated by including the *id-etsi-qcs-QcCompliance* statement in this extension. Certificates for the electronic signature MAY indicate that the private key that is part of the public key in the certificate is saved on a secure signature creation device (SSCD) complying with annex III of the European Directive. This compliance is indicated by including the *id-etsi-qcs-QcSSCD* statement in this extension.	RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	The aforementioned QcStatement identifiers relate to the following OIDs: id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4

Profile of the CRL

General requirements in relation to the CRL

- The CRLs have to fulfil the X.509v3 standard for public key certificates and 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 (in accordance with the Electronic Signatures Act).

CRL attributes

Field / Attribute	Criteria	Description	Standard reference1	Type	Explanation
Version	V	MUST be set to 1 (X.509v2 CRL profile).	RFC5280	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.	RFC5280	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 CSP certificate (for validation).
Issuer.countryName	V	MUST contain the country code of the country where the issuing organization of the certificate is located.	ISO3166, X.520	Printable String	C = NL for CSPs located in the Netherlands.
Issuer.stateOrProvinceName	N	Is not used.	PKIo	UTF8String	-
Issuer.OrganizationName	V	Full name in accordance with the accepted document or basic registry	ETSI TS 102280: 5.2.4	UTF8String	

Field / Attribute	Criteria	Description	Standard reference1	Type	Explanation
Issuer. organizationalUnitName	O	Optional specification of an organizational entity. This field MUST NOT include a function indication or similar. It may include, if applicable, the types of certificates that are supported.	ETSI TS 102280: 5.2.4	UTF8String	Several instances of this attribute MAY be used.
Issuer.localityName	N	Is not used.	PKIo	UTF8String	-
Issuer.serialNumber	O	MUST be used if required for unambiguous naming	RFC 3739	Printable String	
Issuer.commonName	V	MUST include the name of the CA in accordance with accepted document or basic registry, MAY include the Domain label and/or the types of certificates that are supported	PKIo, RFC 5280	UTF8String	
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.
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.

CRL extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference1	Type	Explanation
authorityKeyIdentifier	O	No	This attribute is interesting if a CSP 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 CSP/CA).
IssuerAltName	A	No	This attribute allows alternative names to be used for the CSP (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 a 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 CSP 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.
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.

Field / Attribute	Criteria	Critical?	Description	Standard reference1	Type	Explanation
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	If used, this gives the reason why a certificate has been revoked.	RFC 5280	reasonCode	If no reason is given, this field MUST be omitted
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 CSP 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	

Profile OCSP

The OCSP certificate profile can be found in the appendix to the CP Services certificates.

Appendix B Reference matrix

Based on chapters 1 to 9 inclusive, a reference matrix is included in appendix B. In accordance with the RFC 3647 structure, the matrix contains a reference to the applicable requirements within the PKI for the government. Here a distinction is made between the Dutch legislation, ETSI EN 319 411-2 and the PKIo requirements.

In the table below, the first and second column correspond with the chapter and paragraph division used in RFC 3647. Subsequently, the column 'ETSI requirement' outlines which requirements from ETSI apply to the relevant paragraph from the Certificate Policy applied within PKIoverheid. When an ETSI requirement applies to several paragraphs from RFC 3647, the reference to the relevant ETSI requirement is included once. As already indicated in PoR part 1, the requirements from ETSI apply to all types of certificates, unless stated otherwise.

In addition, the table states which requirements from the legal framework are not covered by ETSI and on which parts in the CP these legal requirements apply. Harmonization is sought with the Electronic Signature Regulation, which states which requirements from the Electronic Signature Regulation are not covered by ETSI. Also included in the table below are the articles from the Electronic Signature Act that relate to liability. This has been done because these articles are detailed further in PKIo requirements.

In the final column, for the PKIo requirements it is stated to which paragraph from the CP these requirements apply. The ETSI requirements written in italics have been detailed further in PKIo requirements. In the table, a PKIo requirement may be included without an ETSI requirement being linked to this. This is caused by the fact that a PKIo requirement is sometimes based on a part of an ETSI requirement, whilst that ETSI requirement as a whole fits in better with a different RFC paragraph. Also, several PKIo requirements can sometimes use the same ETSI requirement as a source, whilst every ETSI requirement is only mentioned once.

For a number of RFC paragraphs no requirements have been included. This means that no requirements apply to the relevant RFC paragraph or that the requirements are already incorporated in another RFC paragraph[5]. The PA has specifically decided to include all requirements just once.

5 This is partially caused by the fact that ETSI EN 319 411-2 is not constructed in accordance with the RFC 3647 structure.

No.	CP reference	ETSI requirement	Legal requirement	PKIo requirement
1	**Introduction to the Certificate Policy**			
1.1	**Overview**			1.1
1.2	**References to this CP**			1.2
1.3	**User community**			1.3
1.4	**Certificate Usage**			1.4
1.5	**Contact information Policy Authority**			1.5
2	**Publication and Repository Responsibilities**			
2.1	**Electronic Repository**	*7.3.1.b* *7.3.4.b* *7.3.5.e* *7.3.5.f*		2.1-1 2.1-2
2.2	**Publication of CSP Information**	*5.2.b*		2.2-1

		7.1.a 7.1.b 7.1.d 7.3.2.b 7.3.4 7.3.4.a 7.3.5 7.3.5.c 7.3.5.d 7.3.6.a		2.2-2 2.2-3 2.2-4
2.3	**Frequency of Publication**			
2.4	**Access to Published Information**	*7.1.c* 7.3.6.k		2.4-1
3	**Identification and Authentication**			
3.1	**Naming**			
3.1.1	Types of names			3.1.1-1
3.1.2	Need for names to be meaningful			
3.1.3	Anonymity or pseudonimity of certificate holders			3.1.3-1

3.1.4	Rules for interpreting various name forms			
3.1.5	Uniqueness of names	7.3.3.e		
3.1.6	Recognition, authentication and role of trademarks			
3.2	**Initial identity validation**			
3.2.1	Method to prove possession of private key	7.3.1.k *7.3.1.l*		
3.2.2	Authentication of organization identity			
3.2.3	Authentication of individual identity	6.2 6.2.a 7.3.1 7.3.1.a 7.3.1.c 7.3.1.d 7.3.1.g 7.3.1.h		3.2.3-1
3.2.4	Non-verified subscriber information			
3.2.5	Validation of authority			

3.2.6	Criteria for interoperation			
3.3	**Identification and Authentication for Re-key Requests**			
3.3.1	Identification and authentication for routine re-key	7.3.2 *7.3.2.a* *7.3.2.c* *7.3.2.d*		3.3.1-1 3.3.1-2 3.3.1.3
3.3.2	Identification and authentication for re-key after revocation			3.3.2-1
3.4	**Identification and Authentication Revocation Requests**	7.3.6.c		
4	**Certificate Life-Cycle Operational Requirements**			
4.1	**Certificate Application**			
4.2	**Certificate Application Processing**			
4.3	**Certificate Issuance**			
4.3.1	CA actions during certificate issuance	7.3.3 *7.3.3.a* 7.3.3.b 7.3.3.c 7.3.3.d		

4.3.2	Notification to subscriber by the CA of the issuance of the certificate	7.3.5.a		
4.4	**Certificate Acceptance**			
4.4.1	Conduct constituting certificate acceptance			4.4.1-1
4.4.2	Publication of the certificate by CSP			
4.4.3	Notification of certificate issuance by the CSP to other entities			
4.5	**Key Pair and Certificate Usage**			
4.5.1	Subscriber private key and certificate usage	6.2 6.2.b 6.2.c 6.2.e 6.2.f 6.2.g 6.2.h 6.2.i		
4.5.2	Relying party public key and certificate usage	6.3 *6.3.a* 6.3.b 6.3.c		4.5.2-1

4.6	**Certificate Renewal**			
4.7	**Certificate Re-key**			
4.8	**Certificate Modification**			
4.9	**Certificate Revocation and Suspension**	7.3.6 7.3.6.f		
4.9.1	Circumstances for revocation			4.9.1-1
4.9.2	Who can request revocation			4.9.2-1
4.9.3	Procedures for revocation request	7.3.6.e *7.3.6.h*	Electronic Signature Regulation (BEH)6 article 2 paragraph 1l	4.9.3-1 4.9.3-2 4.9.3-3 4.9.3-4
4.9.4	Revocation request grace period			
4.9.5	Time within which CSP must process the revocation request	*7.3.6.a* 7.3.6.b		4.9.5-1
4.9.6	Revocation checking requirement for relying parties			4.9.6-1 4.9.6-2

6*BEH stands for Electronic Signature Directive.*

4.9.7	CRL issuance frequency	*7.3.6.g*		4.9.7-1
4.9.8	Maximum latency for CRLs			
4.9.9	On-line revocation/status verification availability			4.9.9-1 4.9.9-2 4.9.9-3 4.9.9-4 4.9.9-5 4.9.9-6
4.9.10	On-line revocation checking requirements			
4.9.11	Other forms of revocation advertisements available			
4.9.12	Special requirements re key compromise			
4.9.13	Circumstances for suspension	*7.3.6.d*		4.9.13-1
4.10	**Certificate Status Services**			
4.10.1	Operational characteristics	7.3.6.j 7.3.6.l		
4.10.2	Service availability	*7.3.6.i*		4.10.2-1

4.10.3	Optional features			
4.11	**End of Subscription**			
4.12	**Key Escrow and Recovery**	See par. 6.2.3		
5	**Facility, Management and Operational Controls**	7.4.1 7.4.1.a 7.4.1.b 7.4.1.c 7.4.1.d 7.4.1.e 7.4.1.f 7.4.1.g		
5.1	**Physical Security Controls**	7.4.4		
5.1.1	Site location and construction	7.4.4.d 7.4.4.f		
5.1.2	Physical access	7.4.4.a 7.4.4.b 7.4.4.c 7.4.4.e 7.4.4.h		

5.1.3	Power and air conditioning	7.4.4.g		
5.1.4	Water exposures			
5.1.5	Fire prevention and protection			
5.1.6	Media storage	7.4.5.c 7.4.5.d 7.4.5.f		
5.1.7	Waste disposal			
5.1.8	Off-site backup			
5.2	**Procedural Controls**	7.4.5.a 7.4.5.b 7.4.5.c 7.4.5.d		5.2-1 5.2-2
5.2.1	Trusted roles	7.4.3.g *7.4.3.h* 7.4.3.i		
5.2.2	Number of persons required for each task			
5.2.3	Identification and authentication for each role			

5.2.4	Roles that require separation of duties	7.4.5.k		5.2.4-1 5.2.4-2
5.3	**Personnel Controls**	7.4.3 7.4.3.c *7.4.3.d* 7.4.3.e 7.4.5.e 7.5.h 7.5.i		
5.3.1	Qualifications, experience, and clearance requirements	7.4.3.a 7.4.3.f		
5.3.2	Background checks procedures	7.4.3.j	Electronic Signature Regulation art.2, paragraph 1s Electronic Signature Regulation art.2, paragraph 2 Electronic Signature Regulation art.2, paragraph 3	5.3.2-1
5.3.3	Training requirements			
5.3.4	Retraining frequency and requirements			
5.3.5	Job rotation frequency and sequence			

5.3.6	Sanctions for unauthorized actions	7.4.3.b		
5.3.7	Independent contractor requirements			
5.3.8	Documentation supplied to personnel			
5.4	**Audit Logging Procedures**			
5.4.1	Types of events recorded	7.4.5.i 7.4.11.g 7.4.11.h 7.4.11.d 7.4.11.k 7.4.11.l 7.4.11.m 7.4.11.n 7.4.11.o		5.4.1-1
5.4.2	Frequency processing log	7.4.5.j		
5.4.3	Retention period for audit log	See 5.5.2		5.4.3-1
5.4.4	Protection of audit log	7.4.11.a 7.4.11.f		
5.4.5	Audit log backup procedures			

5.4.6	Audit collection system (internal vs. External)			
5.4.7	Notification to event-causing subject			
5.4.8	Vulnerability assessments			
5.5	**Records Archival**			
5.5.1	Types of records archived	7.4.11 7.4.11.i 7.3.1.f *7.3.1.i*		
5.5.2	Retention period for archive	*7.4.11.e* 7.3.1.j		5.5.2-1
5.5.3	Protection of archive	7.4.10.a 7.4.11.b		
5.5.4	Archive backup procedures			
5.5.5	Requirements for time-stamping of records			
5.5.6	Archive collection system (internal or external)			

5.5.7	Procedures to obtain and verify archive information			
5.6	**Key Changeover**			
5.7	**Compromise and Disaster Recovery**			
5.7.1	Incident and compromise handling procedures	*7.4.8.e*		5.7.1-1 5.7.1-2
5.7.2	Computing resources, software, and/or data are corrupted			
5.7.3	Entity private key compromise procedures	7.4.8.d 7.4.8.f		
5.7.4	Business continuity capabilities after a disaster	7.4.8 7.4.8.a 7.4.8.b 7.4.8.c		5.7.4-1
5.8	**CSP Termination**	7.4.9 7.4.9.a 7.4.9.b 7.4.9.c	Electronic Signature Regulation art.2, paragraph 1p Electronic Signature Regulation art.2, paragraph 1q	
6	**Technical Security Controls**			

6.1	**Key Pair Generation and Installation**			
6.1.1	Key pair generation for the CSP sub CA	7.2.1 7.2.1.a *7.2.1.c* *7.2.1.d*		6.1.1-1
	Key pair generation of the certificate holders	6.2.d 7.2.8 *7.2.8.a*		6.1.1-2 6.1.1-3
6.1.2	Private key and SSCD delivery to certificate holder	*7.2.8.c* *7.2.8.d* 7.2.8.e 7.2.9 7.2.9.a 7.2.9.b 7.2.9.c		6.1.2-1
6.1.3	Public key delivery to certificate issuer			
6.1.4	CA public key delivery to relying parties	7.2.3 7.2.3.a		
6.1.5	Key sizes	*7.2.8.b*		6.1.5-1

6.1.6	Public key parameters generation and quality checking			
6.1.7	Key usage purposes (as per X.509 v3 key usage field)	*7.2.5* 7.2.5.a 7.2.5.b		6.1.7-1
6.2	**Private Key Protection and Cryptographic Module Engineering Controls**			
6.2.1	Cryptographic module standards and controls	7.2.1.b 7.2.2 7.2.2.a 7.2.2.b		
6.2.2	Private CSP key (n out of m) multi-person control			
6.2.3	Private key escrow of certificate holder key	*7.2.4*		6.2.3-1 6.2.3-2 6.2.3-3 6.2.3-4
6.2.4.	Private key backup	7.2.2.c 7.2.2.d 7.2.4 7.2.8.e		6.2.4-1
6.2.5	Private key archival of certificate holders key			6.2.5-1

6.2.6	Private key transfer into or from a cryptographic module	7.2.2.e		
6.2.7	Private key storage on cryptographic module			
6.2.8	Method of activating private key			
6.2.9	Method of deactivating private key			
6.2.10	Method of destroying private key	7.2.6.a		
6.2.11	Cryptographic Module Rating	*5.3.1.c*		6.2.11-1 6.2.11-2 6.2.11-3
6.3	**Other Aspects of Key Pair Management**			
6.3.1	Public key archival			6.3.1-1
6.3.2	Certificate operational periods and key pair usage periods	7.2.1.e *7.2.6*		6.3.2-1 6.3.2-2
6.4	**Activation data**			
6.4.1	Activation data generation and installation	*7.2.9.d*		6.4.1-1 6.4.1-2

6.4.2	Activation data protection			
6.4.3	Other aspects of activation data			
6.5	**Computer Security Controls**			
6.5.1	Specific computer security technical requirements	7.4.6 7.4.6.c 7.4.6.d 7.4.6.e 7.4.6.f 7.4.6.j 7.4.6.l		6.5.1-1 6.5.1-2 6.5.1-3
6.5.2	Computer security rating	7.4.2 7.4.2.a		
6.6	**Life Cycle Technical Controls**			
6.6.1	System development controls	*7.4.7* 7.4.7.a 7.4.7.b		6.6.1-1
6.6.2	Security Management Controls			
6.6.3	Life cycle security controls			

6.6.4	Life cycle of cryptographic hardware for signing certificates	7.2.7 7.2.7.a 7.2.7.b 7.2.7.c 7.2.7.d 7.2.7.e		
6.7	**Network Security Controls**	7.4.6.a 7.4.6.b 7.4.6.g 7.4.6.h 7.4.6.i 7.4.6.k 7.3.3.f 7.3.3.g		6.7.1-1 6.7.1-2 6.7.1-3
6.8	**Time-stamping**			
7	**Certificate, CRL and OSCP Profiles**			
7.1	**Certificate Profile**			7.1-1
7.2	**CRL Profile**			7.2-1
7.3	**OCSP Profile**			7.3-1

8	**Complicance Audit and Other Assessments**			See chapter 8
9	**Other Business and Legal Matters**			
9.1	**Fees**			
9.2	**Financial Responsibility**			
9.2.1	Insurance cover	*7.5.d*		9.2.1-1
9.2.2	Other resources			9.2.2-1
9.3	**Confidentiality of Business Information**			
9.4	**Privacy of Personal Information**			
9.4.1	Privacy plan			
9.4.2	Information treated as private	7.4.11.j		
9.4.3	Information not deemed private			
9.4.4	Responsibility to protect private information	7.4.10.c		
9.4.5	Notice and consent to use private information	7.3.5.b 7.4.10.b		

		7.4.10.d		
9.4.6	Disclosure pursuant to judicial or administrative process	7.4.11.c		
9.4.7	Other information disclosure circumstances			
9.5	**Intellectual Property Rights**			9.5-1
9.6	**Representations and Warranties**			
9.6.1	CSP representations and warranties	6.4 Annex A	[OID 2.16.528.1.1003.1.2.3.2] Civil Code7 art. 196b, paragraph 1 and paragraph 2	9.6.1-1 9.6.1-2 9.6.1-3 9.6.1-4
9.6.2 to 9.6.5	Various articles concerning liability			
9.7	**Disclaimers of Warranties**			
9.8	**Limitations of Liability**			9.8-1 9.8-2
9.9	**Indemnities**			

7 BW stands for Civil Code

9.10	**Term and Termination**			
9.11	**Individual notices and communications with participants**			
9.12	**Amendments**			
9.12.1	Procedure for amendment			9.12.1
9.12.2	Notification mechanism and period			9.12.2-1
9.12.3	Circumstances under which OID must be changed			
9.13	**Dispute Resolution Provisions**	*7.5.f*	Electronic Signature Regulation art.2, paragraph 1n	9.13-1
9.14	**Governing Law**			9.14
9.15	**Compliance with Applicable Law**	7.4.10		
9.16	**Miscellaneous Provisions**			
9.17	**Other provisions**	6.1 7.1.e 7.1.f 7.1.i 7.5		9.17-1

		7.5.a 7.5.b 7.5.c 7.5.e 7.5.g		

10 Revisions

10.1 Amendments between version 3.5 and 3.6

10.1.1 Amendments

- Certification against ETSI EN 319 411-2 (effective date 4 weeks after publication of PoR 3.6);
- Adjustment reference numbers ETSI EN 319 401 and ETSI 319 411-2 (effective date 4 weeks after publication of PoR 3.6);

10.1.2 Editorial

- Requirement 4.9.9-3 (effective date 4 weeks after publication of PoR 3.6);
- Requirement 5.2 (effective date 4 weeks after publication of PoR 3.6);
- Requirement 6.1.1-1 (effective date 4 weeks after publication of PoR 3.6);
- Requirement 6.1.1-2 (effective date 4 weeks after publication of PoR 3.6);
- Requirement 6.1.1-3 (effective date 4 weeks after publication of PoR 3.6);
- Requirement 6.2 (effective date 4 weeks after publication of PoR 3.6);
- Requirement 6.3.2-1 (effective date 4 weeks after publication of PoR 3.6);
- Appendix A: CRL profile

10.2 Amendments from version 3.4 to 3.5

10.2.1 Modifications

- Description and explanation of attribute QcStatement (effective date no later than 4 weeks after publication of PoR 3);
- Explanation of attribute SerialNumber (effective date no later than 4 weeks after publication of PoR 3.5);

10.3 Amendments from version 3.3 to 3.4

10.3.1 New

- Requirement 5.2.5-2 (effective date no later than 4 weeks after publication of PoR 3.4);
- Requirement 5.3.2-1 (effective date no later than 4 weeks after publication of PoR 3.4);

10.3.2 Modifications

- Description and explanation in respect of subject.Countryname (effective date no later than 4 weeks after publication of PoR 3.4 ;

10.3.3 Editorial

- Requirement 5.4.1-1 (effective date no later than 4 weeks after publication of PoR 3.4);

10.4 Amendments from version 3.2 to 3.3

10.4.1 New

- Requirement 5.2-1 (effective date no later than 1-12-2012)
- Requirement 5.4.3-1
- Requirement 5.7.4-1 (effective date no later than 1-12-2012)

10.4.2 Modifications

- Requirement 4.9.1-1
- Requirement 5.4.1-1
- Requirement 5.7.1-1 (effective date no later than 1-10-2012)
- Requirement 5.7.1-2 (effective date no later than 1-10-2012)
- Requirement 6.5.1-3
- Requirement 6.7.1-1

10.4.3 Editorial

A number of editorial changes have been made but these do not affect the content of the information.

10.5 Amendments from version 3.1 to 3.2

10.5.1 New

- Requirement 5.2.4-2
- Requirement 5.4.1-1 (effective date no later than 1-6-2012)
- Requirement 6.5.1-3 (effective date no later than 1-7-2012)
- Requirement 6.7.1-1 (effective date no later than 1-7-2012)
- Requirement 6.7.1-2 (effective date no later than 1-7-2012)
- Requirement 6.7.1-3

10.5.2 Amendments

- Requirement 4.5.2-1 (effective date no later than 1-2-2012)
- Requirement 5.7.1-2
- Requirement 6.2.3-2
- Explanation of SubjectAltName.rfc822Name.

10.5.3 Editorial

A number of editorial changes have been made but these do not affect the content of the information.

10.6 Amendments from version 3.0 to 3.1

10.6.1 New

- Requirement 4.9.7-1, 4.9.9-6, 6.5.1-1 and 6.5.1-2.

10.6.2 Amendments

- Requirement 4.9.1-1;
- Explanation of attribute SerialNumber.

10.6.3 Editorial

A number of editorial changes have been made but these do not affect the content of the information.

10.7 Amendments from version 2.1 to 3.0

10.7.1 New

No changes.

10.7.2 Amendments

- Requirement 4.9.2-1;
- Explanation of attribute Signature.

10.7.3 Editorial

A number of editorial changes have been made but these do not affect the content of the information.

10.8 Amendments from version 2.0 to 2.1

10.8.1 Editorial

Only a few editorial changes have been made but these do not affect the content of the information.

10.9 Amendments from version 1.2 to 2.0

10.9.1 New

- Requirement 4.9.3-1;
- Attribute authorityInfoAccess under CRL extensions.

10.9.2 Modifications

No changes.

10.9.3 Editorial

A number of editorial changes have been made but these do not affect the content of the information.

10.10 Amendments from version 1.1 to 1.2

10.10.1 New

No changes.

10.10.2 Modifications

- Requirement 6.1.1-1, 6.1.1-2, 6.1.1-3, 6.1.5-1, 6.1.7-1, 6.2.3-4, 6.2.4.2-1, 6.2.5-1 9.8-1 and 9.8-2.
- Explanation of attribute Signature.

10.10.3 Editorial

A number of editorial changes have been made but these do not affect the content of the information.

10.11 Amendments from version 1.0 to 1.1

10.11.1 New

No changes.

10.11.2 Modifications

- Paragraph 1.4.

10.11.3 Editorial

A number of editorial changes have been made but these do not affect the content of the information.

10.12 Version 1.0

First version.