Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Programme of Requirements part 3b: Certificate Policy – Organization Services (G3) Appendix to CP Government/Companies (G1) and Organization (G2) domains

Date 28 January 2014

Government/Companies Domain (G1):

Services - Authenticity	2.16.528.1.1003.1.2.2.4
Services - Confidentiality	2.16.528.1.1003.1.2.2.5
Services - Server	2.16.528.1.1003.1.2.2.6

Organization Domain (G2) / Organization Services Domain (G3):

Services - Authenticity	2.16.528.1.1003.1.2.5.4
Services - Confidentiality	2.16.528.1.1003.1.2.5.5
Services - Server	2.16.528.1.1003.1.2.5.6

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 2012

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 3b 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 services certificates issued by CSPs in the Government/Companies and Organization domains.

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 standard ETSI TS 102 042, where
  - for services certificates the policy NCP+[2] is applicable necessitating the use of a SUD (ETSI CP OID 0.4.0.2042.1.2);
  - for services server certificates (extendedKeyUsage client and server authentication) the policies NCP in combination with OVCP, PTC-BR en Netsec are applicable. **Please note that Netsec requirements 1h, 3a, 3e, 4c.i and 4f are not normative** (ETSI CP OID 0.4.0.2042.1.7);
- 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[3].
Number	Unique number of the PKIo requirement. In each paragraph, consecutive

[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] The CP services are based on an underlying standard different to that of the CPs for ersonal certificates. Because services certificates are not personal and are not qualified certificates in accordance to the "Wet Elektronische Handtekeningen" (Electronic Signature Act), the requirements for services certificates differ on certain points from the requirements for other types of certificates

[3] Chapters 2 to 9 inclusive only include those paragraphs from RFC 3647 to which a PKIorequirement applies.

	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 TS 102 042 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 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 services certificates and status information certificate 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 the requirements originating from Dutch law, requirements from ETSI TS 102 042 and the PKIo requirements.

1.1.2 Status

This is version 3.6 of part 3b of the PoR. The current version has been updated up to and including January 2014.

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 algorithm (G1) and roots based on the SHA-256 algorithm (G2 and G3) are used. Furthermore, the roots are divided into different domains.

For the G-1 root these domains are the Government/Companies domains (these two domains have merged over time)and Citizen domain.

Under the G-2 root there are domains for Organization,Citizen, and Autonomous Devices.

Under the G-3 root there are domains for Organization Person, Organization Services, Citizen, and Autonomous Devices.

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

Government/Companies Domain:	
OID	**CP**
2.16.528.1.1003.1.2.2.4	for the authenticity certificate for services within the Government/Companies domain, that contains the public key for identification and authentication.
2.16.528.1.1003.1.2.2.5	for the confidentiality certificate for services within the Government/Companies domain, that contains the public key for confidentiality.
2.16.528.1.1003.1.2.2.6	for the server certificate within the Government/Companies domain, that contains the public key for authenticity and 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). government and companies domains (2). authenticity (4)/ confidentiality (5)/ server (6). version number}.

Organization / Organization Services Domains:	
OID	**CP**
2.16.528.1.1003.1.2.5.4	for the authenticity certificate for services within the Organization domain, that contains the public key for identification and authentication.
2.16.528.1.1003.1.2.5.5	for the confidentiality certificate for services within the Organization domain, that contains the public key for confidentiality.
2.16.528.1.1003.1.2.5.6	for the server certificate for services within the Organization domain, that contains the public key for authenticity and 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). organization domain (5). authenticity (4)/ confidentiality (5)/ server (6). 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

Within the Government/Companies and Organization domains, the user community consists of subscribers who are organizational entities within the government and business community (see PKIo 3.2.2-1) and of certificate holders, who also belong to these subscribers. In addition there are relying parties, who act with a reliance on certificates of the relevant certificate holders.

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

- A subscriber is a natural or legal personality who enters into an agreement with a CSP on behalf of one or more certificate holders for the certification of public keys.
- 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. The certificate holder is part of an organizational entity, for which a subscriber is the contracting party.

  Within the Certificate Policy Services, the term certificate holder means:
    - a device or a system (a non-natural person), operated by or on behalf of an organizational entity; or
    - a function of an organizational entity.
      In this CP we use the name "service" for the foregoing certificate holders. To perform the actions in respect of the lifecycle of the certificate holder's certificate, intervention by a party other than the certificate holder is required. The subscriber is responsible for this and has to appoint a certificate manager to perform these actions.
- A certificate manager is a natural person who performs actions on behalf of the subscriber in respect of the certificate holder's certificate. The subscriber instructs the certificate manager to perform the relevant actions and records these in a certificate manager's testimony.
- 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.
  Other than for personal certificates, relying parties mainly derive security from the connection of a service (device or feature) to the organizational entity to which the service belongs. The CP Services therefore places the emphasis on providing certainty about the connection of a message sent by or a web service provided by a device, system or (staff) position with the relevant organization. In view of this, establishing the identity of the certificate holder (device or feature) is less important than establishing the certificate holder's connection to the organizational entity.

1.4 Certificate Usage

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

[OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4]
Authenticity certificates, issued under this CP, can be used to identify and authenticate, by electronic means, the service that is part of the organizational entity, that is responsible for the relevant service. Issuance of code signing certificates is NOT allowed under this CP.

[OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5]

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

[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6]
Server certificates that are issued under this CP, can be used to secure a connection between a specific client and a server that is part of the organizational entity listed as the subscriber in the relevant certificate.

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.ii
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.c 7.3.4.b 7.3.5.f
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 TS 102 042. 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.c
PKIo	The CPS has to be written in Dutch.

RFC 3647	2.2 Publication of CSP information
Number	2
ETSI	5.2.b
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.c
PKIo	All information has to be available in Dutch.

RFC 3647	2.2 Publication of CSP information
Number	4
ETSI	7.1.a
PKIo	[2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] The following clause has to be incorporated in the CPS and in all agreements with parties that are involved in issuing services server certificates of the CSP (such as, for example, the Registration Authority): "CSP [name] conforms to the current version of the Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates as published at http://www.cabforum.org. In the event of any inconsistencies between the PKIoverheid Programme of Requirements part 3b and the relevant Requirements, because of which it is not possible to (at the very least) fulfil the aforementioned minimum requirements, which is at the discretion of the PA, the provisions in the Requirements shall prevail."

RFC 3647	2.2 Publication of CSP information
Number	5
ETSI	7.1.d.3
PKIo	The certification practice statement of the CSP has to be structured in accordance with RFC 2527, RFC 3647 or the Programme of Requirements of PKIoverheid that is based on RFC 3647 and has to include all relevant chapters described in RFC 2527, RFC 3647 or the PoR of PKIoverheid.

2.4 Access to Published Information

RFC 3647	2.4 Access to published information
Number	1
ETSI	7.1.d.1
PKIo	It has to be possible for anyone to consult the CPS of a Certification Service Provider within PKIoverheid.
PKIo comment	'Anyone' means that, in addition to the subscribers, certificate holders and administrators, 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 7.3.6.i
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.

3.2 Initial Identity Validation

RFC 3647	3.2.1. Method to prove possession of the private key
Number	1
ETSI	7.3.1
PKIo	The CSP is responsible for ensuring that the subscriber supplies the certificate signing request (CSR) securely. The secure delivery must take place in the following manner: • the entry of the CSR on the CSP's application developed especially for that purpose, using an SSL connection with a PKIoverheid SSL certificate or similar or; • the entry of the CSR on the HTTPS website of the CSP that uses a PKIoverheid SSL certificate or similar or; • sending the CSR by e-mail, along with a qualified electronic signature of the certificate manager that uses a PKIoverheid qualified certificate or similar or; • entering or sending a CSR in a way that is at least equivalent to the aforementioned ways.
Comment	In the event of an emergency, where an emergency procedure agreed in advance with the subscriber takes effect, this requirement can be deviated from. In these cases, as soon as the CSR has been received, at the very least the CSP has to contact the subscriber by telephone in order for the subscriber to approve the CSR.

RFC 3647	3.2.2 Authentication of organizational entity
Number	1
ETSI	7.3.1.g

PKIo	The CSP has to verify that the subscriber is an existing organization.

RFC 3647	3.2.2 Authentication of organizational entity
Number	2
ETSI	7.3.1.g
PKIo	The CSP has to verify that the organization name registered by the subscriber that is included in the certificate is correct and complete.

RFC 3647	3.2.3 Authentication of individual identity
Number	1
ETSI	7.3.1.e
PKIo	In accordance with Dutch legislation and regulations, the CSP has to check the identity and, if applicable, specific properties of the certificate manager. Proof of identity has to be verified based on the physical appearance of the person himself, either directly or indirectly, using means by which the same certainty can be obtained as with personal presence. The proof of identity can be supplied on paper or electronically.

RFC 3647	3.2.3 Authentication of individual identity
Number	2
ETSI	7.3.1.e
PKIo	To detail the provisions in 3.2.3-1, the identity of the certificate manager can only be established using the valid documents referred to in article 1 of the Compulsory Identification Act (Wet op de identificatieplicht). The CSP has to check the validity and authenticity of these documents.
Comment	If the personal identity of the certificate manager is verified when a certificate is requested in the Government, Companies and Organization Domains, then the identity verification of the certificate manager will be considered to have taken place under this CP.

RFC 3647	3.2.3 Authentication of individual identity
Number	3
ETSI	7.3.1.g

PKIo	The certificate manager is a person whose identity has to be established in conjunction with an organizational entity. Proof has to be submitted of: • full name, including surname, first name, initials or other first (names) (if applicable) and surname prefixes (if applicable); • date of birth and place of birth, a nationally applicable registration number, or other characteristics of the certificate manager that can be used in order to, as far as possible, distinguish this person from other persons with the same name; • proof that the certificate manager is entitled to receive a certificate for a certificate holder on behalf of the legal personality or other organizational entity.

RFC 3647	3.2.5 Validation of authority
Number	1
ETSI	7.3.1.d 7.3.1.h 7.3.1.i
PKIo	The CSP has to verify that: • the proof that the certificate holder is authorized to receive a certificate on behalf of the subscriber, is authentic; • the certificate manager has received permission from the subscriber to perform the actions that he has been asked to perform (if the certificate manager performs the registration process).
Comment	The "certificate manager" who takes over those actions from the certificate holder does not necessarily have to be the same person as the system administrator or personnel officer. Also the knowledge of the activation data of the key material (for example PIN) can be shared by various people if the organization of the certificate management requires that. However, it is recommended that as few people as possible have knowledge of the PIN. It also would be wise to take measures that limit access to the PIN. An example of this is placing the PIN in a safe to which only authorized persons can gain access in certain situations.

RFC 3647	3.2.5 Validation of authority
Number	2
ETSI	6.2.h
PKIo	The agreement that the CSP enters into with the subscriber has to state that the subscriber is responsible for immediately informing the CSP of any relevant changes to the relationship between the subscriber and certificate manager and/or service. When the service no longer exists, this has to take place by means of a revocation request.

RFC 3647	3.2.5 Authorization of the certificate holder
Number	3
ETSI	7.3.1.i.i
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] The CSP has to verify that the domain name does not appear on a spam and/or phishing black list. Use, to this end, at least http://www.phishtank.com. If the domain name is mentioned on phishtank or a different black list that is consulted, the CSP has to handle the request for the relevant services server certificate with particular care during the verification process.

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
PKIo	[OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] 7.3.2.d is applicable.
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
PKIo	[OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] and [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] 7.3.2.d do not apply.
Comment	The requirement means that certificates cannot be renewed without a re-key for the authenticity and server certificate.

RFC 3647	3.3.1 Identification and authentication for routine re-key
Number	3
ETSI	7.3.2.a 7.3.2.c
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
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

4.1 Certificate Application

RFC 3647	4.1 Certificate Application
Number	1
ETSI	6.2
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] Before a services server certificate is issued, the CSP must enter into an agreement with the subscriber and receive a certificate request signed by the certificate manager. At the very least, the agreement has to fulfil the following conditions: • the agreement has to be signed by the subscriber's Authorized Representative or Representation; • the subscriber must declare that the information that is provided in the context of a services server certificate request process, is complete and correct; • the subscriber must declare that appropriate measures will be taken to ensure that the private key (and the corresponding access information, e.g. a PIN code), belonging to the public key in the relevant services server certificate, is kept under his control and secret and to protect this; • the subscriber must declare that the services server certificate will not be installed and used until the correctness and completeness has been verified; • If the Fully Qualified Domain Name (FQDN) listed in a services server certificate is identifiable and addressable through the Internet, the subscriber has to declare that the services server certificate is only placed on a server that, at the very least, can be reached using one of the FQDNs in this services server certificate; • the subscriber must declare that the services server certificate will only be used in line with the regulation that applies to its business operations and only in relation to the subscriber's activities and in line with the provisions of this agreement; • the subscriber must declare that it will immediately discontinue use of the services server certificate if it becomes clear that the information in the services server certificate is incorrect or incomplete or if there are signs that the private key, belonging to the public key of the relevant services server certificate, has been compromised; • the subscriber must declare that it will immediately discontinue use of the private key, belonging to the public key of the relevant services server certificate, if the validity of the services server certificate has expired or if the services server certificate has been revoked; • The subscriber has to state that it will respond to instructions from the CSP within the period of time stipulated by the CSP in the event of infringement of the private key or certificate misuse; • The subscriber must accept that the CSP is entitled to revoke the certificate if the subscriber has violated the user agreement or if the CSP has discovered that the certificate is being used for criminal activities, such as phishing, fraud or the dissemination of malware.

4.4 Certificate Acceptance

RFC 3647	4.4.1 Conduct constituting acceptance of certificates
Number	1
ETSI	7.3.1.m
PKIo	After a certificate is issued, the certificate holder or certificate manager has to specifically confirm to the CSP the delivery of the key material that is part of the certificate.
Comment	If keys that are protected by software are used (see [6.2.11-3]), whereby the private key is generated by the certificate manager and not by the CSP, transfer of the key material and receipt confirmation does not apply. The information that is requested in 7.3.1.m still has to be recorded.

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
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 Revocation and Suspension of Certificates

RFC 3647	4.9.1 Circumstances for revocation
Number	1
ETSI	7.3.6.a
PKIo	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 SUD is lost or suspected to be lost, if the key or SUD is stolen or suspected to be stolen, or if the key or SUD 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 become aware that the use of the domain name in the certificate is no longer legally permitted (e.g. by a judgement of a court); • 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 (service); • 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 subscriber uses a “code signing” certificate to digitally sign “hostile code” (including spyware, malware, Trojans, etc.). • 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
PKIo	The following parties can request revocation of an end user certificate: • the certificate manager; • the subscriber; • the CSP; • any other party or person that has an interest, at the discretion of the CSP.

RFC 3647	4.9.3 Procedures for revocation request
Number	1
ETSI	7.3.6.a

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 Procedures for revocation request
Number	2
ETSI	7.3.6
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 Procedures for revocation request
Number	3
ETSI	7.3.6.a
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 Procedures for revocation request
Number	4
ETSI	7.3.6.j (and Electronic Signature Directive article 2 paragraph 1l)
PKIo	In any case, the CSP has to use a CRL to make the certificate status information available. [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] The CSP has to use an OCSP and a CRL to make the certificate status information available.

RFC 3647	4.9.5 The time within which CA must process the revocation request
Number	1
ETSI	7.3.6.a
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
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
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
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.j
PKIo	[OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] and [OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] 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.j
PKIo	If the CSP supports the Online Certificate Status Protocol (OCSP), this must be in line with {16} IETF RFC 2560.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	3
ETSI	7.3.6.j
PKIo	To detail the provisions of {16} 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; • the private key of a responder appointed by the CSP that holds an OCSP Signing Certificate that is signed for this purpose by the private (CA) key with which the certificate is also signed, the status of which has to be requested; If a CSP chooses the second option, the OCSP Signing certificate which the responder holds MUST fulfil the following additional conditions (see RFC2560 and the requirement PoR part 3b, 4.9.9-6): • The OCSP Signing Certificate is given the extension id-pkix-ocsp-nocheck that is not marked as "critical" and is given the value "NULL".

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4
ETSI	7.3.6.j
PKIo	To detail the provisions of {16} 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.j
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.j
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	4.9.9 On-line revocation/status checking availability
Number	7
ETSI	7.3.6.h.iv
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] The CSP MUST support the GET method when offering OCSP responses in accordance with RFC5019.
Comment	Http based OCSP requests can use either the GET or the POST method to submit a request. To enable http caching, the CSP has to support the GET method.

RFC 3647	4.9.9 Online revocation/status verification
Number	8
ETSI	7.3.6.h.iv
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] If the OCSP responder of the CSP receives a status request from a certificate that has not been issued, the responder may not answer with the status “good”. The CSP must register such requests to the responder as part of the security procedures and, if necessary, take action on these.

RFC 3647	4.9.13 Circumstances for suspension
Number	1
ETSI	7.3.6.e
PKIo	Suspension of a certificate CANNOT be supported.

4.10 Certificate Status Services

RFC 3647	4.10.1 Operational characteristics
Number	1
ETSI	7.3.6
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] With regard to its OCSP and CRL services, the CSP must retain appropriate server capacity which guarantees a response time of 10 seconds or less under normal conditions.

RFC 3647	4.10.2 Service availability
Number	1
ETSI	7.3.6.j
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	7.4.1.a 7.4.5
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	NCP 7.4.1.b
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	7.4.3.d and 7.4.3.h
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	7.4.3.d and 7.4.3.h
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	7.4.3.e
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	5.3.1 Qualifications, experience and clearance requirements
Number	1
ETSI	7.4.3.l
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] Before services server certificates can be issued the CSP has to: ▪ ensure that all staff who will be involved in monitoring and approving services server certificates undergo training, which covers general knowledge about PKI, authentication and verification policies and procedures with regard to the monitoring and the approvals process and threats, including phishing and other social engineering tactics; ▪ ensure that all staff take an internal exam, which must be successfully completed; ▪ keep records of the training course(s) and the exam and make sure that the skills of the relevant staff remain at the required level.

RFC 3647	5.3.2 Background checks procedures
Number	1
ETSI	7.4.3-l
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 Loggin Procedures

RFC 3647	5.4.1 Types of events recorded
Number	1
ETSI	7.4.5.j
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	7.4.11.e
PKIo	The CSP has to store log files for incidents relating to: • CA key life cycle management and; • Certificate life cycle 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	5.5.1 Types of events recorded
Number	1
ETSI	7.3.1.j
PKIo	The CSP has to save all information that is used for verifying the identity of the subscriber and certificate manager, including reference numbers of the documentation that is used for verification, as well as restrictions in respect of the validity.

RFC 3647	5.5.1 Types of events recorded

Number	2
ETSI	7.4.11
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] The CSP has to maintain a register of all revoked services server certificates and all rejected requests for a services server certificate, in connection with the suspicion of phishing or other possible misuse, which will be at the discretion of the CSP, and has to report these to http://www.phishtank.com.

RFC 3647	5.5.2 Retention period for archive
Number	1
ETSI	7.4.11.e
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.

RFC 3647	5.5.2 Retention period for archive
Number	2
ETSI	7.4.11.e
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] Once the validity of the service server certificate has expired, the CSP has to save all information relating to the request and revocation, if any, of the services server certificate and all information used to verify the identity of the subscriber and the certificate manager, for at least 7 years.

5.7 Compromise and Disaster Recovery

RFC 3647	5.7.1 Incident and compromise handling procedures.
Number	1
ETSI	7.4.8.f
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 inactivation 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
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	7.4.8.a
PKIo	The CSP must 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
PKIo	The algorithm and the length of the cryptographic keys 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
PKIo	[OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] and [OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] The keys of certificate holders (or data for creating electronic signatures) have to be generated using a device that fulfils the requirements mentioned in {7} CWA 14169 Secure signature-creation devices "EAL 4+" or similar security criteria.
PKIo Comment	See paragraph 6.1.1.-6 for the possibility that subscribers generate the keypair. See paragraph 6.2.11 for the options for software-based generation and storage of the key material of the certificate holders in the case of services server certificates..

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	3
ETSI	7.2.8.a and 7.2.8.b
PKIo	The algorithm and the length of the cryptographic keys used by the CSP for generating the keys of certificate holders 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	6.1.1 Key pair generation for the certificate holders
Number	4
ETSI	7.2.8.d
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] If the CSP generates the private key for the subscriber, this MUST be supplied encrypted to the subscriber to safeguard the integrity and confidentiality of the private key. The following measures must then be taken into account: a. The CSP MUST generate the private key for the subscriber in the secured environment to which the PKIoverheid PoR and the corresponding audit apply; b. Once the private key has been generated for the subscriber, it MUST be stored encrypted using a strong algorithm (in accordance with the requirements of ETSI TS 102 176) within the CSP's secured environment; c. When storing this key, the CSP MUST apply the P12 standard, where the privacy mode and the integrity mode are used. To this end, the CSP MAY encrypt the P12 file with a personal PKI certificate of the subscriber/certificate manager. If this is not available, the CSP MUST use a password supplied by the subscriber. This password MUST be supplied by the subscriber through the CSP's website, for which an SSL/TLS connection is used, or via a similar procedure which guarantees the same trustworthiness and security; d. If a password is used to encrypt the P12, this password has to contain at least 8 positions including at least one number and two special characters; e. The CSP MAY NEVER send the password that is used to encrypt/decrypt the P12 in cleartext over a network or store it on a server. The password MUST be encrypted using a strong algorithm (in accordance with the requirements of ETSI TS 102 176); f. The P12 file MUST be sent to the subscriber over an SSL/TLS secured network, or be supplied out-of-band on a data carrier (e.g. USB stick or CD-Rom). g. If the P12 is supplied out-of-band, this must be additionally encrypted with a key other than the P12 file. In addition, the P12 MUST be delivered to the subscriber using a courier certified by the OPTA, or by a representative of the CSP in a seal bag,

	h. If the P12 file is sent over a SSL/TLS secured network the CSP MUST ensure that the P12 file is successfully downloaded no more than once. Access to the P12 file when transferring via SSL/TLS has to be blocked after three attempts.
Comment	Best practice is that the subscriber himself generates the private key that belongs to the public key. When the CSP generates the private key belonging to the public key on behalf of the subscriber, this has to fulfil the aforementioned requirements. When generating the key, it is important to realize that not only is the P12 file encrypted, but that the access to the P12 file is secured when the transfer is made.

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	5
ETSI	7.2.8.c
PKIo	A CSP of PKIoverheid is not allowed to issued code signing certificates under CP part 3b.

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6
ETSI	6.2.f and 6.2.g
PKIo	[OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] and [OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] Instead of letting the CSP generate the keypairs, the keypairs of services authenticity and confidentiality certificates may be generated in a SUD by the certificate administrator, where PKCS#10 is used to create a CSR for processing by the CSP, as long as: - The contract between the CSP and the subscriber contains a clause that the certificate administrator generates, saves and uses the private key on a secure device that satisfies the requirements laid down in {7} CWA 14169 Secure signature-creation devices "EAL 4+" or comparable security criteria. The subscriber mustprove that the secure device used for key generation conforms to {7} CWA 14169 Secure signature-creation devices "EAL 4+" or comparable security criteria. The CSP then must ascertain that the used SUD indeed conforms (comparable to “The subscriber MUST prove that the organization can use this name.”) - Indien de certificaatbeheerder bij registratie ten minste een schriftelijke verklaring overlegt dat maatregelen zijn getroffen in de omgeving van het systeem dat de sleutels genereert / bevat. De maatregelen moeten van een dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren. Hierbij dient in de overeenkomst tussen abonnee en CSP te worden opgenomen dat de CSP het recht heeft om een controle uit te voeren

	naar de getroffen maatregelen (conform 6.2.11.3). - Indien een bepaling wordt opgenomen in de overeenkomst tussen de CSP en de Abonnee waarin staat dat de abonnee moet verklaren dat de private sleutel (en de daarbij behorende toegangsinformatie b.v. een PINcode), behorend bij de publieke sleutel in het betreffende SUD, op passende wijze, onder controle van de certificaatbeheerder is gegenereerd en in de toekomst geheim wordt gehouden en beschermd (conform 4.1-1, 3e bullet);

RFC 3647	6.1.2 Pivate key and SUD delivery to the certificate holder
Number	1
ETSI	7.2.8.d and 7.2.8.e
PKIo	[OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] If it is not required that the CSP saves a copy of the certificate holder's private key (Key escrow), once the private key has been delivered to the certificate holder or certificate manager in a manner such that the confidentiality and integrity of the key is not compromised, it can be maintained under the certificate holder's or certificate manager's sole control. Every copy of the certificate holder's private key held by the CSP has to be destroyed.
Comment	This text corresponds with 7.2.8.e, but has been integrated because this requirement only applies to the confidentiality certificate.

RFC 3647	6.1.5 Key sizes
Number	1
ETSI	7.2.8.b
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
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 contained 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.a
PKIo	[OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] and OID [2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] Escrow by the CSP is not allowed for the private keys of the authenticity certificate and server certificate.

RFC 3647	6.2.3 Private key escrow of certificate holder key
Number	2
ETSI	7.2.4.b
PKIo	[OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] 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.b
PKIo	[OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] 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	6.2.4 Private key backup of certificate holder key
Number	1

ETSI	7.2.4.a and 7.2.8.e
PKIo	Back-up of the certificate holders' private keys by the CSP is not allowed.

RFC 3647	6.2.5 Private key archival of certificate holder key
Number	1
ETSI	7.2.4.a and 7.2.8.e
PKIo	Archiving by the CSP of the certificate holders' private keys is not allowed.

RFC 3647	6.2.11 Cryptographic module rating
Number	1
ETSI	3.1
PKIo	Secure devices issued or recommended by the CSP for the storage of keys (SUDs) have to fulfil the requirements laid down in document {7} CWA 14169 Secure signature-creation devices "EAL 4+".

RFC 3647	6.2.11 Cryptographic module rating
Number	2
ETSI	3.1
PKIo	Instead of demonstrating compliance with CWA 14169, CSPs can issue or recommend SUDs 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 trust 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	3.1
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] Instead of using a hardware-based SUD, the keys of a services certificate can be protected by software if compensating measures are taken in the system's environment that contains the keys. The compensating measures must be of such a quality that it is practically impossible to steal or copy the key unnoticed. When registering, the manager of the services certificates that uses this option

	for software-based storage has, at the very least, to submit a written declaration to state that compensating measures have been taken that fulfil the condition stipulated to this end. The agreement between the subscriber and CSP must state that the CSP is entitled to check the measures that have been taken.
Comment	Examples of compensating measures to be considered are a combination of physical access security, logical access security, logging and audit and segregation of functions.

6.3 Other Aspects of Key Pair Management

RFC 3647	6.3.2 Certificate operational periods and key pair usage periods
Number	1
ETSI	7.2.6
PKIo	[OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] and [OID 2.16.528.1.1003.1.2.2.5 2 and 16.528.1.1003.1.2.5.5] 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
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] Private keys that are used by a certificate holder and issued under the responsibility of this CP must not be used for longer than three years. The certificates, that are issued under the responsibility of this CP, have to be valid for no more than three years.

RFC 3647	6.3.2 Certificate operational periods and key pair usage periods
Number	3
ETSI	7.2.6
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
PKIo	The CSP attaches activation data to the use of an SUD, 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
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
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
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	7.4.6.a
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	7.4.7
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 Directive 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	7.4.6
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)[4]" 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
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
ETSI	7.4.6
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,

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

	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[5]” (how to perform penetration testing) published by the NCSC. If necessary, the PA can instruct the CSP to perform additional pen tests.

[5] *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
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.i
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	7.5.d
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
PKIo	[OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] 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
PKIo	[OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] 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
PKIo	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] 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 server certificate" is read; b. for "signatory": "certificate holder" is read; c. for "creation of electronic signatures": "verification of authenticity features and creating encrypted data" is read; d. For "verification of electronic signatures": "deciphering authentication features and encrypted data" is read.

RFC 3647	9.6.1 CA Representations and Warranties by CSPs
Number	4
ETSI	6.4
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
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
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

9.12.1 Amendment procedure

The procedures relating to managing changes in the PoR of PKIoverheid are incorporated in the Certificate Policy Statement of PKIoverheid. 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	7.5.f
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.
PKIo	The CSP has to be capable of issuing all types of services 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 services certificates for the Government/Companies and Organisation domains

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 included in RFC5280.
- The [X.509] standard allows unlimited extension of the attributes within a certificate. In connection with interoperability requirements, this may not be used within the PKI for the government. Only attributes indicated in this appendix as Compulsory, Optional or Advised Against may be used.

Services certificates

Basic attributes

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Version	V	MUST be set at 2 (X.509v3).	RFC 5280	Integer	Describes the version of the certificate, the value 2 stands for X.509 version 3.
SerialNumber	V	A serial number that MUST uniquely identify the certificate within the publishing CA domain.	RFC 5280	Integer	All end user certificates have to contain at least 8 bytes of unpredictable random data in the certificate's serial number (SerialNumber).
Signature	V	MUST be created on the algorithm, as stipulated by the PA.	RFC 5280, ETSI TS 102176	OID	MUST be the same as the field signatureAlgorithm. For maximum interoperability, for certificates under the G1 root certificate, only sha-1WithRSAEncryption is allowed. 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

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
					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	-
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	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	

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
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 3739	UTF8String	The commonName attribute MUST NOT be needed 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 (service) MUST mention the subject in a unique way and include information about the subscriber organization. The field has the following attributes:	PKIo, RFC3739, ETSI TS 102 280		MUST contain a Distinguished Name (DN). Attributes other than those mentioned below MUST NOT be used.
Subject.countryName	V	complete C with two-letter country code in accordance with ISO 3166-1. If an official alpha-2 code is missing, the CSP MAY use the user-assigned code XX.	RFC 3739, X520, ISO 3166, PKIo	PrintableString	The country code that is used in Subject.countryName MUST correspond with the subscriber's address in accordance with the accepted document or registry.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.commonName	V/A	Name that identifies the service or server. Compulsory; In services certificates this field is compulsory Advised against; In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] the use of this field is advised against. If this field is used, this MUST contain no more than 1 "fully-qualified domain name (FQDN)" (see the definition in part 4). This FQDN MUST also be included in the SubjectAltName.dNSName field.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	[OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] and [OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] Incorporated in the subject.commonname is the function of an organizational entity or the name by which the device or system is known. [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] If the subject.commonname is used for services server certificates, a FQDN has to be incorporated here. In this attribute wildcard FQDNs, local domain names, private IP addresses, only a host name, internationalized domain names (IDNs) and null characters \0 MUST NOT be used. The subscriber MUST prove that the organization can use this name. In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] the CSP MUST check recognized registers (Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA)) to find out whether the subscriber is the domain name owner or whether the subscriber is exclusively authorized by the registered domain name owner to use the domain name

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
					on behalf of the registered domain name owner. [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] In exceptional situations, the CSP MAY issue another services server certificate without FQDN. The following additional requirements apply: with effect from 1 July 2012, the CSP MUST inform the subscriber that the use of server certificates without FQDN is advised against and that by no later than 1 October 2016, all server certificates that are still valid without FQDN will be revoked. If a CSP issues a server certificate on or after 1 July 2012 without FQDN, 1 November 2015 at the latest MUST be used as "date of validity up to". [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] The CSP must register the issueance of services server certificates without FQDN and hands over a copy of that registration tot the PA once a month. The non-FQDN must not contain new generic Top Level Domains (gTLD's) that ICANN has taken into consideration (https://gtldresult.icann.org/application-result/applicationstatus/viewstatus). Within 120 days after approval of a new gTLD the CSP must revoke all

Field / Attribute	**Criteria**	**Description**	**Standard reference**	**Type**	**Explanation**
					certificates that contain a non-FQDN of which the gTLD is a part, unless the Subscriber is the owner of the domainname of has been exclusively authorized by the owner to use the name. Approval of new gTLDs is published via the ICANN mailing list on https://mm.icann.org/mailman/listinfo/gtldnotification.
Subject.Surname	N	Is not used for services certificates.			Services certificates are not personal. The use of this attribute is therefore not allowed, to avoid confusion.
Subject.givenName	N	Is not used for services certificates.			Services certificates are not personal. The use of this attribute is therefore not allowed, to avoid confusion.
Subject.pseudonym	N	Pseudonyms may not be used.	ETSI TS 102 280, RFC 3739, PKIo		
Subject.organizationName	V	The full name of the subscriber's organization in accordance with the accepted document or Basic Registry.	PKIo	UTF8String	The subscriber organization is the organization with which the CSP has entered into an agreement and on behalf of which the certificate holder (service/server) communicates or acts.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.organizationalUnitName	O	Optional specification of an organizational entity. This attribute MUST NOT include a function indication or similar.	PKIo		This attribute MAY appear several times. The field MUST contain a valid name of an organizational entity of the subscriber in accordance with an accepted document or registry.
Subject.stateOrProvinceName	V/A	[OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] MUST include the province of the subscriber's branch, in accordance with the accepted document or Basic registry. [OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] and [OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] The use is advised against. If present, this field MUST contain the province in which the subscriber is established in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the province MUST correspond with the address of the subscriber in accordance with the accepted document or registry.
Subject.localityName	V/A	[OID 2.16.528.1.1003.1.2.2.6 and	PKIo, RFC 3739	UTF8String	Name of the location MUST correspond with the address of the subscriber

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		2.16.528.1.1003.1.2.5.6] MUST include the location of the subscriber, in accordance with the accepted document or Basic registry. [OID 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.5.4] and [OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] The use is advised against. If present, this field MUST contain the location of the subscriber in accordance with an accepted document or Basic registry.			in accordance with the accepted document or registry.
Subject.postalAddress	A	The use is advised against. If present, this field MUST contain the postal address of the subscriber in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	The address MUST correspond with the address of the subscriber in accordance with the accepted document or registry.
Subject.emailAddress	N	Use is not allowed.	RFC 5280	IA5String	This field MUST NOT be used in new certificates.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.serialNumber	O	The CSP is responsible for safeguarding the uniqueness of the subject (service). The Subject.serialNumber MUST be used to identify the subject uniquely. The use of 20 positions is only allowed for OIN and HRN after additional arrangements with Logius.	RFC 3739, X 520, PKIo	Printable String	The number is determined by the CSP and/or the government. The number can differ for each domain and can be used for several applications.
Subject.title	N	The use of the title attribute is not allowed for services certificates.	ETSI TS 102 280, RFC 3739, RFC 5280		This attribute is only used in personal certificates and therefore not in services certificates.
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.	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			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. In server certificates the digitalSignature, keyEncipherment and keyAgreement bits 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	RFC 3739	OID, String, String	For services certificates in the Government/Companies domain the OIDs: 2.16.528.1.1003.1.2.2.4, 2.16.528.1.1003.1.2.2.5 and

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			government OID scheme is described in the CP.			2.16.528.1.1003.1.2.2.6. For services certificates in the Organization domain the OIDs are: 2.16.528.1.1003.1.2.5.4 2.16.528.1.1003.1.2.5.5 and 2.16.528.1.1003.1.2.5.6 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 worldwide unique number that identifies the service.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MUST include a unique identifier in the dnsName for server certificates or the othername attribute for services certificates. Attributes other than those mentioned below MUST NOT be used.
SubjectAltName.dNSName[6]	V/N		Name that identifies the service or server.	RFC2818, RFC5280	IA5String	The subscriber MUST prove that the organization can use this name.

[6] This field/attribute has to be included in certificates that are issued as from 1-7-2011.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			Compulsory; In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] this field MUST include at least 1 "fully-qualified domain name (FQDN)" (see the definition in part 4). A services server certificate may contain multiple FQDNs of different domains on the condition that these domains are registered to the same subscriber or an autorization of the same subscriber is present. It is therefore NOT allowed to combine FQDNs in a single certificate that both stem from different domains and are registered to different owners. Not allowed; For other services certificates [OID 2.16.528.1.1003.1.2.2.4 and			For services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] additional wildcard FQDNs, local domain names, private IP addresses, only a host name, internationalized domain names (IDNs) and null characters \0 MUST NOT be used. In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] the CSP MUST check recognized registers (Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA)) to find out whether the subscriber is the domain name owner or whether the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner. [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] In exceptional situations, the CSP MAY issue another services server certificate without FQDN. The following additional requirements apply: with effect from 1 July 2012, the CSP MUST inform the subscriber that the use of server certificates without FQDN is advised against and that by no later than 1 October 2016, all server certificates that are still valid without FQDN will be revoked.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			2.16.528.1.1003.1.2.5.4] and [OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] this field MUST NOT be used.			If a CSP issues a server certificate on or after 1 July 2012 without FQDN, 1 November 2015 at the latest MUST be used as "date valid to". [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] The CSP must register the issueance of services server certificates without FQDN and hands over a copy of that registration tot the PA once a month. The non-FQDN must not contain new generic Top Level Domains (gTLD's) that ICANN has taken into consideration (https://gtldresult.icann.org/application-result/applicationstatus/viewstatus). Within 120 days after approval of a new gTLD the CSP must revoke all certificates that contain a non-FQDN of which the gTLD is a part, unless the Subscriber is the owner of the domainname of has been exclusively authorized by the owner to use the name. Approval of new gTLDs is published via the ICANN mailing list on https://mm.icann.org/mailman/listinfo/gtldnotification.
SubjectAltName.iPAddress	A	No	MAY include the public IP address of the	RFC 5280, RFC	Octet string	The CSP MUST verify that the subscriber is the owner of the public

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			server of which the subscriber is the owner or that is hosted by a supplier at the instruction of the subscriber.	791, RFC 2460		IP address or that a supplier may use the public IP address at the instruction of the subscriber. Private IP addresses MUST NOT be included in this attribute.
SubjectAltName.otherName	O		MAY be used containing a unique identification number that identifies the certificate holder. In addition, in the authentication certificate, as othername a PrincipalName (UPN) MAY be included for use with SSO (Single Sign On).	PKIo	IA5String, Microsoft UPN, IBM Principal-Name or Permanent-Identifier	Includes the OID of the CSP and a number that always uniquely identifies the subject (service), separated by a point or hyphen ('-'). It is recommended that an existing registration number from back office systems is used, along with a code for the organization. In combination with the CSP's OID number, this identifier is unique throughout the world. This number MUST be persistent. If an othername for Single Sign On is also included in the certificate, the SSO othername MUST be the first in the SubjectAltName, before the PKIoverheid format othername described above, in order to guarantee effective functioning of the SSO mechanism.
SubjectAltName.rfc822Name	A		MAY be used for the service's e-mail address, for applications that need the e-mail address in order to be able to function	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.

Field / Attribute	**Criteria**	**Critical?**	**Description**	**Standard reference**	**Type**	**Explanation**
			properly.			
IssuerAltName	N		Is not used.	RFC 5280		
subjectDirectoryAttributes	N		Is not used.	RFC 5280; RFC 3739		This use of this extension is not allowed.
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 ("Subjecttype = 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	V/O	Yes / No	Is only used if needed for the specific service.	RFC 5280	KeyPurposeId's	In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] this extension MUST be included, this extension MUST NOT be labelled “critical”, this extension MUST include the KeyPurposIds id-kp-serverAuth and id-kp-clientAuth, additionally the KeyPurposeId id-kp-emailProtection MAY be included, MAY additionally also include every other KeyPurposeId defined in an open or accepted standard that is used to identify a service based on its FQDN and other KeyPurposeIds MUST NOT be included. Other service certificates MAY use ExtendedKeyUsage, in which case the KeyPurposeId id-kp-serverAuth MUST NOT be included, that the KeyPurposeId id-kp-codeSigning MUST NOT be included, that the KeyPurposeId AnyextendedKeyusage MUST NOT be included, that every KeyPurposeId that is only intended for identification of a service based on its FDQN MUST NOT be included but the following MAY be included: every other KeyPurposeld defined in an open or accepted standard that corresponds with the key use shown in the KeyUsage extension.
InhibitAnyPolicy	N		Is not used.	RFC 5280		Is not used in end user certificates.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
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.
BiometricInfo	N		Are not used in services certificates.	PKIo		Biometric information is not advisable in non-personal certificates, such as services certificates.
QcStatement	N	No		RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	This attribute is only used in personal certificates and is not allowed in services certificates.

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).	RFC 5280	Integer	Describes the version of the CRL profile, the value 1 stands for X.509 version 2.
Signature	V	MUST be set to the algorithm, as stipulated by the PA.	RFC 5280	OID	MUST be the same as the field signatureAlgorithm. For maximum interoperability, for certificates under the G1 root certificate, only sha-1WithRSAEncryption is allowed. For certificates under the G2 root certificate, only sha-256WithRSAEncryption is allowed.
Issuer	V	MUST contain a Distinguished Name (DN). The field has attributes as described in the following rows.	PKIo, RFC 5280		Attributes other than those mentioned below MUST NOT be used. The attributes that are used MUST be the same as the corresponding attributes in the Subject field of the CSP certificate (for validation).

Field / Attribute	Criteria	Description	Standard reference1	Type	Explanation
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	
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	PKIo, RFC 5280	UTF8String	

Field / Attribute	Criteria	Description	Standard reference1	Type	Explanation
		accordance with accepted document or basic registry, optionally including the Domain label and/or the types of certificates that are supported			
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	RFC 5280		If used, this field MUST fulfil the specifications in RFC 5280

			additional information (such as a limited set of reason codes why the certificate has been revoked).			
FreshestCRL	O	No	This attribute is also known by the name 'Delta CRL Distribution Point'. If used it MUST contain the URI of a Delta CRL distribution point. This is never present in a Delta CRL.	RFC 5280		This field is used in complete CRLs and indicates where Delta CRL information can be found that will update the complete CRL.
authorityInfoAccess	O	No	Optional reference to the certificate of the CRL.Issuer.	RFC 5280	id-ad-caIssuers (URI)	MUST conform to § 5.2.7 of RFC 5280.
CRLReason	O	No	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 can be used to identify the original issuer of the certificate.	RFC 5280	GeneralNames	

Profile OCSP

General requirements in respect of OCSP

- If the CSP supports the Online Certificate Status Protocol (OCSP), OCSP responses and OCSPSigning certificates MUST fulfil the requirements relating to this stipulated in IETF RFC 2560.
- OCSPSigning certificates MUST correspond with the X.509v3 standard for public key certificates. General requirements in relation to certificates are listed in RFC5280
- The [X.509] standard allows unlimited extension of the attributes within a certificate. In connection with interoperability requirements, this may not be used within the PKI for the government. Only attributes indicated in this appendix as Compulsory (V), Optional (O) or Advised Against (A) may be used.
- OCSPSigning certificates must fulfil the profile for services certificates indicated above, with the following exceptions:

OCSP Signing certificate attributes

Field / Attribute	**Criteria**	**Description**	**Standard reference1**	**Type**	**Explanation**
Issuer	V	MUST contain a Distinguished Name (DN).	PKIo		An OCSPSigning certificate MUST have been issued under the hierarchy of the PKI for the government.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
KeyUsage	V	Yes	The attribute extension specifies the intended purpose of the key incorporated in the certificate. In the PKI for the government, for each certificate type various bits are incorporated in the keyUsage extension. In OCSPSigning certificates, the digitalSignature bit MUST be incorporated and the extension marked as being critical. The non-Repudiation bit MUST NOT be included.	RFC 5280, RFC 2560	BitString	
CertificatePolicies	V	No	MUST contain the OID of the PKIoverheid certificate policy (CP) for authenticity certificates, the URI of the CPS, and a user notice. The OID schedule to be used in the PKI for the government is described in the CP - Services.	RFC 3739	OID, String, String	For services authentication certificates in the Government/Companies domain the OID is: 2.16.528.1.1003.1.2.2.4. For services authentication certificates in the Organization domain the OID is: 2.16.528.1.1003.1.2.5.4.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
ExtKeyUsage	V	Yes	MUST be used with the value id-kp-OCSPSigning.	RFC 5280		
ocspNoCheck	O			RFC 2560		

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 TS 102 042 NCP 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[7]. The PA has specifically decided to include all requirements just once.

[7] *This is partially caused by the fact that ETSI TS 102 042 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.c* *7.3.4.b* *7.3.5.e.ii* *7.3.5.f*		2.1-1 2.1-2
2.2	**Publication of CSP Information**	*5.2.b* 7.1.a 7.1.c 7.1.e		2.2-1 2.2-2 2.2-3 2.2-4

		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		2.2-5
2.3	**Frequency of Publication**			
2.4	**Access to Published Information**	*7.1.d.1* 7.3.6.o		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			
3.1.4	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.o		3.2.1-1
3.2.2	Authentication of organization identity			3.2.2-1 3.2.2-2
3.2.3	Authentication of individual identity	6.2 6.2.a 7.3.1 7.3.1.a 7.3.1.d *7.3.1.e* *7.3.1.g* 7.3.1.l		3.2.3-1 3.2.3-2 3.2.3-3
3.2.4	Non-verified subscriber information			
3.2.5	Validation of authority	*7.3.1.h* *7.3.1.i* *6.2.h*		3.2.5-1 3.2.5-2 3.2.5-3
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.d		
4	**Certificate Life-Cycle Operational Requirements**			
4.1	**Certificate Application**			4.1-1
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.f 6.2.g 6.2.i 6.2.j		
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.g		
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.f	Electronic Signature Regulation (BEH)[8] 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
4.9.7	CRL issuance frequency	*7.3.6.h* *7.3.6.i*		4.9.7-1

[8] *BEH stands for Electronic Signature Directive*.

4.9.8	Maximum latency for CRLs			
4.9.9	Online revocation/status checking 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 4.9.9-7 4.9.9-8
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.e*		4.9.13-1
4.10	**Certificate Status Services**			
4.10.1	Operational characteristics	7.3.6.n 7.3.6.p		4.10.1-1
4.10.2	Service availability	*7.3.6.j*		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 7.4.5.a 7.4.5.b 7.4.5.g 7.4.5.h		5.2.5-1 5.2.5-2
5.2.1	Trusted roles	7.4.3.g *7.4.3.h* 7.4.3.i		
5.2.2	Number of people 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
5.3.1	Qualifications, experience, and clearance requirements	7.4.3.a 7.4.3.f		5.3.1-1
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 logs	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.j* *7.3.1.m*		5.5.1-1 5.5.1-2
5.5.2	Retention period for archive	*7.4.11.e* 7.3.1.n		5.5.2-1 5.5.2-2
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.f*		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.g		
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 6.2.e 6.2.f 6.2.g 7.2.8 *7.2.8.a*		6.1.1-2 6.1.1-3 6.1.1-4 6.1.1-5 6.1.1-6
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 *7.2.4.a* *7.2.4.b*		6.2.3-1 6.2.3-2 6.2.3-3
6.2.4	Private key backup			
6.2.4.1	Private key backup of the CSP key	7.2.2.c		

		7.2.2.d		
6.2.4.2	Private key backup of certificate holder key			6.2.4.2-1
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.b		
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			
6.3.2	Certificate operational periods and key pair usage periods	7.2.1.e *7.2.6*		6.3.2-1 6.3.2-2

				6.3.2-3
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 Profiles**			7.1-1
7.2	**CRL Profiles**			7.2-1
7.3	**OCSP Profiles**			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 assets			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*		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**			
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 9.12.2-2
9.12.3	Circumstances under which OID must be changed			
9.13	**Dispute Resolution Procedures**	*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.f 7.1.g 7.1.j 7.5 7.5.a 7.5.b 7.5.c 7.5.e 7.5.g		9.17-1 9.17-2 9.17-3 9.17-4

10 Revisions

10.1 Amendments from version 3.5 to 3.6

10.1.1 New

- Certification against ETSI TS 102 042 in par.1.1.1 + PTC-BR where applicable (effective date 1 juni 2014);
- Certificering against ETSI TS 102 042 in par.1.1.1 + PTC-BR + Netsec where applicable (effective date 1 December 2014);
- Eis 6.1.1-5 (effective date 4 weeks after publication of PoR 3.6);
- Eis 6.1.1-6 (effective date 4 weeks after publication of PoR 3.6);

10.1.2 Modifications

- Explanation of the attributes subject.commonName and subjectAltName.dNSName (already in effect through the accelerated change procedure since 16 September 2013);
- Explanation of the attribute subjectAltname.dNSNAme (effective date 4 weeks after publication of PoR 3.6);
- The use of subjectAltname.otherName is no longer mandatory but optional (effective date 4 weeks after publication of PoR 3.6);
- With the ban on the issuance of code-signing certificates the following requirements have been deleted: Paragraph 1.4, Requirements 6.3.2-2, 9.17-2, 9.17-3 and 9.17-4 (effective date 4 weeks after publication of PoR 3.6);

10.1.3 Editorial

- 2.2-5 (effective date 4 weeks after publication of PoR 3.6);
- 4.9.9-3 (effective date 4 weeks after publication of PoR 3.6);
- 5.2 (effective date 4 weeks after publication of PoR 3.6);
- 6.1.1-2 (effective date 4 weeks after publication of PoR 3.6);
- 6.2.4-1 (effective date 4 weeks after publication of PoR 3.6);
- Chapter ten 4.9.9-3 (effective date 4 weeks after publication of PoR 3.6);

10.2 Amendments from version 3.4 to 3.5

10.2.1 New

- Requirement 4.9.9-8 (effective date 4 weeks after publication of PoR 3.4);

10.2.2 Modifications

- Explanation of attribute SerialNumber (effective date 4 weeks after publication of PoR 3.5);

10.2.3 Editorial

- Explanation of attribute SubjectAltname.dnsName (effective date 4 weeks after publication of PoR 3.5);
- Explanation of attribute Subject.commonName (effective date 4 weeks after publication of PoR 3.5);

10.3 Amendments from version 3.3 to 3.4

10.3.1 *New*

- Requirement 2.2-5 (effective date 4 weeks after publication of PoR 3.4);
- Requirement 5.2.5-2 (effective date 4 weeks after publication of PoR 3.4);
- Requirement 5.3.1-1 (effective date 1-7-2013)
- Requirement 5.3.2-1 (effective date 4 weeks after publication of PoR 3.4);

10.3.2 *Modifications*

- Requirement 4.1-1 (effective date 4 weeks after publication of PoR 3.4);
- Requirement 4.9.9-7 (effective date 4 weeks after publication of PoR 3.4);
- Requirement 6.1.1-4 (already became effective through accelerated change procedure on 1-10-2012);
- Description and explanation of subject.Countryname (already effective by means of accelerated amendment procedure on 1-10-2012);
- Paragraph 9.12.1 relating to the change procedure

10.3.3 *Editorial*

- Requirement 5.4.1-1 (effective date 4 weeks after publication of PoR 3.4);

10.4 Amendments from version 3.2 to 3.3

10.4.1 *New*

- Requirement 2.2-4
- Requirement 3.2.5-3
- Requirement 4.1-1
- Requirement 4.10.1-1
- Requirement 5.2.5-1 (effective date 1-12-2012)
- Requirement 5.4.3-1
- Requirement 5.5.1-2
- Requirement 5.5.2-2
- Requirement 5.7.4-1 (effective date 1-12-2012).

10.4.2 *Modifications*

- Requirement 4.9.1-1;
- Requirement 4.9.9-1
- Requirement 4.9.9-3
- Requirement 5.4.1-1
- Requirement 5.7.1-1 (effective date 1-10-2012)
- Requirement 5.7.1-2 (effective date 1-10-2012)
- Requirement 6.1.1-4
- Requirement 6.3.2-2 (effective date 1-10-2012)
- Requirement 6.5.1-3
- Requirement 6.7.1-1
- Description of attributes Subject.stateOrProvinceName and Subject.localityName;
- Explanation with attributes Subject.commonName, SubjectAltName.iPAddress, SubjectAltName.dNSName and Extkeyusage.

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 1-6-2012)
- Requirement 6.1.1-4 (effective date 1-7-2012)
- Requirement 6.5.1-3 (effective date 1-7-2012)
- Requirement 6.7.1-1 (effective date 1-7-2012)
- Requirement 6.7.1-2 (effective date 1-7-2012)
- Requirement 6.7.1-3

10.5.2 *Modifications*

- Requirement 3.2.1-1
- Requirement 4.5.2-1 (effective date 1-2-2012)
- Requirement 4.9.3-4 (effective date 1-4-2012)
- Requirement 5.7.1-2
- Requirement 6.2.3-2
- Description of attribute Subject.serialNumber.

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 3.2.1-1, 4.9.7-1, 4.9.9-6, 6.3.2-2, 6.5.1-1, 6.5.1-2, 9.17-2, 9.17-3 and 9.17-4.

10.6.2 *Modifications*

- Requirement 4.9.1-1 and 6.3.2-1;
- 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*

- Attribute SubjectAltName.dNSName.

10.7.2 *Modifications*

- Paragraph 1.3;
- Requirement 4.9.2-1 and 6.2.11-3;
- 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*

- Explanation of attribute Subject.commonName.

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*

- Paragraphs 1.2 and 1.4;
- Requirement 3.3.1-1, 3.3.1-2, 6.1.1-1, 6.1.1-2, 6.1.1-3, 6.1.2-1, 6.1.5-1, 6.1.7-1, 6.2.3-1, 6.2.3-2, 6.2.3-3, 6.2.4.2-1, 6.2.5-1, 6.3.1-1, 9.6.1-1, 9.6.1-2, 9.6.1-3, 9.8-1 and 9.8-2;
- Explanation of attribute Signature and CertificatePolicies;
- Attribute Subject.serialNumber.

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*

- Requirement 4.4.1-1
- Explanation of attribute Subject.commonName.

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.