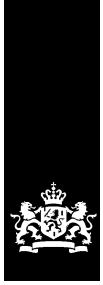


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3: Additional Requirements PKIoverheid

Datum 25 August 2015

Publisher's imprint

Version number	4.1
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**
40	12-2014	Ratified by the Ministry of the Interior and Kingdom Relations December 2014
4.1	07-2015	Ratified by the Ministry of the Interior and Kingdom Relations July 2015
4.1	08-2015	Correction to faulty modification of requirement 3.2.2-pkio147

1 Introduction

1.1 Overview

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

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

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 Policies

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

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

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

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

All PKIoverheid requirements have an unique and persistent number which also contains a reference to RFC 3647. Furthermore each

PKIoverheid requirement is an addition to one or more ETSI requirements for the issuance of PKI certificates and is thus reference to the ETSI norm(s) in question. These references are listed in a separate Excel sheet named *Reference Matrix PKIoverheid and ETSI*.

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

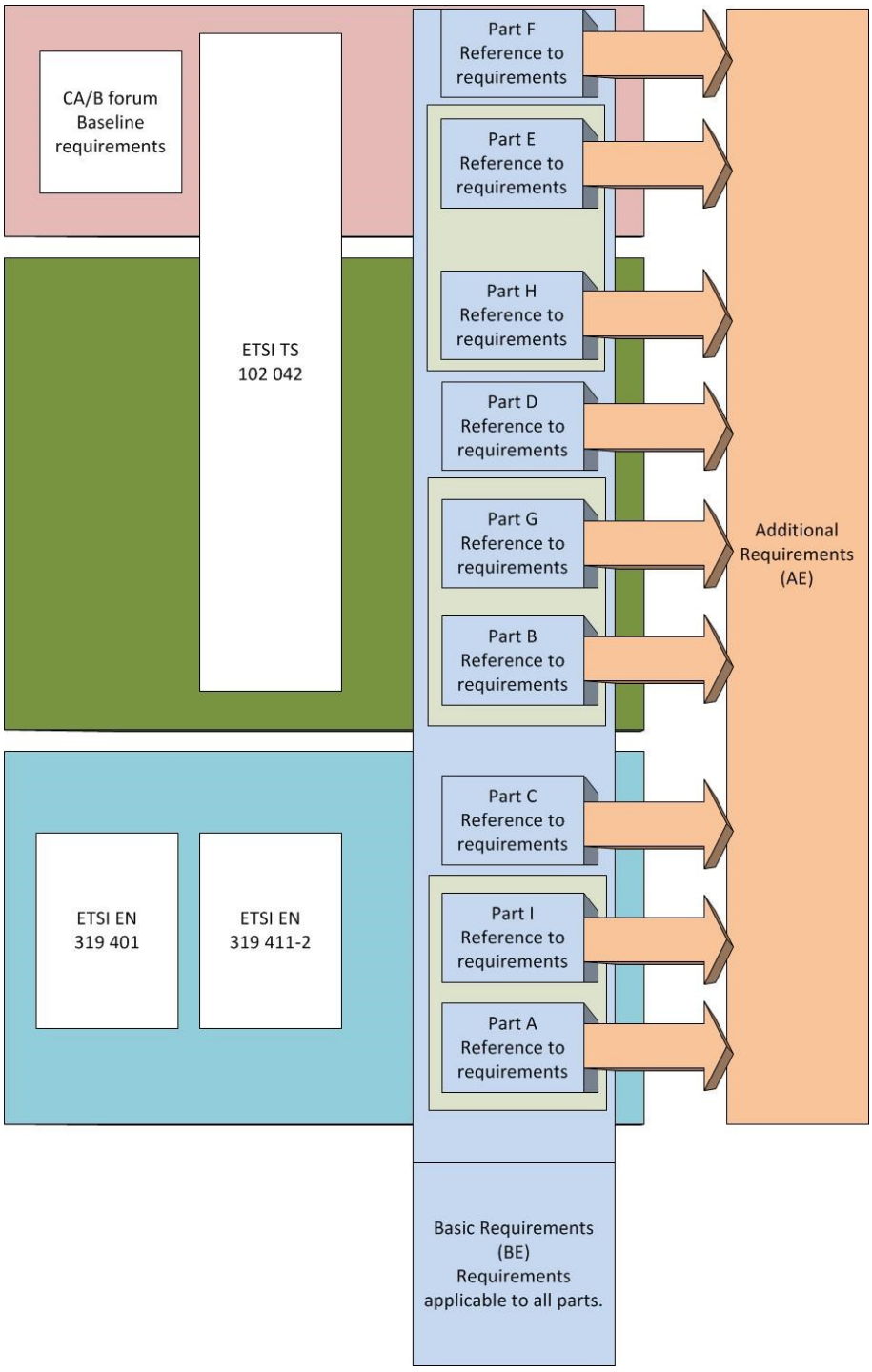
To comply with a specific CP the applicable ETSI standard, the *Basic Requirements* and part of the *Additional Requirements* of PKIoverheid must be met.

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

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[1].
Number	Unique number of the PKIo requirement. In each paragraph, consecutive numbering is used for the PKIo requirements. In combination with the RFC 3647 paragraph number, this forms a unique label for the PKIo requirement.
ETSI	Reference to the applicable ETSI requirement(s) from which the PKIo requirement is derived or to which it provides further detail.
PKIo	The PKIo requirement that applies to this domain of the PKI for the government.
Comment	To provide a better understanding of the context in which the requirement has to be placed a comment has been added to a number of PKIo requirements.

The following figure gives a graphical overview of the structure of part 3 of the Programme of Requirements:

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



1.1.2 Status

This is version 4.1 of part 3 Additional Requirements of the Programme of Requirements. The current version has been updated up to and including August 2015.

The PA has devoted the utmost attention and care to the data and information incorporated in these Additional Requirements of the PoR. 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 these Additional Requirements, if these Additional

Requirements are used for purposes other than for the use of certificates described in paragraph 1.4 of the individual PoR parts.

1.2 Contact information Policy Authority

The PA is responsible for these Additional Requirements. Questions relating to the Additional Requirements can be directed to the PA; the address can be found at: http://www.logius.nl/pkioverheid.

2 Publication and Repository Responsibilities

2.1 Electronic Repository

Contains no additional requirements.

2.2 Publication of CSP Information

RFC 3647	2.2 Publication of CSP information	
Number	2.2-pkio7	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.a -
PKIo	The CSP has to actively inform the citizen and to state in the conditions that the authenticity certificate is not referred to in the Compulsory Identification Act (Wid) as an identity document and therefore cannot be used to identify persons in cases where the law requires that the identity of persons is established using a document referred to in the Compulsory Identification Act. The CSP has to express that the authenticity certificate cannot be used when using government services, where the law requires that the identity of persons is established using a document in the Compulsory Identification Act.	

RFC 3647	2.2 Publication of CSP information	
Number	2.2-pkio8	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.1.d.3
PKIo	The Certification Practice Statement of the CSP must be structured according to RFC 2527, RFC 3647 or the Programme of Requirements of PKIoverheid that is based on RFC 3647 and must contain all relevant chapters as described in RFC 2527, RFC 3647 or the PoR PKIoverheid.	

RFC 3647	2.2 Publication of CSP-information	
Number	2.2-pkio9	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.1.b
PKIo	The CPS should only relate to the issuance of EV SSL certificates.	

3 Identification and Authentication

3.1 Naming

RFC 3647	3.1.3 Anonymity or pseudonimity of certificate holders	
Number	3.1.3-pkio11	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.3.a -
PKIo	Pseudonyms MUST NOT be used in certificates.	

3.2 Initial Identity Validation

RFC 3647	3.2.1. Method to prove possession of the private key	
Number	3.2.1-pkio13	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 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.	

RFC 3647	3.2.2 Authentication of organizational entity	
Number	3.2.2-pkio14	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.e -
PKIo	When issuing organization-linked certificates the CSP has to verify that the subscriber is an existing organization.	

RFC 3647	3.2.2 Authentication of organizational entity	
Number	3.2.2-pkio4	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 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	3.2.2-pkio147	
ETSI	EN 319 401 EN 319 411-2 EN 319 411-3 TS 102 042	- - - 7.3.1.d, 7.3.1.h.i, 7.3.1.r and 7.3.1.t
PKIo	The CSP has to verify that the subscriber is an existing and legal organization, and who the Authorised Representative (or Representation) of the subscriber is. As evidence that it is an existing and legal organization and of the correctness and existence of the Authorised Representative (or Representation) registered by the subscriber, the CSP has to request and verify at least the following supporting documents: ▪ For government organizations, a recently certified excerpt (no more than 1 month old) from the Chamber of Commerce's Trade Register or a law, deed of incorporation or a general governmental decree. If registration in the Trade Register has nog yet taken place, a copy of the corresponding page from the most recent version of the Staatsalmanak where the Authorised Representative (or Representation) is mentioned; ▪ For bodies governed by private law with and without a legal personality with a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register where the Authorised Representative (or Representation) is mentioned. The CSP must verify if the Organization and Authorised Representative appear on the latest EU list of prohibited terrorists and terrorist organizations, published by the European Council These lists can be found on the web page: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001E0931:NL:NOT These are decisions concerning updating the list of people, groups and entities referred to in articles 2, 3 and 4 of Common Position 2001/931/GBVB concerning the use of specific measures to combat terrorism. The CSP must not issue EV SSL certificates to an organization or its	

	Authorized Representative that appears on this list.

RFC 3647	3.2.2 Authentication of organizational entity	
Number	3.2.2-pkio16	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.e -
PKIo	In terms of organization-linked certificates, the CSP has to verify that the name of the organization registered by the subscriber that is incorporated in the certificate is correct and complete.	

RFC 3647	3.2.2 Authentication of organizational entity	
Number	3.2.2-pkio144	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.3.1.g
PKIo	The CSP has to verify that the name of the organization registered by the subscriber that is incorporated in the certificate is correct and complete.	

RFC 3647	3.2.3 Authentication of individual identity	
Number	3.2.3-pkio21	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.d and 7.3.1.e -
PKIo	When issuing certificates to natural persons the CSP has to verify that the full name used by the certificate holder that is incorporated in the certificate is correct and complete, including the surname, first forename, initials or other forename(s) (if applicable) and surname prefixes (if applicable).	

RFC 3647	3.2.3 Authentication of individual identity	
Number	3.2.3-pkio22	
ETSI	EN 319 401	-

	EN 319 411-2 TS 102 042	- 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	3.2.3-pkio24	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.3.1.e
PKIo	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	3.2.3-pkio26	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 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	3.2.3 Authentication of individual identity

Number	3.2.3-pkio27	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.3.1.d, 7.3.1.k and 7.3.1.r
PKIo	To detail the provisions in 3.2.3- pkio22, the identity of the certificate manager can only be established using the valid documents referred to in article 1 of the Compulsory Identification Act. The CSP has to check the validity and authenticity of these documents. The CSP must also establish whether the certificate manager appears on the latest EU list of prohibited terrorists and terrorist organizations: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:028:0057:0059:EN:PDF The CSP may not issue an EV SSL certificate to an organization or its certificate manager that is included on this list.	

RFC 3647	3.2.5 Validation of authority	
Number	3.2.5-pkio29	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.e -
PKIo	In terms of organization-linked certificate holders, the CSP has to check that: • the proof that the certificate holder, authorized to receive a certificate on behalf of the subscriber, is authentic; • the name and identity markers mentioned in this proof correspond with the certificate holder's identity established under 3.2.3-pkio21. In terms of profession-linked certificate holders, the CSP has to check that: • the proof, that the certificate holder is authorised to practise the recognized profession, is authentic; • the name and identity markers mentioned in this proof correspond with the certificate holder's identity established under 3.2.3-pkio21.	
Comment	Only considered to be authentic proof for practising a recognized profession is: a. either a valid proof of registration in a (professional) register recognized by the relevant professional group, to which disciplinary rules stipulated by law apply; b. or an appointment by a Minister; c. or valid proof (e.g. a permit) that the legal requirements in relation to practising a profession, are fulfilled. Understood to be meant by valid proof is proof that has not expired or that has not (temporarily or provisionally) been revoked. PoR part 4 contains a limitative list of the professions referred to under a and b. In the reference matrix in appendix B there is a reference to all requirements that relate to paragraph 3.2.3.	

RFC 3647	3.2.5 Validation of authority	
Number	3.2.5-pkio30	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.3.1.d, 7.3.1.h, 7.3.1.i, 7.3.1.k and 7.3.1.m.vi
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	3.2.5-pkio31	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.3.1.d, 7.3.1.h and 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 the consent of the subscriber to perform the actions that he has been asked to perform (if the certificate manager performs the registration process).
	• the requested certificate in combination with the permanently stored data in the certificate holder (device) contain information to be able to trace the following unequivocally:
	  ○ the device's identity (e.g. manufacturer and serial number);
	  ○ the proof that the device and its production process conform to the framework of standards established by the party responsible for establishing the framework.	

Comment	The "certificate manager" who takes over those actions from the certificate holder does not necessarily have to be the same person as the person who produces or uses the certificate holder (the device). 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 would also be wise to take measures that restrict 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	3.2.5-pkio32	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.2.g -
PKIo	Subscriber is a legal personality (organization-linked certificates): 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 that have been made to the relationship between the subscriber and the certificate holder, by means of a revocation request. Relevant changes can, in this respect, for instance be termination of employment and suspension. Subscriber is a natural person (occupation-linked certificates): 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 that have been made by means of a revocation request. A relevant change in this respect is, in any case, no longer having legal proof as outlined in 3.2.5-pkio29.	

RFC 3647	3.2.5 Validation of authority	
Number	3.2.5-pkio33	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 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 Validation of authority	
Number	3.2.5-pkio34	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 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 amendments to the relation between the subscriber and certificate manager and/or certificate holder (autonomous device). If the device fails, this has to be done using a revocation request.

RFC 3647	3.2.5 Validation of authority	
Number	3.2.5-pkio35	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.3.1.i.i, 7.3.1.r and 7.3.3.a.x
PKIo	The CSP has to verify that the subscriber is the registered owner of the domain name listed in the request (FQDN) or that the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner. This verification may not be contracted out by the CSP to Registration Authorities or other parties. If the subscriber states that he/she is the registered owner of the domain name listed in the request, the CSP has to: ▪ verify that the domain name is registered with a registrar or domain manager, such as SIDN (The Netherlands Internet Domain Registration Foundation), affiliated with the Internet Corporation for Assigned Names and Numbers (ICANN) or an organization that is a member of the Internet Assigned Numbers Authority (IANA), and; ▪ use a WHOIS service, of an organization affiliated with or that is a member of ICANN or IANA, that offers the information via HTTPS or the de CSP must use a command line programme if a WHOIS service is used that offers information via HTTP, and; ▪ in the WHOIS service, verify the name, the residential address and the administrative contact person of the organization and compare this information to the verified subscriber information and establish that there are no inconsistencies between the two sets of information, and; ▪ The CSP must verify that the domain name does not appear on a spam list and/or phishing black list. Use, to this end, at least http://www.phishtank.com. If the domain name is mentioned on phish tank or a different black list that is consulted, during the verification process the CSP has to deal particularly carefully with the request for the relevant services server certificate. The information that the CSP uses to verify that the subscriber is the registered owner of the domain name (FQDN) listed in the application may not be older than 13 months, otherwise the information has to be requested and verified again. If the subscriber states that it is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner, as well as the checks listed above, the CSP has to:	

	▪ verify that the domain name (FQDN) is not a generic TopLevelDomein (gTLD) or country code TopLevelDomein (ccTLD). For these domain names, only the subscriber, as registered domain name owner, is allowed to submit an application, and; ▪ request a declaration from the registered domain name owner (e.g. by e-mail or telephone) in which the registered domain name owner has to confirm that the subscriber has the exclusive right to use the domain name (FQDN), or; ▪ request and verify a written and signed declaration from a notary or external accountant which must state for which domain name (FQDN) the subscriber has been given the exclusive user right on behalf of the registered domain name owner.. A declaration from the registered domain name owner or notary or external accountant may not be older than 13 months.

RFC 3647	3.2.5 Validation of authority	
Number	3.2.5-pkio146	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.3.1.v
PKIo	A CSP must verify if the subscriber is the owner of the FQDN that is incorporated in the server or EV certificate. The Baseline Requirements stipulate under 4.2.1 that additional verification activity must be undertaken for High Risk Requests. PKIoverheid understands that to mean at least the following: • A domain name of a Fortune Global 500 company • A domain name with a second level domain equal to a second level domain of the top 500 domain names worldwide and specific to the Netherlands • A domain name that appears on a known spam- and/or phishing blacklist Once it is established that the holder is an organization belonging to the global 500 or if the second level domain name is equal to the top 500 domain names, the CSP may only issue a certificate after the expressed permission of an accountable manager of the CSP who is not part of the standard approval process. If the domain name appears on a phishing blacklist a certificate may not be issued.	
Comment	Largest organizations: http://fortune.com/global500/ Most used domain names: http://www.alexa.com/topsites Phishing: http://www.phishtank.com. Examples of high risk requests as described above are twitter.nl, account.twitter.com. In case of the use of a domain authorization letter extra attention must be paid to the verification and authenticity of the domain authorization letter.	

3.3 Identification and Authentication for Re-key Requests

Contains no additional requirements.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

RFC 3647	4.1 Certificate Application	
Number	4.1-pkio47	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 6.2
PKIo	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. The agreement must be signed by the Authorized Representative or Representation of the subscriber.	

RFC 3647	4.1 Certificate Application	
Number	4.1-pkio48	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.3.1.u

PKIo	Before issuing an EV SSL certificate, the CSP has to have received a fully completed application, signed by the certificate manager on behalf of the subscriber. The application must contain the following information:
	▪ the name of the organization;
	▪ the domain name (FQDN);
	▪ Chamber of Commerce number or Government Identification Number;
	▪ subscriber's address consisting of:
	  ○ street name and house number;
	  ○ town or city;
	  ○ province;
	  ○ country;
	  ○ postcode and
	  ○ general telephone number.
	▪ certificate manager's name.	

4.4 Certificate Acceptance

Contains no additional requirements.

4.5 Key Pair and Certificate Usage

RFC 3647	4.5.2 Relying party public key and certificate usage	
Number	4.5.2-pkio145	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 6.3
PKIo	When issuing Extended Validation certificates under this CP the CSP MUST adhere to the requirements in relation to certificate transparency.	
Comment	See http://www.chromium.org/Home/chromium-security/root-ca-policy/EVCTPlan19Mar2014.pdf.	

4.9 Certificate Revocation and Suspension

RFC 3647	4.9.1 Circumstances for revocation	
Number	4.9.1-pkio52	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.a 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 SSCD is lost or suspected to be lost, if the key or SSCD is stolen or suspected to be stolen, or if the key or SSCD is destroyed; • a subscriber does not fulfil its obligations outlined in this CP or the corresponding CPS of the CSP or the agreement that the CSP has entered into with the subscriber; • the CSP is informed or otherwise becomes aware of a substantial change in the information that is provided in the certificate. An example of that is: a change in the name of the certificate holder; • the CSP determines that the certificate has not been issued in line with this CP or the corresponding CPS of the CSP or the agreement that the CSP has entered into with the subscriber; • the CSP determines that information in the certificate is incorrect or misleading; • the CSP ceases its work and the CRL and OCSP services are not taken over by a different CSP. • The PA of PKIoverheid determines that the technical content of the certificate entails an irresponsible risk to subscribers, relying parties and third parties (e.g. browser parties).	

Comment	In addition, certificates can be revoked as a measure to prevent or to combat an emergency. Considered to be an emergency is definitely the compromise or suspected compromise of the private key of the CSP used to sign certificates.

RFC 3647	4.9.3 Procedure for revocation request	
Number	4.9.3-pkio57	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.i 6.3 note 1, 7.3.6.h.iii, 7.3.6.j and 7.3.6.k
PKIo	In any case, the CSP has to use a CRL to make the certificate status information available.	

RFC 3647	4.9.3 Procedure for revocation request	
Number	4.9.3-pkio58	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.3.6
PKIo	The CSP has to publish the procedure for revocation and, in that publication, provide unambiguous definitions of the following sub-processes, summarized in chronological order: • The receipt of a request for revocation; • The identification and authentication of the party that submits the request for revocation; • The trustworthiness investigation with regard to the request for revocation; • The processing of (the trustworthy request for) the revocation; • The publication of the (processed) revocation. The definition of every sub-process has to include as a minimum the conditions for following the sub-process and the data to be registered in that sub-process.	

RFC 3647	4.9.3 Procedures for revocation request	
Number	4.9.3-pkio60	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 6.3 Note 1, 7.3.6.h.iii, 7.3.6.j.iii and 7.3.6.k
PKIo	If there is an issuing subordinate CA under a CSP CA then: ▪ the CSP has to use an OCSP and a CRL to make available the certificate status information, relating to the issuing subordinate CA; ▪ the CSP has to record the reason for the revocation of the issuing	

	subordinate CA certificate; ▪ the validity of the CRL, with regard to the certificate status information of the issuing subordinate CA, is no more than 7 days.

RFC 3647	4.9.5 Time within which CA must process the revocation request	
Number	4.9.5-pkio62	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 6.3 Note 1, 7.3.6.h.iii, 7.3.6.j.iii and 7.3.6.k
PKIo	In the case of an issuing subordinate CA, the maximum delay between the time at which the decision is taken to revoke an issuing subordinate CA (recorded in a report) and the amendment of the revocation status information, which is available to all relying parties, is 72 hours.	

RFC 3647	4.9.7 CRL issuance frequency	
Number	4.9.7-pkio65	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6 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	4.9.9-pkio66	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.i 7.3.6.j
PKIo	The revocation management services of the CSP can support the Online Certificate Status Protocol (OCSP) as an addition to the publication of CRL information. If this support is available, this has to be stated in the CPS.	
Comment	If OCSP is offered the following requirements are applicable: • 3.1.1-pkio10 (basic requirement) • 4.9.5-pkio61 (basic requirement) • 4.9.9-pkio67 • 4.9.9-pkio68 • 4.9.5-pkio69 (basic requirement) • 4.9.9-pkio70 • 4.9.9-pkio71	

	• 4.10.2-pkio73 (basic requirement) NB: (EV) server certificates MUST use OCSP services as stipulated in ETSI TS 102 042 and the Baseline Requirements.

RFC 3647	4.9.9 On-line revocation/status checking availability	
Number	4.9.9-pkio67	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.i 7.3.6.j
PKIo	If the CSP supports the Online Certificate Status Protocol (OCSP), this must conform to IETF RFC 2560.	

RFC 3647	4.9.9 On-line revocation/status checking availability	
Number	4.9.9-pkio68	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.i -
PKIo	To detail the provisions of IETF RFC 2560, OCSP responses have to be signed digitally by either: • the private (CA) key with which the certificate is signed of which the status is requested, or; • a responder appointed by the CSP which holds an OCSP Signing certificate issued for this purpose by the CSP, or; • a responder that holds an OCSP Signing certificate that falls under the hierarchy of the PKI for the government.	

RFC 3647	4.9.9 On-line revocation/status checking availability	
Number	4.9.9-pkio70	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.i 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	4.9.9-pkio71	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.i 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.	

4.10 Certificate Status Services

Contains no additional requirements.

5 Facility, Management and Operational Controls

5.2 Procedural Controls

Contains no additional requirements.

5.3 Personnel Controls

RFC 3647	5.3.2 Background check procedures	
Number	5.3.2-pkio79	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.3.j - -
PKIo	Before engaging the services of someone to work on one or more PKIoverheid core services, the CSP or external supplier that performs part of this work MUST verify the identity and the security of this employee.	

5.4 Audit Logging Procedures

RFC 3647	5.4.1 Types of events recorded	
Number	5.4.1-pkio80	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.5.j - 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); • Destination addresses (IP addresses if available); • Time and date; • User IDs (if available); • Name of the incident; • Description of the incident.
Comment	Based on a risk analysis the CSP determines which data it should save.

5.5 Records Archival

RFC 3647	5.5.1 Types of records that are archived	
Number	5.5.1-pkio82	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.f 7.3.1.j, 7.3.1.n and 7.4.11 note 2
PKIo	The CSP MUST archive all information used to verify the identity of the subscriber, certificate manager and applicants of revocation requests. This information includes reference numbers of the documentation used for verification, including limitations concerning the validity.	

5.7 Compromise and Disaster Recovery

RFC 3647	5.7.4 Business continuity capabilities after a disaster.	
Number	5.7.4-pkio86	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.4.8 7.4.8.a
PKIo	The CSP has to draw up a business continuity plan (BCP) for, at the very least, the core services dissemination service, revocation management service and revocation status service, the aim being, in the event of a security breach or emergency, to inform, reasonably protect and to continue the CSP services for subscribers, relying parties and third parties (including browser parties). The CSP has to test, assess and update the BCP annually. At the very least, the BCP has to describe the following processes: ▪ Requirements relating to entry into force; ▪ Emergency procedure/fall-back procedure; ▪ Requirements relating to restarting CSP services; ▪ Maintenance schedule and test plan that cover the annual testing, assessment and update of the BCP; ▪ Provisions in respect of highlighting the importance of business continuity; ▪ Tasks, responsibilities and competences of the involved agents;	

	▪ Intended Recovery Time or Recovery Time Objective (RTO); ▪ Recording the frequency of back-ups of critical business information and software; ▪ Recording the distance of the fall-back facility to the CSP's main site; and ▪ Recording the procedures for securing the facility during the period following a security breach or emergency and for the organization of a secure environment at the main site or fall-back facility.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

RFC 3647	6.1.1 Key pair generation for the CSP sub CA	
Number	6.1.1-pkio87	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.1.c and 7.2.1.d 7.2.1.c, 7.2.1.d and 7.2.8.b
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	6.1.1-pkio88	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.8.c and 7.3.1.l 7.2.8.c
PKIo	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 comparable security criteria.	

RFC 3647	6.1.1 Key pair generation for the certificate holders	
Number	6.1.1-pkio89	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.8.a 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 keys of certificate holders has to fulfil the requirements laid down in that respect in the list of cryptographic algorithms and key lengths as defined in ETSI TS 102 176-1.	

Comment	Although ETSI TS 102 176 outlines the recommended algorithms and key lengths, these are compulsory within the PKI for the government. Requests relating to the use of other algorithms have to be submitted, along with the reasoning behind this, to the PA of the PKI for the government.

RFC 3647	6.1.1 Key pair generation for the certificate holders	
Number	6.1.1-pkio90	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.2.8.d
PKIo	The generation of the certificate holder's key, where the CSP also generates the private key (PKCS#12) is not allowed	

RFC 3647	6.1.1 Key pair generation for the certificate holders	
Number	6.1.1-pkio91	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.2.8.d
PKIo	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	6.1.1-pkio92	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.2.8
PKIo	A CSP within PKIoverheid is not allowed to issue code signing certificates.	

RFC 3647	6.1.1 Key pair generation for the certificate holders	
Number	6.1.1-pkio93	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 6.2.f and 6.2.g
PKIo	Using PKCS#10 to deliver the CSR to the CSP for signing, the certificate manager MAY generate the keys of the services authenticity and encryption certificates in a SUD instead of the CSP, under the following conditions: - The agreement between the CSP and the subscriber stipulates that the certificate manager generates, saves and uses the private key on a secure device that conforms to the requirements of CWA 14169 "Secure signature-creation devices "EAL 4+"" or comparable security criteria.	

	With the request he subscriber must prove that the secure device used for key generation conforms to CWA 14169 "Secure signature-creation devices "EAL 4+"" or comparable security criteria. The CSP must then verify that the SUD in question conforms (comparable to “The subscriber MUST prove that the organization may use this name.”) - On registration the certificate manager must at least produce a written statement that measures have been taken in the environment of the system that generates/contains the keys. The measures must be of such quality that is practically impossible to steal or copy the keys unnoticed. The agreement between the subscriber and the CSP must stipulate that the CSP has the right to perform an audit on the measures taken (conform 6.2.11-pkio107) - The agreement between the subscriber and the CSP must contain the following condition. The subscriber must declare that the private key (and the corresponding access information such as a PIN code), relating to the public key in het SUD in question has, in an appropriate manner, been generated under the control of the certificate manager and will be kept secret and protected in the future.

RFC 3647	6.1.2 Private key and SSCD delivery to certificate holder	
Number	6.1.2-pkio94	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.8.d -
PKIo	[OID 2.16.528.1.1003.1.2.2.2 and 2.16.528.1.1003.1.2.5.2], [OID 2.16.528.1.1003.1.2.2.1 and 2.16.528.1.1003.1.2.5.1] and [OID 2.16.528.1.1003.1.2.3.2 and 2.16.528.1.1003.1.2.3.1]. The certificate holder's private key has to be delivered to the certificate holder, if required through the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the certificate holder, the private key can be maintained under the certificate holder’s sole control.	
Comment	This text corresponds with 7.2.8.d, but has been integrated because this requirement only applies to signature and authenticity certificates.	

RFC 3647	6.1.2 Private key and SUD delivery to the certificate holder	
Number	6.1.2-pkio95	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 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],	

	[OID 2.16.528.1.1003.1.2.6.2] and [OID 2.16.528.1.1003.1.2.8.5] 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.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

RFC 3647	6.2.3 Private key escrow of certificate holder key	
Number	6.2.3-pkio99	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.4 7.2.4.b
PKIo	The authorized persons who can gain access to the private key of the confidentiality certificate held in Escrow by the CSP (if applicable), have to identify themselves using the valid documents listed in article 1 of the Compulsory Identification Act (Wet op de identificatieplicht), or a valid qualified certificate (limited to a PKIoverheid signature certificate or equivalent).	

RFC 3647	6.2.3 Private key escrow of certificate holder key	
Number	6.2.3-pkio100	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.4 7.2.4.b
PKIo	The CSP has to describe in the CPS which parties can have access to the private key of the confidentiality certificate held in Escrow and under which conditions.	

RFC 3647	6.2.3 Private key escrow of certificate holder key	
Number	6.2.3-pkio101	
ETSI	EN 319 401	-

	EN 319 411-2 TS 102 042	7.2.4 -
PKIo	If the CSP keeps the private key of the confidentiality certificate in Escrow, the CSP has to guarantee that this private key is kept secret and only made available to appropriately authorized persons.	
Comment	Although this requirement corresponds with ETSI TS 102 042 7.2.4.b, this requirement is nevertheless positioned as a PKIo requirement in order to make sure that this forms part of the approved audit statement that the CSP has to submit.	

RFC 3647	6.2.11 Cryptographic module rating	
Number	6.2.11-pkio104	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 5.3.1.c -
PKIo	Secure devices issued or recommended by the CSP for creating electronic signatures (SSCDs) have to fulfil the requirements laid down in document CWA 14169 "Secure signature-creation devices "EAL 4+"" and the requirements outlined in or pursuant to the Electronic Signatures Decree article 5, parts a, b, c and d.	
Comment	The use of different types of secure devices, such as a smartcard or a USB key, is allowed. The condition is that the SSCD meets the substantive requirements as specified in 6.2.11-pkio104, 6.2.11-pkio105 and 6.2.11-pkio106.	

RFC 3647	6.2.11 Cryptographic module rating	
Number	6.2.11-pkio125	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 3.1
PKIo	Secure devices issued or recommended by the CSP for storage of keys (SUDs) have to fulfil the requirements laid down in document CWA 14169 "Secure signature-creation devices "EAL 4+""	

RFC 3647	6.2.11 Cryptographic module rating	
Number	6.2.11-pkio105	
ETSI	EN 319 401 EN 319 411-2	- 5.3.1.c

	TS 102 042	3.1
PKIo	Instead of demonstrating compliance with CWA 14169, CSPs can issue or recommend SSCDs or 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 security level. This has to be established by a test laboratory that is accredited for performing Common Criteria evaluations.	

RFC 3647	6.2.11 Cryptographic module rating	
Number	6.2.11-pkio106	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 5.3.1.c -
PKIo	The concurrence of SSCDs with the requirements outlined in PKIo requirement no. 6.2.11-1 has to have been ratified by a government body appointed to inspect the secure devices, for the creation of electronic signatures in accordance with the Dutch Telecommunications Act (TW) article 18.17, third paragraph. In this respect, also see the Ruling on Electronic Signatures, articles 4 and 5.	

RFC 3647	6.2.11 Cryptographic module rating	
Number	6.2.11-pkio107	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 3.1
PKIo	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	6.3.1 Public key archival	
Number	6.3.1-pkio108	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.11.e - -
PKIo	[OID 2.16.528.1.1003.1.2.2.2, 2.16.528.1.1003.1.2.5.2 and 2.16.528.1.1003.1.2.3.2] The signature certificate has to be saved during the term of validity and furthermore during a period of at least seven years after the date on which the validity of the certificate expired.	
Comment	The Electronic Signature Regulation article 2, paragraph 1i stipulates a term of seven years. No further provisions apply to the authenticity certificate and the confidentiality certificate in relation to archiving public keys.	

RFC 3647	6.3.2 Certificate operational periods and key pair usage periods	
Number	6.3.2-pkio109	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.6 7.2.6
PKIo	Private keys that are used by a certificate holder and issued under the responsibility of this CP must not be used for more than five years. The certificates, which are issued under the responsibility of this CP, must not be valid for 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.	

RFC 3647	6.3.2 Certificate operational periods and key pair usage periods	
Number	6.3.2-pkio111	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 7.2.6
PKIo	Private keys that are used by a certificate holder and issued under the responsibility of this CP must not be used for more than ten years. The certificates, which are issued under the responsibility of this CP, must not be valid for more than ten years.	

Comment	The CSPs within the Autonomous Devices domain of the PKI for the government cannot issue certificates with a maximum term of validity of ten years until the PA has provided explicit permission for this.

6.4 Activation data

RFC 3647	6.4.1 Activation data generation and installation	
Number	6.4.1-pkio112	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.9.d 7.2.9.d
PKIo	The CSP attaches activation data to the use of an SSCD, to protect the private keys of the certificate holders.	
Comment	The requirements that the activation data (for example the PIN code) have to fulfil can be determined by the CSPs themselves based on, for example, a risk analysis. Requirements that could be considered are the length of the PIN code and use of special characters.	

RFC 3647	6.4.1 Activation data generation and installation	
Number	6.4.1-pkio113	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.9.d 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

Contains no additional requirements.

6.6 Life Cycle Technical Controls

Contains no additional requirements.

6.7 Network Security Controls

Contains no additional requirements.

7 Certificate, CRL and OSCP profiles

7.1 Certificate Profile

Contains no additional requirements.

7.2 CRL Profile

Contains no additional requirements.

7.3 OCSP Profile

RFC 3647	7.3 OCSP profile
Number	7.3-pkio123
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 the Basic Requirements, "CRL and OCSP certificate Profiles for certificate status information ".

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. Financial Responsibility	
Number	9.2-pkio124	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.5.c - 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

Contains no additional requirements.

9.6 Representations and Warranties

RFC 3647	9.6.1 Representations and Warranties by CSPs	
Number	9.6.1-pkio127	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.4 and Annex A 6.4
PKIo	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 Representations and Warranties by CSPs	
Number	9.6.1-pkio128	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 6.4
PKIo	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 Representations and Warranties by CSPs	
Number	9.6.1-pkio129	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.4 and Annex A 6.4
PKIo	[OID 2.16.528.1.1003.1.2.2.3 and 2.16.528.1.1003.1.2.5.3], [OID 2.16.528.1.1003.1.2.2.5 and 2.16.528.1.1003.1.2.5.5] and [OID 2.16.528.1.1003.1.2.3.3] In the agreement between the CSP and the subscriber, a clause (a clause as specified in article 6:253 of the Civil Code) will be included in which the CSP champions the interests of a third party relying on the certificate. This clause addresses a liability of the CSP in accordance with article 6:196b, first up to and including third paragraph, of the Civil Code, with the proviso that: a. for "a qualified certificate specified in article 1.1, division ss Telecommunications Act": "a confidentiality certificate" is read; b. for "signatory": "certificate holder" is read; c. for "creation of electronic signatures": "creation of encrypted data" is read; d. For "verification of electronic signatures": "decoding of encrypted data" is read.	

RFC 3647	9.6.1 Representations and Warranties by CSPs	
Number	9.6.1-pkio142	
ETSI	EN 319 401	-

	EN 319 411-2 TS 102 042	- 6.4
PKIo	[OID 2.16.528.1.1003.1.2.6.2] 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 from the PKIoverheid Autonomous Devices domain" 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 Representations and Warranties by CSPs	
Number	9.6.1-pkio131	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.4 and Annex A -
PKIo	The CSP can include in a non-repudiation certificate restrictions with regard to the use of the certificate, provided that the restrictions are clear to third parties. The CSP is not liable for losses that results from the use of a signature certificate that is contrary to the provisions in accordance with the previous sentence listed therein.	
Comment	This article is based on Civil Code art. 196b, paragraph 3	

RFC 3647	9.6.1 Representations and Warranties by CSPs	
Number	9.6.1-pkio132	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.4 and Annex A 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	9.8-pkio133	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.4 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	9.8-pkio143	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 6.4
PKIo	The CSP is allowed to place restrictions on the use of certificates within the scope of certificates as mentioned in paragraph 1.4 of the applicable PoR part for that type of certificate.	

RFC 3647	9.8 Limitations of Liability	
Number	9.8-pkio134	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- - 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 EV SSL certificates.	

9.12 Amendments

Contains no additional requirements.

9.13 Dispute Resolution Provisions

Contains no additional requirements.

9.14 Governing Law

Contains no additional requirements.

9.17 Other Provisions

RFC 3647	9.17 Other Provisions
Number	9.17-pkio139
ETSI	This subject is not covered in ETSI, as ETSI has been specifically drafted for qualified certificates.
PKIo	The CSP has to be capable of issuing all types of personal certificates listed under [1.2] of the applicable PoR part for that type of certificate.

RFC 3647	9.17 Other Provisions
Number	9.17-pkio140
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] of the applicable PoR part for that type of certificate.

RFC 3647	9.17 Other Provisions
Number	9.17-pkio141
ETSI	This subject is not covered in ETSI.
PKIo	The CSP has to be capable of issuing at least one type of certificate listed under [1.2] of the applicable PoR part for that type of certificate.

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 101 456 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[2]. The PA has specifically decided to include all requirements just once.

[2] *This is partially caused by the fact that ETSI TS 101 456 is not constructed in accordance with the RFC 3647 structure.*

10 Revisions

10.1 Amendments between version 4.0 and 4.1

Revision control is not applied to this document. Modifications are kept track of in the appropriate PoR part.

10.2 Amendments between version 3.7 and 4.0

10.2.1 New

None.

10.2.2 Modifications

- PoR requirements have been renumbered according to a new naming convention;
- The creation of a document containing the basic and additional requirements;

10.2.3 Editorial

None