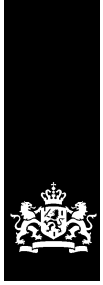


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3: Additional Requirements PKIoverheid

Date 8 February 2019

Publisher's imprint

Version number	4.7
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 a trust framework. This framework 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 (TSPs) to the PKI for the government and preparing the administration;
- supervising and monitoring the activities of TSPs 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
4.2	01-2016	Ratified by the Ministry of the Interior and Kingdom Relations January 2016
4.3	07-2016	Ratified by the Ministry of the Interior and Kingdom Relations July 2016
4.4	02-2017	Ratified by the Ministry of the Interior and Kingdom Relations February 2017
4.5	07-2017	Ratified by the Ministry of the Interior and Kingdom Relations June 2017
4.6	01-2018	Ratified by the Ministry of the Interior and Kingdom Relations January 2018
4.7	02-2019	Ratified by the Ministry of the Interior and Kingdom Relations February 2019

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 (TSP) within the PKI for the government. Within the PKI for the government , a distinction is made between various domains. These additional requirements relate to all types of certificate issued under these domains, whereby the distinction is made in the corresponding PoR parts.

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

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 consists 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 issuance 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 persistant number which also contains a reference to RFC 3647.

Furthermore each PKIoverheid requirement can have a relation with one or more ETSI requirements for the issuance of PKI certificates. In a separate Excel tabsheet in the OoA template "Referentiematrix PKIoverheid and ETSI" this relationship is listed, aiding in interpreting the PKIoverheid requirements in the context of the ETSI requirements.

The PKIoverheid requirements are divided into the *Basic Requirements* and the *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.

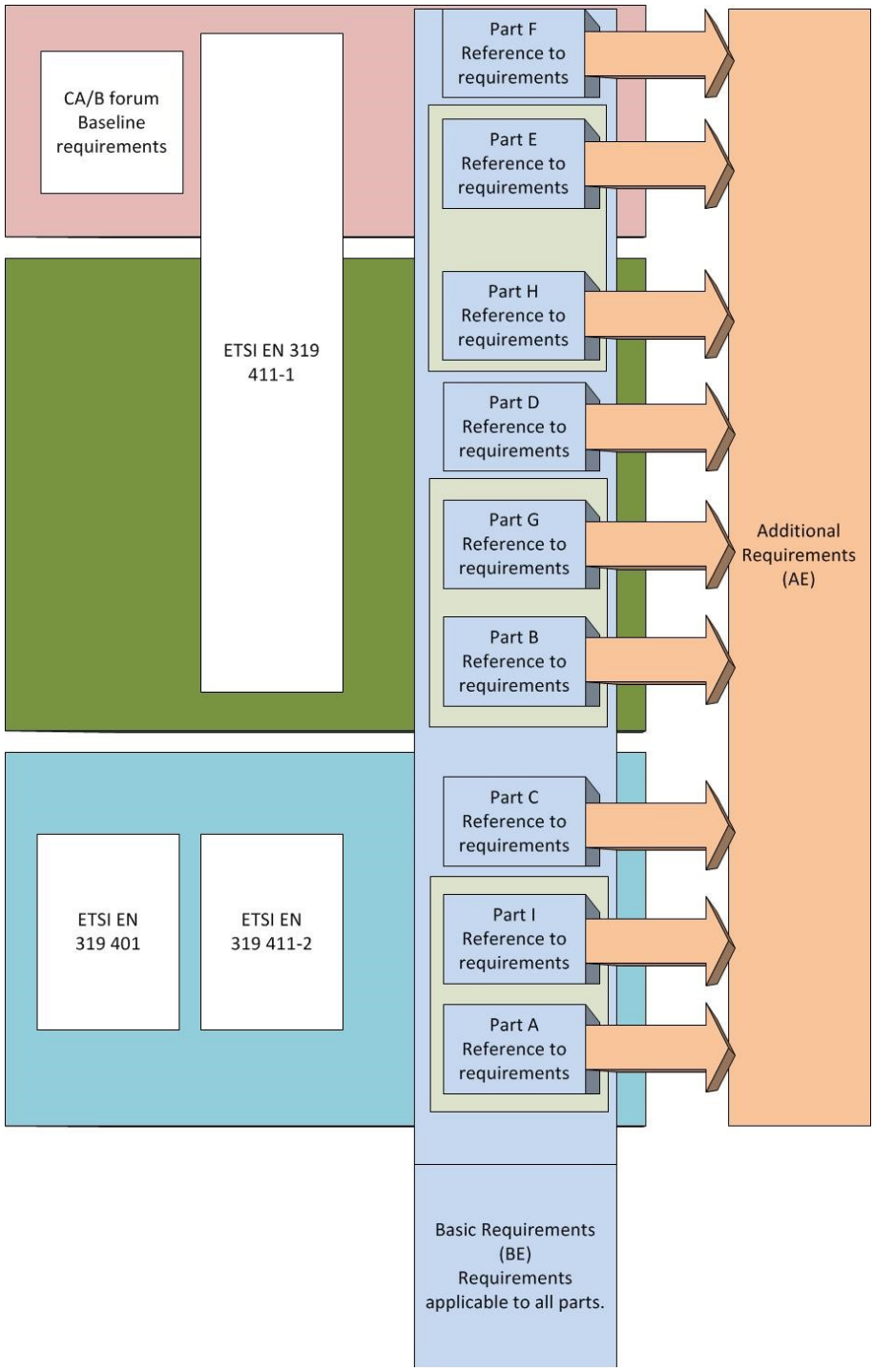
To comply with a specific CP, the TSP must meet requirements from the applicable ETSI standard, the *Basic Requirements* and part of the *Additional Requirements* required by the relevant PKIoverheid CP*.*

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.
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 4.7 of part 3 Additional Requirements of the Programme of Requirements. The current version has been updated up to and including 8 February 2019.

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 TSP Information

RFC 3647	2.2 Publication of TSP information
Number	2.2-pkio3
PKIo	The CPS shall be made available in English. In addition the TSP may issue a CPS in Dutch. There may be no substantial substantive difference between the two versions.

RFC 3647	2.2 Publication of TSP information
Number	2.2-pkio7
PKIo	The TSP 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 TSP 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 TSP information
Number	2.2-pkio8
PKIo	The Certification Practice Statement of the TSP 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 TSP-information
Number	2.2-pkio156
PKIo	The CPS must be reviewed and renewed yearly. The TSP must report a renewal to the PA.

RFC 3647	2.2 Publication of TSP-information
Number	2.2-pkio157
PKIo	The CPS shall be made available in English and/or in Dutch. There may be no substantial substantive difference between the two versions.

RFC 3647	2.2 Publication of TSP-information
Number	2.2-pkio155
PKIo	The CPS MUST indicate which method of the Baseline Requirements has been used to perform domain validation. The indication must contain a reference to the appropriate paragraph (3.2.2.4.x) of the Baseline Requirements and must be placed in the relevant paragraph of the CPS.

RFC 3647	2.2 Publication of TSP-information
Number	2.2-pkio166
PKIo	The TSP MUST describe in its CPS which validation method for validating IP-adresses and/or FQDNs it uses for inclusion in the Subject.CommonName field, the SubjectAltName.dNSName field and/or the SubjectAltName.iPAdress field , including a reference to the appropriate chapter of the Baseline Requirements.

RFC 3647	2.2 Publication of TSP-information
Number	2.2pkio167
PKIo	The TSP MUST describe in its CPS which validation methods for validating FQDNs it uses for inclusion in the Subject.CommonName field and the SubjectAltName.dNSName field including a reference to the relevant chapter of the Baseline Requirements.

RFC 3647	2.2 Publication of TSP-information
Number	2.2-pkio168
PKIo	The TSP MUST describe in its CPS which validation methods for validating IP addresses and / or FQDNs it uses for inclusion in the Subject.CommonName field, the SubjectAltName.dNSName field and / or theSubjectAltName.iPAdress field with a reference to the relevant chapter of the Baseline Requirements OR

	a reference to the number provided by the PA in the event of custom validation methods as described in requirement 3.2.5-pkio162.

3 Identification and Authentication

3.1 Naming

RFC 3647	3.1.3 Anonymity or pseudonimity of certificate holders
Number	3.1.3-pkio11
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
PKIo	The TSP is responsible for ensuring that the subscriber supplies the certificate signing request (CSR) securely. The secure delivery must take place in the following manner: • the entry of the CSR on the TSP's application developed especially for that purpose, using an SSL connection with a PKIoverheid SSL certificate or similar or; • the entry of the CSR on the HTTPS website of the TSP that uses a PKIoverheid SSL certificate or similar or; • sending the CSR by e-mail, along with a qualified electronic signature of the certificate manager that uses a PKIoverheid qualified certificate or similar or; • entering or sending a CSR in a way that is at least equivalent to the aforementioned ways.

RFC 3647	3.2.2 Authentication of organizational entity
Number	3.2.2-pkio14
PKIo	When issuing organization-linked certificates the TSP has to verify that the subscriber is an existing organization.

RFC 3647	3.2.2 Authentication of organizational entity
Number	3.2.2-pkio4
PKIo	The TSP has to verify that the subscriber is an existing organization.

RFC 3647	3.2.2 Authentication of organizational entity
Number	3.2.2-pkio147
PKIo	The TSP 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 TSP 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 TSP 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 TSP 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
PKIo	In terms of organization-linked certificates, the TSP 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

PKIo	The TSP 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
PKIo	When issuing certificates to natural persons the TSP 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
PKIo	In accordance with Dutch legislation and regulations, the TSP 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
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 TSP 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
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
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 TSP has to check the validity and authenticity of these documents. The TSP 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 TSP may not issue an EV SSL certificate to an organization or its certificate manager that is included on this list.

RFC 3647	3.2.3 Authentication of personal identity
Number	3.2.3-pkio169
PKIo	For certificates that are suitable for signing and / or securing e-mail messages and which include the e-mail address of the certificate holder, the TSP will take appropriate measures to ensure that the applicant has control over the e-mail address in question OR that he / she is authorized by the holder of the e-mail address to have this e-mail address included in a certificate. The TSP must clearly state in its CPS which procedures are carried out to confirm the above.

RFC 3647	3.2.5 Validation of authority
Number	3.2.5-pkio29
PKIo	In terms of organization-linked certificate holders, the TSP 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 TSP 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
PKIo	The TSP 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
PKIo	The TSP 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: o the device's identity (e.g. manufacturer and serial number); o 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
PKIo	Subscriber is a legal personality (organization-linked certificates): The agreement that the TSP enters into with the subscriber has to state that the subscriber is responsible for immediately informing the TSP 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 TSP enters into with the subscriber has to state that the subscriber is responsible for immediately informing the TSP 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
PKIo	The agreement that the TSP enters into with the subscriber has to state that the subscriber is responsible for immediately informing the TSP 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
PKIo	The agreement that the TSP enters into with the subscriber has to state that the subscriber is responsible for immediately informing the TSP 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-pkio146
PKIo	A TSP 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 TSP may only issue a certificate after the expressed permission of an accountable manager of the TSP 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.

RFC 3647	3.2.5 Authorization of the certificate holder
Number	3.2.5-pkio160
PKIo	The restrictive list of recognized professions for which professional certificates can be issued is as follows: 1. Accountant-Administratieconsulent (Accountant-Administration Officer); 2. Advocaat (Lawyer); 3. Octrooigemachtigde (Patent Agent); 4. Registerloods (Marine pilot); 5a. Those who have been entered into a register as meant in article 3 of the Professions in the individual healthcare Act (Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)) 5b. Those who practice a profession of which the education is mandated through article 34, section 1 and article 36a of the Professions in the individual healthcare Act (Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)). 6. Notaris (Civil Law Notary); 7. Kandidaat notaris (Junior Civil Law Notary); 8. Toegevoegd Notaris (Added Notary); 9. Gerechtsdeurwaarder (Court Bailiff); 10. Waarnemend gerechtsdeuraarder (Acting Court Bailiff); 11. Toegevoegd gerechtsdeurwaarder (Additional Court Bailiff); 12. Kandidaat gerechtsdeurwaarder (Junior Court Bailiff); 13. Registeraccountant (Registered Accountant); 14. Dierenarts (Veterinary Surgeon) 15. Zeevarende (Seafarer); 16. (Hoofd)bewaarder ((Head) Registrar); 17. Gemandateerd bewaarder Mandated Registrar; 18. Technisch Medewerker schapen (Ships Technician); 19. Inspecteur Scheepsregistraties (Ship Registration Inspector); 20. Belastingdeurwaarder (Government-appointed Tax Bailiff); 21. Rijksdeurwaarder (Government Bailiff). 22. Gemeentelijk Belastingdeurwaarder (Municipal Tax Bailiff)

RFC 3647	3.2.5 Authorization of the certificate holder
Number	3.2.5-pkio161
PKIo	The TSP MUST check that the FQDNs supplied by the subscriber (see definition in Part 4) included in a certificate are: - Actually in the name of the subscriber OR; - Authorized by the registered domain owner OR; - That the subscriber can show that it exercises (technical) control over the FQDN in question. This must be done for every FQDN that is included in a certificate. The TSP must limit itself to the methods as prescribed in the applicable version of the Baseline Requirements of the CABForum (chapter 3.2.2.4). The TSP must also adhere to the requirements in the EV Guidelines (EVCG) chapter 11. The verified data may be reused in a subsequent application, provided that it is not older than 13 months. If the data is older than 13 months, the above check must be carried out again. The TSP must also keep a record of the validation method (s) used for the included FQDNs per certificate. This verification may not be outsourced by the TSP to external (sub) contractors

RFC 3647	3.2.5 Authorization of the certificate holder
Number	3.2.5-pkio162
PKIo	If an FQDN is included in the certificate, the TSP MUST check whether the FQDNs supplied by the subscriber (see definition in Part 4), included in a certificate, are: - Actually in the name of the subscriber OR; - Authorized by the registered domain owner OR; - That the subscriber can show that it exercises (technical) control over the FQDN in question. The verified data may be reused in a subsequent application, provided that it is not older than 39 months. If the data is older than 39 months, the above check must be carried out again This must be done for every FQDN that is included in a certificate. The TSP must limit itself to: - the methods as prescribed in the applicable version of the Baseline Requirements of the CABForum (chapter 3.2.2.4) OR; - an alternative method approved in advance by the PA. The TSP must also keep a record of the validation method (s) used for the included FQDNs per certificate.

	This verification may not be outsourced by the TSP to external (sub) contractors

RFC 3647	3.2.5 Authorization of the certificate holder
Number	3.2.5-pkio170
PKIo	The TSP MUST check whether the FQDNs supplied by the subscriber (see definition in Part 4) or IP addresses, included in a certificate, are: - Actually in the name of the subscriber OR; - Authorized by the registered domain owner OR; - That the subscriber can show that he exercises (technical) control over the FQDN in question. This must be done for every FQDN that is included in a certificate. The TSP must limit itself to the methods as prescribed in the applicable version of the Baseline Requirements of the CABForum (chapter 3.2.2.4 for FQDNs and 3.2.2.5 for IP addresses). The foregoing also holds that "Any Other Method" from 3.2.2.5 may not be used (for both 3.2.2.4.8 and for IP addresses). The verified data may be reused in a subsequent application, provided that it is no older than 825 days. If the data is older than 825 days, the above check must be carried out again. The TSP must also keep a record of the validation method (s) used for the included FQDNs per certificate. This verification may not be outsourced by the TSP to external (sub) contractors

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

RFC 3647	4.1 Certificate Application
Number	4.1-pkio48

PKIo	Before issuing an EV SSL certificate, the TSP 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

RFC 3647	4.4.3 Notification of the certificate issuance by the CA to other entities
Number	4.4.3-pkio154
PKIo	The certificate SHALL contain at least the following number of SCTs:

Validity period of certificate	Number of SCT's
<15 months	2
>= 15, <= 27 months	3
> 27, <= 39 months	4
> 39 months	5

	The SCTs come from a log that is either qualified or awaiting qualification at the time of certificate issue. A qualified log is defined as a CT log that complies with Chromium's Certificate Transparency Log Policy and has been included by Chromium. At least one SCT comes from a log maintained by Google and one SCT from a log not maintained by Google. When recording more than 2 SCTs (see table), the requirement remains that at least 1 of the SCTs of the logs where the certificate is submitted to is from Google.
Comment	The above requirement is in line with the CT Policy adopted by Google for use in Chrome.

4.5 Key Pair and Certificate Usage

RFC 3647	4.5.2 Relying party public key and certificate usage
Number	4.5.2-pkio145
PKIo	When issuing Extended Validation certificates under this CP the TSP MUST adhere to the requirements in relation to certificate transparency.
Comment	See http://www.chromium.org/Home/chromium-security/root-ca-policy/EVCTPlan19Mar2014.pdf.

4.8 Compliance, audit and assessment

Contains no additional requirements

4.9 Certificate Revocation and Suspension

RFC 3647	4.9.1 Circumstances for revocation
Number	4.9.1-pkio52
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 TSP 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, SSCD, SUD or QSCD, is lost or suspected to be lost, if the key, SSCD, SUD or QSCD, is stolen or suspected to be stolen, or if the key or SSCD, SUD or QSCD is destroyed; • a subscriber does not fulfil its obligations outlined in this CP or the corresponding CPS of the TSP or the agreement that the TSP has entered into with the subscriber; • the TSP 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 TSP determines that the certificate has not been issued in line with this CP or the corresponding CPS of the TSP or the agreement that the TSP has entered into with the subscriber; • the TSP determines that information in the certificate is incorrect or misleading; • the TSP ceases its work and the CRL and OCSP services are not taken over by a different TSP. • 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 TSP used to sign certificates.

RFC 3647	4.9.3 Procedure for revocation request
Number	4.9.3-pkio57
PKIo	In any case, the TSP 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
PKIo	The TSP 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
PKIo	If there is an issuing subordinate CA under a TSP CA then: ▪ the TSP has to use an OCSP and a CRL to make available the certificate status information, relating to the issuing subordinate CA; ▪ the TSP 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
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
PKIo	The TSP 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
PKIo	The revocation management services of the TSP 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 EN 319 411-1 and the Baseline Requirements.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4.9.9-pkio67
PKIo	If the TSP supports the Online Certificate Status Protocol (OCSP), this must conform to IETF RFC 6960.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4.9.9-pkio68
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 TSP which holds an OCSP Signing certificate issued for this purpose by the TSP, 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
PKIo	If the TSP 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
PKIo	If the TSP supports OCSP, the TSP 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. In addition OCSP responses must contain the "nextUpdate" field in conformance to RFC6960.

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4.9.9-pkio152
PKIo	If the TSP supports OCSP, the OCSP response must have a minimum validity of 8 hours and a maximum validity of 7 calendar days. The next update must be available no later than half of the validity of an OCSP response.

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

Contains no additional requirements.

5.4 Audit Logging Procedures

RFC 3647	5.4.1 Types of events recorded
Number	5.4.1-pkio80

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 TSP 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 TSP 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
PKIo	The TSP 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
PKIo	The TSP 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 TSP services for subscribers, relying parties and third parties (including browser parties). The TSP 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 TSP 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 TSP'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 TSP sub CA
Number	6.1.1-pkio87
PKIo	The algorithm and the length of the cryptographic keys that are used for generating the keys for the TSP 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 119 312.
Comment	Although ETSI TS 119 312 outlines the recommended algorithms and key lengths, these are compulsory within the PKI for the government. Requests relating to the use of other algorithms have to be submitted, along with the reasoning behind this, to the PA of the PKI for the government.

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio88
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 EN 419 211 for QSCD's or CWA 14169 for SSCD's (transitional permission regime) "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
PKIo	The algorithm and the length of the cryptographic keys used by the TSP 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 119 312.
Comment	Although ETSI TS 119 312 outlines the recommended algorithms and key lengths, these are compulsory within the PKI for the government. Requests relating to the use of other algorithms have to be submitted, along with the reasoning behind this, to the PA of the PKI for the government.

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio90
PKIo	The generation of key pairs the certificate holder's key by the TSP is not allowed

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio91
PKIo	If the TSP 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 TSP 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 TSP's secured environment; c. When storing this key, the TSP MUST apply the P12 standard, where the privacy mode and the integrity mode are used. To this end, the TSP MAY encrypt the P12 file with a personal PKI certificate of the subscriber/certificate manager. If this is not available, the TSP MUST use a password supplied by the subscriber. This password MUST be supplied by the subscriber through the TSP'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 TSP 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 119 312); 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 certified courier, or by

	a representative of the TSP in a seal bag. The courier must be certified in accordance with the requirements dictated in part 2 under paragraph 2.2 for the specific service applicable here. h. If the P12 file is sent over a SSL/TLS secured network the TSP 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 TSP 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
PKIo	A TSP 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
PKIo	Instead of the TSP generating the keys, the certificate manager MAY generate the keys of the services authenticity and encryption certificates in a SUD using PKCS#10 to deliver the CSR to the TSP for signing, under the following conditions: - The agreement between the TSP 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 for a Secure signature-creation devices or EN 419 211 for Qualified signature-creation devices "EAL 4+" or comparable security criteria. With the request the subscriber must prove that the secure device used for key generation conforms to CWA 14169 for a Secure signature-creation devices or EN 419 211 for Qualified signature-creation devices EAL 4+"" or comparable security criteria. The TSP 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 TSP must stipulate that the TSP has the right to perform an audit on the measures taken (conform 6.2.11-pkio107)

	- The agreement between the subscriber and the TSP 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	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio153
PKIo	Subject key generation of a qualified digital seal certificate for the use of mass automated signing of standardised data is allowed in ETSI 319 411-2. ETSI does not stipulate the applicable security requirements. Subject key generation within PKIoverheid is possible under the following conditions: - The contract between the TSP and the subscriber contains an assertion that the subscriber will generate, store and use the private key on a qualified device for electronic signatures – such as a HSM – which meets the requirements of {7} CWA 14169 Secure signature-creation devices or EN 419 211 for Qualified signature-creation devices "EAL 4+" or equivalent security criteria such as FIPS 140-2 level 3. The subscriber shall hand over evidence to this effect with the certificate request by submitting the certification of the secure device and, if applicable, a screenshot of the settings of the secure device on FIPS140-2 level 3. - The contract between the TSP and the subscriber contains an assertion in which the subscriber states that the private key (and associated activation data, such as a PIN code) related to the public key is generated in the qualified device and is kept secret and protected in future. The subscriber shall hand over evidence to this effect of the PKI ceremony script which is used during the implementation of the qualified device for electronic signatures and the generation of the key pair. - The TSP is present during the PKI ceremony for the commissioning of the qualified device for electronic signatures and the generation of the key pair. This enables the TSP to check the effectiveness of the security measures. - During registration the Subscriber submits a written statement of demonstrably satisfying the requirements and/or conditions placed either on the use of the qualified device for electronic signatures, or by the certification of the device on the environment in which it is administrated and the administration itself. - The Subscriber submits a written statement that the certificate holder has explicitly mandated the system administrators of the qualified device for electronic signatures for the administration and that access to this device is always subject to dual control.
Comment	If the de TSP generates the key pair and the certificate and distributes these to the subscriber on a secure device it is not necessary to be present at the ceremony.

RFC 3647	6.1.2 Private key and SSCD or QSCD delivery to certificate holder
Number	6.1.2-pkio94
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.

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
PKIo	The authorized persons who can gain access to the private key of the confidentiality certificate held in Escrow by the TSP (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
PKIo	The TSP 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
PKIo	If the TSP keeps the private key of the confidentiality certificate in Escrow, the TSP 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 EN 319 411-1 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 TSP has to submit.

RFC 3647	6.2.11 Cryptographic module rating
Number	6.2.11-pkio104
PKIo	Secure devices issued or recommended by the TSP for creating electronic signatures (SSCDs or QSCDs) have to fulfil the requirements laid down in document CWA 14169 "Secure signature-creation devices or EN 419 211 for Qualified 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 or QSCD 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-pkio105
PKIo	Instead of demonstrating compliance with CWA 14169 (for SSCD's or SUD's) or EN 419 211 (for QSCD's), TSPs can issue or recommend SSCDs, SUDs or QSCDs 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
PKIo	The concurrence of SSCDs or QSCDs with the requirements outlined in PKIo requirement no. 6.2.11-pkio104 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
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 TSP must state that the TSP 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.

RFC 3647	6.2.11 Cryptographic module rating
Number	6.2.11-pkio125
PKIo	Secure devices issued or recommended by the TSP for storage of keys (SUDs) have to fulfil the requirements laid down in document CWA 14169 "Secure signature-creation devices "EAL 4+""

6.3 Other Aspects of Key Pair Management

RFC 3647	6.3.1 Public key archival
Number	6.3.1-pkio108
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
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.

RFC 3647	6.3.2 Certificate operational periods and key pair usage periods
Number	6.3.2-pkio111
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 TSPs 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
PKIo	The TSP attaches activation data to the use of a SUD, SSCD or QSCD, 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 TSPs 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
PKIo	An unlocking code can only be used if the TSP 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

RFC 3647	7.1 Certificate profile
Number	7.1-pkio149
PKIo	The certificate extension Extended Key Usage MUST be present, MUST NOT be marked "critical", and MUST contain at least the following KeyPurposIds: For an authenticity certificate: client Authentication =1.3.6.1.5.5.7.3.2 document Signing =1.3.6.1.4.1.311.10.3.12 emailProtection = 1.3.6.1.5.5.7.3.4 For a signature certificate: document Signing =1.3.6.1.4.1.311.10.3.12 emailProtection = 1.3.6.1.5.5.7.3.4 (mandatory for G3, optional for G2) For an confidentiality certificate: emailProtection =1.3.6.1.5.5.7.3.4 Encrypting File System =1.3.6.1.4.1.311.10.3.4 The KeyPurposeId id-kp-serverAuth MUST NOT be present and the KeyPurposeId id-kp-codeSigning MUST NOT be present. Specifically for G2 certificates any other KeyPurposeId defined in an open or accepted standard corresponding to the key usage as indicated by the KeyUsage extension MAY be present. In the G3 and following generations this extension MAY NOT be present.

RFC 3647	7.1 Certificate profile
Number	7.1-pkio150
PKIo	The certificate extension Extended Key Usage MUST be present, MUST NOT be marked "critical", and MUST contain at least the following KeyPurposIds: For a services authentication certificate: client Authentication =1.3.6.1.5.5.7.3.2 document Signing =1.3.6.1.4.1.311.10.3.12 For a services confidentiality certificate: emailProtection =1.3.6.1.5.5.7.3.4 Encrypting File System =1.3.6.1.4.1.311.10.3.4 emailProtection = 1.3.6.1.5.5.7.3.4 For a seal certificate document Signing =1.3.6.1.4.1.311.10.3.12

	emailProtection = 1.3.6.1.5.5.7.3.4 The KeyPurposeId id-kp-serverAuth MUST NOT be present, the KeyPurposeId id-kp-codeSigning MUST NOT be present, the KeyPurposeId AnyextendedKeyusage MUST NOT be present and any KeyPurposeId solely intended to identify a service based on its FQDN MUST NOT be present. Specifically for G2 certificates any other KeyPurposeId defined in an open or accepted standard corresponding to the key usage as indicated by the KeyUsage extension MAY be present. In the G3 and following generations this extension MAY NOT be present.

RFC 3647	7.1 Certificate profile
Number	7.1-pkio151
PKIo	The certificate extension Extended Key Usage MUST be present, MUST NOT be marked "critical", and MUST contain at least the following KeyPurposIds: For an Autonomous Devices – authenticity certificate: Client Authentication =1.3.6.1.5.5.7.3.2 For an Autonomous Devices – confidentiality certificate: emailProtection =1.3.6.1.5.5.7.3.4 Encrypting File System =1.3.6.1.4.1.311.10.3.4 For an Autonomous Devices – combination certificate: client Authentication =1.3.6.1.5.5.7.3.2 document Signing =1.3.6.1.4.1.311.10.3.12 emailProtection =1.3.6.1.5.5.7.3.4 Encrypting File System =1.3.6.1.4.1.311.10.3.4 The KeyPurposeId id-kp-serverAuth MUST NOT be present, the KeyPurposeId id-kp-codeSigning MUST NOT be present, the KeyPurposeId AnyextendedKeyusage MUST NOT be present and any KeyPurposeId solely intended to identify a service based on its FQDN MUST NOT be present. Specifically for G2 certificates any other KeyPurposeId defined in an open or accepted standard corresponding to the key usage as indicated by the KeyUsage extension MAY be present. In the G3 and following generations this extension MAY NOT be present.

RFC 3647	7.1 Certificate profiles
Number	7.1-pkio163
PKIo	The Subject.CommonName field (if included) MUST contain a FQDN (Fully Qualified Domain Name). An FQDN MUST also appear in the SubjectAltName.DNsName field. An IP address MUST also appear in the SubjectAltName.iPAdress field.

	A server certificate MAY contain multiple FQDNs from different domains on condition that these domains are registered in the name of the same subscriber or is authorization by the same subscriber. This means that a TSP cannot combine FQDNs in one certificate that are both from different domains and are registered in the name of different owners. The following is NOT allowed to be included in the Subject.Commonname field, SubjectAltName.iPAdress or the SubjectAltName.DNname field - wildcard FQDNs - local domain names, - private IP addresses - internationalized domain names (IDNs) - null characters \ 0 - generic TopLevel Domain (gTLD) - Country code TopLevelDomein (ccTLD)

RFC 3647	7.1 Certificate profiles
Number	7.1-pkio164
PKIo	The Subject.CommonName field MUST contain a FQDN (Fully Qualified Domain Name). An FQDN MUST also appear in the SubjectAltName.DNsName field. An Extended Validation certificate MAY contain several FQDNs. Every FQDN MUST fall under the same main domain. (e.g., www.logius.nl, application.logius.nl, secure.logius.nl etc.). The following is NOT permitted to include in the Subject.Commonname field or the SubjectAltName.DNname field - wildcard FQDNs - local domain names, - private IP addresses - internationalized domain names (IDNs) - null characters \ 0 - generic TopLevel Domain (gTLD) - Country code TopLevelDomein (ccTLD)

RFC 3647	7.1 Certificate profiles
Number	7.1-pkio165
PKIo	The Subject.CommonName SHOULD contain an FQDN (Fully Qualified Domain Name) or an IP address. An FQDN must also appear in the SubjectAltName.DNsName field. An IP address must also appear in the SubjectAltName.iPAdress field. A server certificate may contain multiple FQDNs from different domains on condition that these domains are registered in the name of the same subscriber or are authorized by the same subscriber. This means that a TSP cannot combine FQDNs in one certificate that are both from different domains and are registered in the name of different owners. If it is not possible or desirable to include an FQDN in the subject.commonName field, but the field is necessary for the server to function properly, it is allowed to use the function of an organizational entity or the name with which the service, device or system is indicated. The following is not permitted to be included in the Subject.Commonname field, SubjectAltName.iPadres or the SubjectAltName.DNname field - wildcard FQDNs - local domain names,

	- private IP addresses - internationalized domain names (IDNs) - null characters \ 0 - generic TopLevel Domain (gTLD) - Country code TopLevelDomein (ccTLD)

RFC 3647	7.1 Certificate profiles
Number	7.1-pkio171
PKIo	From ETSI TS 119 312, the TSP MUST choose from 1 of the following options for the Signature field in a certificate: • sha256WithRSAEncryption: 1.2.840.113549.1.1.11 (OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }) • ecdsa-with-SHA256: 1.2.840.10045.4.3.2 {OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }}) • sha384WithRSAEncryption : 1.2.840.113549.1.1.12 {OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 } • ecdsa-with-SHA384:1.2.840.10045.4.3.3 {OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

RFC 3647	7.1 Certificate profiles
Nummer	7.1-pkio172
PKIo	The Authority Information Access field must contain the following entries: Access Method = - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1). This field must contain the URI where the OCSP responder can be found that is authorized by the issuing CA of the certificate to be checked; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2). This field must contain the URI where the certificate of the issuing CA can be found.

RFC 3647	7.1 Certificate profiles
Number	7.1-pkio173
PKIo	All end-user certificates must contain at least 64 bits of unpredictable random data generated by a Cryptographically Secure Pseudorandom Number Generator (CSPRNG).

RFC 3647	7.1 Certificate profiles
Number	7.1-pkio177
PKIo	All end-user certificates must contain at least 64 bits of unpredictable random data, preferably generated by a Cryptographically Secure Pseudo-random Number Generator (CSPRNG).

7.2 CRL Profile

Contains no additional requirements.

7.3 OCSP Profile

RFC 3647	7.3 OCSP profile
Number	7.3-pkio123
PKIo	If the TSP supports the Online Certificate Status Protocol (OCSP), the TSP 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

RFC 3647	8.6 Demonstration of BR conformity
Nummer	8.6-pkio158
	The PA informs TSPs about relevant changes to the Baseline Requirements and / or the Extended Validation Guidelines. TSPs must prove that they comply with stated changes by submitting a signed statement from or on behalf of the authorized director to the PA before the effective date of the change in question. The PA provides a template for this. If a TSP cannot comply on time or does not submit a signed declaration on time, the PA reserves the right to (temporarily) suspend certificate issuance at the relevant TSP until the TSP can (demonstrably) comply with the stated change.

9 Other Business and Legal Matters

9.2 Financial Responsibility

RFC 3647	9.2. Financial Responsibility
Number	9.2-pkio124
PKIo	By means, for example, of insurance or its financial position, the TSP 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 TSP, which is in line with the current situation. When TSPs 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 TSPs
Number	9.6.1-pkio127
PKIo	In the agreement between the TSP and the subscriber, a clause (a clause as specified in article 6:253 of the Civil Code) will be included in which the TSP champions the interests of a third party relying on the certificate. This clause addresses a liability of the TSP 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 TSPs
Number	9.6.1-pkio128
PKIo	In the agreement between the TSP and the subscriber, a clause (a clause as specified in article 6:253 of the Civil Code) will be included in which the TSP champions the interests of a third party relying on the certificate. This clause

	addresses a liability of the TSP 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 TSPs
Number	9.6.1-pkio129
PKIo	In the agreement between the TSP and the subscriber, a clause (a clause as specified in article 6:253 of the Civil Code) will be included in which the TSP champions the interests of a third party relying on the certificate. This clause addresses a liability of the TSP 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 TSPs
Number	9.6.1-pkio142
PKIo	[OID 2.16.528.1.1003.1.2.6.2] In the agreement between the TSP and the subscriber, a clause (a clause as specified in article 6:253 of the Civil Code) will be included in which the TSP champions the interests of a third party relying on the certificate. This clause addresses a liability of the TSP 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 TSPs
Number	9.6.1-pkio131
PKIo	The TSP 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 TSP 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 TSPs
Number	9.6.1-pkio132
PKIo	The TSP 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
PKIo	Within the scope of certificates as mentioned in paragraph 1.4 in this CP the TSP is not allowed to place restrictions on the use of certificates.

RFC 3647	9.8 Limitations of Liability
Number	9.8-pkio134
PKIo	Within the scope of certificates as mentioned in paragraph 1.4 in this CP the TSP is not allowed to place restrictions on the use of EV SSL certificates.

RFC 3647	9.8 Limitations of Liability
Number	9.8-pkio143
PKIo	The TSP 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.

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
PKIo	The TSP 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
PKIo	The TSP 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
PKIo	The TSP 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.

10 Revisions

10.1 Amendments

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

10.2 Amendments from version 4.5 naar versie 4.7

10.2.1 Editorial

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

10.3 Amendments from version 4.0 to 4.5

10.3.1 Editorial

- Replaced the term CSP (Certificate Service Provider) with TSP (Trust Service Provider) in line with eIDAS directive.

10.4 Amendments from version 3.7 to 4.0

10.4.1 New

- None.

10.4.2 Modifications

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

10.4.3 Editorial

- None