Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3: Additional Requirements PKIoverheid

Version	4.9
Date	July 1, 2021

Publishers imprint

Version number	4.9
Contact person	Policy Authority of PKIoverheid

Organization	Logius

Street address
Wilhelmina van Pruisenweg 52

Postal address
Postbus 96810
2509 JE DEN HAAG

T 0900-555 4555
servicecentrum@logius.nl

Contents

1. INTRODUCTION

1.1 Overview

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

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

1.1.1 Design of the Certificate Policies

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

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

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

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

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

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

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

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

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

1.2 Document name and identification

1.2.1 Revisions

1.2.1.1 Version 3.7 to 4.0

New

None.

Modifications

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

Editorial

None.

1.2.1.2 Version 4.0 to 4.5

New

None.

Modifications

None.

Editorial

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

1.2.1.3 Version 4.5 to 4.7

New

None.

Modifications

None.

Editorial

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

1.2.1.4 Version 4.7 to 4.8

New

None.

Modifications

- Changes in serial number requirements in requirement 7.1-pkio173;
- Changes in serial number requirements in requirement 7.1-pkio177.

Editorial

None.

1.2.1.5 Version 4.8 to 4.9

New

None.

Modifications

- Requirement 6.1.1-pkio87 has been removed (effective date immediately after publication PoR 4.9).

Editorial

None.

1.2.2 Relevant dates

Version	Date	Description
4.0	12-2014	Ratified by the Ministry of the Interior and Kingdom Relations December 2014
4.1	07-2015	Ratified by the Ministry of the Interior and Kingdom Relations July 2015
4.2	01-2016	Ratified by the Ministry of the Interior and Kingdom Relations January 2016
4.3	07-2016	Ratified by the Ministry of the Interior and Kingdom Relations July 2016
4.4	02-2017	Ratified by the Ministry of the Interior and Kingdom Relations February 2017
4.5	07-2017	Ratified by the Ministry of the Interior and Kingdom Relations July 2017
4.6	01-2018	Ratified by the Ministry of the Interior and Kingdom Relations January 2018
4.7	01-2019	Ratified by the Ministry of the Interior and Kingdom Relations January 2019

4.8	02-2020	Ratified by the Ministry of the Interior and Kingdom Relations February 2020
4.9	02-2021	Ratified by the Ministry of the Interior and Kingdom Relations February 2021

1.3 PKI participants

1.3.1 Certification authorities

In this document the distinction is made between the term Certification Authority (CA) and Trust Service Provider. In international usage, "CA" is an umbrella term that refers to all entities authorized to issue, manage, revoke, and renew certificates. This can apply to the actual CA certificate as well as the organization. In this CP, the organization which holds a CA is refered to as a TSP. The term CA is used to refer to the infrastructure and keymaterial from which a TSP issues and signs certificates.

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

1.3.2 Registration authorities

Registration Authorities (RAs) are entities that approve and authenticate requests to obtain, renew, or revoke certificates. RA tasks within PKIoverheid are as follows:

- Identify and authenticate subscribers
- Verify that subscribers are authorizated to request or revoke certificates
- Approving individuals, entities, and/or devices that are to be included in a certificate.

After performing the tasks listed above they will authorize and/or request a TSP to issue, renew, or revoke a certificate.

1.3.3 Subscribers

Subscribers within the PKIoverheid hierarchy are defined as organizations or individuals (working for organizations) to whom a TSP has issued (a) PKIoverheid TRIAL certificate(s). Before issuance of the first certificate the subscriber has to agree to a Subscriber agreement supplied by the TSP. Requirements for this subscriber agreement are listed in relevant sections of this CP.

1.3.4 Relying parties

No stipulation.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

[OID 2.16.528.1.1003.1.2.5.1]

Authenticity certificates, that are issued under this CP, can be used to reliably identify and authenticate persons, organizations and resources electronically. This concerns both the mutual identification of people and identification between people and computerized devices.

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

[OID 2.16.528.1.1003.1.2.5.2]

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

[OID 2.16.528.1.1003.1.2.5.3]

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

1.4.2 Prohibited certificate uses

Refer to Programme of Requirements part 3 Basic Requirements.

1.5 Policy administration

1.5.1 Organization administering the document

The Ministry of Interior and Kingdom Relations (BZK) is responsible for this CPS. BZK has delegated this responsibility to Logius, including approval of changes of this document.

1.5.2 Contact person

Policy Authority PKIoverheid
Wilhelmina van Pruisenweg 52
Postbus 96810
2509 JE DEN HAAG
http://www.logius.nl/pkioverheid
servicecentrum@logius.nl[1]

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CP approval procedures

The PA PKIoverheid reserves the right to amend this CP. Changes are applicable from the date that is listed in section *1.2.2. Relevant dates*. The management of Logius is responsible for following the procedures as listed in section *9.12 Amendments* and final approval of this CP.

1 mailto:servicecentrum@logius.nl

1.6 Definitions and acronyms

1.6.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”,“SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in these Requirements MUST be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

No stipulation.

2.2 Publication of certification information

2.2-pkio166 —

Description	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 the SubjectAltName.iPAdress field with it a reference to the correct chapter number of the Baseline Requirements.
Comment	-

2.2-pkio167 —

Description	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.
Comment	-

2.2-pkio168 —

Description	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.
Comment	-

2.2-pkio191 —

Description	The CPS of the TSP MUST follow the layout according to RFC 3647. All sections and subsections as defined in RFC3647 MUST be included in the CPS. Empty passages are not allowed. If there is no further requirement or explanation from a TSP for that paragraph, the text "No stipulation" MUST be included. Additional sections may be included, as long as they come after the sections and subsections defined by RFC 3647 and therefore do not change the RFC numbering.
Comment	-

2.2-pkio3 —

Description	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.

Comment	-

2.3 Time or frequency of publication

No stipulation.

2.4 Access controls on repositories

No stipulation.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

No stipulation.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

3.1.3-pkio11 —

Description	Pseudonyms MUST NOT be used in certificates.
Comment	-

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

3.2.1-pkio13 —

Description	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.
Comment	-

3.2.2 Authentication of organization identity

3.2.2-pkio14 —

Description	When issuing organization-linked certificates the TSP has to verify that the subscriber is an existing organization.
Comment	-

3.2.2-pkio144 —

Description	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
Comment	-

3.2.2-pkio147 —

Description	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.
Comment	-

3.2.2-pkio16 —

Description	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.
Comment	-

3.2.2-pkio186 —

Description	If an organization changes its name but the underlying registration number (e.g. HRN) remains the same, then the subscriber DOES NOT have to go through the subscription registration again. If the organization name remains the same but the underlying registration number changes, then the TSP MUST perform the subscription registration again. In both cases, the existing certificate must be withdrawn because the data in the certificate no longer conforms to the originally validated data.
Comment	-

3.2.2-pkio4 —

Description	The TSP has to verify that the subscriber is an existing organization.
Comment	-

3.2.3 Authentication of individual identity

3.2.3-pkio169 —

Description	For certificates that are suitable for signing and / or encrypting 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 state clearly in its CPS which procedures have been implemented to confirm the above. In these procedures, the TSP MUST perform validation of the domain part (@domain.com[2]) itself. This check MUST NOT be performed by third parties.
Comment	-

3.2.3-pkio21 —

Description	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).
Comment	-

3.2.3-pkio22 —

2 http://domain.com

Description	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.
Comment	-

3.2.3-pkio24 —

Description	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.

3.2.3-pkio26 —

Description	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.
Comment	-

3.2.3-pkio27 —

Description	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.
Comment	-

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

3.2.5-pkio146 —

Description	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[3], account.twitter.com[4]. 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.

3.2.5-pkio160 —

3 http://twitter.nl
4 http://account.twitter.com

Description	The restrictive list of recognized professions for which professional certificates can be issued is as follows: • Accountant-Administratieconsulent (Accountant-Administration Officer); • Advocaat (Lawyer); • Octrooigemachtigde (Patent Agent); • Registerloods (Marine pilot); • 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)); • 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)); • Notaris (Civil Law Notary); • Kandidaat notaris (Junior Civil Law Notary); • Toegevoegd Notaris (Added Notary); • Gerechtsdeurwaarder (Court Bailiff); • Waarnemend gerechtsdeuraarder (Acting Court Bailiff); • Toegevoegd gerechtsdeurwaarder (Additional Court Bailiff); • Kandidaat gerechtsdeurwaarder (Junior Court Bailiff); • Registeraccountant (Registered Accountant); • Dierenarts (Veterinary Surgeon); • Zeevarende (Seafarer); • (Hoofd)bewaarder ((Head) Registrar); • Gemandateerd bewaarder Mandated Registrar; • Technisch Medewerker schepen (Ships Technician); • Inspecteur Scheepsregistraties (Ship Registration Inspector); • Belastingdeurwaarder (Government-appointed Tax Bailiff); • Rijksdeurwaarder (Government Bailiff); • Gemeentelijk Belastingdeurwaarder (Municipal Tax Bailiff).
Comment	-

3.2.5-pkio161 —

Description	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.
Comment	-

3.2.5-pkio162 —

Description	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.
Comment	-

3.2.5-pkio170 —

Description	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.
Comment	-

3.2.5-pkio29 —

Description	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. **d**. or an appointment by a municipal official or mayor (only in case of municipal tax bailiff). Understood to be meant by valid proof is proof that has not expired or that has not (temporarily or provisionally) been revoked. PoR requirement 3.2.5-pkio160 contains a limitative list of the professions referred to under a, b, and c. In the reference matrix in appendix B there is a reference to all requirements that relate to paragraph 3.2.3.

3.2.5-pkio30 —

Description	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.

3.2.5-pkio31 —

Description	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: - 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.

3.2.5-pkio32 —

Description	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.
Comment	-

3.2.5-pkio33 —

Description	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.
Comment	-

3.2.5-pkio34 —

Description	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.
Comment	-

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

No stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1-pkio47 —

Description	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.
Comment	-

4.1-pkio48 —

Description	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;
	  • general telephone number.
	• certificate manager's name.

Comment	-

4.1.1 Who can submit a certificate application

No stipulation.

4.1.2 Enrollment process and responsibilities

No stipulation.

4.2 Certificate application processing

4.2-pkio179 —

Description	A CA must be able to replace its total population of outstanding, still valid certificates within 5 days, provided the subscriber cooperates in a timely manner.

Comment	With "cooperation by the subscriber", the PA means the provision of any and all data required by the TSP to process and deliver a certificate (request) such as domain validation and Certificate Signing Request (CSR). To ensure that a subscriber is able to provide such data in a timely manner, the TSP may, for example, take the following measures: • Setting up a customer portal that facilitates and speeds up the process; • Periodically checking (domain) validation so that data is "fresh" at the time it is needed; • (Partially) automating the certificate issuing process via an API (e.g. RFC8555).

4.2.1 Performing identification and authentication functions

No stipulation.

4.2.2 Approval or rejection of certificate applications

No stipulation.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

No stipulation.

4.3.2 Notification to subscriber by the CA of issuance of Certificate

No stipulation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other Entities

4.4.3-pkio154 —

<table>
<tr><td>Description</td><td>The certificate SHALL contain at least the following number of SCTs:

<table><tr><td>Validity period of certificate</td><td>Number of SCT’s</td></tr><tr><td><15 months</td><td>2</td></tr><tr><td>>= 15, <= 27 months</td><td>3</td></tr><tr><td>> 27, <= 39 months</td><td>4</td></tr><tr><td>> 39 months</td><td>5</td></tr></table>
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.</td></tr>
<tr><td>Comment</td><td>The above requirement is in line with the CT Policy adopted by Google for use in Chrome.</td></tr>
</table>

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

No stipulation.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1-pkio192 —

Description	Certificates will be revoked when: • the subscriber indicates that the original request for a certificate was not allowed and the subscriber does not grant permission retroactively; • the TSP has sufficient evidence that the subscriber's private key (associated with the corresponding certificate) has been compromised or there is a suspicion of compromise, inherent security weakness, or that the certificate has been misused in another way . A key is considered compromised in the event of unauthorized access or suspected unauthorized access to the private key, lost or presumably lost private key, SSCD, SUD or QSCD, stolen or presumably stolen key, SSCD, SUD or QSCD or destroyed key, SSCD, SUD or QSCD if applicable; • a subscriber does not fulfill his obligations as set out in this CP or the corresponding CPS of the TSP or the agreement that the TSP has with the subscriber; • the TSP is informed or otherwise becomes aware of a material change in the information contained in the certificate. An example of this is: change of the name of the certificate holder (service); • the TSP determines that the certificate has not been issued in accordance with this CP or the associated CPS of the TSP or the agreement that the TSP has with the subscriber; • the TSP determines that information in the certificate is incorrect or misleading; • the TSP ceases its activities and the CRL and OCSP services are not continued by another TSP; • the PA of PKIoverheid determines that the technical content of the certificate entails an irresponsible risk for subscribers, relying parties and third parties (e.g. browser parties); • one of the events occurs, as described in chapter 6.2 of the Mozilla Root Store Policy[5].
Comment	-

4.9.1-pkio193 —

5 https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

Description	Certificates will be revoked when: • the subscriber indicates that the original request for a certificate was not allowed and the subscriber does not grant permission retroactively; • the TSP has sufficient evidence that the subscriber's private key (associated with the corresponding certificate) has been compromised or there is a suspicion of compromise, or there is an inherent security weakness, or that the certificate has been misused in another way . A key is considered compromised in the event of unauthorized access or suspected unauthorized access to the private key, lost or presumably lost private key, SSCD, SUD or QSCD, stolen or presumably stolen key, SSCD, SUD or QSCD or destroyed key, SSCD, SUD or QSCD if applicable; • a subscriber does not meet his obligations as set out in this CP or the corresponding CPS of the TSP or the agreement that the TSP has concluded with the subscriber; • the TSP is informed or otherwise becomes aware of a material change in the information contained in the certificate. An example of this is: change of the name of the certificate holder (service); • the TSP determines that the certificate has not been issued in accordance with this CP or the associated CPS of the TSP or the agreement that the TSP has concluded with the subscriber; • the TSP determines that information in the certificate is incorrect or misleading; • the TSP ceases its activities and the CRL and OCSP services are not continued by another TSP; • the PA of PKIoverheid determines that the technical content of the certificate entails an irresponsible risk for subscribers, relying parties and third parties (e.g. browser parties). • one of the events occurs, as described in chapter 6.2 of the Mozilla Root Store Policy[6]. The TSP must adhere to the revocation deadlines as stated in chapter 6.1 of the previous document.
Comment	-

4.9.1-pkio52 —

6 https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

Description	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.

4.9.2 Who can request revocation

No stipulation.

4.9.3 Procedure for revocation request

4.9.3-pkio57 —

Description	In any case, the TSP has to use a CRL to make the certificate status information available.
Comment	-

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

Content by label

There is no content with the specified labels

4.9.6 Revocation checking requirement for relying parties

No stipulation.

4.9.7 CRL issuance frequency (if applicable)

4.9.7-pkio65 —

Description	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.
Comment	-

4.9.8 Maximum latency for CRLs (if applicable)

No stipulation.

4.9.9 On-line revocation/status checking availability

4.9.9-pkio152 —

Description	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.
Comment	-

4.9.9-pkio66 —

Description	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: • 1.1-pkio10 (basic requirement) • 9.5-pkio61 (basic requirement) • 9.9-pkio67 • 9.9-pkio68 • 9.5-pkio69 (basic requirement) • 9.9-pkio70 • 9.9-pkio71 • 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.

4.9.9-pkio67 —

Description	If the TSP supports the Online Certificate Status Protocol (OCSP), this must conform to IETF RFC 6960.
Comment	-

4.9.9-pkio68 —

Description	To detail the provisions of IETF RFC 6960, 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.
Comment	-

4.9.9-pkio70 —

Description	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.
Comment	-

4.9.9-pkio71 —

Description	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.
Comment	-

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements related to key compromise

No stipulation.

4.9.13 Circumstances for suspension

No stipulation.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

No stipulation.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

No stipulation.

5.1.2 Physical access

No stipulation.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

No stipulation.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

No stipulation.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

No stipulation.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No stipulation.

5.4 Audit logging procedures

5.4.1 Types of events recorded

5.4.1-pkio80 —

Description	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.

5.4.2 Frequency of processing log

No stipulation.

5.4.3 Retention period for audit log

No stipulation.

5.4.4 Protection of audit log

No stipulation.

5.4.5 Audit log backup procedures

No stipulation.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

5.5.1-pkio82 —

Description	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.
Comment	-

5.5.2 Retention period for archive

No stipulation.

5.5.3 Protection of archive

No stipulation.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

No stipulation.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

No stipulation.

5.7.2 Computing resources, software, and_or data are corrupted

No stipulation.

5.7.3 Entity private key compromise procedures

No stipulation.

5.7.4 Business continuity capabilities after a disaster

5.7.4-pkio86 —

Description	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.
Comment	-

5.8 CA or RA termination

No stipulation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1-pkio153 —

Description	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.

6.1.1-pkio88 —

Description	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.
Comment	-

6.1.1-pkio89 —

Description	The algorithm and length of the cryptographic keys that the TSP uses to generate the keys of certificate holders must meet the requirements set in the list of cryptographic algorithms and key lengths, as defined in ETSI TS 119 312. In addition, the TSP must also follow the requirements described in Chapters 5.1 and 5.1.1 of the most current Mozilla Root Store Policy. The use of RSA-PSS is permitted, but is not recommended.
Comment	Although ETSI TS 119 312 outlines the recommended algorithms and key lengths, these are compulsory within the PKI for the government. Requests relating to the use of other algorithms have to be submitted, along with the reasoning behind this, to the PA of the PKI for the government.

6.1.1-pkio90 —

Description	The generation of key pairs the certificate holder's key by the TSP is not allowed
Comment	-

6.1.1-pkio91 —

Description	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: • The TSP MUST generate the private key for the subscriber in the secured environment to which the PKIoverheid PoR and the corresponding audit apply; • 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 119 312) within the TSP's secured environment; • 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; • 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; • 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); • 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). • 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. • 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.

6.1.1-pkio92 —

Description	A TSP within PKIoverheid is not allowed to issue code signing certificates.
Comment	-

6.1.1-pkio93 —

Description	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.
Comment	-

6.1.2 Private key delivery to subscriber

6.1.2-pkio94 —

Description	[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 ETSI EN 319 411-1 SDP 6.3.3-09, but has been integrated because this requirement only applies to signature and authenticity certificates.

6.1.3 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to relying parties

No stipulation.

6.1.5 Key sizes

No stipulation.

6.1.6 Public key parameters generation and quality checking

No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

No stipulation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

No stipulation.

6.2.2 Private key (n out of m) multi-person control

No stipulation.

6.2.3 Private key escrow

6.2.3-pkio100 —

Description	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.
Comment	-

6.2.3-pkio99 —

Description	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).
Comment	-

6.2.4 Private key backup

No stipulation.

6.2.5 Private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

No stipulation.

6.2.8 Method of activating private key

No stipulation.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

No stipulation.

6.2.11 Cryptographic Module Rating

6.2.11-pkio104 —

Description	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.

6.2.11-pkio105 —

Description	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.
Comment	-

6.2.11-pkio106 —

Description	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.
Comment	-

6.2.11-pkio107 —

Description	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.

6.2.11-pkio125 —

Description	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+""
Comment	-

6.3 Other aspects of key pair management

6.3.1 Public key archival

6.3.1-pkio108 —

Description	[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.

6.3.2 Certificate operational periods and key pair usage periods

6.3.2-pkio109 —

Description	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	-

6.3.2-pkio111 —

Description	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.

6.3.2-pkio178 —

Description	Private keys used by a certificate holder and issued under the responsibility of this CP MAY NOT be used for more than two (2) years. Certificates issued under the responsibility of this CP MAY NOT be valid for more than 397 days. In the event that a certificate is replaced following revocation under section 4.9.1.1 of the Baseline Requirements, the private key of a certificate MAY NOT be reused, except in the case of revocation under point 7 (certificate not issued in accordance with BR or CP/CPS of TSP).
Comment	-

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.1-pkio112 —

Description	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.

6.4.1-pkio113 —

Description	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.
Comment	-

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

No stipulation.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

6.7.1 Network security controls (duplicate)

No stipulation.

6.8 Time-stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1-pkio149 —

Description	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. The above should take into account the EKUs included in the issuing TSP CA. If the issuing TSP CA is not provided with the mandatory EKUs stated above, these MAY NOT be included in the end-user certificate.
Comment	-

7.1-pkio150 —

Description	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 • emailProtection =1.3.6.1.5.5.7.3.4 For a services confidentiality certificate: • 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. The above should take into account the EKUs included in the issuing TSP CA. If the issuing TSP CA is not provided with the mandatory EKUs stated above, these MAY NOT be included in the end-user certificate.
Comment	-

7.1-pkio151 —

Description	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. The above should take into account the EKUs included in the issuing TSP CA. If the issuing TSP CA is not provided with the mandatory EKUs stated above, these MAY NOT be included in the end-user certificate.
Comment	-

7.1-pkio163 —

Description	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)
Comment	-

7.1-pkio164 —

Description	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[7], application.logius.nl[8], secure.logius.nl[9] 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)
Comment	-

7.1-pkio165 —

7 http://www.logius.nl
8 http://application.logius.nl
9 http://secure.logius.nl

Description	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)
Comment	-

7.1-pkio171 —

Description	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 }
Comment	A TSP MUST limit itself to the signature algorithms as defined in chapter 5.1 (and subsections) of the Mozilla Root Store Policy. The use of RSA-PSS is permitted, but is not recommended.

7.1-pkio172 —

Description	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.
Comment	-

7.1-pkio173 —

Description	The serial number of all end-user certificates must meet the following requirements: a. The value of the serial number MUST NOT be 0 (zero); b. The value of the serial number MUST NOT be negative; c. The value of the serial number MUST be unique within the population of end-user certificates issued under an issuing TSP CA; d. The serial number MUST have a minimum length of 96 bits (12 octets); e. The value of the serial number MUST contain at least 64 bits of unpredictable random data; f. Said random data MUST be generated by a Cryptographically Secure Pseudorandom Number Generator (CSPRNG); g. The serial number MUST NOT be longer than 160 bits (20 octets).
Comment	-

7.1-pkio177 —

Description	The serial number of all end-user certificates must meet the following requirements: a. The value of the serial number MUST NOT be 0 (zero) b. The value of the serial number MUST NOT be negative c. The value of the serial number MUST be unique within the population of end-user certificates issued under an issuing TSP CA. d. The serial number MUST have a minimum length of 96 bits (12 octets) e. The value of the serial number MUST contain at least 64 bits of unpredictable random data f. Said random data SHOULD be generated by a Cryptographically Secure Pseudorandom Number Generator (CSPRNG). g. The serial number MUST NOT be longer than 160 bits (20 octets).
Comment	-

7.1-pkio182 —

Description	The CertificatePolicies field MUST contain the following fields: • OID of PvE (CP) part 3e: 2.16.528.1.1003.1.2.5.6; • OV OID from the CA / Browser Forum: 2.23.140.1.2.2; • the URI of the certification practice statement (CPS); • a user note. The OID scheme to be used in the "PKI voor de overheid" is described in the CP. For the user note, the TSP WILL use UTF8String but may also use IA5String.
Comment	It is not recommended to refer to paragraph numbers of the PvE / CP in the user note because persistence cannot be guaranteed (as opposed to the OID number of the CP).

7.1.1 Version number(s)

No stipulation.

7.1.2 Certificate extensions

No stipulation.

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

No stipulation.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

No stipulation.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

No stipulation.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

7.3-pkio123 —

Description	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 ".
Comment	-

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

8.1-pkio183 —

Description	A TSP MUST, when requested by the PA, perform a self-assessment against the Baseline Requirements based on a template predetermined by the PA.
Comment	Mozilla requires CAs to make a comparison of their processes (via CP and CPS documents) with the BRs using a template defined by Mozilla to ensure that their processes (and practices) continue to comply with CA's Baseline Requirements / Browser Forum.

8.1-pkio188 —

Description	Contrary to what is stated in requirement 8.1-pkio187 sub 1, a TSP can choose to undergo an audit against "Webtrust for Certification Authorities - Extended Validation". The certification must take place against the current version at the time of the commencement of the audit period.
Comment	-

8.1-pkio189 —

Description	If the TSP issues or intends to issue qualified certificates under PKIoverheid, the following additional requirements apply in addition to those set out in requirement 8.1-pkio187: a. The TSP must be certified against ETSI EN 319 411-2 b. The certification must be done by a CB that is accredited in accordance with the ETSI EN 319 403 scheme by an accreditation body within the meaning of Article 4 of Regulation (EC) No 765/2008 c. The certification must take place against the most recent version of ETSI EN 319 411-2 d. In addition, the report must state that the TSP meets the eIDAS (910/2014) regulation requirements. e. The TSP is registered with AT. The CA with which the TSP wants to issue qualified certificates MUST be on the Trusted List (TSL) at AT before issuance of qualified certificates can start.
Comment	-

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessors relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

No stipulation.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

8.6-pkio158 —

Description	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.
Comment	-

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2-pkio124 —

Description	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.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

9.6.1-pkio127 —

Description	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.

Comment	-

9.6.1-pkio128 —

Description	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.
Comment	-

9.6.1-pkio129 —

Description	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.
Comment	-

9.6.1-pkio131 —

Description	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

9.6.1-pkio132 —

Description	The TSP excludes all liability for damages if the certificate is not used in accordance with the certificate use described in paragraph 1.4.
Comment	-

9.6.1-pkio142 —

Description	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.
Comment	-

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

9.8-pkio133 —

Description	Within the scope of certificates as mentioned in paragraph 1.4 in this CP the TSP is not allowed to place restrictions on the use of certificates.
Comment	-

9.8-pkio143 —

Description	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.
Comment	-

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

9.17-pkio180 —

Description	CAs MUST actively inform their subscribers at least once every six months that, according to the terms and conditions, certificates are revoked under the conditions of - and within the time limits of - the BRG requirements specified in 4.9.1.1.
Comment	-