Logius
*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*

# CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid for Extended Validation CA certificates to be issued by the Policy Authority of the PKI for the Dutch government

| | |
|---|---|
| Version | 2.0 |
| Date | July 2020 |

## Publisher's imprint

| | |
|---|---|
| Version number | 2.0 |
| 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

*Revision history*

| Version | Date of approval | Date Entry into force | Status | Author | Manager | Description |
|---|---|---|---|---|---|---|
| 1.0 | 18-01-2011 | 25-01-2011 | Adopted by the Director of Logius 18 January 2011 | Policy Authority | H. Verweij | |
| 1.1 | 24-06-2011 | 01-07-2011 | Adopted by the Director of Logius 24-06-2011 | Policy Authority | H. Verweij | Change in relation to new address details of Logius plus some editorial changes. |
| 1.2 | 04-02-2013 | 04-02-2013 | Adopted by the Ministry of the Interior and Kingdom Relations | Policy Authority | H. Verweij | The change procedure is attached as Appendix C. |
| 1.3 | June 2014 | July 2014 | Adopted by the Director of Logius | Policy Authority | Mark Janssen | Rewritten CPS based on on RFC 3647. Various changes made in response to the WebTrust EV audit. |
| 1.4 | February 2015 | February 2015 | Adopted by the Director of Logius | Policy Authority | Mark Janssen | Editorial changes + changes to the certificate profile EKU + remark concerning verification of CAA records |
| 1.5 | October 2016 | October 2016 | Adopted by the Director of Logius | Policy Authority | Mark Janssen | Editorial changes + change of the ETSI framework of standards TS 102 042 to EN 319 411-1. Also various editorial changes. |
| 1.6 | December 2017 | December 2017 | Adopted by the PA PKIoverheid | Policy Authority | Mark Janssen | Yearly check (no changes) |
| 1.7 | December 2018 | December 2018 | Adopted by the Director of Logius | Policy Authority | Mark Janssen | Major revision as a result of BR self-assesment:<br>• Updated section 4.2 regarding CAA issuance, specific information about CAA records is to be found in the CPS of issuing CAs.<br>• Small update to section 1.2 regarding explanation of the additional "non RFC3647" sections.<br>• English translation is now the prevailing version in case of discrepancies between Dutch and English versions of this CPS |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | • Updated references RFC2560 to RFC 6960<br>• Appendix C of this CPS now refers to Appendix B of the "regular" CPS to avoid errors and duplication<br>• Updated chapter 4.8 to reflect current practices about certificate modification<br>• Removed superfluous sections with general PKI information<br>• Updated chapters 4.3 , 4.5, 5.2, 7.1, 5.2 and 9.10 to better reflect the requirements put on PKIoverheid by the BRGs and Software Application Suppliers<br>• Updated Appendix A & D to better reflect BRGs<br>• Removed superfluous sections with general PKI information<br>• Several small editorial changes. |
| 1.8 | December 2019 | December 2019 | | Policy Authority | Jorik van 't Hof | • Updated Chapter 1.2<br>• Updated Chapter 4.2 |
| 2.0 | July 2020 | July 2020 | Adopted by the Director of Logius | Policy Authority | Jorik van 't Hof | • major revision<br>  • Updated chapters to be fully compliant with RFC3647.<br>  • Revision of CA hiearchy due to introduction of new Server 2020 domain CA<br>  • Removal of s uperfluous (general) information about PKIoverheid and it's framework. these will be outlined in an introduction to the CP |

# 1. Introduction PKIoverheid EV Root CA

## 1.1 Overview

### *1.1.1 Policy Authority PKIoverheid*

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

PKIoverheid is an frameworkwhich enables generic and large-scale use of the electronic signature, and it also facilitates remote identification and confidential communication.

The responsibilities of the PA of PKIoverheid are:

- contributing towards the development and the maintenance of the framework of standards that underlies the PKI for the government, the Programme of Requirements (PoR), the PKIoverheid Certificate Policy (CP);
- assisting in the process of admittance by Trust Service Providers (TSPs) to the PKI for the government and preparing the administration;
- regulating and monitoring the activities of TSPs that issue certificates under the root of the PKI for the government.

PKIoverheid conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

The Policy Authority (PA) is responsible for managing the top tiers (level 1 and 2) of the hiearchy. PKIoverheid is structured in such a way that external organizations, the Trust Service Providers (TSPs), can be admitted to the PKI for the government under certain conditions. Participating TSPs are responsible for the services for subscribers within the PKIoverheid framework. The PA supervises the the TSPs, and as such ensures the trustworthiness of PKIoverheid as a whole.

Within the scope of the "Staat der Nederlanden EV Root CA", the PA is responsible for:

1. management of the PKIoverheid CP (the Programme of Requirements section 3f and 3j);
2. management of Object Identifiers, the unique numbers for TSPs and their CPSs;
3. creation and management of the key pair and the corresponding root certificate;
4. periodic publication of the CRLs for both Root (level 1) and domain (level 2) CAs;
5. creation and management of key pairs and the corresponding Intermediate (level 2) certificates;
6. preparing and supervising the admission of TSPs to the PKIoverheid framework;
7. supervision of admitted TSPs;
8. preparing and supervising the renewal of TSP CA certificates;
9. registration and assessment of audit (ETSI/Webtrust) reports
10. registation and assessments of (external) threats to the PKIoverheid framework

KPN BV is responsible for the technical management of the Staat der Nederlanden EV Root CA and the level 2 domain CAs plus the corresponding Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCPS) responders.

The Policy Authority of the PKI for the government is responsible for managing the root certificate. This organization is part of Logius ( http://www.logius.nl ), digital government service of the Ministry of the Interior and Kingdom Relations.

## 1.2 Document name and identification

The Certification Practice Statement EV certificates within the PKI for the government (hereinafter referred to as CPS) provides *TSPs, subscribers and relying parties* with information regarding the procedures and measures taken in respect of the PA's services with regard to certificates issued by the "Staat der Nederlanden EV Root CA". This CPS describes the processes, procedures and control measures for applying for, producing, issuing, managing and revoking CA certificates, insofar as the PA is directly responsible for this. This means that this CPS only relates to PKIoverheid CA level 1 (Staat der Nederlanden EV Root CA) and Level 2 (domain/intermediair) CAs.

This CPS also describes the processes and procedures for applying for, producing, issuing and revoking Level 3 TSP PKIoverheid CA certificates.
For a description of the processes, procedures and control measures for applying for, producing, issuing, managing and revoking Level 4 (SSL certificates), please refer to the relevant Certification Practice Statements of the PKIoverheid Trust Service Providers.

Formally, this document is referred to as the "CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid for TLS certificates to be issued by TSPs operating under the "Staat der Nederlandend EV Root CA"".

Currently, only an English version of this CPS is maintained published. In the event that this CPS will be translated and published in another language, care will be taken that the translation will remain faithful to the original version. In case discrepancies do appear between the English and other language versions of this document, the English version shall prevail.

| CPS | Description |
|---|---|
| Naming | CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid for TLS certificates to be issued by TSPs operating under the "Staat der Nederlandend EV Root CA" |
| Link | https://cps.pkioverheid.nl |
| OID | N/A |

Public information about the PA or the PKI for the government is available at http://www.logius.nl/pkioverheid.

This CPS applies to the following intermediate CAs issued by the "Staat der Nederlanden EV Root CA":

| Certificate Authority | SHA2-fingerprint | Policy OIDs | Remarks |
|---|---|---|---|
| Staat der Nederlanden EV Root CA | 4D2491414CFE956746EC4CEFA6CF6F72E28A1329432F9D8A907AC4CB5DADC15A | N/A | |
| Staat der Nederlanden EV Intermediair CA | DC862A3F025EF7F252FA9413CB60DE25E57E6AA7E1FB1DCA7B59D2C2217106EA | 2.16.528.1.1003.1.2.7 | Will be retired and subsequently revoked by September 1, 2020 |
| Staat der Nederlanden Server Domein CA 2020 | | 2.16.528.1.1003.1.2.5.8<br>2.16.528.1.1003.1.2.5.9<br>2.23.140.1.2.2 | Issuance of OV TLS certificates only. |

## 1.3 PKI Participants

### *1.3.1 Certification authorities*

*The Ministry of the Interior and Kingdom Relations (BZK)* is responsible for PKIoverheid. The Ministry of the Interior and Kingdom Relations makes decisions regarding the layout of the infrastructure and the participation of TSPs with the PKIoverheid framework. The director of Logius represents the Ministry of the Interior and Kingdom Relations in this matter.

The *PA* advises the director of Logius and is responsible for managing the level 1 and level 2 CAs of the PKI for the government and supervising and monitoring the work of TSPs that issue certificates to end-users.

One or more *TSPs* operate in each domain of the PKI for the government. Within a domain of the PKI for the government, a TSP will issue certificates to the certificate users. The requirements for issuance of these certificates are defined in the Programme of Requirements (C), part 3f (EV) and 3j (OV).

1.3.2 Registration authorities

RA responsibility for level 1, level 2 and level 3 CAs has been delegated by BZK to the PA PKIoverheid. As such, the PA PKIoverheid is responsible for identification and registration of the TSPs and their associated key personell. For more information, see chapter 3.

### *1.3.3 Subscribers*

Due to the fact that the PA PKIoverheid only issues CA certificates to TSPs, they act as "subscribers" for the purpose of this document. All requirements and responsibilities of the TSPs are detailled in the CP (Programme of Requirements) PKIoverheid. To legally enforce the CP, a separate contract is drafted and signed by the parties involved. For details regarding agreement between end-users and TSPs, please refer to the relevant CSP of the TSP in question.

### *1.3.4 Relying parties*

The *relying party* is the recipient of a certificate issued within the PKI for the government and acts on the basis of trust inthe certificate. The relying party is obliged to check the validity of the full chain of certificates through to the source (root certificate) on which trust is placed.

### *1.3.5 Other participants*

No Stipulation.

## 1.4 Certificate Usage

### *1.4.1 Permitted Certificate Usage*

Within the PKI for the government, different types of certificates are defined at four levels, which are:

- Root certificate;
- Domain certificate;
- TSP certificate;
- End user certificate.

The root certificate, the domain certificates and the TSP certificates can only be used to verify the issuer's signature and are issued by the Policy Authority. End user certificates are issued by the TSPs.

### *1.4.2 Prohibited Certificate Usage*

Certificates issued under this CPS may not be used other than as described above.

## 1.5 Policy Administration

### *1.5.1 The organization responsible for managing the CPS*

The Ministry of the Interior and Kingdom Relations is responsible for this CPS. The Ministry has delegated this task to Logius. This also includes the approval of changes to this CPS.

### *1.5.2 Contact Person*

Policy Authority PKIoverheid
Wilhelmina van Pruisenweg 52
P.O. Box 96810
2509 JE THE HAGUE
http://www.logius.nl/pkioverheid
General telephone number: +31(0)708896360
Email: servicecentrum@logius.nl[1]

#### 1.5.2.1 Revocation Reporting

In case of any issues with PKIoverheid end-user certificates, Subcribers, Relying Parties and any other third party should contact the TSP which issued the end-user certificate (contact details are found in their respective CPS).

In case of any issues relating to the TSP CA (level 3), Domain CA (level 2), Root CA (level 1) and/ or their associated OCSP responders and/or CRLs the reporting party should contact Logius directly via the details provided in section 1.5.2. The phone number listed is available 24/7. Outside office hours the on-duty stand-by manager will answer any calls.

Application Software Suppliers are advised to contact the PA PKIoverheid by either the 24/7 phone number listed above or via email: pkioverheid@logius.nl[2] (only inside of office hours)

Revocation procedures are also described in section 4.9.1. and 4.9.3. of this CPS.

### *1.5.3 Person determining CPS suitability for the policy*

The PA PKIoverheid determines the suitability and applicabitliy of this CPS.

### *1.5.4 CPS Approval Procedures*

The PA of PKIoverheid is entitled to change or to add to this CPS. Changes apply as from the time that the new CPS is published, in accordance with the provisions in paragraph 9.10. The management of Logius is responsible that the procedure described in paragraph 9.12 is followed accurately and she is responsiblefor the ultimate approval of this CPS in accordance with this procedure. Only in case of editorial changes the head of the PA PKIoverheid can approve a new version of the CPS for publication.

This CPS is reviewed and approved at least on an annual basis. In case that no (new) changes are required, this will still be listed in the change history, noting the review and changing the version number.

## 1.6 Definitions and abbreviations

In PoR part 4, an explanation is given regarding the definitions and acronyms used in the Programme of Requirements.

For a list of the used definitions and abbreviations, reference is made to https://www.logius.nl/sites/default/files/public/bestanden/English/PKIoverheid/Program-Requirements-EN-part4_0.pdf

1 mailto:servicecentrum@logius.nl
2 mailto:pkioverheid@logius.nl

# 2. Publication and electronic repository responsibilities

## 2.1 Electronic repository

The PA publishes the root certificate, the domain certificates and the TSP certificates on its website.

Also available on the website is information regarding the use of the root certificate, the domain certificates and the TSP certificates and CRLs for the Domain and TSP CA certificates.

An admitted TSP publishes the TSP certificates issued by the PA on its own website. A reference is also included to the root certificate and the domain certificates on the PA's website.

The CRLs relating to the end user EV SSL certificates can be found on the websites of the various TSPs.

## 2.2 Publication certificate information

The following EV certificates are published:

- Staat der Nederlanden EV Root CA;
- The Staat der Nederlanden EV Intermediair CA;
- <Name TSP> PKIoverheid EV CA.
- The Staat der Nederlanden Domein Server CA 2020
- <Name TSP> PKIoverheid Server CA 2020

The CAs can be found at the following URL: https://cert.pkioverheid.nl

This CPS can be found at the following URL: https://cps.pkioverheid.nl

The following CRLs are published. These can also be found on the website http://crl.pkioverheid.nl. Below are the direct links to the CRLs:

| Issuing CA | URI | Remarks |
|---|---|---|
| Staat der Nederlanden EV Root CA | http://crl.pkioverheid.nl/EVRootLatestCRL.crl | For revocation status of level 2 domain CAs and OCSP responder certificates issued by the Root CA |
| Staat der Nederlanden EV Intermediair CA | http://crl.pkioverheid.nl/EVIntermediairLatestCRL.crl | For revocation status of the level 3 TSP CAs and OCSP responder certificates issued by the EV Intermediair CA |
| Staat der Nederlanden Domein Server CA 2020 | http://crl.pkioverheid.nl/DomeinServerCa2020LatestCRL.crl | For revocation stauts of the level 3 TSP CAs and OCSP responder certificates issed by the Domein Server CA 2020 |

Test Websites for Application Software Suppliers (per BRG 2.2) are available:

- https://roottest-ev.pkioverheid.n[3]l
- https://roottest-ev-expired.pkioverheid.nl
- https://roottest-ev-revoked.pkioverheid.nl

3 https://roottest-ev.pkioverheid.nl

*2.2.1 Official electronic notification*

Information needed to identify the Staat der Nederlanden EV Root CA root certificate are published in the Official Gazette (Staatscourant) issue 2011, no. 527, of which an excerpt is listed under Appendix B

## 2.3 Time or frequency of publication

The information in the electronic repository will be published or updated as quickly as possible. When a new version of the CPS is published, the TSPs participating in the PKIoverheid framework will be informed by email.

The PA publishes lists of revoked certificates, the CRLs. The CRLs for the "Staat der Nederlanden EV Root CA" and "Staat der Nederlanden Domein Server CA 2020" are renewed annually or ad-hoc after revocation of intermediate CAs as both CAs are off-line. The CRL for the "Staat der Nederlanden EV intermediair CA" renewed every 12 hours and remains valid for 7 days. This CRL is published ad-hoc after revocation of an EV TSP CA certificate. Each CRL contains the time of the next planned CRL release. These CRLs can be found at: http://crl.pkioverheid.nl.

As well as the publication of the CRL, the PA also offers status information) through the Online Certificate Status Protocol (OCSP). To this end, the following OCSP responders are available:

1. http://evrootocsp.pkioverheid.nl provides status information about level 2 domain CAs
2. http://ocsp.pkioverheid.nl provides status information about the TSP certificates issued by the EV Intermediair CA
3. http://domserver2020ocsp.pkioverheid.nl[4] provides status information about the TSP certificates issued by the Domein Server CA 2020

The OCSP responders conform to RFC6960

The CRL and OCSP locations relating to the end user SSL certificates can be found on the websites of the various TSPs.

## 2.4 Access controls to publication

Published information is public in nature and freely accessible. The Electronic Repository can be accessed twenty-four hours a day, seven days a week. The Electronic Repository is protected against unauthorized changes being made.

In the event of system faillure , or other factors that have a negative impact on the availability of the Electronic Repository, an appropriate set of continuity measures have been prepared to ensure that the CRL will be available once again within 4 hours and the other parts of the Electronic Repository within 24 hours. An example of such a measure is having created a fall-back facility and scenario. In addition, every year the Electronic Repository will undergo a penetration test. This is carried out by an external IT security company.

4 http://domserver2020ocsp.pkioverheid.nl/

# 3. Identification and Authentication

## 3.1 Naming

### *3.1.1. Types of names*

All EV certificates issued by the PA of PKIoverheid contain a 'subject' field (DistinguishedName) which lists the name of the holder. The names consist of the following components:

| Attribute | Staat der Nederlanden EV Root CA | The Staat der Nederlanden EV Intermediair CA* | <TSP name> PKIoverheid EV CA* | Staat der Nederlanden Server Domain CA 2020 | <TSP name> PKIoverheid Server CA 2020 |
|---|---|---|---|---|---|
| Country (C) | NL | NL | NL | NL | NL |
| Organization (O) | Staat der Nederlanden | Staat der Nederlanden | <TSP Organization name> | Staat der Nederlanden | <TSP Organization Name> |
| CommonName (CN) | Staat der Nederlanden EV Root CA | The Staat der Nederlanden EV Intermediair CA | <TSP Organization name> PKIoverheid EV CA | Staat der Nederlanden Server Domain CA 2020 | <TSP name> PKIoverheid Server CA 2020 |

Also see Appendix A for the full certificate profiles of Staat der Nederlanden EV Root CA and level 2 domain CAs.

### *3.1.2 Need for names to be meaningful*

No Stipulation.

### *3.1.3 Pseudonyms*

The use of pseudonyms or anonymous certificates is not permitted.

### *3.1.4 Rules for interpreting various name forms*

The name of the TSP CA that is to be included in the Subject.OrganisationName field of the TSP CA certificate is taken from the extract in the National Trade Register (NHR) *National Handelsregister, in the Netherlands managed by the Kamer van Koophandel: www.kvk.nl*[5] and is entered as an exact match.

### *3.1.5 Uniqueness of names*

All certificates issued under this CPS, MUST contain a unique subject field (*DistinguishedName*).

### *3.1.6 Recognition, authentication and role of trademarks*

The PA assumes the the name of organizations as listed in the Dutch Trade Register of the Chamber of Commerce is correct. As such, the PA is not required to and does not dertimne wheter a Certificate Applicant (the TSP) has intellectual property rights.

5 http://www.kvk.nl

## 3.2 Initial identity validation

For the requirements with regards to the initial registration process of a TSP, see the PKIoverheid Programme of Requirements, part 2 of PKIoverheid.

### *3.2.1 Method to prove possession of private key*

Logius ensures that Certificate Signing Requests (CSRs_ generated by TSPs for signing TSP CAs will be sent in a secure manner. As such the following methods are allowed:

- sending the CSR via e-mail with a qualified Electronic Signature from the authorized contact person which uses a PKIoverheid qualified Certificate or equivalent or;
- sending the CSR via e-mail as an encrypted attachment using at least AES-256 or equivalent.

### *3.2.2 Authentication of organizational identity*

Based on the application form and the evidence that is supplied, the PA verifies that:

- That the TSP is an existing organization listed in the Dutch National Trade Register (NHR) or an organisational entity that forms part of an existing organization listed in the NHR. If a government organization is not listed in the NHR, the Staatsalmanak *http://staatsalmanak.sdu.nl/* is consulted;
- That the name of the organization and country name registered by the TSP to be incorporated in the certificate are correct and complete and that the applicant is authorised to represent the organization;
- The presence of the relevant registration information of the prospective TSP, with the corresponding evidence (excerpt from the Chamber of Commerce, etc.). The excerpt must be original and must not be older than 1 months.

Note: If the aspiring TSP has existed for less than three years and does not appear in the latest version of the registration sources listed above, the identity and validity of the prospective TSP may be established using a parent company or ministry that is registered in the NHR or the Staatsalmanak.

### *3.2.3 Authentication of individual identity*

Upon initial admittance to the PKIoverheid framework, the PA verifies the listed personal data of the authorised representative of the TSP using an identity document under art. 1 of the Compulsory Identification Act (WID), limited to the following documents:

- a valid travel document referred to in the Passport Act (Paspoortwet);
- a valid driving licence issued on the basis of the Road Traffic Act (Wegenverkeerswet), under article 107 of the Road Traffic Act (Wegenverkeerswet) 1994.

### *3.2.4 Non-verified subscriber information*

Not applicable.

### *3.2.5 Validation of authority*

See section 3.2.3.

### *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*

In the case of CA certificate re-key, an abbreviated procedure can be applied for the identification validation, because the TSP CA is already known to the PA and has been admitted to PKIoverheid.

It is then sufficient for the PA to verify whether the organization name and name of the country provided in the Naming document / CSR is still correct. This can be verified as follows:

1. By online consultation of the NHR to verify whether the TSP CA is an existing organization;
2. By online consultation of a database such as Dunn & Bradstreet, which is kept up-to-date and which is considered to be a trustworthy source.

In addition, the PA must verify that the application came from the actual TSP. An application can be submitted in two ways:

1. The authorised representative can send an application form by email and electronically sign this using a PKIoverheidcertificate *Specifically, using an end-user certificate with policy OID 2.16.528.1.1003.1.2.5.2 issued to the authorised representative*;
2. The authorised representative can sign an application form and send this by post.

In the second case, the PA PKIoverheid registered authorised representative of the TSP CA should also be contacted to verify the application. For purposes of verification, identifying details of the contact person or organization can be requested.

This identification verification by the PA is recorded and archived in the TSP CA case file.

### *3.3.2 Identification and authentication for re-key after revocation*

See 3.3.1.

## 3.4 Identification and authentication for Revocation Requests

A request for revocation of a certificate can be submitted by the TSP CA. When a request for revocation is made, the reason for this must always be given.
Identification and authentication of the party submitting the request to revoke the TSP CA can take place as follows:

- A request by email to the PA, where the request is signed digitally with a qualified electronic signature;
- A request by signed letter.

In both cases, the PA will contact the authorised representative of the TSP CA by telephone to establish whether the request for revocation is genuine. For purposes of verification, identifying details of the contact person or organization can be requested.

# 4. Certificate Life-Cycle Operational Requirements

## 4.1 Certificate Application

Staat der Nederlanden EV Root CA, The Staat der Nederlanden EV Intermediair CA, EV TSP CA, Staat der Nederlanden Domein Server CA 2020 and TSP Domein Server CA 2020 certificates are created by the the Policy Authority (PA), at the instruction of the Ministry of the Interior and Kingdom Relations.

### *4.1.1 Who can submit a certificate application*

Only a TSP which has been admitted to the PKI for the government can and may apply for a TSP CA certificate to be created under the EV root.

*For TLS (EV) certificates issued under the PKIoverheid hierarchy by TSP's, each TSP (issuing CA) has a specific CAA identifier, which can be found in their respective CPS documents. Besides TSP specific CAA records, a CAA issue record with the value "*pkioverheid.nl[6]*" or "*www.pkioverheid.nl[7]*" permits issuance for all TSP's who issue PKIoverheid TLS (EV) certificates.*

### *4.1.2 Enrollment process and responsibilities*

The instruction to create EV TSP CA certificates is of a request (PKCS#10) to this end by a TSP. See PoR section 2 for extra information.

## 4.2 Certificate application processing

### *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

The root certificate, the domain certificates and TSP certificates are created and/or signed during special creation ceremonies. A certified Webtrustauditor acts as witness during the signing ceremonies signing of TSP CAs For each key ceremony, a detailed script is produced which lists all tasks to be carried out.

This main purpose of this script is to prevent any input errors during the ceremony. A creation ceremony takes place in accordance with the script in the presence of independent witnesses. The identity of the persons present is verified using the valid documents referred to under article 1 of the Compulsory Identification Act ("Wet op de identificatieplicht").

The creation and/or signing key ceremonies take place for all of the listed types of certificates in a similar manner. In this case, the certificate user is the PA or the TSP. During the ceremony, the following steps take place:

1. building the computer system;
2. installing and configuring the PKI software;

6 http://pkioverheid.nl
7 http://www.pkioverheid.nl

3. activating the Hardware Security Module (HSM), where several shareholders each introduce part of the activation data;
4. generating the key pairs (only applicable to Root and Domain CAs);
5. generating certificates for each key pair;
6. dismantling the computer system and
7. securing the computer system and the critical components.

The Policy Authority does not generate the key pair for a (prospective) TSP but only creates certificates based on a CSR (PKCS10) file supplied by the TSP in a thrustworthy manner.

The requirements which a TSP must fulfil when issuing the certificates are formulated in part 3 (Certificate Policies) of the Programme of Requirements. The way in which a TSP implements these requirements must be defined by the TSP itself in a Certification Practice Statement (CPS). The description of the services by TSPs therefore falls outside the scope of the specification of this CPS.

There is no separate CP for the issuance of certificates by the PA, as the PA does not issue end user certificates. The measures that the PA has taken to guarantee the trustworthiness of the EV CA certificates to be issued by the PA are described in this CPS.

#### *4.3.1 CA actions during certificate issuance*

The Policy Authority only issues CA certificates (excluding certificates used for revocation status services like OCSP). Issuance of any certificate is only possible by human intervention. Chapter 5.2 describes this process in more detail.

#### *4.3.2 Notification to subscriber by the CA of issuance of Certificate*

No stipulation.

### 4.4 Certificate acceptance

The script associated with the creation ceremonies also contains the procedure for ascertaining the accuracy and accepting the certificates that are created. Also listed in the script are the names of the people involved. The PA establishes the accuracy of the certificates. The TSP then accepts the TSP certificates.

#### *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*

No stipulation.

### 4.5 Key pair and certificate usage

Staat der Nederlanden EV Root CA, The Staat der Nederlanden EV Intermediair CA, EV TSP CA, Staat der Nederlanden Domein Server CA 2020 and TSP Domein Server CA 2020 certificatess are primarily used to verify the issuer's signature and are issued by the PA. These certificates are also used for CRL signing and issuance of OCSP signing certificates. These certificates may not be used for other purposes. The end user EV and Domein Server 2020 SSL certificates are issued by the TSPs.

*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*

Certificates have to be renewed when (part of) the information that forms the basis of the certificate changes or is out of date. For example, if the name of a TSP shown in the certificate changes or if the strength of a cryptographic algorithm is deemed insufficient and a stronger algorithm is needed.

*Certificate Renewal* where the existing key pair is maintained and the maximum validity period certificate is extended is not applied within PKIoverheid.

The time of (routine) renewal of certificates is related to the lifecycle of certificates and signing keys. For the relying party, during the term of an end user certificate, it must also be possible to verify the validity of the certificate. When an end user certificate is verified, the validity of the aforementioned certificates of issuing TSPs is also verified. Therefore the TSP certificate, the domain certificate and the root certificate will have to be valid during the course of the validity period of an end user certificate.

*4.6.2 Who may request renewal*

No stipulation.

*4.6.3 Processing certificate renewal requests*

Taking the required verification period into account, a TSP can create new signing keys (or arrange for these to be created) and also submit a request to the PA to create the new TSP Domein Server CA 2020 certificate. EV TSP CA cwerificates will no longer be created.

This request is the first step of the internal procedure in TSP certificate renewal. This procedure broadly comprises the following steps:

- Submission of an application form to renew an TSP Domein Server CA 2020 under the new root by the authorised representative of the TSP;
- Verification of the validity of the application by the PA;
- Validation of the data in the application form;
- Submission of the Naming Document for the new TSP Domein Server CA 2020 certificate by the TSP;
- Verification of the Naming Document by the PA;
- Submission of the Certificate Signing Request (CSR) by TSP for the Test TSP CA;
- Creation of a Test TSP Domein Server CA 2020 certificate by the technical administrator of the EV root;
- Verification Test of TSP Domein Server CA 2020 certificate by the PA and TSP;
- Submission of a Certificate Signing Request (CSR) by TSP for Production TSP CA;
- Instruction from the PA to the technical administrator EV Root for the creation of a new TSP Domein Server CA 2020 certificate;
- Execution of a creation ceremony of new TSP Domein Server CA 2020 certificate by the technical administrator of the root;
- Verification by PA of new TSP Domein Server CA 2020 certificate;
- Handover by PA of new TSP Domein Server CA 2020 certificate to the TSP;
- Discharge of PA to the technical administrator of the EV Root.

*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

*Certificate Re-key* where the existing public key of a certificate is changed, is not applied within the central hierarchy of PKIoverheid.

*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*

Revocation of a domain certificate or a TSP certificate will in any cases be considered if the signing key belonging to the certificate is compromised or suspected to be compromised. The TSP is considered to be compromised if unauthorised access is gained to this signing key or when carriers of the private key are stolen or lost. To effect this, the PA keeps records of incidents and/or other events that can lead to revocation of a domain certificate or a TSP certificate. All messages are registered by the PA and are dealt with.

The PA considers compromise of the signing key to be an emergency. Should an emergency occur, the emergency plan will take effect and all relevant parties will immediately be informed. The emergency plan is discussed in paragraph 5.7 of this CPS.

*4.9.2 Who can request revocation*

The PA.

*4.9.3 Procedure for revocation request*

Prior to the revocation of a domain (intermediate) CA or an EV TSP CA certificate, a careful assessment process is followed. The emergency team will perform this assessment and will initiate any activities that may ensue from this, or arrange for these to be initiated.

If a TSP no longer fulfils the conditions for participation in the PKIoverheid Extended Validation, the PA can revoke the relevant EV TSP CA certificate. The revocation of a certificate can be effectuated within one day. The PA informs the TSP prior to the certificate being revoked.

The decision to Staat der Nederlanden EV Intermediair CA and Staat der Nederlanden Domein Server CA 2020 certificate will be accompanied by a decision on whether or not a new certificate will be issued to replace the revoked certificate.

*4.9.4 Revocation request grace period*

No stipulation.

*4.9.5 Time within which CA must process the revocation request*

The revocation of a certificate can be effectuated within one day.

*4.9.6 Revocation checking requirement for relying parties*

No stipulation.

*4.9.7 CRL issuance frequency (if applicable)*

No stipulation.

*4.9.8 Maximum latency for CRLs (if applicable)*

The revocation of the Staat der Nederlanden EV Intermediair CA certificate, Staat der Nederlanden Domein Server CA 2020, or a TSP Domein Server CA 2020 certificate always leads to ad-hoc publication of the relevant modified CRL. The new CRL will be published a maximum of 24 hours after revocation of the domain or TSP CA.

*4.9.9 On-line revocation/status checking availability*

No stipulation.

*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*

Certificate suspension is not supported within PKIoverheid.

*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*

The validity of certificates can be consulted using the published CRL which is available through the electronic repository (see 2.1). For the CRLs, the PA uses the X.509 version 2 format.

In addition to publishing the CRL, the PA offers an Online Certificate Status Protocol (OCSP) service. The OCSP service is normally updated every 12 hours. An OCSP response from this service remains valid for up to 7 days. In the event of the revocation of an EV TSP CA certificate, the OCSP service is updated ad-hoc. The OCSP service supports the GET method for requesting a response.

With regard to its CRL and OCSP services, the TSP retains appropriate server capacity, meaning a response time will be guaranteed of 10 seconds or less under normal circumstances.

During the lifetime of the aforementioned CA, the status of revoked certificates will remain available on the CRL and through OCSP.

#### *4.10.2 Service availability*

The CRL and OCSP are available 24 hours a day, 7 days a week.

The maximum period of time within which the availability of the revocation status information (the status of a revoked certificate) has to be restored is four hours.

#### *4.10.3 Optional features*

No further provisions for the certificate services of TSP.

### 4.11 End of subscription

If the Ministry of the Interior and Kingdom Relations decides to end the PKIoverheid Extended Validation service, the following actions will be undertaken:

1. All involved parties (subscribers, cross-certifying CAs, TSPs and relying parties) of the PKIoverheid Extended Validation service shall be informed six months before the service ends;
2. All EV certificates that are issued after annoucement of termination of the service has been communicated SHALL NOT contain a NotAfter date which is later than the planned termination date of PKIoverheid Extended Validation;
3. When the service ends, all certificates that are still valid SHALL be revoked;
4. On the termination date, PKIoverheid Extended Validation ceases to distribute certificates and CRLs.

#### *4.11.1 Transfer of PKIoverheid (non RFC3647)*

If the Ministry of the Interior and Kingdom Relations decides to transfer the PKIoverheid EV service to a different organization, all involved parties (subscribers, Application Software Suppliers, TSP's and relying parties) of the PKIoverheid EV service will be informed of this transfer at least 3 months in advance. The new organization will transfer the provisions from this CPS to its own CPS.

### 4.12 Key escrow and recovery

#### *4.12.1 Key escrow and recovery policy and practices*

The PA PKIoverheid has cloned the key pairs of the root and domain certificates and they are stored at the Disaster Recovery site of PKIoverheid.

#### *4.12.2 Session key encapsulation and recovery policy and practices*

No stipulation.

# 5. Facility Management, Operational, and Physical Controls

## 5.1 Physical controls

The secured environment of Staat der Nederlanden EV Root CA is set up based on the requirements formulated in the Programme of Requirements and the requirements in the Civil Service Information Security (Classified Information) Decree (Voorschrift Informatiebeveiliging Rijksdienst voor Bijzondere Informatie (VIR-BI)).

### *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

Specific processes and procedures have been implemented to handle incidents and emergencies.

The Policy Authority performs a system-wide risk analysis annually and describes the control measures taken to mitigate and/or reduce the risks within the system. A risk analysis is also performed when there are significant changes in internal or external factors.

In addition, every year a risk analysis is performed for the technical management of the central hierarchy of PKIoverheid.

The computer systems for the production environment are solely used for the purpose of PKIoverheid CA operations. Separate systems have been set up to test or accept new or modified software and/or hardware. Apart from this separation of hardware, procedures are in force that ensure that all employees respect the principle of a strict separation between the test and the production environment.

The responsibilities of the PA are allocated between different functions and persons. The software checks the segregation of duties and enforces this. Generally, it is ensured that the implementation

of security tasks and of regulation and verification take place independently of the implementation of production tasks. More PKI-specific measures are taken in respect of producing the key material and EV certificates. The PA can only generate key material and EV certificates in the simultaneous presence of various key holders. Each key holder only has access to part of the activation data that is required to be able to use the signing key. When producing and publishing CRLs, this so-called N out of M principle is also applied [For reasons of confidentiality, this CPS does not state between how many key holders the activation data are distributed.]. Other conditions are:

- The Root CA systems are stand-alone systems, which have no external network links. The Intermediate CA is housed on a network HSM and is online;
- During operational use, Root CA systems are situated in a secure room that can only be accessed by persons authorised to do so;
- After use, the Root CA system along with all peripheral equipment and key parts are stored in a safe that is located in the aforementioned secure room. The access key parts of the EV Intermediair CA are also stored in a safe in the secure room;
- The CA systems are operated by a key manager, who works strictly according to the scripts and under the constant observation of a witness. Depending on the ceremony, this is an independent external witness and/or a representative of the PA. Any deviations from the script will be meticulously recorded;
- From the very start (retrieving CA systems and key parts) to the end (storing CA systems and key parts), the entire ceremony is video recorded and saved. The recordings are stored and are available for playback for the Webtrust Auditor.
- During the ceremony, the partial activation keys are in the possession of the relevant key holders. The distribution of the activation keys between the key carriers is such that a specific activity cannot be carried out by the technical administrator without at least 2 civil servants being present. The N out of M principle means that several activation keys and key holders are required. This way access to the CA Private key is only possible by persons in a trusted role using at least dual control.
- A request for certification (signing or revocation) is presented by the PA to the technical administrator, signed by the general director of Logius.

*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*

The PA employs personnel who have the required expertise, experience and qualifications for the relevant positions.

*5.3.2 Background check procedures*

The PA shall ensure that trusted personnel have no conflicting interests, in order to safeguard the impartiality of the activities of the PA. If this is considered necessary, the PA will only take on people in positions of trust whenthey have passed a security screening performed by the General Intelligence and Security Service (AIVD) or by the Dutch Military Intelligence and Security Service (MIVD)[8].

*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*

For the purpose of auditing, the PA keeps computer log files with the changes in the CA systems that form part of the technical infrastructure of the top of the hierarchy and that are of importance for the trustworthiness of the services. Examples of this are creating accounts, installation of software, back-ups, closing and (re)starting the system, hardware changes and securing audit-log files.

All activities of the PA relating to generating keys and producing certificates and CRLs are logged in such a way that retrospective reconstruction of the system operations is possible.

*5.4.2 Frequency of processing log*

During every key ceremony, the log files of the CA systems are checked to confirm that no unauthorized changes have been made to these systems.

*5.4.3 Retention period for audit log*

No stipulation.

*5.4.4 Protection of audit log*

No stipulation.

8 https://en.wikipedia.org/wiki/Dutch_Military_Intelligence_and_Security_Service

#### *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*

After each key ceremony, a full secure backup of the CA system (including database). The back-ups are stored offsite. With this mechanism the PA makes sure that at least 7 years of log files are kept at all times.

The PA archives relevant records relating to certificates issued by the PA, for a period of seven years after expiry of the certificate. This includes the documents relating to procedures carried out when creating and revoking the certificates and documents/files required in order to ascertain the validity of root certificate, domain certificates or TSP certificates at a specific point in time. The archived documents are stored by the PA in a secure manner.

The public keys of the root certificate, the domain certificates and the CRL certificates are archived as part of the corresponding certificates.

#### *5.5.2 Retention period for archive*

Once the validity of the TSP certificate has expired, the PA shall save, for a period of at least 7 years, all information relating to the application and revocation, if applicable, of the TSP certificate and all information used to verify the identity of the TSP and the Authorized Representative.

#### *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

Keys of TSP CAs may not be reused once the term of validity has expired, or once the corresponding certificate has been revoked. When certificates are renewed, the key pair is also renewed.

## 5.7 Compromise and disaster recovery

### *5.7.1 Incident and compromise handling procedures*

The PA puts provisions in place to safeguard the continuity of its services in such a way that possible disruptions are kept to a minimum.

The provisions that the PA has put into place include the use of redundant systems, Intrusion Detection Systems and back-ups.

In anticipation ofpotential emergencies that may arise within PKIoverheid Extended Validation the PA has prepared an emergency plan. Described in this plan are the measures to resolve an emergency as quickly as possible. The emergency plan therefore outlines how an emergency team will immediately be convened, with certain authorities and resources, which will take appropriate action.

Several parties are active within the PKIoverheid Extended Validation (Ministry of the Interior and Kingdom Relations, PA, TSPs and the technical administrator of the root). Any of these parties can have an emergency, which can potentially have an impact on other parts of the PKIoverheid Extended Validation system. To be able to act in a coordinated manner In the event of an emergency, the emergency plans of the various parties are coordinated with one another.

To be properly prepared for potential emergencies and to limit the impact of an emergency, the PA's emergency plan is tested periodically, at least annually The coordination and communication with the involved parties from the PKIoverheid Extended Validation system are then also tested.

### *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*

No stipulation.

## 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*

The PA's key pairs are generated during the various creation ceremonies. For this, only stand-alone computer systems are used. These computer systems are not connected to a network; all communication between systems takes place through media such as CD-ROM, floppy disk or smartcard. Because the generation and the use of the PA's signing key takes place occasionally, the computer systems are only used for this purpose. For the majority of the time, the critical components of the computer systems are stored in a safe.

### *6.1.2 Private key delivery to subscriber*

No stipulation.

### *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*

The following key lengths apply:

- EV TSP CA certificates 4096 bit RSA keys
- The Staat der Nederlanden EV Intermediair CA 4096 bit RSA keys
- Staat der Nederlanden EV Root CA 4096 bit RSA keys
- OCSP certificates 4096 bit RSA keys

### *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*

The active signing keys of the PA are always located in the secure housing of a cryptographic module (HSM) which meets the following:

- the requirements laid down in the standard FIPS PUB 140-2 level 3 or higher, or;
- a trustworthy system that (as a minimum) is certified in accordance with ISO 15408 at evaluation guarantee level EAL 4+ or equivalent security criteria.

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

All actions with the signing keys of the PA take place in accordance with pre-defined procedures. The people who must be present when these actions are being performed are appointed

beforehand. The signing keys of the PA can only be unlocked for use when these people are present.

*6.2.3 Private key escrow*

Under no circumstances are the PA's signing keys of the PA passed on to a third party for storage.

*6.2.4 Private key backup*

Under no circumstances are the PA's signing keys of the PA passed on to a third party for storage. As described in section 4.12, the private keys of the CA managed by the PA are stored on the DR location with the same (technical) security controls as the operational private keys.

*6.2.5 Private key archival*

If the signing keys are taken out of service at the end of the life time, for security reasons, these signing keys will not be archived. The signing keys are destroyed in an appropriate manner, to prevent them from being reused.

*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*

No stipulation.

### 6.3 Other aspects of key pair management

*6.3.1 Public key archival*

No stipulation.

*6.3.2 Certificate operational periods and key pair usage periods*

All EV certificates have a maximum period of validity:

- EV TSP certificates 12 years minus 2 days;
- The Staat der Nederlanden EV Intermediair CA12 years minus 1 day;
- Staat der Nederlanden EV Root CA 12 years;
- OCSP Responder certificates 14 month.

## 6.4 Activation data

### *6.4.1 Activation data generation and installation*

No stipulation.

### *6.4.2 Activation data protection*

Activation data for the information systems, such as passwords and PIN codes are, like partials key, stored in separate seal bags in separated compartments in the PKIoverheid safe.

### *6.4.3 Other aspects of activation data*

No stipulation.

## 6.5 Computer security controls

### *6.5.1 Specific computer security technical requirements*

The PA computer systems used to manage and access a CA private key can only be accessed by authorised members of staff. Software-based checks are incorporated in the systemswhich take care of access control.The software checks the authorisation of the staff member before the relevant actions can take place on the computer system. The actions performed on the computer systems are logged in such a way that, at a later stage, it can be ascertained which staff member performed which actions. The logs that are kept are verified during every key ceremony.

The computer systems of the PA referred to, are set up in such a way that only the essential actions can be performed. All unnecessary components in that respect, such as additional software installed with the OSare removed. The Root CA computer systems are stand-alone and airgapped systems, therefore provisions relating to network security do not apply.

Only the system used separate directory server for publishing the CRL and certificates is connected to a public network. This connection has extra security, in the form of a firewall.

Measures have also been taken to detect unauthorised and/or failed attempts to access the systems in a timely manner.

The PA ensures that the cryptographic hardware and software used by the PA to sign certificates can never be amended unnoticed. This is monitored throughout the entire lifecycle of the cryptographic hardware and software.

### *6.5.2 Computer security rating*

The hardware and software used in the central hierarchy for the key management is classified by the NBV *Netherlands National Communications Security Agency (Nationaal Bureau voor Verbindingsbeveiliging)_at level "Staatsgeheim confidentieel" _Comparable to "confidential" in UK/ US government classifications* . If any changes are made to the information systems, another evaluation is performed.

## 6.6 Life cycle technical controls

### *6.6.1 System development controls*

After extensive testing, CA systems are taken in production and maintained by the technical administrator.

### *6.6.2 Security management controls*

No stipulation.

### *6.6.3 Life cycle security controls*

Software updates are carefully implemented after consultation with and in the presence of the PA PKIoverheid.

## 6.7 Network security controls

Staat der Nederlanden EV Root CA is offline. The Staat der Nederlanden EV Intermediair CA is online for the purpose of signing the CRL. The CRLs described in this in CPS are also online in the Certificate Status Service. The technical administrator of the EV Root of Logius has taken measures to safeguard the stability, the trustworthiness and the security of the network. This includes, for example, measures to regulate data traffic and to prevent unwanted data traffic, as well as the inclusion of firewalls in order to guarantee the integrity and exclusivity of the network. Measures have also been taken to detect unauthorised and/or failed attempts to access the systems in a timely manner.

The Staat der Nederlanden EV Intermediair CA and Certificate Status Service is part of the annual WebTrust audit. The Certificate Status Service also undergoes an annual penetration test. This is carried out by an external IT security company.

## 6.8 Time-stamping

The PA does not support a timestamping service as part of its services

# 7. Certificate and CRL, and OCSP profiles

## 7.1 Certificate profile

Appendix A contains an overview of the content of the fields of the Staat der Nederlanden EV Root CA and the Staat der Nederlanden EV Intermediair CA.

The PA validates all the information to be listed in a TSP CA certificate that is supplied by the TSP in question, like the OrganisationName and LocalityName. This information will be verified according to guidelines established in BRG 3.2.2.2. The PA allows only unique common names for newly signed TSP CAs. See also the Programme of Requirements part 2 for more information about this subject.

### *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

The CRLs comply with the X.509v2 standard for public key certificates and CRLs.

The CRL of the EV Root CA is valid for one year. The CRL of the TSP EV Intermediate CA is valid for 7 days.

| **Attribute** | |
|---|---|
| Version | V2<br>Describes the version of the CRL profile.<br>Value 1 represents X.509 version 2 CRL profile. |
| Provider | CN = Staat der Nederlanden EV Root CA or Staat der Nederlanden EV Intermediair CA<br>O = The State of the Netherlands<br>C = NL |
| Effective date | Effective date of the CRL |
| Next update | The latest date on which an update can be expected, however an earlier update is possible.<br>Contains the date and time on which the next version of the CRL is expected (at the latest). |
| Algorithm for the signature | SHA256<br>The value is equal to the field signatureAlgorithm and contains the algorithm that is used for signing.<br>The signing algorithm is SHA-256WithRSAEncryption. |
| Revocation list | Revoked certificates with the date of revocation.<br>Includes the date and time of revocation and serialNumber of the revoked certificates. |
| CRL number | Sequential number of publication of the CRL in hexadecimal notation |

### *7.2.1 Version number(s)*

No stipulation.

### *7.2.2 CRL and CRL entry extensions*

No stipulation.

## 7.3 OCSP profile

### *7.3.1 Version number(s)*

No stipulation.

### *7.3.2 OCSP extensions*

The EV root CA and the EV Intermediate CA use OCSP and OCSP signing certificates. OCSP signing certificates are valid for 14 months and are re-signed annually.

The OCSP responses and OCSP signing certificates fulfil the requirements laid down in this respect in IETF RFC 6960. OCSP signing certificates are in line with the X.509v3 standard for public key certificates.

| Basic Extensions | OID | Critical | Value |
|---|---|---|---|
| Certificate | | | N/A |
| SignatureAlgorithm | { pkcs-1 5 } | | N/A |
| Algorithm | | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| SignatureValue | | | Signature generated by Staat der Nederlanden EV Root CA or Staat der Nederlanden EV Intermediair CA |
| TBSCertificate | | | N/A |
| Version | | | 2 |
| serial number | | | SHA1 hash of public key generated by Staat der Nederlanden EV Root CA or Staat der Nederlanden EV Intermediair CA |
| Issuer DN | | | C=NL<br>O=Staat der Nederlanden<br>CN=Staat der Nederlanden EV Root CA or Staat der Nederlanden EV Intermediair CA |
| Subject DN | | | C=NL<br>O=Staat der Nederlanden<br>CN=Staat der Nederlanden EV Root CA OCSP Responder n or Staat der Nederlanden EV Intermediair CA OCSP Responder n (n= 1, 2, 3) |
| Validity | | | |
| notBefore | | | dd-mm-yyyy (Date of the ceremony) |
| notAfter | | | dd-mm-yyyy (14 months after the date of the ceremony) |
| Public Key Algorithm | | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Public Key Length | | | 4096 |
| **Standard Extensions** | **OID** | **Critical** | **Value** |
| BasicConstraints | {id-ce 19} | TRUE | N/A |

| | | | |
|---|---|---|---|
| CA | | | Clear (FALSE) |
| pathLenConstraint | | | N/A |
| KeyUsage | {id-ce 15} | TRUE | N/A |
| Digital Signature | | | Set |
| SubjectKeyIdentifier | {id-ce 14} | FALSE | N/A |
| KeyIdentifier | | | |
| authorityKeyIdentifier | {id-ce 35} | FALSE | N/A |
| KeyIdentifier | | | Hash of public key of Issuing CA |
| CRLDistributionPoints | {id-ce 31} | FALSE | N/A |
| DistributionPoint | | | N/A |
| Full Name (URI) | | | http://crl.pkioverheid.nl/EVRootLatestCRL.crl or http://crl.pkioverheid.nl/EVIntermediairLatestCRL.crl |
| extendedKeyUsage | {id-ce 37 } | TRUE | N/A |
| Key Purpose - OCSPsigning | {id-kp 9} | | 1.3.6.1.5.5.7.3.9 |
| PrivateExtensions | OID | Critical | Value |
| id-pkix-oTSP-nocheck | 1.3.6.1.5.5.7.48.1.5 | FALSE | 05 00 (Null) |

# 8. Compliance Audit and Other Assessment

## 8.1 Frequency or circumstances of assessment

The PA of PKIoverheid complies with the requirements described in the latest version of the WebTrust Principles and Criteria for Certification Authorities, WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL[9] and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security[10]. Each year, the PA of PKIoverheid undergoes a full period-of-time audit to confirm this. http://www.webtrust.org/principles-and-criteria/item83172.aspx

The PA PKIoverheid actively monitors the changes in the WebTrust Principles that affect this CPS. The PA PKIoverheid also actively monitor changes in the *Baseline Requirements* of the CA / Browser Forum that affect this CPS and the Programme of Requirements of PKIoverheid. The impact of these changes on the CPS and PoR of PKIoverheid shall be assessed.

The PA PKIoverheid also conforms with established government policy in relation to information security and privacy.

## 8.2 Identity/qualifications of assessor

Audits are performed by an external certified WebTrust for CAs auditor.

## 8.3 Assessor's relationship to assessed entity

No stipulation.

## 8.4 Topics covered by assessment

This audit determines whether the quality and the security measures of the organization that has been set up meet the stipulated WebTrust standards.

### *8.4.1 Admittance of TSPs*

See "section 2 of the Programme of Requirements PKIoverheid" *https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-TSP/programma-van-eisen/*

## 8.5 Actions taken as a result of deficiency

If additional security measures are recommended, the PA shall immediately take actions to implement these measures.

## 8.6 Communication of results

Through a WebTrust seal, published on the Logius website, each year PA PKIoverheid demonstrates that it meets the WebTrust standards.

The PA publishes this seal and accompanying Management Assertion no longer than 3 months after expiry of the previous audit period. Audit Statements of the issuing CAs (TSP CAs) are submitted to the Common Certificate Authority Database (CCADB) and are also published on the websites of the respective TSPs.

9 http://www.webtrust.org/principles-and-criteria/docs/item85117.pdf
10 http://www.webtrust.org/principles-and-criteria/docs/item83987.pdf

# 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*

The Staat der Nederlanden Server CA 2020 CA and the TSP Server CA 2020 certificates contain a reference to this CPS. No fee is charged for consulting these certificates or the information referred to. This applies to:

- consulting the certificates;
- consulting the revocation status information (CRLs) and;
- consulting the Programme of Requirements section 3: Certificate Policies;
- consulting this CPS.

### *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

### *9.2.1 Insurance coverage*

In terms of liability, the general rules of Dutch law apply with respect to the content and scope of the statutory obligation to pay compensation.

The Ministry of the Interior and Kingdom Relations and a TSP enter into an agreement or contract regarding participation of the relevant TSP in PKIoverheid Extended Validation. In essence, this means that the TSP is obliged to provide services under the conditions stipulated by the Ministry of the Interior and Kingdom Relations, particularly the conditions laid down in the Programme of Requirements section 3: basic requirements and section 3j. In this respect, the PA is the point of contact for the TSP.

Provisions regarding the liability of the Ministry of the Interior and Kingdom Relations towards a TSP are included in an agreement or contract between the Ministry of the Interior and Kingdom Relations and the TSP. The requirements that the liability of the TSP must meet, are stated in the Programme of Requirements part 3: Certificate Policies.

### *9.2.2 Other assets*

No stipulation.

### *9.2.3 Insurance or warranty coverage for end-entities*

The TSP enters into agreements with subscribers and relying parties. Also laid down in these agreements is the liability of the TSP in respect of subscribers and relying parties. The

requirements that this liability must meet are included in the General Provisions of the Programme of Requirements section 3: basic requirements and section 3j.

## 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*

The Policy Authority PKIoverheid handles company data confidentially. Only employees of the PA PKIoverheid have access to this data.

Company data, such as audit reports and Corrective Action Plans of TSPs will be sent securely (encypted).

## 9.4 Privacy of personal information

### *9.4.1 Privacy plan*

Unlike the TSPs, PA PKIoverheid does not issue certificates to natural persons. A register with the personal data of certificate users is therefore not available.

### *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



11 https://creativecommons.org/licenses/by-nd/4.0/

## 9.6 Representations and warranties

### *9.6.1 CA representations and warranties*

See paragraph 9.2.

### *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

See paragraph 9.2.

## 9.8 Limitations of liability

See paragraph 9.2.

## 9.9 Indemnities

See paragraph 9.2.

## 9.10 Term and termination

### *9.10.1 Term*

This is version 1.7 of the "CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid for Extended Validation CA certificates to be issued by the Policy Authority of the PKI for the government", December 2018.

This CPS is valid as from the date of entry into force. The CPS is valid for the period of time that the services of the PKI for the government continue or until the CPS is replaced by a newer version. The PA will review the CPS and make changes if deemed necessary, at least once a year. Newer versions are marked with a higher version number (vX.x). Newer versions are published on the following PA website (https://cps.pkioverheid.nl).

### *9.10.2 Termination*

No stipulation.

### *9.10.3 Effect of termination and survival*

No stipulation.

## 9.11 Individual notices and communications with participants

If TSPs have any questions, they can contact the PA PKIoverheid.

Regular communication takes place by email between the PA and the TSPs that participate in the PKIoverheid framework.

TSPs are immediately informed about the publication of a new version of the CPS or Programme of Requirements. Intended changes of the PoR are announced as soon as possible.

Besides communications with the TSPs, frequent contact also takes place with AT *Radiocommunications Agency. See also https://www.agentschaptelecom.nl/onderwerpen/zakelijk-gebruik/eidas-elektronische-vertrouwensdiensten/trust-service-providers* and the auditor(s) of the participating TSPs.

## 9.12 Amendments

### *9.12.1 Procedure for amendment*

The Ministry of the Interior and Kingdom Relations is responsible for this CPS. The Ministry has delegated this task to Logius. This also includes the approval of changes to this CPS.

### *9.12.2 Notification mechanism and period*

Any changes not considered to be changes of an editorial nature, are announced and result in a new version of the CPS.

### *9.12.3 Circumstances under which OID must be changed*

No stipulation.

## 9.13 Dispute resolution provisions

Refer to the individual agreements between Logius PKIoverheid and TSPs.

## 9.14 Governing law

Dutch law shall apply.

## 9.15 Compliance with applicable law

The PA function is performed by Logius. Logius is a digital government service and is part of the Ministry of the Interior and Kingdom Relations The General Administrative Law Act *https://wetten.overheid.nl/BWBR0005537/2018-09-19 (in Dutch)* applies to Logius.

## 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

No stipulation.

# Appendix A. Content fields EV Root & Domein Server CA 2020 intermediate certificate

| | **Staat der Nederlanden EV Root CA** | **The Staat der Nederlanden Server CA 2020** |
|---|---|---|
| Version | V3 | V3 |
| Serial number | 0098968D | 5c:09:9a:34:75:34:a0:ab:11:49:3b:19:d5:5a:53:8a:c6:ac:74:b8 |
| Algorithm for signature | sha256WithRSAEncryption (1.2.840.113549.1.1.11) | sha256WithRSAEncryption |
| Valid from | Wednesday 8 December 2010 12:19:29 | Jul 29 17:26:24 2020 GMT |
| Valid until | Thursday 8 December 2022 12:10:28 | Dec 6 00:00:00 2022 GMT |
| Subject | CN = Staat der Nederlanden EV Root CA<br>O = Staat der Nederlanden<br>C = NL | CN = Staat der Nederlanden Domein Server CA 2020<br>O = Staat der Nederlanden<br>C = NL |
| Public Key | RSA (4096 Bits) | RSA (4096 Bits) |
| Certificate Policies | N/A | Policy: 2.16.528.1.1003.1.2.5.8<br>Policy: 2.16.528.1.1003.1.2.5.9<br>CPS: https://cps.pkioverheid.nl<br>Policy: 2.23.140.1.2.2 |
| Key ID of CA | N/A | keyid:FE:AB:00:90:98:9E:24:FC:A9:CC:1A:8A:FB:27:B8:BF:30:6E:A8:3B |
| CRL distribution | N/A | http://crl.pkioverheid.nl/EVRootLatestCRL.crl |
| Key ID of subject | fe ab 00 90 98 9e 24 fc a9 cc 1a 8a fb 27 b8 bf 30 6e a8 3b | 5A:5D:34:25:C1:88:91:73:F9:DE:E1:0C:D5:F4:EA:18:BF:30:34:6E |
| Essential constraints | Subjecttype=CA<br>Constraint for path length=None | Subjecttype=CA<br>Constraint for path length=None |
| Key usage | Certificate signing , Offline CRL signing, CRL signing | Certificate Sign, CRL Sign |
| SHA256 Fingerprint | 4D2491414CFE956746EC4CEFA6CF6F72E28A1329432F9D8A907AC4CB5DADC15A | 0DA914FB7125F6E644EB7AA261DE9EB809DC7F925B6B2A7D8A7EDD8736398B5B |
| SHA-1 Fingerprint | 76E27EC14FDB82C1C0A675B505BE3D29B4EDDBBB | A2AF8FB631DE777D4DDA9B0B6634EC5A96C52B7C |

# Appendix B. Publication of Official Gazette (Staatscourant) announcement root certificate PKI State of the Netherlands EV Root CA

(Underneath is an English translation of the original publication17. In case of discrepancies the original Dutch version prevails)

The Ministry of the Interior and Kingdom Relations announces that, on the 8th of December 2010, a new root certificate of the PKI for the government has been created under the name

**Staat der Nederlanden EV Root CA**

This root certificate is the central part of PKIoverheid Extended Validation. The root certificate is the pivotal point of trust for PKIoverheid Extended Validation SSL certificates that can be used to secure a connection between a certain client and a server, through the TLS/SSL protocol.

The root certificate holder is identified as (Common name), The State of the Netherlands (Organization), NL (Country).

The serial number of the root certificate is 10000013 (hexadecimal 0098 968C).

The root certificate is valid until: Thursday 8 December 2022 11:10:28 (GMT)

The identification of the root certificate (the fingerprint in hexadecimal form) based on the SHA1 algorithm is: 76E2 7EC1 4FDB 82C1 C0A6 75B5 05BE 3D29 B4ED DBBB

This root certificate, the underlying documents related to this certificate and further information about this root certificate are available in digital format on the website: https://cert.pkioverheid.nl. This website provides an explanation of how the root certificate can be identified.

The Policy Authority of the PKI for the government is responsible for managing the root certificate. This organization is part of Logius, digital government service of the Ministry of the Interior and Kingdom Relations.

*The Ministry of the Interior and Kingdom Relations,*
*P.H. Donner.*

# Appendix C. Procedures for the change control of the PoR PKIoverheid

See Appendix B of the CPS PA PKIoverheid Reguliere Root" which can be found on https://cps.pkioverheid.nl

# Appendix D. Certificate profile TSP CA

| Basic Extensions | OID | Critical | Value |
|---|---|---|---|
| Certificate | | | N/A |
| SignatureAlgorithm•Algorithm | { pkcs-1 5 } | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| SignatureValue | | | Signature by Staat der Nederlanden EV Intermediair CA |
| TBSCertificate | | | N/A |
| Version | | | 2 |
| SerialNumber | | | generated by Staat der Nederlanden EV Intermediair CA |
| Signature | | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Issuer•CountryName | C | | NL |
| Issuer•OrganisationName | O | | Staat der Nederlanden |
| Issuer• CommonName | CN | | The Staat der Nederlanden EV Intermediair CA |
| Validity•NotBefore | | | dd-mm-yyyy |
| Validity•NotAfter | | | dd-mm-yyyy |
| SubjectCountryName | C | | NL |
| Subject•OrganisationName | O | | [name TSP] |
| Subject•CommonName | CN | | [name TSP] PKIoverheid EV CA |
| subjectPublicKeyInfo | | | Public key TSP-CA (Keylength=4096) |
| **Standard Extensions** | **OID** | **Critical** | **Value** |
| CertificatePolicies | {id-ce 32} | FALSE | N/A |
| policyIdentifier | | | 2.16.528.1.1003.1.2.7 |
| PolicyQualifierID | | | 1.3.6.1.5.5.7.2.1 (id-qt-cps) |
| Qualifier | | | https://cps.pkioverheid.nl |

| | | | |
|---|---|---|---|
| KeyUsage | {id-ce 15} | TRUE | N/A |
| KeyCertSign | | | Set |
| CRLSign | | | Set |
| authorityKeyIdentifier | {id-ce 35} | FALSE | N/A |
| KeyIdentifier | | | 160-bit SHA-1 Hash value of the EV Intermediate CA |
| SubjectKeyIdentifier | {id-ce 14} | FALSE | N/A |
| KeyIdentifier | | | 160-bit SHA-1 Hash value of this TSP CA |
| authorityInfoAccess | {id-pe 1} | FALSE | |
| accessMethod | 1.3.6.1.5.5.7.48.1 | | OCSP |
| accessLocation: URI | | | http://ocsp.pkioverheid.nl |
| accessMethod | 1.3.6.1.5.5.48.2 | | Certification Authority Issuer |
| accessLocation: URI | | | https://cert.pkioverheid.nl/EVIntermediairCA.cer |
| CRLDistributionPoints | {id-ce 31} | FALSE | N/A |
| DistributionPoint•FullName | | | http://crl.pkioverheid.nl/EVIntermediairLatestCRL.crl |
| ExtendedKeyUsage | {id-ce 37 } | FALSE | N/A |
| Id-kp-serverAuth | {id-kp 1} | | 1.3.6.1.5.5.7.3.1 |
| Id-kp-clientAuth | {id-kp 2} | | 1.3.6.1.5.5.7.3.2 |
| Id-kp-OTSPsigning | {id-kp 9} | | 1.3.6.1.5.5.7.3.9 |
| BasicConstraints | {id-ce 19} | TRUE | N/A |
| CA | | | Set |
| PathLenConstraint | | | 0 |