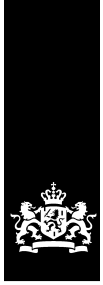

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

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

Date December 2019
Version 1.8

Publisher's imprint

Version number	1.8
Contact	Policy Authority PKIoverheid
Organization	Logius
	Street address Wilhelmina van Pruisenweg 85
	Postal address P.O. Box 96810 2509 JE THE HAGUE
	T +31(0)708896360 servicecentrum@logius.nl

Content

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: - Updated section 4.2 regarding CAA issuance, specific information about CAA records is to be found in the CPS of issuing CAs. - Small update to section 1.2 regarding explanation of the additional "non RFC3647" sections. - 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 - Appendix C of this CPS now refers to Appendix B of the "regular" CPS to avoid errors and duplication - Updated chapter 4.8 to reflect current practices about certificate modification - Removed superfluous sections with general PKI information - 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 - Updated Appendix A & D to better reflect BRGs - Removed superfluous sections with general PKI information - Several small editorial changes.

1.8	December 2019	December 2019		Policy Authority	Jorik van 't Hof	- Updated Chapter 1.2 - Updated Chapter 4.2

1 Introduction

1.1 Overview

1.1.1 *Policy Authority for the PKI for the government*

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

The PKI for the government is an frameworkwhich enables generic and large-scale use of the electronic signature, and it also facilitates remote identification and confidential communication.
The tasks of the PA of PKIoverheid are:

- contributing towards the development and the maintenance of the framework of standards that underlies the PKI for the government, the Programme of Requirements (PoR);
- assisting in the process of admittance by 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.

The Policy Authority (PA) is responsible for managing the entire infrastructure. The PKI for the government 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 within the PKI for the government. The PA oversees the trustworthiness of the entire PKI for the government[1].

Within the scope of PKIoverheid Extended Validation, the PA is generally responsible for:

1. management of the standards system of the PKI for the government, the Programme of Requirements section 3f;
2. management of Object Identifiers, the unique numbers for TSPs and their CPSs;
3. creation and management of the key pair and the corresponding EV root certificate;
4. revoking the EV root certificate and ad-hoc publication of the CRL;
5. periodic publication of the EV CRL;
6. creation and management of key pairs and the corresponding EV Intermediate certificate;
7. revoking the EV Intermediate certificate and ad-hoc publication of the corresponding CRL;
8. preparation concerning the admission of TSPs to the PKIoverheid Extended Validation;
9. implementation of the admission of TSPs, including creation, issuance and management of EV TSP CA certificates;

[1] *See https://zoek.officielebekendmakingen.nl/kst-26387-9.html (in Dutch) for more information.*

10. preparation concerning the revocation of EV TSP CA certificates;
11. implementation of the revocation of EV TSP CA certificates;
12. supervision of admitted TSPs;
13. preparation concerning the renewal of EV TSP CA certificates;
14. implementation of the renewal of EV TSP CA certificates, including creation, issuance and management of new EV TSP CA certificates;
15. registration and assessment of reports regarding infringement of the PKIoverheid Extended Validation.

KPN BV is responsible for the technical management of the Staat der Nederlanden EV Root CA, the Staat der Nederlanden EV Intermediair CA 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.

The purpose of the Policy Authority is:
Maintaining a practicable and trustworthy framework of standards for PKI services that provides an established level of security for the government's communication needs and which is transparent for the users.

1.1.2 *CA model PKIoverheid Extended Validation (non RFC 3647)*
The government's Public Key Infrastructure (PKI) has a structure consisting of a central part managed by Logius (Root CA and Domain CA) and a TSP (Trust Service Provider) or local level. The TSP issues end-user certificates. See for more information Appendix D and part 1 of the Programme of Requirements (CP)[2]

All CAs are based on the **SHA-256** algorithm.

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, relying parties and certificate users* [3] with information regarding the procedures and measures taken in respect of the PA's services with regard to EV certificates. The CPS describes the processes, procedures and control measures for applying for, producing, issuing, managing and revoking EV certificates, insofar as the PA is directly responsible for this. This means that this CPS only relates to PKIoverheid Extended Validation Level 1 (Staat der Nederlanden EV Root CA) and Level 2 (Staat der Nederlanden EV Intermediair CA).

Subject: C = NL, O = Staat der Nederlanden, CN = Staat der Nederlanden EV Root CA

2 https://www.logius.nl/english/pkioverheid/
3 For more information regarding abbreviations, refer to the Programme of Requirements PKIoverheid section 4: definitions and abbreviations (https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-TSP/programma-van-eisen/)

This CPS also describes the processes and procedures for applying for, producing, issuing and revoking Level 3 EV TSP PKIoverheid CA certificates.

For a description of the processes, procedures and control measures for applying for, producing, issuing, managing and revoking Level 4 (EV SSL certificates), please refer to the relevant EV Certification Practice Statements of the PKIoverheid Trust Service Providers

The format of this CPS is in accordance with the RFC3647[4] standard (in full: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework") of the Internet Engineering Task Force. This CPS also includes chapters that are not from the RFC3647 standard. This is indicated by adding 'non RFC3647' to the title of the segment in question. This is for specific PKIoverheid matters, which are not a part of RFC3647.

Formally, this document is referred to as the "CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid for Extended Validation certificates to be issued by the Policy Authority of the PKI for the Dutch government".

The PA publishes only an English version of this CPS; If and when in the future this CPS will be published in another language version, care will be taken in ensuring parity in language versions. In case of discrepancies 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 Extended Validation CA certificates to be issued by the Policy Authority of the PKI for the Dutch government
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.

1.2.1 Objective of CPS (non RFC 3647)

This CPS provides information to *TSPs, subscribers, relying parties and certificate userusers* regarding the procedures and measures taken with regard to the PA's services concerning PKIoverheid Extended Validation. The quality of the services underpins the trust that can be placed in the PKIoverheid Extended Validation. In this respect, the relationship between the PA and Trust Service Providers (TSPs) is also of importance. This relationship and the conditions under which TSPs can participate in the

4 http://www.ietf.org/rfc/rfc3647.txt?number=3647

PKIoverheid Extended Validation are described in general terms. TSPs interested in participating in the PKIoverheid Extended Validation can obtain more detailed information about this subject from the PKIoverheid Programme of Requirements section 2.

1.2.2 Relationship between CPS and CP (non RFC 3647)

CP PoR section 3f describes the minimum requirements laid down in respect of the services of a TSP within PKIoverheid Extended Validation in addition to the basic requirements that apply to all CPs. This CPS states how the PKIoverheid Extended Validation services will be put into practice, insofar as this is under the direct responsibility of the PA, .

1.2.3 CA/Browser Forum Baseline Requirements (non RFC 3647)

The PA of PKIoverheid conforms to the current version of the Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates as published at http://www.cabforum.org. In the event of any discrepancies between PoR section 3f (Policy OID 2.16.528.1.1003.1.2.7), this CPS and the relevant Guidelines, the provisions in the Baseline Requirements shall prevail.

1.2.4 Certificate Policies (CPs) (non RFC 3647)

part 3 of the Programme of Requirements relates to the requirements laid down for the services of a Certification Service Provider (TSP). Nine areas are identified, each of which are covered in a separate part, which are:
Part 3a – Certificate Policy for Organization and Organization Person Domain;
Part 3b – Certificate Policy for Organization and Organization Services Domain;
Part 3c – Certificate Policy for Citizen Domain;
Part 3d – Certificate Policy for Autonomous Devices Domain;
Part 3e – Certificate Policy for Server Certificates.
Part 3f – Certificate Policy for Extended Validation
Part 3g – Certificate Policy for Private Services
Part 3h – Certificate Policy for Private server certificates
Part 3i – Certificate Policy for Private Persons
This CPS only relates to section 3f – Certificate Policy for Extended Validation. The "CPS Policy Authority PKIoverheid
for certificates to be issued by the Policy Authority of the PKI for the government" relates to the other PoR sections (except for partsg, h and i, which are covered by "CPS Policy Authority PKIoverheid for Private Root").

1.2.4.1 *Positioning of the Programme of Requirements (non RFC 3647)*

The *Programme of Requirements* is at the heart of the PA's services. Laid down in the Programme of Requirements are the requirements for the PKI for the government; these requirements are derived from international standards and the applicable legislation.

1.2.4.2 Introduction to the Programme of Requirements (non RFC 3647)

This section (section 1) includes an introduction to the Programme of Requirements and the PKI for the government.

1.2.4.3 Admittance to and regulation (non RFC 3647)
Section 2 describes how a TSP can join the PKI for the government, can demonstrate compliance with the requirements and which formalities have to be met. It also describes how the PA regulates the TSPs that have been admitted.

1.3 PKI Participants

The following parties are involved in the PKI for the government:
1. The Ministry of the Interior and Kingdom Relations;
2. PA;
3. TSP;
4. Subscriber;
5. Certificate user;
6. Relying parties.

The Ministry of the Interior and Kingdom Relations is responsible for PKIoverheid Extended Validation. The Ministry of the Interior and Kingdom Relations makes decisions regarding the layout of the infrastructure and the participation of TSPs in the PKIoverheid Extended Validation. 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 central part[5] of the PKI for the government and supervising and monitoring the work of TSPs that issue certificates under the Staat der Nederlanden EV Root CA of the PKI for the government.
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 obligations of the TSPs that form part of the PKI for the government are defined in the Programme of Requirements, part 3f: Certificate Policies.

A *subscriber* enters into an agreement with a TSP on behalf of one or more certificate users. How the delivery of EV certificates takes place is organized between the subscriber and the TSP.
certificate usercertificate user
The *certificate user* is the holder of the private key belonging to the public key mentioned in the EV certificate. . End users receive the EV SSL certificates from the TSPs. The PA issues certificates to itself (Staat der Nederlanden EV Root CA and The Staat der Nederlanden EV Intermediair CA) and signsEV TSP CA certificates.

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. This obligation is included in the Programme of Requirements, part 3:

5 The central part concerns Staat der Nederlanden EV Root CA and Staat der Nederlanden EV Intermediar CA.

Certificate Policies.

1.4 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. These certificates may not be used for other purposes. The EV SSL end user certificate is issued by the TSPs.

This CPS relates to the trustworthiness of the Policy Authority's services, therefore this paragraph only covers the procedures relating to root, domain and TSP certificates and not the end user/entity certificates.

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 information*

Should there be any complaints, questions or alerts, TSPs within the PKIoverheid framework can contact staff of the PA PKIoverheid through the usual channels. The PA PKIoverheid is available during office hours and will respond as quickly as possible. In the event of reports of incidents or emergencies outside of office hours, the Logius Service Centre should be contacted, which is available 24 hours a day.

Subscribers who have questions concerning the issuance of certificates are asked to initially contact their (potential) TSP.

Other involved parties can contact the Logius Service Centre. The service centre registers the question and will answer this within the stipulated period of time. If necessary, questions asked through the service centre are forwarded to the PA PKIoverheid, or in the event of an incident, to the on-duty incident manager.

Contact information
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

1.5.3 The person who verifies the eligibility of CPS for the CP
The PA PKIoverheid does not have its own Certificate Policy. Approval of the CPS is discussed in 1.5.4.

1.5.4 Change procedure CPS
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.

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/begrippenlijst (in Dutch).

1.7 Guarantees (non RFC3647)

When issuing a PKIoverheid EV certificate, the following parties are recognised:
A. Subscriber;
B. End user;
C. Application Software Suppliers;
D. Relying parties.

These parties are informed that:

The PA of PKIoverheid guarantees that sub-CAs within the PKIoverheid framework are known to the PA and remain under the control of the TSP that has created a sub-CA. In addition these sub-CAs shall not be used for man-in-the middle (*MITM)* purposes.

All valid sub-CA certificates issued within the PKI for the government are listed on this website:
https://cert.pkioverheid.nl

PKIoverheid Extended Validation and its Trust Service Providers guarantee that, when a PKIoverheid EV (SSL) certificate is issued, they have adhered to the requirements as laid down in the, at that time version of the CA/Browser Forum Baseline Requirements for Issuance and Management of Extended Validation Certificates and the PoR section 3f (Policy OID 2.16.528.1.1003.1.7) and that they checked the information included in the EV (SSL) certificate for accuracy and completeness.

For a description of the safeguards, please refer to the relevant EV Certification Practice Statements of the PKIoverheid Trust Service Providers.

1.8 Programme of Requirements and framework council

PKIoverheid Framework Council (non RFC3647)

The Programme of Requirements is the formal framework of standards in respect of the trustworthiness and quality of services within the PKI for the government. When the PA maintains these standards, it is important that the practical experiences and ideas of users are also taken into account. To be able to generate this support for the use of the Programme of Requirements, a PKIoverheid framework council has been set up that is consulted regarding decision-making about change proposals in respect of the Programme of Requirements. Also dealt with during this consultation are subjects that are generally relevant to the PKI developments.
The full set of procedure for the change control of the Programme of Requirements of PKIoverheid are attached as Annex C.

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.

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:

- For revoked Staat der Nederlanden EV Intermediair CA and OCSP respondercertificate(s):
  http://crl.pkioverheid.nl/EVRootLatestCRL.crl
- For revoked EV TSP CA certificates:
  http://crl.pkioverheid.nl/EVIntermediairLatestCRL.crl

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

  - https://roottest-ev.pkioverheid.nl (valid EV PKIoverheid certificate)
  - https://roottest-ev-expired.pkioverheid.nl
  - https://roottest-ev-revoked.pkioverheid.nl

2.2.1 Official electronic notification (non RFC 3647)

The identifying data of Staat der Nederlanden EV Root CA root certificate are published in the Official Gazette (Staatscourant) issue 2011, no. 527, certificate userand is attached to this CPS as Appendix B

2.2.2 Distribution of public key (non RFC 3647)

The public key of Staat der Nederlanden EV Root CA root certificate is published through the trusted root certificate programmes of various software suppliers. An up-to-date list of the software products containing

in Staat der Nederlanden EV Root CA root certificate can be found at https://www.logius.nl/ondersteuning/pkioverheid/browserondersteuning-pkioverheid/ (in Dutch).

Staat der Nederlanden EV Root CA root certificate is also provided in a trustworthy manner at https://cert.pkioverheid.nl.

2.3 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 the lists of revoked certificates, the CRLs. A CRL is generated for both The Staat der Nederlanden EV Root CA and the Staat der Nederlanden Intermediair CA certificate. The CRL for the root is renewed annually or ad-hoc after revocation of The Staat der Nederlanden EV Intermediair CA certificate.

The CRL with revoked EV TSP CA certificates is 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 two OCSP responders are available:

1. http://evrootocsp.pkioverheid.nl provides status information about the EV Intermediair EV certificate
2. http://ocsp.pkioverheid.nl provides status information about the TSP certificates issued by the EV Intermediair CA

The OCSP responders conform to RFC6960[6].

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

2.4 Access 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

6 http://www.ietf.org/rfc/rfc2560.txt

Electronic Repository will undergo a penetration test. This is carried out by an external IT security company.

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 used in the EV certificates fulfil the X.501 name standard. 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
Country (C)	NL	NL	NL
Organization (O)	Staat der Nederlanden	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

Also see Appendix A for the full certificate profiles of Staat der Nederlanden EV Root CA and the Staat der Nederlanden EV Intermediair CA.

3.1.2 Need for names to be meanigful

There are no other provisions in this respect for the certificate services by the PA.

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) [7] and is entered as an exact match.

3.1.5 Uniqueness of names

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

3.1.6 Recognition, authentication and role of trademarks

The PA assumes the correctness of the name of organizations as listed in the Dutch Trade Register of the Chamber of Commerce.

7 National Handelsregister, in the Netherlands managed by the Kamer van Koophandel: www.kvk.nl

3.2 Initial identity validation

3.2.1 Initial Registration Process

For the requirements laid down in relation to the initial registration process, see the PKIoverheid Programme of Requirements, part 2 of PKIoverheid.

3.2.2 Authentication of organizational identity

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

- That the TSP is an existing organization listed in the 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[8] 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 13 months.

Note: If the participating party 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, 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.

3.3 Identification and authentication for Re-Key Requests

Often, a TSP is already part of PKIoverheid when a new TSP CA has to be created under a new generation of the regular root. It is also possible that a TSP that is already part of PKIoverheid, wishes to issue certificates under a new domain or a different root. In that case, 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.

8 http://staatsalmanak.sdu.nl/

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[9];
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 file.

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 reasons for this must always be given. In consultation with the parties involved, it will be examined to what extent the request can be complied with, as revocation of a TSP CA means that the underlying certificates will no longer be valid.

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.

9 Specifically, using an end-user certificate with policy OID 2.16.528.1.1003.1.2.5.2 issued to the authorised representative

4 Certificate Life-Cycle Operational Requirements

4.1 Scope

Within the PKIoverheid Extended Validation, different types of certificates are defined at four levels, which are:

- Staat der Nederlanden EV Root CA;
- The Staat der Nederlanden EV Intermediair CA;
- EV TSP CA;
- End user EV SSL certificates.

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. These certificates may not be used for other purposes. The end user certificate is issued by the TSPs.

This CPS relates to the trustworthiness of the Policy Authority's services, therefore this paragraph only covers the procedures relating to root, domain and TSP certificates.

4.2 Certificate Application

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

The instruction to create EV TSP CA certificates is of a request (PKCS#10) to this end by a TSP. Only a TSP which has been admitted to the PKI for the government (see PoR section 2) can and may apply for an EV TSP CA certificate to be created.

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" or "www.pkioverheid.nl" permits issuance for all TSP's who issue PKIoverheid TLS (EV) certificates.

.

4.2.1 Methodology with regard to creating certificates

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;
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

4.3 Certificate Issuance

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.

4.4 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.

4.5 Key Pair and Certificate Usage

Staat der Nederlanden EV Root CA, The Staat der Nederlanden EV Intermediair CA and the EV TSP CA certificates 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 SSL certificates are issued by the TSPs.

4.6 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.

Approximately 3 to 4 years before expiry of the term of validity of Staat der Nederlanden EV Root CA and The Staat der Nederlanden EV Intermediair CA certificate, the PA of PKIoverheid will create a new generation (G2) of the EV Root CA and the EV Intermediate CA.

A new (G2) EV TSP CA certificate must be applied for and be issued plenty of time before, under an existing EV TSP CA, it will no longer be possible to issue an end user EV SSL certificate with a maximum term of validity of 825 days.

Taking this 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 EV TSP CA certificate.

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 EV TSP CA 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 EV TSP CA 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 EV TSP CA certificate by the technical administrator of the EV root;

- Verification Test of EV TSP CA 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 EV TSP CA certificate;
- Execution of a creation ceremony of new EV TSP CA certificate by the technical administrator of the root;
- Verification by PA of new EV TSP CA certificate;
- Handover by PA of new EV TSP CA certificate to the TSP;
- Discharge of PA to the technical administrator of the EV Root.

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.

4.8 Certificate Modification

Certificate Modification is not applied within the central hierarchy of PKIoverheid

4.9 Certificate Revocation and Suspension

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.

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 certificate will be accompanied by a decision on whether or not a new certificate will be issued to replace the revoked certificate.

The revocation of The Staat der Nederlanden EV Intermediair CA certificate or an EV TSP CA certificate always leads to ad-hoc publication of the relevant modified CRL. The revocation of certificates and the issue of CRLs takes place in accordance with a pre-prepared script. The new

CRL will be published a maximum of 24 hours after revocation of the domain or TSP CA.

Certificate suspension is not supported within PKIoverheid.

4.10 Certificate Status Services

4.10.1 *Operational characteristics of the Certificate Status Service*
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 *Certificate Status 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 attributes of the certificate status service*
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

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.

5 Management, Operational, and Physical Controls

This CPS contains a high-level description of the security measures taken by the PA.

The PA has implemented control measures in order to prevent loss, theft, damage or compromise of infrastructural assets and disruption of activities. The physical set-up is made up of various layers which require separate access control, each layer requiring a higher level of security.A series of measures have also been taken to protect against fire, natural disasters, failure of supporting facilities (such as electricity and telecommunication facilities), the risk of collapse, leakages, etc.

5.1 Physical Security 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)).

5.2 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[10]. 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.

5.3 Personnel Security Controls

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)

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

10 For reasons of confidentiality, this CPS does not state between how many key holders the activation data are distributed.

5.4 Audit logging procedures for security audits

For the purpose of auditing, the PA keeps computer log fileswith 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.

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.

5.5 Records Archival

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.

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

5.6 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

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.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

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.

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

6.2 Private key Protection and Cryptographic Module Engineering 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.

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.

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

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.

6.3 Other aspects of key pair management

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.

All EV certificates have a maximum period of validity:

EV TSP certificates	12 years minus 2 days
The Staat der Nederlanden EV Intermediair CA	12 years minus 1 day
Staat der Nederlanden EV Root CA	12 years
OCSP Responder certificates	14 months

6.4 Activation data

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.

6.5 Computer Security Controls

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.

6.6 Life C

6.7 ycle Security Controls

The hardware and software used in the central hierarchy for the key management is classified by the NBV[11]at level "Staatsgeheim confidentieel"[12]. If any changes are made to the information systems, another evaluation is performed.

After extensive testing, CA systems are taken in production and maintained by the technical administrator. Software updates are carefully implemented after consultation with and in the presence of the PA PKIoverheid.

6.8 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.

6.9 Time-stamping

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

11 Netherlands National Communications Security Agency (Nationaal Bureau voor Verbindingsbeveiliging)

12 Comparable to "confidential" in UK/US government classifications

7 Certificate and CRL profiles

7.1 Certificate Profiles

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.

7.2 CRL profiles

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 Describes the version of the CRL profile. Value 1 represents X.509 version 2 CRL profile.
Provider	CN = Staat der Nederlanden EV Root CA or Staat der Nederlanden EV Intermediair CA O = The State of the Netherlands 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. Contains the date and time on which the next version of the CRL is expected (at the latest).
Algorithm for the signature	SHA256 The value is equal to the field signatureAlgorithm and contains the algorithm that is used for signing. The signing algorithm is SHA-256WithRSAEncryption.
Revocation list	Revoked certificates with the date of revocation. 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

7.3 OCSP profiles

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 O=Staat der Nederlanden CN=Staat der Nederlanden EV Root CA or Staat der Nederlanden EV Intermediair CA
Subject DN			C=NL O=Staat der Nederlanden 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 and circumstances of the conformity 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 and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security . Each year, the PA of PKIoverheid undergoes a full period-of-time audit to confirm this.[13]

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 the auditor

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

8.3 Topics covered by the conformity 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 Actions based on deviations

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

8.5 Communicating the 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.

8.6 Admittance of TSPs to the PKI for the government

See "section 2 of the Programme of Requirements PKIoverheid"[14]

13 http://www.webtrust.org/principles-and-criteria/item83172.aspx

14 https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-TSP/programma-van-eisen/

9 Other Business and Legal Matters

9.1 Fees

The Staat der Nederlanden EV Intermediair CA and the EV TSP CA 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.

9.2 Financial Responsibility

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 3f. 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.

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 3f.

The State of the Netherlands has not taken out insurance for claims for compensation in respect of any liability.

9.3 Confidentiality of Business 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 Confidentiality of Personal Information

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.

9.5 Intellectual Property Rights

This document is made available to the general public under the CC-BY-ND 4.0 license.

9.6 Representations and Warranties

See paragraph 9.2.

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

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).

9.11 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[15] and the auditor(s) of the participating TSPs.

9.12 Amendments

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.

15 Radiocommunications Agency. See also https://www.agentschaptelecom.nl/onderwerpen/zakelijk-gebruik/eidas-elektronische-vertrouwensdiensten/trust-service-providers

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

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[16] applies to Logius.

16 https://wetten.overheid.nl/BWBR0005537/2018-09-19 (in Dutch)

Appendix A. Content fields EV Root & Intermediate certificate

	Staat der Nederlanden EV Root CA	**The Staat der Nederlanden EV Intermediair CA**
Version	V3	
Serial number	0098968D	0098969a
Algorithm for signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Valid from	Wednesday 8 December 2010 12:19:29	Wednesday 8 December 2010 13:41:43
Valid until	Thursday 8 December 2022 12:10:28	Wednesday 7 December 2022 13:38:55
Subject	CN = Staat der Nederlanden EV Root CA O = Staat der Nederlanden C = NL	CN = The Staat der Nederlanden EV Intermediair CA O = Staat der Nederlanden C = NL
Public Key	RSA (4096 Bits)	RSA (4096 Bits)
Certificate Policies	N/A	PolicyQualifiers:policyQualifierId: 2.16.528.1.1003.1.2.7 (PKIoverheid explicit EV policy identifier) Qualifier:cPSuri: https://cps.pkioverheid.nl
Key ID of CA	N/A	Key-ID= 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	25 80 eb d8 9f a6 c3 11 41 37 c7 78 59 88 1e 69 ef b1 d3 ea
Essential constraints	Subjecttype=CA Constraint for path length=None	
Key usage	Certificate signing , Offline CRL signing, CRL signing	

	Staat der Nederlanden EV Root CA	**The Staat der Nederlanden EV Intermediair CA**
Fingerprint algorithm	SHA256	
SHA-1 Fingerprint	4D:24:91:41:4C:FE:95:67:46:EC:4C:EF:A6:CF:6F:72:E2:8A:13:29:43:2F:9D:8A:90:7A:C4:CB:5D:AD:C1:5A	DC:86:2A:3F:02:5E:F7:F2:52:FA:94:13:CB:60:DE:25:E5:7E:6A:A7:E1:FB:1D:CA:7B:59:D2:C2:21:71:06:EA

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.

17 https://zoek.officielebekendmakingen.nl/stcrt-2011-527.html

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

See Appendix B of theCPS 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