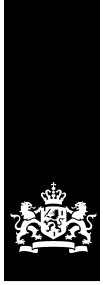

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

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

Date December 2019
Version 1.5

Publisher's imprint

Version number	1.5
Contact	Policy Authority PKIoverheid
Organization	Logius
	Street address Wilhelmina van Pruisenweg 52
	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 of entry into force	Status	Author	Description
1.0	June 2014	July 2014	Adopted by the Director of Logius	Policy Authority	First version of the CPS for the private root
1.1	February 2015	February 2015	Adopted by the Director of Logius	Policy Authority	Editorial changes
1.2	October 2016	October 2016	Adopted by the Director of Logius	Policy Authority	Amendment of ETSI TS 102 042 to ETSI EN 319 411-1 and some editorial changes
1.3	December 2017	December 2017	Adopted by the PA PKIoverheid	Policy Authority	Mark Janssen
1.4	December 2018	December 2018	Adopted by the Director of Logius	Policy Authority	Changes to bring the CPS for the Private Root in line with the CPS for EV and regular (publicly trusted) certificates: - 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 - Updated change procedure in annex B to list possibility of changes being effective

					immediately after publication of a new version of the PoR - Updated change procedure PoR (CP) to reflect current practices - Updated chapter 4.8 to reflect current practices about certificate modification - Removed superfluous sections with general PKI information - Several small editorial changes.
1.5	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 (MinBZK) in managing the PKI for the government.

The PKI for the government is a framework which 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:

1. contributing towards the development and the maintenance of the framework of standards that underlies the PKI for the government, the Programme of Requirements (PoR);
2. assisting in the process of admittance by Trust Service Providers (TSPs) to the PKI for the government and preparing the administration;
3. 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 (private root), the PA is generally responsible for:

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

[1] *See in this respect the paper "De Elektronische Overheid aan het begin van de 21e eeuw" (House of Representatives, session Lower House 2000-2001, 26 387, no. 9) by the Minister for Major Cities - and Integration Policies to the President of the House of Representatives of the States - General.*

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

KPN BV is responsible for the technical management of the Staat der Nederlanden Root CA and Staat der Nederlanden <Domain> CAs and the corresponding Certificate Revocation Lists (CRLs). The PA doesn't support an Online Certificate Status Protocol (OCPS) service under the Private Root CA.

The management of root certificates and domain certificates is entrusted to the Policy Authority of the PKI for the government. 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 (non RFC3647)

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 within the PKI for the government (hereinafter referred to as CPS) provides *TSPs, subscribers, relying parties and certificate holders* with information regarding the procedures and measures taken in respect of the PA's services with regard to certificates. The CPS describes the processes, procedures and control measures for applying for, producing, issuing, managing and revoking certificates, insofar as the PA is directly responsible for this. This means that this CPS only relates to PKIoverheid Level 1 (Staat der Nederlanden Private Root CA – G1) and Level 2 (Staat der Nederlanden Private Services CA – G1.

Subject: C = NL, O = Staat der Nederlanden, CN = Staat der Nederlanden Private Root CA - G1

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

2 https://www.logius.nl/english/pkioverheid/

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

The format of this CPS is, as far as possible, in accordance with the RFC3647[3] standard (in full: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework") of the Internet Engineering Task Force. When this CPS included 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 Private Root certificates to be issued by the Policy Authority of the PKI for the dutch government ".

The PA ~~for now~~ publishes only an English version of this CPS; If and when in the future this CPS will be published in another language version, ~~Great~~ care will be taken in ensuring parity in language versions. In case of discrepancies between the English and Dutch ~~other language~~ versions of this document, the English version shall prevail.

CPS	Description
Naming	CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid for Private Root 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 RFC3647)

This CPS provides information to *TSPs, subscribers, relying parties and certificate holders* regarding the procedures and measures taken with regard to the PA's services. The quality of the services underpins the trust that can be placed in the PKI for the government. 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 PKI for the government are broadly described. TSPs interested in participating in the PKI for the government can obtain more detailed information about this subject from the PKIoverheid Programme of Requirements part 2.

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

1.2.2 Relationship between CPS and CP (non RFC3647)

The CP PoR parts 3g through 3i describes the minimum requirements stipulated in relation to the services of a TSP within PKIoverheid. This CPS states how the PKIoverheid 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 RFC3647)

The Staat der Nederlanden Private Root CA is not publicly trusted by any Application Software Suppliers. As such, the Baseline Requirements of the CA/Browser Forum do not apply. However, the PA monitors the current developments of the BRG and will include controls and requirements from the BRG if deemed necessary for PKIoverheid Private Root certificates.

1.2.4 Certificate Policies (CPs) (non RFC3647)

This part relates to the requirements laid down for the services of a Trust 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 CP parts 3g through 3i. The "CPS Policy Authority PKIoverheid for Extended Validation certificates to be issued by the Policy Authority of the PKI for the government" relates to CP part 3f. The "CPS Policy Authority PKIoverheid for certificates to be issued by the Policy Authority of the PKI for the government" relates to sections 3a to 3e inclusive.

1.2.4.1 *Positioning Programme of Requirements (non RFC3647)*

The Programme of Requirements forms the basis 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. The Programme of Requirements is made up of four parts and in each part, a specific aspect of the PKI for the government is elaborated on in further detail.

1.2.4.2 Introduction Programme of Requirements (non RFC3647)

This part includes an introduction to the Programme of Requirements and the PKI for the government.

1.2.4.3 Admittance and supervision (non RFC3647)

Part 2 describes how a TSP can be admitted to 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

In this CPS, six parties are identified, each with their own responsibility within the PKI for the government. Consecutively, these parties are:

1. the Ministry of the Interior and Kingdom Relations;
2. the Policy Authority (PA);
3. the Trust Service Provider (TSP);
4. Subscriber;
5. Certificate holder;
6. The relying party.

The Ministry of the Interior and Kingdom Relations is responsible for the PKI for the government. The Ministry of the Interior and Kingdom Relations makes decisions regarding the layout of the infrastructure and the participation of TSPs in the PKI for the government. 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[4] of the PKI for the government and supervising and monitoring the work of TSPs that issue certificates under the Staat der Nederlanden 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 holders. The obligations of the TSPs that form part of the PKI for the government are defined in the Programme of Requirements, parts 3a through 3e: Certificate Policies.

A *subscriber* enters into an agreement with a TSP on behalf of one or more certificate holders. How the delivery of certificates takes place is organized between the subscriber and the TSP.

The *certificate holder* is the holder of the private key belonging to the public key contained in the certificate. Certificate holders can be found at all levels in the hierarchy of the PKI for the government. End users receive the certificates from the TSPs. The PA issues certificates to itself (Staat der Nederlanden Root CA and Staat der Nederlanden <Domain> CAs) and to TSPs (TSP CA).

The *relying party* is the recipient of a certificate issued within the PKI for the government and acts on the basis of trust in the 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: Certificate Policies.

4 The central part concerns Staat der Nederlanden Root CA and Staat der Nederlanden <domain> CAs.

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 end user certificate is issued by the TSPs. End user certificates can be used for authenticity, non-repudiation, confidentiality and a combination of authenticity and confidentiality.

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.

1.5 Policy Administration

1.5.1 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 for observing the procedure described in paragraph 9.12 accurately and for the ultimate approval of this CPS in accordance with this procedure.

1.6 Definitions and Acronyms

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

For a list of the used definitions and acronyms, please refer to http://www.logius.nl/begrippenlijst (in Dutch).

1.7 Guarantees (non RFC3647)

When issuing PKIoverheid certificates, 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

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

1.8 Programme of Requirements and 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. While 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. The Council also discusses subjects that are generally relevant to the PKI developments.
The full set of procedures for the change control of the Programme of Requirements of PKIoverheid is attached as Annex B.

2 Publication and 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.

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 certificates can be found on the websites of the various TSPs.

2.2 Publication certificate information

The following certificates are published:

- Staat der Nederlanden Private Root CA – G1;
- Staat der Nederlanden Private Personen CA –G1;
- Staat der Nederlanden Private Services CA – G1;
- <Name TSP> PKIoverheid Privates Services CA – G1;
- <Name TSP> PKIoverheid Private Personen CA – G1.

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 https://crl.pkioverheid.nl. Below are the direct links to the CRLs:

- For revoked State of the Netherlands CA domain certificates:
  http://crl.pkioverheid.nl/PrivateRootLatestCRL-G1.crl

- For revoked TSP CA certificates:
- http://crl.pkioverheid.nl/DomPrivatePersonenLatestCRL-G1.crl
- http://crl.pkioverheid.nl/DomPrivateServicesLatestCRL-G1.crl

2.2.1 Official electronic notification (non RFC3647)
The attributes of the root certificate The State of the Netherlands Private root CA – G1 are published in the Official Gazette (Staatscourant) and attached in Appendix A.

2.2.2 Distribution Public Key (non RFC3647)
The public key of the root certificate is not distributed in any browser. Acceptance of the Root CA and issued certificates depends on manual installation of the Staat der Nederlanden Private Root CA.

The root certificates are 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 Certificate Revocation Lists (CRLs). There is a CRL with revoked domain certificates. This CRL is renewed every 12 months. This CRL is published ad-hoc after revocation of a domain certificate.

For each domain, there is a CRL with revoked TSP certificates within that domain. A domain CRL is renewed every 12 months. A domain CRL is published ad-hoc after revocation of a TSP certificate.

Each CRL contains the time of the next planned CRL release. These CRLs can be found at: https://crl.pkioverheid.nl.

The PA doesn't support OCSP for the Private Root.

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 unauthorised changes being made.

In the event of system failure 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 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 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 certificates issued by the PA of PKIoverheid contain a 'subject' field (DistinguishedName) which lists the name of the holder. The names used in the certificates fulfil the X.501 name standard. The names consist of the following components:

Attribute	Staat der Nederlanden Root Private Root CA CA – G1	Staat der Nederlanden Private <Domain> CA – G1	<TSP name> PKIoverheid Private <domain name>CA – G1
Country (C)	NL	NL	NL
Organization (O)	Staat der Nederlanden	Staat der Nederlanden	<TSP Organization name>
CommonName (CN)	Staat der Nederlanden Private Root CA-G1	Staat der Nederlanden Private <domain> CA – G1	<TSP name> PKIoverheid Private <domain> CA – G1

Figure 4 - Staat der Nederlanden Private naming scheme

For other provisions regarding the way in which identification and authentication take place within PKIoverheid, please refer to the relevant Certification Practice Statements of the PKIoverheid Trust Service Providers.

Need for names to be meaningful

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

3.1.2 Pseudonyms

The use of pseudonyms or anonymous certificates is not permitted.

3.1.3 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 Dutch Trade Register and entered as an exact match.

3.1.4 Uniqueness of names

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

3.1.5 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.

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.

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 State Almanac 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 State Almanac.

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 issued 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.

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 PKIoverheid certificate[5];
2. The authorised representative can sign an application form and send this by post.

In the second case, the registered authorised representative of the TSP CA should also be contacted by the PA 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;

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

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 Scope

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

- Root certificate (Staat der Nederlanden Root CA – Gx
- Domain certificate (Staat der Nederlanden Domein <name> - Gx;
- 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 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

The root certificate, the domain certificates and TSP certificates are created by the Policy Authority, at the instruction of the Ministry of the Interior and Kingdom Relations.

The instruction to create TSP CA certificates is by means of a request to this end by a TSP. For more information, see PKIoverheid PoR part 2.

When TSP CAs are signed, the PA PKIoverheid does not verify CAA records.

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 external IT auditor acts as witness during the creation ceremonies of the Staat der Nederlanden Root CA and Staat der Nederlanden <Domain> CA. A certified Webtrust auditor is also present as witness during the signing of the TSP CAs. For every key ceremony, a detailed script is produced which lists all tasks to be carried out. The 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 in a similar manner for all of the listed types of certificates, where the certificate holder is either 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), with enforced multi person access control, where several security key guardians each introduce part of the necessary security key access;
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 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 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

The Staat der Nederlanden Private Root CA – G1, Staat der Nederlanden Private <Domain> CAs and the TSP CAs certificates are primarily used to verify the issuer's signature and are issued by the PA. These certificates are also used for CRL signing. These certificates may not be used for other purposes. The end user 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 as included in the certificate, changes or if the strength of a cryptographic algorithm is deemed insufficient and a stronger cryptographic algorithm is needed.

Certificate Renewal, where the existing key pair is maintained and the maximum validity period of a certificate is extended, is not applied within the central hierarchy of 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.

Once every five years, the PA will generate new signing keys (for root and domains) and issue new certificates (root certificate and domain certificates). The new signing keys replace the previous versions; the original certificates will continue to exist alongside the new certificates. The original certificates can be used to verify certificates that are issued under the original root.

The signing keys of a TSP have to be renewed at the time at which the lifespan of the parent certificate (TSP certificate, domain certificate or root certificate) expires, minus the term of validity of the end user certificate. Taking this required verification period into account, a TSP has to create new signing keys (or arrange for these to be created) and also submit a request to the PA to create the new TSP certificate.

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

- Submission of an application form to renew a TSP CA under the new root by the authorised representative of the TSP;
- Verification of the validity of the request by the PA;
- Validation of the data in the application form;
- Submission of the Naming Document for the new TSP CA certificate by the TSP;
- Verification of the Naming Document by the PA;
- Submission of the Certificate Signing Request (CSR) by TSP for Test TSP CA;
- Creation of a Test TSP CA certificate by the technical administrator of the root;
- Verification Test of 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 of the root for the creation of a new TSP CA certificate;
- Execution of a creation ceremony of new TSP CA certificate by the technical administrator of the root;

- Verification by PA of new TSP CA certificate;
- Handover by PA of new TSP CA certificate to the TSP;
- Discharge of the technical administrator of the root by PA.

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 case 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 revocation of a root certificate, a domain certificate or a TSP certificate and the keys associated with this 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 PKI for the government, the PA can revoke the relevant TSP certificate. The revocation of a certificate can be effectuated within one day. The PA informs the TSP prior to the certificate being revoked.

In the event of the revocation of a domain certificate, the PA can inform the child CAs (TSPs).

The decision to revoke a domain 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 a domain certificate or a TSP 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 a 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.

With regard to its CRL service, 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 .

4.10.2 Certificate Status Service availability
The CRL service is 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 service, the following actions will be undertaken:

1. All involved parties (subscribers, cross-certifying CAs, TSPs and relying parties) of the PKIoverheid service shall be informed six months before the service ends.
2. All certificates that are issued after announcement of termination of the service has been communicated SHALL NOT contain a NotAfter date which is later than the planned termination date of PKIoverheid.
3. When the service ends, all certificates that are still valid SHALL be revoked.
4. On the termination date, PKIoverheid 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 service to a different organization, all involved parties (subscribers, cross-certifying CAs, parent CAs and relying parties) of the PKIoverheid 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 the root of the PKI for the government is set up based on the requirements formulated in the *WebTrust Program for Certification Authorities*, 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 on 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 certificates. The PA can only generate key material and 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[6]. Other conditions are:

- The CA systems are stand-alone systems, without external network links;
- During operational use, CA systems are situated in a secure room that can only be accessed by persons authorised to do so;
- After use, the CA system along with all peripheral equipment and key parts are stored in a safe that is located in the aforementioned 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. Where considered necessary, the PA will let people in positions of trust be screened via 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.

5.4 Audit Logging Procedures for security audits

For the purpose of auditing, the PA keeps computer log files on 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.

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

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 certificate holders 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 of potential emergencies that may arise within the PKI for the government, 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 PKI for the government (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 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 system are then also tested.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

The key pairs of the PA 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 USB stick or smartcard. Because the generation and the use of the signing key of the PA 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 signing keys of the the Private Root CAs have the following key lengths:

TSP certificates	4096 bit RSA keys
Domain certificates	4096 bit RSA keys
Root certificate	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:

1. the requirements laid down in the standard FIPS PUB 140-2 level 3 or higher, or;
2. 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 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.

For the certificates of the Private Root hierarchy the following term of validity applies:

TSP certificates	15 years minus 2 days
Staat der Nederlanden Private <Domain> CA – G1	15 years minus 1 day
Staat der Nederlanden Root CA –<Gen>	15 years

6.4 Activation data

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

6.5 Computer Security Controls

The PA computer systems used to perform actions with a CA private key can only be accessed by authorised members of staff. Software-based checks are incorporated in the systems which are taking 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 implemented in such a way that only the essential actions can be performed. All unnecessary components, such as additional software installed with the OS, are removed. The computer systems are stand-alone and airgapped systems, therefore provisions relating to network security do not apply.

Only the 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 modified unnoticed. This is monitored throughout the entire lifecycle of the cryptographic hardware and software.

6.6 Life Cycle Security Controls

The hardware and software used in the central hierarchy for the key management are classified by the NBV[7] at the level "Staatsgeheim

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

confidentieel”[8]. 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.

6.7 Network Security Controls

The Staat der Nederlanden Private Root CA – G1 is offline. The Staat der Nederlanden Private <Domain> CAs are also offline. The CRLs described in this in CPS are provisioned online by means of the Certificate Status Service. The technical administrator of the Staat der Nederlanden Root CA 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 Certificate Status Services are part of the annual Webtrust audit.. In addition, every year Certificate Status Services undergoes a 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.

8 Comparable to “confidential” in UK/US government classifications

7 Certificate and CRL profiles

7.1 Certificate Profile

Appendix C contains an overview of the content of the fields of the Private Root CA certificate and of the Private domain CA certificates.

The PA validates that 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 CRLs of PrivateRoot CAs are valid for one year. This is also the case for the CRLs of the Private domain CAs.

Attribute	
Version	V2 Describes the version of the CRL profile. Value 1 represents X.509 version 2 CRL profile.
Provider	CN = Staat der Nederlanden Private Root CA – G1 or Staat der Nederlanden Private <Domain> CA – G1 O = Staat der Nederlanden 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

OCSP service is not supported within level 1 and 2 (Root and Domain CA) of the Staat der Nederlanden Private Root hierarchy.

8 Compliance Audit and Other Assessment

8.1 Frequency and circumstances of the conformity assessment

The PA of PKIoverheid shall comply with the requirements described in the latest version of the WebTrust Principles and Criteria for Certification Authorities. Each year, the PA of PKIoverheid undergoes an full period-of-time audit for this.[9]

The PA PKIoverheid shall actively monitor the changes in the WebTrust Principles that affect this CPS. The PA PKIoverheid will 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 and, if deemed necessary, incorporated in the PoR and/or this CPS.

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 of results

Through a WebTrust seal, published yearly on the Logius website, the PA PKIoverheid demonstrates that it meets the WebTrust requirements.

8.6 Admittance of TSPs to the PKI for the government

See "part 2 of the Programme of Requirements PKIoverheid"[10]

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

10 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 <Domain> CAs 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);
- consulting the Programme of Requirements: Certificate Policies and;
- 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 concerning participation of the relevant TSP in the PKI for the government. 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. 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, part 3: Certificate Policies.

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 encrypted before exchange will take place.

9.4 Confidentiality of Personal Information

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

9.5 Intellectual Property Rights

This CPS is the property of Logius. Unaltered copies of this CPS may be distributed and published without consent, provided that the source is quoted.

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 1.4 of the "CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid for Private Root CA certificates to be issued by the Policy Authority of the PKI for the Dutch 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 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[11]and the auditor(s) of the participating TSPs.

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

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.

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 Government organisations. The General Administrative Law Act[12] applies to Logius.

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

Appendix A. Publication of Root Certificate announcement

(Underneath is an English translation of the original publication[13]. In case of discrepancies the original Dutch version prevails)

The Minister of the Interior and Kingdom Relations announces that, on the 15th of November 2013, a new root certificate of the PKI for the government has been created under the name

Staat de Nederlanden Private Root CA - G1

This root certificate is the central part of the PKI for the government. The root certificate is the pivotal point for trust in electronic transactions from and with the government when establishing identity, issuing indications of wishes and communicating confidentially.

The root certificate holder is identified as Staat der Nederlanden Private Root CA – G1 (Common name), Staat der Nederlanden (Organization), NL (Country).

The serial number of the root certificate is 10004001 (hexadecimaal 00 98 a6 21).

The root certificate is valid until: Tuesday 14 November 2028 0:00:00 hours.

The identification of the root certificate (the fingerprint in hexadecimal form) based on the SHA1 algorithm is: 2a fd b9 2b 1e fa c3 84 87 06 db 81 ff 86 97 75 0d eb 01 8b.

13 https://zoek.officielebekendmakingen.nl/stcrt-2015-6676.html

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: http://www.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 Minister of the Interior and Kingdom Relations.

Appendix B. Procedures for the change management of the PoR PKIoverheid

See appendix B of the "CPS Policy Authority PKIoverheid for CA certificates to be issued by the Policy Authority of the PKI for the Dutch government"

Appendix C. Content fields Private Root CA – G1 certificate and domain certificates

Attribute	**Staat der Nederlanden Private Root CA - G1**	**Staat der Nederlanden Private Personen CA – G1**	**Staat der Nederlanden Private Services CA – G1**
Version	V3		
Serial number	00 98 a6 21	98 00 a8 96	98 00 a8 86
SignatureAlgorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		
Issuer	CN = Staat der Nederlanden Private Root CA – G1 O = Staat der Nederlanden C = NL		
notBefore	Thursday 14 November 2013 14:48:55	Friday 15 November 2013 11:52:33	Friday 15 November 2013 11:04:13
notAfter	Tuesday 14 November 2028 0:00:00	Monday 13 November 2028 0:00:00	Monday 13 November 2028 0:00:00

Attribute	**Staat der Nederlanden Private Root CA - G1**	**Staat der Nederlanden Private Personen CA – G1**	**Staat der Nederlanden Private Services CA – G1**
Subject	CN = Staat der Nederlanden Private Root CA – G1 O = Staat der Nederlanden C = NL	CN = Staat der Nederlanden Private Personen CA – G1 O = Staat der Nederlanden C = NL	CN = Staat der Nederlanden Private Services CA – G1 O = Staat der Nederlanden C = NL
Public Key	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)
Certificate Policies	N/A	2.16.528.1.1003.1.2.8.1 2.16.528.1.1003.1.2.8.2 2.16.528.1.1003.1.2.8.3 Policy qualification-ID=CPS https://cps.pkioverheid.nl	2.16.528.1.1003.1.2.8.4 2.16.528.1.1003.1.2.8.5 2.16.528.1.1003.1.2.8.6 Policy qualification-ID=CPS https://cps.pkioverheid.nl
Authority Key Identifier (AKI)	N/A	Key-ID= 2a fd b9 2b 1e fa c3 84 87 06 db 81 ff 86 97 75 0d eb 01 8b	
CRL distribution	N/A	URL= http://crl.pkioverheid.nl/PrivateRootLatestCRL-G1.crl	
Subject Key Identifier (SKI)	2a fd b9 2b 1e fa c3 84 87 06 db 81 ff 86 97 75 0d eb 01 8b	a0 04 23 5c 21 bd 07 73 81 e1 64 63 56 64 b2 6a bd d6 55 6d	3e af a8 0f 87 a2 2c 41 7b 14 6c 1b f3 db 68 d3 92 a7 44 a8
Access to CA data	N/A	N/A	N/A

Attribute	**Staat der Nederlanden Private Root CA - G1**	**Staat der Nederlanden Private Personen CA – G1**	**Staat der Nederlanden Private Services CA – G1**
Essential constraints	Subjecttype=CA Constraint for path length=None		
SHA256 fingerprint	02:57:CE:27:B5:24:08:E2:4E:E2:C0:94:56:40:B7:23:C5:BC:66:DD:BD:A4:AD:A5:8C:60:35:76:04:F0:E6:75	DC:49:94:98:82:D6:AC:E7:EC:23:52:0B:B2:A6:25:C6:F0:B0:8F:41:60:24:49:E4:2A:D7:F5:CE:8B:5D:46:59	2E:AA:F6:78:E6:45:DC:26:EA:82:C0:16:EF:39:60:93:56:59:CF:81:B4:C4:4D:9B:2D:0F:B1:A1:42:66:6C:98

Appendix D. Certificate profile TSP CA

TSP CA Private Personen

Basic Extensions	OID	Critical	Value
Certificate			N/A
SignatureAlgorithm•Algorithm	{ pkcs-1 5 }		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
SignatureValue			Signature generated by Staat der Nederlanden Private PersonenCA – G1
TBSCertificate			N/A
Version			2
SerialNumber			generated by Staat der Nederlanden Private Personen CA – G1
Signature			sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer•CountryName	C		NL
Issuer•OrganisationName	O		Staat der Nederlanden
Issuer• CommonName	CN		Staat der Nederlanden Private Personen CA – G1
Validity•NotBefore			dd-mm-yyyy
Validity•NotAfter			dd-mm-yyyy
SubjectCountryName	C		NL
Subject•OrganisationName	O		[TSP name]
Subject.OrganisationIdentifier			<NTR number> or <Government Identification Number> number of TSP in accordance with syntax from paragraph 5.1.4 of ETSI EN 319 412-1
Subject•CommonName	CN		[TSP Name] PKIoverheid Private Personen CA – G1

subjectPublicKeyInfo			Public key CSP-CA (Keylength=4096)
Standard Extensions	OID	Critical	Value
CertificatePolicies	{id-ce 32}	FALSE	N/A
policyIdentifier			2.16.528.1.1003.1.2.8.1
policyIdentifier			2.16.528.1.1003.1.2.8.2
policyIdentifier			2.16.528.1.1003.1.2.8.3
Qualifier•CPSURL			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 Private Personen CA – G1
SubjectKeyIdentifier	{id-ce 14}	FALSE	N/A
KeyIdentifier			160-bit SHA-1 Hash value of this TSP CA
authorityInfoAccess		FALSE	
accessMethod	1.3.6.1.5.5.48.2		Certification Authority Issuer
accessLocation: URI			http://cert.pkioverheid.nl/DomPrivatePersonenCA-G<nummer>
CRLDistributionPoints	{id-ce 31}	FALSE	N/A
DistributionPoint•FullName			http://crl.pkioverheid.nl/DomPrivatePersonenLatestCRL-G<nummer>.crl
BasicConstraints	{id-ce 19}	TRUE	N/A
CA			Set
PathLenConstraint			0

QcStatement2	{ id-qcs-pkixQCSyntax-v2 }	FALSE	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)

TSP CA Private Services

Basic Extensions	OID	Critical	Value
Certificate			N/A
SignatureAlgorithm•Algorithm	{ pkcs-1 5 }		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
SignatureValue			Signature generated by Domain Private Services CA – G1
TBSCertificate			N/A
Version			2
SerialNumber			generated by Domain Private Services CA – G1
Signature			sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer•CountryName	C		NL
Issuer•OrganisationName	O		Staat der Nederlanden
Issuer• CommonName	CN		Staat der Nederlanden Private Services CA – G1
Validity•NotBefore			dd-mm-yyyy
Validity•NotAfter			dd-mm-yyyy
SubjectCountryName	C		NL
Subject•OrganisationName	O		[TSP name]
Subject.OrganisationIdentifier			<NTR number> or <Government Identification Number> number of TSP in accordance with syntax from paragraph 5.1.4 of ETSI EN 319 412-1
Subject•CommonName	CN		[TSP Name] PKIoverheid Private Services CA – G1
subjectPublicKeyInfo			Public key CSP-CA (Keylength=4096)
Standard Extensions	**OID**	**Critical**	**Value**
CertificatePolicies	{id-ce 32}	FALSE	N/A
policyIdentifier			2.16.528.1.1003.1.2.8.4
policyIdentifier			2.16.528.1.1003.1.2.8.5

policyIdentifier			2.16.528.1.1003.1.2.8.6
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 Private Services CA – G1
SubjectKeyIdentifier	{id-ce 14}	FALSE	N/A
KeyIdentifier			160-bit SHA-1 Hash value of this CSP CA
authorityInfoAccess		FALSE	
accessMethod	1.3.6.1.5.5.48.2		Certification Authority Issuer
accessLocation: URI			http://cert.pkioverheid.nl/DomPrivateServicesCA-G1cer
CRLDistributionPoints	{id-ce 31}	FALSE	N/A
DistributionPoint•FullName			http://crl.pkioverheid.nl/DomPrivateServicesLatestCRL-G1crl
BasicConstraints	{id-ce 19}	TRUE	N/A
CA			Set
PathLenConstraint			0
QcStatement2	{ id-qcs-pkixQCSyntax-v2 }	FALSE	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)