



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

CERTIFICATION PRACTICE STATEMENT (CPS)
Policy Authority PKIoverheid for G2 and G3 CA
certificates to be issued by the Policy Authority of the
PKI for the Dutch government

Date December 2020
Version 4.4

Publisher's imprint

Version number 4.4
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

Publisher's imprint.....	2
Content	3
1 Introduction.....	9
1.1 <i>Overview.....</i>	9
1.1.1 Policy Authority for the PKI for the government	9
1.1.2 CA model PKIoverheid (non RFC3647)	10
1.2 <i>Document Name and Identification.....</i>	10
1.2.1 Objective of CPS (non RFC3647).....	11
1.2.2 Relationship between CPS and CP (non RFC3647).....	12
1.2.3 CA/Browser Forum Baseline Requirements (non RFC3647)	12
1.2.4 Certificate Policies (CPs) (non RFC3647)	12
1.3 <i>PKI Participants.....</i>	13
1.4 <i>Certificate Usage.....</i>	14
1.5 <i>Policy Administration.....</i>	14
1.5.1 Organization responsible for managing the CPS	14
1.5.2 Contact information.....	14
1.5.3 The person who verifies the eligibility of CPS for the CP	15
1.5.4 Change procedure CPS.....	15
1.6 <i>Definitions and Acronyms.....</i>	15
1.7 <i>Guarantees (non RFC3647).....</i>	15
1.8 <i>Programme of Requirements and PKIoverheid Framework Council (non RFC3647).....</i>	16
2 Publication and Repository Responsibilities	17
2.1 <i>Electronic repository.....</i>	17
2.2 <i>Publication certificate information.....</i>	17
2.2.1 Official electronic notification (non RFC3647)	18
2.2.2 Distribution Public Key (non RFC3647).....	18
2.3 <i>Frequency of Publication.....</i>	18
2.4 <i>Access to publication.....</i>	19
3 Identification and Authentication.....	20
3.1 <i>Naming.....</i>	20
3.1.1 Types of names	20
3.1.2 Pseudonyms	21
3.1.3 Rules for interpreting various name forms.....	21
3.1.4 Uniqueness of names.....	21
3.1.5 Recognition, authentication and role of trademarks.....	21

3.2	<i>Initial Identity Validation</i>	21
3.2.1	<i>Initial Registration Process</i>	21
3.2.2	<i>Authentication of organizational identity</i>	21
3.2.3	<i>Authentication of individual identity</i>	22
3.3	<i>Identification and Authentication for Re-key Requests</i>	22
3.4	<i>Identification and Authentication for Revocation Requests</i>	23
4	Certificate Life-Cycle Operational Requirements	24
4.1	<i>Scope</i>	24
4.2	<i>Certificate Application</i>	24
4.2.1	<i>Methodology with regard to creating certificates</i>	24
4.3	<i>Certificate Issuance</i>	25
4.3.1	<i>CA Actions during Certificate Issuance</i>	25
4.4	<i>Certificate Acceptance</i>	25
4.5	<i>Key Pair and Certificate Usage</i>	25
4.6	<i>Certificate Renewal</i>	26
4.7	<i>Certificate Re-key</i>	27
4.8	<i>Certificate Modification</i>	27
4.9	<i>Certificate Revocation and Suspension</i>	27
4.10	<i>Certificate Status Services</i>	28
4.10.1	<i>Operational characteristics of the Certificate Status Service</i> 28	
4.10.2	<i>Certificate Status Service availability</i>	28
4.10.3	<i>Optional attributes of the certificate status service</i>	28
4.11	<i>End of Subscription</i>	28
4.11.1	<i>Transfer of PKIoverheid (non RFC3647)</i>	29
4.12	<i>Key Escrow and Recovery</i>	29
5	Management, Operational, and Physical Controls	30
5.1	<i>Physical Security Controls</i>	30
5.2	<i>Procedural Controls</i>	30
5.3	<i>Personnel Security Controls</i>	31
5.4	<i>Audit Logging Procedures for security audits</i>	31
5.5	<i>Records Archival</i>	32
5.6	<i>Key Changeover</i>	32
5.7	<i>Compromise and Disaster Recovery</i>	32
6	Technical Security Controls	34
6.1	<i>Key Pair Generation and Installation</i>	34
6.2	<i>Private Key Protection and Cryptographic Module Engineering Controls</i>	34

6.3	<i>Other Aspects of Key Pair Management</i>	35
6.4	<i>Activation data</i>	35
6.5	<i>Computer Security Controls</i>	35
6.6	<i>Life Cycle Security Controls</i>	36
6.7	<i>Network Security Controls</i>	36
6.8	<i>Time-stamping</i>	36
7	Certificate and CRL profiles	37
7.1	<i>Certificate Profile</i>	37
7.2	<i>CRL profiles</i>	37
7.3	<i>OCSP profiles</i>	38
8	Compliance Audit and Other Assessment	40
8.1	<i>Frequency and circumstances of the conformity assessment</i>	40
8.2	<i>Identity, qualifications of the auditor</i>	40
8.3	<i>Topics covered by the conformity assessment</i>	40
8.4	<i>Actions based on deviations</i>	40
8.5	<i>Communicating of results</i>	40
8.6	<i>Admittance of TSPs to the PKI for the government</i>	40
9	Other Business and Legal Matters	41
9.1	<i>Fees</i>	41
9.2	<i>Financial Responsibility</i>	41
9.3	<i>Confidentiality of Business Information</i>	41
9.4	<i>Confidentiality of Personal Information</i>	41
9.5	<i>Intellectual Property Rights</i>	42
9.6	<i>Representations and Warranties</i>	42
9.7	<i>Disclaimers of Warranties</i>	42
9.8	<i>Limitations of Liability</i>	42
9.9	<i>Indemnities</i>	42
9.10	<i>Term and Termination</i>	42
9.11	<i>Individual notices and communications with participants</i>	42
9.12	<i>Amendments</i>	42
9.13	<i>Dispute Resolution Provisions</i>	43
9.14	<i>Governing Law</i>	43
9.15	<i>Compliance with Applicable Law</i>	43

Appendix A. Publication of Root Certificate announcement	45
Appendix B. Procedures for the change management of the PoR PKIoverheid	47
Appendix C. Certificate profile TSP CA G3	52
Appendix D. Content fields G2 root certificates and domain certificates	55
Appendix E. Content fields G3 root certificates and domain certificates	58

Revision history

Version	Date of approval	Date of entry into force	Status	Author	Manager	Description
3.4	24-06-2011	01-07-2011	Adopted by the Director of Logius 24-06-2011	Policy Authority	H. Verweij	Editorial changes, including (but not limited to) application of RFC3647
3.5	29-06-2012	01-07-2012	Adopted by the Director of Logius 29-06-2012	Policy Authority	H. Verweij	Changes in response to the Baseline Requirements of the CA/B forum and recommendations ensuing from the WebTrust audit
3.6	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 B.
3.7	18-12-2013	18-12-2013	Adopted by the Director of Logius	Policy Authority	Mark Janssen	ETSI TS 101 456 has been replaced by ETSI EN 319 411-2 Inclusion of G3 hierarchy
3.8	June 2014	July 2014	Adopted by the Director of Logius	Policy Authority	Mark Janssen	Paragraph layout based on RFC 3647 refined further still. Various changes made in response to the WebTrust audit.
3.9	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
4.0	October 2016	October 2016	Adopted by the Director of Logius	Policy Authority	Mark Janssen	Replacement of ETSI TS 102 042 by ETSI EN 319 411-1 + removal of references to G1 hierarchy (expired). Also various editorial changes.
4.1	December 2017	December 2017	Adopted by the PA PKIoverheid	Policy Authority	Mark Janssen	Yearly check (no changes).
4.2	November 2018	November 2018	Adopted by the Director of Logius	Policy Authority	Mark Janssen	Major revision as a result of BR self-assesment: <ul style="list-style-type: none"> - 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

						<p>additional "non RFC3647" sections.</p> <ul style="list-style-type: none"> - 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 appendix 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 - 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 D & F to better reflect BRGs - Several small editorial changes.
4.3	December 2019	December 2019		Policy Authority	Jorik van 't Hof	<ul style="list-style-type: none"> - Updated Chapter 1.2 - Updated Chapter 4.2
4.4	December 2020	December 2020		Policy Authority	Alexander Hielkema	<ul style="list-style-type: none"> - Updated Chapter 1.2

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 an 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 government¹.

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

1. management of the standards system of the PKI for the government, the Programme of Requirements parts 3a through e;
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;
11. implementation of the revocation of TSP CA certificates;

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

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 Staat der Nederlanden Root CA and Staat der Nederlanden <Domain> CA, the corresponding Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCPS) responders.

The (policy) 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 users* 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 Root CA – G <number>) and Level 2 (Staat der Nederlanden <Domain> CA – G <number>).

Subject: C = NL, O = Staat der Nederlanden, CN = Staat der Nederlanden Root CA - G2

Subject: C = NL, O = Staat der Nederlanden, CN = Staat der Nederlanden Root CA - G3

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

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

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

The format of this CPS is in accordance with the RFC3647³ 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 CA 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 G2 and G3 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 users* 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 described in general terms. TSPs interested in participating in the PKI for the government can obtain

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

more detailed information about this subject from the PKIoverheid Programme of Requirements part 2.

1.2.2 *Relationship between CPS and CP (non RFC3647)*

The CP PoR parts 3a through e describe 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 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 the PKIoverheid Programme of Requirements part 3e [Policy OID 2.16.528.1.1003.1.2.5.6] and the relevant Requirements, causing the inability to fulfil the minimum requirements put forth herein, the provisions in the Baseline Requirements shall prevail.

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;

Part 3j – Certificate Policy for Domain Server CA 2020.

This CPS only relates to CP section 3a through 3e. 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 Private Root certificates to be issued by the Policy Authority of the PKI for the government" relates to CP parts 3g through 3j.

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.

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 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

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 users;
6. Relying parties.

These parties are described briefly below.

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 part⁴ 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 users. 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 users. How the delivery of certificates takes place is organized between the subscriber and the TSP.

The *certificate user* is the holder of the private key belonging to the public key contained in the certificate. 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 signs 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 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 that the procedure described in paragraph 9.12 is followed accurately and she is responsible for 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 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>

PKIoverheid and its Trust Service Providers guarantee that, when a PKIoverheid services - server certificate is issued, they have adhered to the requirements as laid down in the, at that time current version of the CA/Browser Forum Baseline Requirements and the PoR parts 3e Policy OID [2.16.528.1.1003.1.2.5.6] and that they checked the information included in the server certificate for accuracy and completeness.

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 are 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 Root CA – G2;
- Staat der Nederlanden Burger CA – G2;
- Staat der Nederlanden Organisatie CA – G2;
- Staat der Nederlanden Autonome Apparaten CA - G2;
- Staat der Nederlanden Root CA – G3;
- Staat der Nederlanden Burger CA – G3;
- Staat der Nederlanden Organisatie Services CA – G3;
- Staat der Nederlanden Organisatie Persoon CA – G3;
- Staat der Nederlanden Autonome Apparaten CA – G3;
- <Name TSP> CA – G2;
- <Name TSP> CA – G3.

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 State of the Netherlands CA domain certificates:
<http://crl.pkioverheid.nl/RootLatestCRL-G2.crl>
<http://crl.pkioverheid.nl/RootLatestCRL-G3.crl> (also for OCSP responder certificates)
- For revoked TSP CA certificates:
<http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl>
<http://crl.pkioverheid.nl/DomBurgerLatestCRL-G2.crl>
<http://crl.pkioverheid.nl/DomAutonomeApparatenLatestCRL-G2.crl>
<http://crl.pkioverheid.nl/DomOrganisatieServicesLatestCRL-G3.crl>
<http://crl.pkioverheid.nl/DomOrganisatiePersoonLatestCRL-G3.crl>
<http://crl.pkioverheid.nl/DomBurgerLatestCRL-G3.crl>
<http://crl.pkioverheid.nl/DomAutonomeApparatenLatestCRL-G3.crl>

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

- <https://roottest-g2.pkioverheid.nl> (Valid G2 PKIoverheid certificate)
- <https://roottest-g2-expired.pkioverheid.nl>
- <https://roottest-g2-revoked.pkioverheid.nl>
- <https://roottest-g3.pkioverheid.nl> (Valid G3 PKIoverheid certificate)
- <https://roottest-g3-expired.pkioverheid.nl>
- <https://roottest-g3-revoked.pkioverheid.nl>

2.2.1 *Official electronic notification (non RFC3647)*

The attributes of the root certificates are published in the Official Gazette (Staatscourant) and attached as Appendix A

2.2.2 *Distribution Public Key (non RFC3647)*

The public key of the root certificate is distributed through the trusted root certificate programmes of various software suppliers. An up-to-date list of the software products containing the PKIoverheid root certificate can be found at

<https://www.logius.nl/ondersteuning/pkioverheid/browserondersteuning-pkioverheid/> (in Dutch).

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 republished annually. 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. Both the root and the domain CRLs are 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: <http://crl.pkioverheid.nl>.

As well as the publication of the CRL, the PA also offers status information for the Organization Services domain (G3) through the Online Certificate Status Protocol (OCSP). To this end, the following two OCSP responders are available.

1. <http://rootocsp-g3.ocsp.pkioverheid.nl> provides status information about the Organization Services domain certificate;
2. <http://DomOrganisatieServicesocsp-G3.ocsp.pkioverheid.nl> provides status information about the TSP certificates issued by the Organization Services CA.

The OCSP responders conform to RFC6960⁵.

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 a hot standby (DR) location and fall-back scenario. In addition, every year the repository will undergo a penetration test. This is carried out by an external IT security company.

⁵ <http://www.ietf.org/rfc/rfc2560.txt>

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 CA – G2	Staat der Nederlanden <Domain> CA – G2	<TSP name> CA – G2
Country (C)	NL	NL	NL
Organization (O)	Staat der Nederlanden	Staat der Nederlanden	<TSP Organization name>
CommonName (CN)	Staat der Nederlanden Root CA-G2	Staat der Nederlanden <domain> CA – G2	<TSP name> <domain> CA – G2

Figure 3 - Staat der Nederlanden G2

Attribute	Staat der Nederlanden Root CA – G3	Staat der Nederlanden <Domain> CA – G3	<TSP name> PKIoverheid <domain> CA – G3
Country (C)	NL	NL	NL
Organization (O)	Staat der Nederlanden	Staat der Nederlanden	<TSP Organization name>
CommonName (CN)	Staat der Nederlanden Root CA – G3	Staat der Nederlanden <domain> CA – G3	<TSP name> PKIoverheid <domain> CA – G3
OrganizationIdentifier			The format of the identification string is specified in paragraph 5.1.4 of ETSI EN 319 412-1 and includes: <ul style="list-style-type: none"> • 3 character legal person identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).

Figure 4 - Staat der Nederlanden G2/G3 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.

- 3.1.2 *Need for names to be meaningful*
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) ⁶ and 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.

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 Staatsalmanak⁷ 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.

⁶ National Handelsregister, in the Netherlands managed by the Kamer van Koophandel: www.kvk.nl

⁷ <http://staatsalmanak.sdu.nl/>

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 certificate⁸;
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.

⁸ Specifically, using an end-user certificate with policy OID 2.16.528.1.1003.1.2.5.2 issued to the authorised representative

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.

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 (PKCS#10) to this end by a TSP. For more information, see PKIoverheid PoR part 2.

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. 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")⁹.

⁹ <https://wetten.overheid.nl/BWBR0006297/2017-03-01> (in Dutch)

The creation and/or signing key ceremonies take place in a similar manner for all of the listed types of certificates, where the certificate users 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), 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 trustworthy 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 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 Root CA, Staat der Nederlanden <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 and issuance of OCSP signing certificates (G3 hierarchy only). The G2 hierarchy predates the BRG and doesn't use OCSP services on the root and first intermediate (domain) CA level. 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 (the process where the existing key pair is maintained and the maximum validity period of a 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.

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/domain CA by PA.

4.7 Certificate Re-key

Certificate Re-key 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 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 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 PKIoverheids.

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.

As well as the publication of the CRL, the PA also offers an Online Certificate Status Protocol (OCSP) service for the G3 root certificate and the G3 domain organization services. 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 a G3 Domain or 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 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, Application Software Suppliers, 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 applied¹⁰. 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. If this is considered necessary, the PA will only take on people in positions of trust when, based on 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.

¹⁰ 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) is created. 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. This includes maintaining critical services, including offering the revocation management service, the revocation status service and providing certificate status information through the usual channels.

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 G2 and above have the following key lengths:

TSP sub-CA certificates	4096 bit RSA keys ¹¹
TSP certificates	4096 bit RSA keys
Domain certificates	4096 bit RSA keys
Root certificate	4096 bit RSA keys
OCSF 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:

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.

¹¹ Only applicable for Staat der Nederlanden Root CA – G2

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 certificates of the G2 hierarchy, the following term of validity applies:

TSP sub-CA certificates	12 years minus 3 days
TSP certificates	12 years minus 2 days
Staat der Nederlanden <Domain> CA – G2	12 year minus 1 day
Staat der Nederlanden Root CA – G2	12 years

As from the G3 hierarchy, the following term of validity applies:

TSP certificates	15 years minus 2 days
Staat der Nederlanden <Domain> CA 3	15 years minus 1 day
Staat der Nederlanden Root CA –3	15 years
OCSP Responder certificates	14 months

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 manage and access 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 is classified by the NBV¹² at level "Staatsgeheim confidencieel"¹³. 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 employees of the PA PKIoverheid.

6.7 Network Security Controls

The Staat der Nederlanden Root CA is offline. The Staat der Nederlanden <Domain> CA is 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.

¹² Netherlands National Communications Security Agency (Nationaal Bureau voor Verbindingsbeveiliging)

¹³ Comparable to "confidential" in UK/US government classifications

7 Certificate and CRL profiles

7.1 Certificate Profile

Appendices D and F contain an overview of the content of the fields of the G2 and G3 root certificate and of the domain certificates.

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 CRLs of Root CAs are valid for one year. This is also the case for the CRLs of the 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 Root CA - [version if applicable] or Staat der Nederlanden Domein <name> - [version] 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

The root CA and the domain CA 'Organization Services' 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 Root CA – G<number> or Staat der Nederlanden Organisatie Services CA – G3
TBSCertificate			N/A
Version			2
serial number			SHA1 hash of public key generated by Staat der Nederlanden Root CA – G3 or Staat der Nederlanden Organisatie Services CA – G3
Issuer DN			C=NL O=Staat der Nederlanden CN=Staat der Nederlanden Root CA – G3 or Staat der Nederlanden Organisatie Services CA – G3
Subject DN			C=NL O=Staat der Nederlanden CN=Staat der Nederlanden Root CA – G<number> OCSP Responder n or Staat der Nederlanden Organisatie Services CA – G3 OCSP Responder n (n=1,2,3 etc)
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
digitalSignature			Set
CertificatePolicies	{ id-ce 32 }	FALSE	n/a
policyIdentifiers			2.16.528.1.1003.1.2.1.1 (Root-CA_CP)
policyQualifiers			N/A
policyQualifierID			1.3.6.1.5.5.7.2.1
Qualifier			https://cps.pkioverheid.nl
policyQualifiers			n/a
policyQualifierID			1.3.6.1.5.5.7.2.2

Qualifier			The Certification Practice Statement of the PA PKIoverheid applies to this certificate, which can be consulted at https://cps.pkioverheid.nl
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/RootLatestCRL-G3.crl or http://crl.pkioverheid.nl/DomOrganisatieServicesLatestCRL-G3.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-OCSP-nocheck	1.3.6.1.5.5.7.48.1.5	FALSE	05 00 (Null)

S

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 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.¹⁴

The PA PKIoverheid actively monitors the changes in the WebTrust Principles that affect this CPS. The PA PKIoverheid also actively monitors 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 of results

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

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 “part 2 of the Programme of Requirements PKIoverheid”¹⁵

¹⁴ <http://www.webtrust.org/principles-and-criteria/Item83172.aspx>

¹⁵ <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 sent securely (encrypted).

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 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 4.2 of the "CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid for G2 and G3 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 AT¹⁶ 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.

¹⁶ 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 Government organisations. The General Administrative Law Act¹⁷ applies to Logius.

¹⁷ <https://wetten.overheid.nl/BWBR0005537/2018-09-19> (in Dutch)

Appendix A. Publication of Root Certificate announcement

Root certificate G2

As published in the Official Gazette (Staatscourant) dated Monday 15 December 2008 (no. 243, page 1).¹⁸

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

The Minister of the Interior and Kingdom Relations announces that, on the 26th of March 2008, a new root certificate of the PKI for the government has been created under the name

Staat der Nederlanden Root CA – G2 Certificate

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, indicating volition and communicating confidentially.

The root certificate users is identified as Staat der Nederlanden Root CA – G2 (Common name), Staat der Nederlanden (Organization), NL (Country).

The serial number of the root certificate is 10000012 (hexadecimal 0098 968C).

The root certificate is valid until: Wednesday 25 March 2020 11h:03m:10s GMT.

The identification of the root certificate (the fingerprint in hexadecimal form) based on the SHA1 algorithm is: 59AF 8279 9186 C7B4 7507 CBCF 0357 46EB 04DD B716

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, the joint maintenance organization. Logius is part of the Ministry of the Interior and Kingdom Relations.

The Minister of the Interior and Kingdom Relations,
G. ter Horst.

¹⁸ <https://zoek.officielebekendmakingen.nl/stcrt-2008-1885.html>

Root certificate G3

Translation of the official publication¹⁹

The Minister of the Interior and Kingdom Relations announces that, on the 14th of November 2013, a new root certificate of the PKI for the government has been created under the name

Staat der Nederlanden Root CA - G3

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, indicating volition and communicating confidentially.

The root certificate users is identified as Staat der Nederlanden Root CA – G3 (Common name), The State of the Netherlands Staat der Nederlanden (Organization), NL (Country).

The serial number of the root certificate is 10003001 (hexadecimal 00 98 a2 39).

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: D8EB 6B41 5192 59E0 F3E7 8500 C03D B688 97c9 EEFC.

This root certificate, the underlying documents that support this certificate and further information about this root certificate are available in digital format on the website: <http://www.logius.nl/producten/toegang/pkioverheid/>. 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,

R.H.A. Plasterk

¹⁹ <https://zoek.officielebekendmakingen.nl/stcrt-2014-10020.html>

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

Consultation structure

1. Within the PKIoverheid framework the following bodies are involved in the change management of the Programme of Requirements: The PKIoverheid Change Council and PKIoverheid Framework Council.
2. The Framework Council comprises a delegation of the PA and the TSPs that participate in the PKIoverheid framework. The Change Council is also formed by a delegation of the PA and TSPs and the opportunity is given to invite experts.
3. Auditors of TSPs that participate in the PKIoverheid framework may join in the deliberations of the Change Council and/or Framework Council as a observer. When an auditor is present, he/she will have familiarised him/herself with the change proposals and is able to at least indicate whether a new or amended standard can be audited.
4. The specific aim of these bodies is facilitate consensus on changes to the Programme of Requirements (PoR).
The Change Council congregates to discuss draft change proposals and to reach, as far as possible, consensus on the final change proposals.
The Framework Council is a platform where announcements concerning the PKIoverheid framework by the PA are made and a proposed decision is taken on the inclusion of final change proposals in the next version of the PoR, including an effective date.
5. In principle, the Framework Council is convened twice a year in relation to the publication of a new version of the Programme of Requirements of PKIoverheid.
6. In any case, the Change Council meets one month before a Framework Council meeting, but can be convened more often in order to discuss change proposals which will have a significant impact.
7. Separate meeting are organised to discuss specific subjects, which are not directly related to current PoR changes.

Decision-making

1. During the Framework Council meeting, based on a consensus, an attempt is made to take a proposed decision concerning the content and effective date of changes to the Programme of Requirements.
2. Changes to the PoR are enforced by the Ministry of the Interior and Kingdom Relations, which as the owner has ultimate responsibility for the PKIoverheid framework and makes decisions about enforcing change proposals, sometimes through an accelerated change procedure. The PA provides the owner with advice in this regard.
3. Each proposed change that has been discussed by the Framework Council or as a result of the accelerated change procedure is submitted by the PA for approval to an official

appointed by the Ministry of the Interior and Kingdom Relations, along with a recommendation from the PA and the opinion of the TSPs²⁰.

4. In addition, the official appointed by the Ministry of the Interior and Kingdom Relations will be informed about change proposals that have (temporarily) been revoked.
5. If there is a disagreement with the TSPs on a change proposal, the decision will be justified by the official from the Ministry of the Interior and Kingdom Relations.
6. After approval is given by the official appointed by the Ministry of the Interior and Kingdom Relations, the change will be published by the PA on the website of Logius in a way that is clearly identifiable and uses comprehensible language; also stated is when the change shall take effect.
7. In addition, the PA informs the TSP contact persons and the party that submitted the change proposal electronically and/or in writing of the decision that has been taken.
8. If there is a new version of the PoR, prior to publication a formal signature is required by both the director of Logius and the official appointed by the Ministry of the Interior and Kingdom Relations. In the event of an accelerated change procedure, approval of changes by email will suffice.
9. The official appointed by the Ministry of the Interior and Kingdom Relations reserves the right to make changes to the PoR autonomously in the context of an (imminent) incident, emergency or crisis.

Framework

1. TSPs must comply with the content and effective date of changes approved or published by the official appointed by the Ministry of the Interior and Kingdom Relations.
2. When a TSP cannot meet the effective date of a new or changed requirement, the TSP must ask for formal dispensation for this from the PA PKIoverheid.
3. A request for dispensation is formally submitted at the latest one week after the convening of the Framework Council and must be announced during the meeting.
4. Dispensation has to be requested electronically and/or in writing from the PA PKIoverheid.
5. The PA submits the proposed granting of dispensation for approval to the official appointed to that end by the Ministry of the Interior and Kingdom Relations.
6. The PA shall respond electronically and/or in writing stipulating whether the request is honoured or refused. The auditor of the TSP will receive a copy of this message.

Change proposals

²⁰ Currently, this is the director of the directorate for Information Society and Government from the Ministry of the Interior and Kingdom Relations.

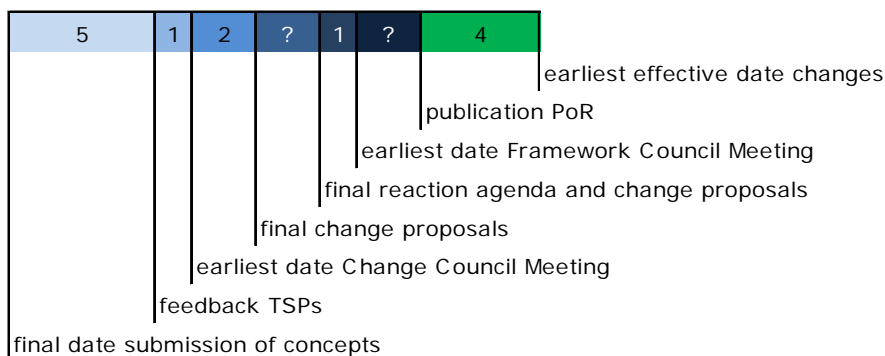
1. The following parties can submit a change proposal regarding a part of, or a provision in the Programme of Requirements (PoR) through the usual or accelerated change procedure:
 - The Ministry of the Interior and Kingdom Relations;
 - the PA PKIoverheid (PA);
 - TSPs within the PKI for the government that use the PoR.
2. The PA can submit change proposals based on the input from end users or other stakeholders. This will be clearly indicated in the change request.
3. Change requests are usually approved by the Change Council and Framework Council. If a change cannot wait until the next version of the PoR, an abbreviated change procedure is available.
4. A change proposal can be submitted by completing the request form "Change proposal Programme of Requirements" and sending this to the PA. This form can be found on the PA's website or can be requested directly from the PA.
5. The PA handles a submitted change proposal regarding a part of, or a provision in the PoR in accordance with documented internal processes. In the event of an actual (material) change the PA will analyse the proposal and has the ability to outright reject said proposal. If the PA agrees with the (goal of the) change proposal it will issue a positive recommendation, including text proposal, impact analysis (for instance: effective dates and possible dispensation, etc.) and reasoning. These are submitted to the TSPs for consultation.

Regular change procedure

1. *In principle, a new version of the PoR is published twice a year. A proposed decision regarding inclusion of a new or amended requirement in the PoR is taken during the meeting of the Framework Council prior to publication.*
2. Change proposals are sent to the TSPs at least ten weeks before the publication of the new PoR version is due.
3. Change requests submitted after this date will not be considered for publication in the next version of the PoR, unless the PA and TSPs agree unanimously that this change can still be included.
4. TSPs have five weeks to analyse change proposals and to give feedback to the PA.
5. This feedback is discussed during the Change Council meeting prior to the meeting of the Framework Council.
6. Taking the Change Council input into consideration, change proposals are finalised.
7. The PA sets the dates for the Change and Framework Council meetings. The meetings will take place as soon as possible after the latest draft proposals for the next version of the PoR have been distributed. There will be a minimum of 2 weeks between the Change Council meeting and the Framework Council meeting.

8. The final change proposals are sent to the TSPs and the auditors no later than 2 working days after the Change Council meeting, along with the agenda for the Framework Council meeting.
9. *The response time of TSPs to the agenda and the final change proposals is at least one week*
10. TSPs are expected not to put forward new insights once the final change proposals have been completed and distributed. This is meant to prevent the PA and other TSPs being forced to take a decision during the Framework Council meeting without the possibility to carefully consider the content of the new proposal.
11. If the delegation from a TSP cannot be present during a Change or Framework Council meeting, the TSP contact person is expected to elaborate on their point of view in advance in writing concerning the content and the effective date of changes.
12. Following the Framework Council meeting, the PoR will be published as soon as possible.
13. The effective dates of changes are specifically included in the PoR.

I Ordinary change process in weeks



Accelerated change procedure

1. Changes are usually dealt with through the regular change procedure. In the event of an (imminent) incident, change in external requirements²¹ emergency or crisis, the official appointed by the Ministry of the Interior and Kingdom Relations can make changes autonomously. In addition, an accelerated change procedure can be followed, if it is necessary to enforce a change well before publication of a new version of the PoR.
2. Using the utmost caution the PA decides when it is necessary to follow an accelerated change procedure.
3. An accelerated change procedure entails the following process:
 - a) The TSPs, the auditors of the TSPs and the official appointed by the Ministry of the Interior and Kingdom Relations are informed by email of the intention of the PA to

²¹ For instance, a change in browser policy

publish a change through an accelerated change procedure on the Logius website , along with the change request.

- b) TSPs have at least one week to submit objections to the content and/or effective date of this change.
- c) Any objections will be carefully considered by the PA PKIoverheid which, in close consultation, shall endeavour to provide sound advice.
- d) The decision making process followed by the Ministry of the Interior and Kingdom Relations is described in the paragraph entitled "Decision-making".
- e) The PA publishes the change on the website and communicates this to the TSPs. The TSPs must adhere to the content and the effective date of the change published on the Logius website.

Miscellaneous

1. The PoR and the approved changes can be obtained in electronic form via the Internet on the PA's website: <http://www.logius.nl/pkioverheid>.
2. In the PoR, reference is made to this change procedure, which is included in the CPS of PKIoverheid.

Appendix C. Certificate profile TSP CA G3

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 <domainname> CA – G32
TBSCertificate			N/A
Version			2
SerialNumber			Generated by Domain <domainname> CA – G3
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 <domain name> CA – G3
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 <domain name> CA – G3
subjectPublicKeyInfo			Public key TSP-CA (Keylength=4096)
Standard Extensions	OID	Critical	Value
CertificatePolicies	{ id-ce 32 }	FALSE	N/A
policyIdentifier			See the relevant PoR parts for PolicyIdentifiers
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 Domain <domain name>CA – G3
SubjectKeyIdentifier	{ id-ce 14 }	FALSE	N/A
KeyIdentifier			160-bit SHA-1 Hash value of this TSP CA
AuthorityInfoAccess*	{ id-pe 1 }	FALSE	
See table below			
CRLDistributionPoints	{ id-ce 31 }	FALSE	N/A
DistributionPoint•FullName			http://crl.pkioverheid.nl/Dom<domain name>LatestCRL-G3.crl
ExtendedKeyUsage**	{ id-ce 37 }	FALSE	N/A
See table below			
BasicConstraints	{ id-ce 19 }	TRUE	N/A
CA			Set

PathLenConstraint			0
OcStatement2	{ id-qcs-pkixQCSyntax-v2 }	FALSE	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)

*** accessMethod**

Only for Server CA certificates and optionally for Services

accessMethod*	1.3.6.1.5.5.7.48.1		OCSP
accessLocation: URI*			http://domorganisatieservicesOCSP-g3.pkioverheid.nl
accessMethod	1.3.6.1.5.5.48.2		Certification Authority Issuer
accessLocation: URI			<a href="http://cert.pkioverheid.nl/Dom<domain namee>-CA-G3.cer">http://cert.pkioverheid.nl/Dom<domain namee>-CA-G3.cer

Other CA Certificates

accessMethod	1.3.6.1.5.5.48.2		Certification Authority Issuer
accessLocation: URI			<a href="http://cert.pkioverheid.nl/Dom<domeinnaam>-CA-G3.cer">http://cert.pkioverheid.nl/Dom<domeinnaam>-CA-G3.cer

****ExtendedKeyUsage**

Only for Server CA certificates:

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-OCSPsigning	{ id-kp 9 }		1.3.6.1.5.5.7.3.9

Other CA certificates:

Id-kp-clientAuth	{ id-kp 2 }		1.3.6.1.5.5.7.3.2
Id-kp-Emailprotection	{ id-kp 4 }		1.3.6.1.5.5.7.3.4
Id-kp-OCSPsigning	{ id-kp 9 }		1.3.6.1.5.5.7.3.9
szOID_KP_DOCUMENT_SIGNING			1.3.6.1.4.1.311.10.3.12
szOID_EFS_CRYPT0 (Encrypting File System)			1.3.6.1.4.1.311.10.3.4

Appendix D. Content fields G2 root certificates and domain certificates

Attribute		Root certificate	Organization Domain	Citizen Domain	Autonomous Devices Domain
Version		V3			
Serial number		0098 968C	0098 96F4	0098 96F3	0098 97BB
Algorithm for signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)			
Provider		CN = Staat der Nederlanden Root CA - G2 O = Staat der Nederlanden C = NL			
Valid from/to		Wednesday 26 March 2008 12:18:17 Wednesday 25 March 2020 12:03:10	Monday 31 March 2008 13:03:09 Tuesday 24 March 2020 14:02:08	Monday 31 March 2008 11:45:11 Tuesday 24 March 2020 12:43:57	Tuesday 3 November 2009 14:35:47 Tuesday 24 March 2020 14:34:41
Subject	CN =	Staat der Nederlanden Root CA - G2	Staat der Nederlanden Organisatie CA - G2	Staat der Nederlanden Burger CA - G2	Staat der Nederlanden Autonome Apparaten CA - G2

Attribute	Root certificate	Organization Domain	Citizen Domain	Autonomous Devices Domain
	O =	O = Staat der Nederlanden	Staat der Nederlanden	Staat der Nederlanden
	C =	NL	NL	NL
Public Key	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)
Certificate Policies	ID=2.5.29.32.0 Policy qualification-ID=CPS http://www.pkioverheid.nl/policies/root-policy-G2	ID=2.5.29.32.0 Policy qualification-ID=CPS http://www.pkioverheid.nl/policies/dom-org-policy-G2	ID=2.5.29.32.0 Policy qualification-ID=CPS http://www.pkioverheid.nl/policies/dom-bu-policy-G2	ID=2.5.29.32.0 Policy qualification-ID=CPS http://www.pkioverheid.nl/policies/dom-aa-policy-G2
Authority Key Identifier (AKI)	N/A	Key ID=91 68 32 87 15 1d 89 e2 b5 f1 ac 36 28 34 8d 0b 7c 62 88 eb		
CRL distribution	N/A	URL= http://crl.pkioverheid.nl/RootLatestCRL-G2.crl		
Subject Key Identifier (SKI)	91 68 32 87 15 1d 89 e2 b5 f1 ac 36 28 34 8d 0b 7c 62 88 eb	39 10 8b 49 92 5c db 61 12 20 cd 49 9d 1a 8e da 9c 67 40 b9	91 a5 0d dd 1d a0 d1 2a 68 a7 1b 8d db 48 9a aa 34 a9 7f 96	7d 76 81 96 1e 4a 29 d1 ce 5e 12 0a 2a d4 d1 d4 ed bc ed 99
Basic Constraints	<u>Critical</u> - CA: True			
Key usage	<u>Critical</u> : - Certificate sign			

Attribute	Root certificate	Organization Domain	Citizen Domain	Autonomous Devices Domain
	- CRL sign			
Fingerprint algorithm	SHA256			
Fingerprint	66:8C:83:94:7D:A6:3B:72:4B:EC:E1:74: 3C:31:A0:E6:AE:DO:DB:8E:C5:B3:1B:E3: 77:BB:78:4F:91:B6:71:6F	85:A8:F5:86:6D:D7:8D:F1:73:B0:66:73:1 7:C5:9B:2D:62:42:DE:59:EB:01:BB:2F:2E :8B:9D:B7:14:B4:CA:27	2F:2F:0C:84:4F:B3:36:A9:42:1A:B6: FA:36:DC:DA:C3:BB:84:E0:38:4C:FF :5D:AD:51:11:3C:8C:A4:24:E6:A4	1B:17:10:02:64:24:7D:70:90:03: 61:16:23:8C:93:F4:58:53:ED:E5: AE:A6:F9:F1:A4:52:4F:69:78:DD: 89:54

Appendix E. Content fields G3 root certificates and domain certificates

Attribute		Root certificate	Citizen Domain	Organization Services Domain	Organization Person Domain	Autonomous Devices Domain
Version		V3				
Serial number		00 98 a2 39	00 98 a2 47	00 98 a2 3c	00 98 a2 46	00 98 a2 a0
Algorithm for signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)				
Provider		CN = Staat der Nederlanden Root CA – G3 O = Staat der Nederlanden C = NL				
Valid from/to		Thursday 14 November 2013 12:28:42 Tuesday 14 November 2028 0:00:00	Thursday 14 November 2013 17:08:12 Monday 13 November 2028 0:00:00	Thursday 14 November 2013 13:27:56 Monday 13 November 2028 0:00:00	Thursday 14 November 2013 16:09:37 Monday 13 November 2028 0:00:00	Friday 15 November 2013 10:04:59 Monday 13 November 2028 0:00:00
Subject	CN =	Staat der Nederlanden Root CA – G3	Staat der Nederlanden Burger CA - G3	Staat der Nederlanden Organisatie Services CA - G3	Staat der Nederlanden Organisatie PersoonCA - G3	Staat der Nederlanden Autonome Apparaten CA - G3

Attribute		Root certificate	Citizen Domain	Organization Services Domain	Organization Person Domain	Autonomous Devices Domain
	O =	Staat der Nederlanden	Staat der Nederlanden	Staat der Nederlanden	Staat der Nederlanden	Staat der Nederlanden
	C =	NL	NL	NL	NL	NL
Public Key		RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)	RSA (4096 Bits)
Certificate Policies		N/A	ID=2.16.528.1.1003.1.2.3.1 ID=2.16.528.1.1003.1.2.3.2 ID=2.16.528.1.1003.1.2.3.3 Policy qualification-id=CPS https://cps.pkioverheid.nl	ID=2.16.528.1.1003.1.2.3.4 ID=2.16.528.1.1003.1.2.3.5 ID=2.16.528.1.1003.1.2.3.6 Policy qualification-id=CPS https://cps.pkioverheid.nl	ID=2.16.528.1.1003.1.2.5.1 ID=2.16.528.1.1003.1.2.5.2 ID=2.16.528.1.1003.1.2.5.3 Policy qualification-id=CPS https://cps.pkioverheid.nl	ID=2.16.528.1.1003.1.2.6.1 ID=2.16.528.1.1003.1.2.6.2 ID=2.16.528.1.1003.1.2.6.3 Policy qualification-id=CPS https://cps.pkioverheid.nl
Authority Key Identifier (AKI)		N/A	Key-ID=54 ad fa c7 92 57 ae ca 35 9c 2e 12 fb e4 ba 5d 20 dc 94 57			
CRL distribution		N/A	URL= http://crl.pkioverheid.nl/RootLatestCRL-G3.crl			
Subject Key Identifier (SKI)		54 ad fa c7 92 57 ae ca 35 9c 2e 12 fb e4 ba 5d 20 dc 94 57	ff 68 75 42 7d fa 6f c7 5a 93 38 9f 35 44 d0 aa 2d 00 b2 89	43 eb 4d 00 d3 95 93 ce a6 7c 40 0d 6d 11 be 39 d1 32 ae e2	ee ac 6d 40 ea d5 04 6a 87 2c 55 7b f5 3f 2d da ee db ac e2	6d 1b 25 02 5d e0 48 f4 6e 13 75 e2 57 84 9d 50 f3 30 14 43

Attribute	Root certificate	Citizen Domain	Organization Services Domain	Organization Person Domain	Autonomous Devices Domain
Authority Information Access	N/A	N/A	OCSPURI=http://rootOCSP-g3.pkioverheid.nl	N/A	N/A
Basic constraints	<u>Critical</u> - CA:TRUE				
Key usage	<u>Critical</u> - Certificate sign - CRL sign				
Fingerprint algorithm	SHA256	SHA256	SHA256	SHA256	SHA256
Fingerprint	3C:4F:B0:B9:5A:B8:B3:00:32:F4:32:B8:6F:53:5F:E1:72:C1:85:D0:FD:39:86:58:37:CF:36:18:7F:A6:F4:28	2E:7A:0A:3B:0C:52:7E:B2:0C:52:25:3C:8D:22:78:CA:10:81:36:A8:CA:3A:4E:A2:2D:A7:B5:9B:AC:90:65:0A	D9:58:1D:BD:E9:9B:39:EE:FF:6C:E5:C8:0D:E1:65:0D:A0:C1:C8:A1:09:70:5E:D2:86:C5:3B:C9:5E:66:55:E4	82:22:BC:4F:E7:A3:DD:CA:9E:F0:BF:0D:68:2A:C8:88:79:9F:87:82:2D:15:33:2A:54:C0:BF:DF:C6:85:4F:7B	AD:49:3D:6E:85:EC:60:8A:B8:13:A8:87:BD:C4:D4:19:6A:0B:C9:B3:3D:25:65:A7:FA:8A:C4:30:F0:8A:99:A5