Certification Practice Statement

PKIoverheid

KPN B.V.

KPN BV
Fauststraat 1
7323 BA Apeldoorn
Postbus 9105
7300 HN Apeldoorn
T +31 (0) 8 86 61 00 00
www.kpn.com
K.v.K. ‘s Gravenhage nr. 27124701
NL009292056B01

Datum	July 14, 2021
Versie	version 5.6
Publication date	July 16 ,2021

Version history

Version	Document date	Changes
5.6	14-07-2021	Changes in CA hierarchy and applicable parts Program of Requirements PKIoverheid. New version Mozilla Root Store Policy. Implementation of linting. Some mistakes corrected, including compliance RFC 3647 and Mozilla bug 1719451.
5.5	30-11-2020	Updates to include SC30, SC31, and SC33 requirements and practices from the CABF. Changes in CA hierarchy. EV SSL en QWAC discontinued
5.4	11-08-2020	Introducing server certificates under KPN PKIoverheid Server CA 2020
5.3	27-05-2020	Introducing eSeal and QWAC certificates
5.2.4	20-02-2020	Last CRL after the expiry date of the Issuing CA
5.2.3	14-01-2020	Updates to include Mozilla Root Store Policy version 2.6
5.2.2	11-12-2019	Policy administration
5.2.1	28-11-2019	Sections aligned with RFC 3647 and typographical/editorial issues fixed
5.2	30-10-2019	Validity period server certificates from 825 to 397 days
5.1	05-04-2019	QSCD and mobile certificates
5.0	30-11-2018	Complete revision of previous CPS version 4.29

Table of contents

1. Introduction to the Certification Practice Statement

The PKI for the Dutch government, shortly PKIoverheid, is an agreements system for enabling the generic and large-scale use of the Electronic Signature, remote identification and confidential electronic communications. All agreements are described in the Program of Requirements PKIoverheid (Logius).

Within PKIoverheid, KPN BV operates as Trust Service Provider (TSP). Hereinafter referred to as KPN. This means KPN as a Trust Service Provider, as a distinction to the other services provided by KPN.

KPN BV is the legal successor to KPN Corporate Market BV as of April 1, 2016. All agreements entered into with KPN Corporate Market BV by subscribers and relying parties, including all obligations and warranties mentioned in this document, are transferred to KPN BV.

One of the requirements in the Program of Requirements is that each Trust Service Provider within the PKIoverheid describes its practices in a so-called Certification Practice Statement (further: CPS). The present document is the CPS of KPN. This document describes the practices of KPN. This chapter contains an introduction to this CPS document. It briefly addresses several important aspects of this document.

1.1 Overview

The format of this CPS is as far as possible in accordance with the RFC3647 Standard (Internet Technology Task Force Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). For more information see https://www.ietf.org.

1.1.1 Target audience and reading guide

The primary target group of this CPS is:

- KPN subscribers.
- Subscriber Contacts.
- Certificate Holder and Subscriber Certificate Managers.
- Relying Parties.

1.1.2 Purpose of the CPS

The CPS is a description of the way in which KPN operates its certification service in the Organization domain of PKIoverheid. The CPS contains, among other things, a description of the procedures that KPN applies to the creation, issuance and revocation of PKIoverheid Certificates.

1.1.3 Relationship between CP and CPS

The CP describes the requirements for issuing and using a Certificate within the Organization domain of PKIoverheid. The CP has been established and is maintained by the Policy Authority of PKIoverheid and is part of the Program of Requirements of the PKIoverheid (https://www.logius.nl/english/pkioverheid).

1.1.4 CA Hierarchy

Staat der Nederlanden Root CA - G3

Staat der Nederlanden Organisatie Persoon CA - G3

KPN BV PKIoverheid Organisatie Persoon CA - G3

▪ Persoon - Authenticiteit	(2.16.528.1.1003.1.2.5.1)
▪ Persoon - Onweerlegbaarheid	(2.16.528.1.1003.1.2.5.2)
▪ Persoon – Vertrouwelijkheid	(2.16.528.1.1003.1.2.5.3)

Staat der Nederlanden Organisatie Services CA - G3

KPN BV PKIoverheid Organisatie Services CA - G3

▪ Services - Authenticiteit	(2.16.528.1.1003.1.2.5.4)
▪ Services - Vertrouwelijkheid	(2.16.528.1.1003.1.2.5.5)
▪ Services - Onweerlegbaarheid	(2.16.528.1.1003.1.2.5.7)

Staat der Nederlanden EV Root CA

Staat der Nederlanden Domein Server CA 2020

KPN PKIoverheid Server CA 2020

▪ OV policy OID	(2.16.528.1.1003.1.2.5.9)

Staat der Nederlanden Private Root CA - G1

Staat der Nederlanden Private Services CA - G1

KPN PKIoverheid Private Services CA - G1

▪ Server	(2.16.528.1.1003.1.2.8.6)

1.2 Document name and identification

Formally this document is referred to as 'Certification Practice Statement PKIoverheid'. In the context of this document, it is also referred to as 'PKIoverheid CPS', but usually shortly as 'CPS'. Where this abbreviation is concerned, this document is intended.

The date on which the validity of this CPS starts is given on the title page of this CPS. The CPS is valid for as long as the KPN service continues, or until the CPS is replaced by a newer version (indicated in the version number with +1 in major changes and +0.1 in editorial edits).

This CPS can be identified through the following Object Identifier (OID): 2.16.528.1.1005.1.1.1.2

KPN issues the following types of certificates:

- qualified certificates for electronic signatures (eIDAS art. 28), in accordance with the policy: QCP-n-qscd.
- public key certificates (non-qualified trust service), in accordance with the policies: NCP+, OVCP and PTC.
- qualified certificates for electronic seals (eIDAS art. 38, ETSI-policy: QCP-l-qscd).

All types of Certificates issued by the KPN have the same level of trust, in accordance with Program of Requirements within PKIoverheid. The Program of Requirements (PoR) PKIoverheid consists of the following relevant parts:

- PoR part 1: Programme of Requirements – Introduction
- PoR part 3a: Organization Persoon
- PoR part 3b: Organization Services
- PoR part 3h: Private Services (server)
- PoR part 3j: Server 2020

For this reason, the CPS applies to all Certificates under the CA hierarchy in section 1.1.4.

Both the Root CAs and the subCAs are managed by PKIoverheid. A description of the management of these CAs can be found in the CPS Policy Authority for certificates issued by the Policy Authority PKIoverheid. Both documents can be found on https://logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen.

KPN conforms to the current version of the Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates as published at https://www.cabforum.org . Should there be an inconsistency between PKIoverheid Program of Requirements and the relevant Baseline Requirements, which does not at least meet the minimum requirements described herein, this is to be determined by the PKI Policy Authority, then the stipulated in the Baseline Requirements prevails.

This CPS describes how KPN fulfils these requirements and meets these requirements.

1.3 PKI participants

1.3.1 Certification authorities

The Policy Authority PKIoverheid is the Certificate Authority (CA) for the Root CAs and subCAs. KPN is the CA for the end-user certificates listed in section 1.1.4.

1.3.2 Registration authorities

A Registration Authority (RA) is a function that performs the validation and identity verification of the applicant when requesting a certificate. Once the Registration Authority has provided approval, then the CA can issue the certificate to the applicant. Once the certificate is issued, the applicant becomes the Subscriber.
The Registration Authority (RA) is performed by KPN. A number of activities are performed by a third party, see section 1.3.5. The contract stipulates that the third party must comply to the policies and applicable standards & regulations as described in this document.
KPN does not delegate domain validation activities to any third parties.

1.3.3 Subscribers

The Subscriber is the entity stated in the subject field of the Certificate, and the holder of the Private Key. Subscribers can be a natural person, a natural person with a registered profession, or a natural person in association with a legal person (Authorised Representative of an organisation).

Subscribers are required to act in accordance with this CPS, Subscriber Agreement, General Conditions KPN and Special Terms and Conditions PKIoverheid.

Holders of Personal Certificates are natural persons. Subscribers of Server Certificates are organisations. The Certificate Manager is a Representative of an organisation and is also the holder of the Private Key.

There are also individuals working in a recognized profession who are both Subscriber and Certificate Holder.

1.3.4 Relying parties

Relying parties are parties who rely upon the trusted status of the certificate. Relying parties will assess the status of the issued certificate before continuing communication with the Subscriber. The status of the certificate can be valid, revoked or expired.

1.3.5 Other participants

Cooperation with Multi-Post Services B.V.
KPN has concluded a cooperation agreement on certificate services with Multi-Post Services B.V. (further: Multi-Post). Under that agreement, KPN has subcontracted out the following work to Multi-Post.

- Stock management of QSCDs / SUD's.
- Generating key pairs for the QSCDs and the insertion of keys in the QSCDs / SUD's.
- Archiving and personalizing QSCDs / SUD's;
- Hand over the QSCD's/SUD's and PINs to the distribution channel.

Cooperation with AMP Logistics B.V
KPN has signed a cooperation agreement on certificate services with AMP Logistics BV (further: AMP). Within that agreement, KPN subcontracts the identification of the Certificate Manager and Certificate Holder to AMP. Identification is done by an AMP employee at a time and place agreed on with the Certificate Manager.

Cooperation with Ubiqu Access B.V.
KPN has entered into a cooperation agreement with Ubiqu Access B.V. (hereafter: Ubiqu) regarding the certification services for the mobile smart card. Within this agreement, Ubiqu will provide amongst others the Authentication App and API with which the certificate holder has Sole control over his private key.

1.4 Certificate usage

The certificates issued by KPN are issued in accordance with the Program of Requirements (PoR) PKIoverheid (sections 3a, 3b, 3h en 3j).

1.4.1 Appropriate Certificate Uses

Personal and Profession certificates (PoR PKIoverheid part 3a)
Within the domain Organization Person (g3), Program of Requirements PKIoverheid part 3a, KPN issues three types of Certificates on behalf of Subscribers to Certificate Holders. These certificates each have their own function, each also has its own policy. These policies are uniquely identified by an OID. It concerns:

1. Signature Certificates
2. Authenticity Certificates
3. Confidentiality Certificates

Signature Certificates, also called Qualified Certificates, as described in the eIDAS regulation), and also called nonrepudiation certificates are intended to provide electronic documents with a qualified electronic signature [domain Organization OID 2.16.528.1.1003.1.2.5.2]. This Qualified Electronic Signature, the Electronic Signature Based on a Qualified Certificate, and that has been created by a Qualified Signature Creation Device (QSCD), meets all legal requirements for a signature and has the same legal force as a handwritten signature for paper documents.

Authenticity certificates are intended to reliably identify and authenticate persons, organizations and resources by electronic means. This concerns both the identification of people and between people and resources [domain Organization OID 2.16.528.1.1003.1.2.5.1]. Authenticity Certificates are not Qualified Certificates.

Confidentiality Certificates are intended to protect the confidentiality of data exchanged and / or stored in electronic form. This concerns both the exchange of information between people and between people and automated means [domain Organization OID 2.16.528.1.1003.1.2.5.3]. Confidentiality Certificates are not Qualified Certificates.

These 3 types of certificates are issued as Certificates for persons with a recognized profession (dutch:”beroepsgebonden certificaten”) and as Personal Certificates (Actually Organizational, as a distinction to the recognized profession certificates) on one of the following data media: Smartcard and USB token. In addition, these certificates can be requested as Mobile certificates, however, no confidentiality certificate will be received. For definitions see 1.11 Definitions and abbreviations.

Group / eSeal certificates (PoR PKIoverheid part 3b)
Within the domain Organization (g3), PoR PKIoverheid part 3b, KPN issues three types of certificates to Subscribers. These certificates each have their own function, also have their own policy. This policy is uniquely identified by an OID. It concerns:

1. Authenticity Certificates;
2. Confidentiality Certificates;
3. Non-Repudiation Certificates (Qualified certificate for electronic seal).

Authenticity Certificates are intended to reliably identify and authenticate a service as belonging to the organizational entity that is responsible for the service by electronic means [Public domain organization OID 2.16. 528.1.1003.1.2.5.4].

Confidentiality Certificates are designed to protect the confidentiality of information exchanged in electronic form [domain Organization OID 2.16.528.1.1003.1.2.5.5].

These 2 types of certificates are issued as Service Certificates. The Authenticity Certificate and Confidentiality Certificate together are called the Group Certificate. For definitions see 1.11 Definitions and abbreviations.

Non-Repudiation Cerificates (Qualified certificate for electronic seals) are intended to reliably identify and authenticate an organizational entity that is responsible for the service by electronic means [Domain organization OID 2.16. 528.1.1003.1.2.5.7].

(Standard) server certificates (PoR PKIoverheid part 3j)
Within the domain Organization (g3), PoR PKIoverheid part 3j, KPN also issues server certificates to Subscribers. These certificates have their own function, also have their own policy. This policy is uniquely identified by an OID.
Server certificates are intended for use, where the confidentiality key is not used to encrypt the data but only aims to encrypt the connection between a particular client and a server [Domain Organization OID 2.16.528.1.1003.1.2.5.9]. This server must belong to the organizational entity named as the Subscriber in the certificate.

The Server Certificates, together with Group Certificates, are called the Services Certificates.
For definitions see Definitions and abbreviations.

Private Services (PoR PKIoverheid part 3h)
The Private Services Server certificates issued by KPN are issued in accordance with the PKIoverheid Program of Requirements (part 3h).
Within PKIoverheid Private Services, Private Services Server certificates are used to secure a connection between a particular client and a server via the TLS/SSL protocol. The PKIoverheid Private Services certificates are identified by the specific unique PKIoverheid Private Services Policy Object Identifier (OID) 2.16.528.1.1003.1.2.8.6. This OID refers to the CP PoR part 3h and is listed in the Certificate Policy (certificatePolicies) field of the State of the Netherlands Private Services CA certificate, the KPN PKIoverheid Private Services CA certificates and the end user Private Services Private Services Server certificates.

The “Staat der Nederlanden” (State of the Netherlands) Private Root CA - G1 is NOT publicly trusted by browsers and other applications.

KPN issues Private Server Certificates under the 'State of the Netherlands Private Root CA - G1'. This root certificate is part of the central part of the hierarchy of PKIoverheid. The root certificate is the anchor point for trust in electronic transactions within a closed user group. Trust is derived from the fact that this root certificate was issued by the State of the Netherlands and published in the Netherlands Government Gazette (Staatscourant). All participating parties must install and trust this certificate manually. Therefore, Private server certificates are intended for application in private user groups as opposed to publicly trusted server certificates where the master certificate is automatically trusted by the important operating systems (such as Windows, Mac OS, Linux, Android and iOS) and browsers (e.g. Mozilla FireFox).

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organisation administering the document

The KPN CPS is managed by a dedicated Policy Management Authority (PMA).

1.5.2 Contact Person

Information regarding this CPS and comments can be directed to:

KPN Security
Attn. Policy Management Authority
PO Box 9105
7300 HN Apeldoorn
pkio.servicedesk@kpn.com

To notify KPN of a service outage or report a suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates, please contact:

pkio.servicedesk@kpn.com

To request an urgent certificate revocation outside office hours (Mon-Fri, 9h-17h), please contact the servicedesk:

+31 88 – 661 06 21 (only for a revocation request)
esd.cic@kpn.com

For the revocation you need the following information:

- Common name
- Subject serial number
- Challenge phrase as received by the cardholder
- E-mail address of the cardholder

1.5.3 Person Determining CPS suitability for the policy

The determination of the suitability of the CPS is part of the CPS approval process (see 1.5.4) of the PMA and is part of the assessment by the independent auditor (see 8).

1.5.4 CPS Approval Procedures

Changes to the KPN CPS are approved by the PMA, after consultation with the relevant stakeholders. Once approved, this document will be published in the Repository. (dutch: Elektronische opslagplaats) on https://certificaat.kpn.com/elektronische-opslagplaats/.

As required by the Baseline Requirements, the CPS is reviewed at least once a year and given a higher version number.

1.6 Definitions and acronyms

For an overview of the definitions and acronyms used, refer to Annexes 1 and 2, respectively.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

KPN ensures the availability of relevant information in the Repository
https://certificaat.kpn.com/elektronische-opslagplaats/repository

2.2 Publication of certification information

2.2.1 Publication of CSP information

At least the following online is available through the Repository:

1. Root certificate;
2. Certificate status information;
   a. In the CRL;
   b. In the Directory Service (see 7);
   c. Using OCSP;
3. Special Conditions;
4. CPS;
5. Certificate Policy – Domains Government / Business (g1), Organization (g2) and Organization Person (g3) Certificate
6. Policy authenticiteit- and confidentiality certificates - Services Organization (g3) Annex CP Domains Government / Companies (g1) and Organization (g2); Certificate Policy Server Certificate - Domain Services Organization (g3) Annex CP Domains Government / Companies (g1) and Organization (g2)
7. Directory Service;
8. Copies of the (full) ETSI EN 319 411- 1 - and ETSI EN 319 411-2 certificates of KPN and ETSI EN 319 411- 1 and ETSI EN 319 411-2 partial certificates acquired by KPN on behalf of and together with other Trust Service Provider's.

2.2.2 Publication of the certificate

Certificates are published using a Directory Service. Through the Directory Service, the Certificate may be consulted by Subscribers, Certificate Managers, Certificate Holders and Relying Parties.

The Directory Service is adequately protected from manipulation and is accessible online. Information regarding the revocation status is available twenty-four hours a day and seven days a week.

The ETSI EN 319 411-2 and ETSI EN 319 411-1 certificates of KPN BV, together with ETSI EN 319 411-2 and ETSI EN 319 411-1 partial certificates, are published in the repository. The relevant certificates indicate that KPN BV complies with ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates and ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements and thus meeting the requirements of The European eIDAS. The audit reports relating to KPN BV's normative references are not stored in the Repository as a result of its security policy.

2.3 Time or frequency of publication

Changes to CSP information shall be published, except as set out in this section, at the time of their occurrence or as soon as possible thereafter and subject to the applicable provisions. See, for example, paragraph 9.12 Changes.

The publication of Certificates takes place immediately after production. The CRL's are renewed every 60 minutes.

2.4 Access controls on repositories

Information in the Repository is public in nature and freely accessible. The Repository can be consulted twenty-four hours a day and seven days a week.
The Repository is protected against unauthorized changes.

For the occurrence of system failure or other factors that negatively affect the availability of the Repository, an appropriate set of continuity measures has been implemented to ensure that the CRL is reachable again within 4 hours and the remaining parts of the repository within 24 hours. An example of such a measure is to have realized a disaster recovery location and -scenario in combination with the regular testing of its functionality.

KPN is not responsible for the unavailability of the Repository due to circumstances where KPN cannot be held responsible.

3. Identification and authentication

This section describes how the identification and authentication of certificate applicants takes place during the initial registration process and the criteria that KPN uses regarding the naming.

3.1 Naming

3.1.1 Types of names

The names used in **Personal Certificates** comply with the X.501 name recommendation. The names consist of the following parts:

Attribute	Value
Country (C)	NL
Organization (O)	Name of the subscriber
Common Name (CN)	Full name of the Certificate holder
Givenname	First name of the Certificate holder
Surname	Last name of the Certificate holder
Subjectserialnumber (SN)	Subjectserialnumber of the Certificate holder
Optional:	
Organizational Unit (OU)	Department of the subscribers' organization

The names used in **Profession Certificates** comply with the X.501 name recommendation. The names consist of the following parts:

Attribute	Value
Country (C)	NL
Organization (O)	Name of the subscriber
Common Name (CN)	Full name of the Certificate holder
Givenname	First name of the Certificate holder
Surname	Last name of the Certificate holder
Subjectserialnumber (SN)	Subjectserialnumber of the Certificate holder
Title	Profession of Cerificate holder

The names used in **Group certificates** comply with the X.501 name recommendation. The names consist of the following parts:

Attribute	Value
Country (C)	NL
Organization (O)	Name of the subscriber
Common Name (CN)	Name of the Certificate holder
Organization Identifier	Identifier for the Subscriber

Optional:	
Organizational Unit (OU)	Department of the subscribers' organization
Subjectserialnumber (SN)	Subjectserialnumber of the Certificate holder

The names used in **eSeal certificates** comply with the X.501 name recommendation. The names consist of the following parts:

Attribute	Value
Country (C)	NL
Organization (O)	Name of the subscriber
Common Name (CN)	Name of the Certificate holder
Organization Identifier	Identifier for the Subscriber
Optional:	
Organizational Unit (OU)	Department of the subscribers' organization
Subjectserialnumber (SN)	Subjectserialnumber of the Certificate holder

The names used in **Server certificates certificates** comply with the X.501 name recommendation. The names consist of the following parts:

Attribute	Value
Country (C)	NL
Organization (O)	Name of the subscriber
Common Name (CN)	FQDN
Locality (L)	Place where the Subscriber is located
Optional:	
Organizational Unit (OU)	Department of the subscribers' organization
Subjectserialnumber (SN)	Subjectserialnumber of the Certificate holder

The names used in **Private Services Server** certificates comply with the X.501 name standard. The names consist of the following parts:

Attribute	Value
Country (C)	NL
Organization (O)	Name of the subscriber
Common Name (CN)	FQDN
Optional:	
Organizational Unit (OU)	Department of the subscribers' organization
Subjectserialnumber (SN)	Subjectserialnumber of the Certificate holder
State or Province (S)	Province where the Subscriber is located
Locality (L)	Place where the Subscriber is located

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

The use of pseudonyms is not allowed within PKIoverheid.

3.1.4 Rules for interpreting various name forms

Names of persons included in the Certificate meet the requirements as stated in the Program of Requirements, Part 3a Certificate Policy - Domain Government / Business and Organization, ANNEX A Profiles and Certificate Status Information.

All names are, in principle, exactly copied from the presented identification documents. The However, the name data may contain special characters that are not part of the standard character set conforming to ISO8859-1 (Latin-1). If the name contains special characters which are no part of this character set, KPN will perform a transition. KPN reserves the right to change the requested name upon registration if this is legally or technically necessary.

3.1.5 Uniqueness of names

The names used identify the Certificate Holder in a unique way. Uniqueness of names within the X.501 name space is the starting point.

KPN ensures the uniqueness of the ‘subjectaltname’ field. This means that the distinguishing name used in an issued certificate can never be assigned to another subject. This is done by including a unique subject serial number in that field.
For personal certificates and group certificates, KPN generates a number for this purpose.

In specific cases, if explicit agreements have been made, a specific number may be added to this subject number.

In cases where parties disagree with the use of names, KPN decides after considering the interests concerned, insofar as this is not provided by mandatory Dutch law or other applicable regulations.

3.1.6 Recognition, authentication, and role of trademarks

Subscribers bear full responsibility for any legal consequences of using the name provided by them.

The name of an organizational entity as mentioned in the extract of a recognized registry, or in the law or decision by which the organizational entity is established, is used in the Certificate.

KPN is not required to investigate possible infringements of trademarks arising from the use of a name that is part of the data contained in the Certificate.

KPN has the right to make changes to name attributes when it appears to be in violation of a trademark or other intellectual property rights.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The key pair, whose Public Key is Certified, is created by KPN.

However, this does not apply to the Server Certificate. The server certificate key pair is created by or on behalf of the Subscriber in the Subscriber's Secure Environment and entered on the (HTTPS) website of KPN. To ensure that that has indeed happened, the Subscriber must sign for this on the Certificate Request form for the Server Certificate.

See Further 3.2.3.3 Server Certificates Authentication and 6.2.11 Requirements for Secure Resources for Storage and Use of Certificates.

3.2.2 Authentication of organization identity (Subscriber authentication)

If an organization wishes to become a subscriber of KPN, it is necessary to complete the web form PKIoverheid Subscriber Registration. This form contains an extensive explanation. With this form the Subscriber must send along several supporting documents.

The information requested is:

- The Chamber of Commerce number;
- Name of the subscriber. The Subscriber may, if desired, use a trade name, provided that it is registered;
- Subscriber contact information;
- Name and function of his authorized representative;
- Billing data;
- Data of the contact to be authorized, such as name and contact details.

The PKIoverheid Subscriber Registration form must be signed by the Subscriber's Authorized Representative. With this signature the Authorized Representative declares:

- to have filled in the Subscriber Registration application completely and truthfully, agreeing to the Special Conditions,
- that the contact person (s) listed on the form are authorized, trusted and knowledgeable in the area, may apply on behalf of the Subscriber for certificates in order to install, administer and, if necessary, revoke, and
- that these contactperson(s) who have a PKIoverheid personal certificate for access to the Self Service Portal are authorised to request qualified certificates for electronic seals (eSeal).

The signature must be a valid signature, so it must be a handwritten or qualified electronic signature. The electronic signature must comply with REGULATION (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT (eIDAS). If the electronic signing is on behalf of an organization (Subscriber), the Qualified Certificate with which the electronic signature is created must also be issued to the Certificate Holder on behalf of the same Subscriber within the Government / Business and Organization PKI Government domain.

The term "Subscriber" is used below. If a Subscriber is to perform an activity, the contact person generally acts on behalf of the Subscriber. However, this is not explicitly indicated.
The proofs that must be submitted at the same time as the form are:

- copy of the identity of the Authorized Representative that meets the requirements of the Dutch Identification Act (hereafter Wid) the Authorized Representative foresees the application of a handwritten signature;

- copy of the identity of each contact that is authorized on the form. This ID must also meet the requirements of the Wid.

If KPN is unable to find evidence of the Competent Representative's competence, it will be requested during the processing of the application to provide that evidence.

For municipalities that arise in the context of a municipal reorganization, but at the time of the application for becoming subscriber not yet formally exist, it is now also possible to apply for a subscription. These (new) municipalities must demonstrate that they will exist on a particular date. For example, by sending a copy of the law in which the relevant municipal reorganization has been arranged. These municipalities may request Server Certificates after approval of the subscriber application. Upon approval of the license application, the requested certificates will be issued under the restrictive condition that the Server Certificates will only be used on or after the date of the (new) municipality formally starts to exist.

If a practitioner of a recognized Profession wishes to become a subscriber of KPN, he / she must fill in the appropriate web form Request PKIoverheid recognized profession Certificates (dutch: webformulier Aanvraag PKIoverheid Beroepsgebonden Certificates). In this form, the application of a Subscription and Certificates has been merged into one form. This is because Subscriber and Certificate holder are one and the same person. This web form is available when you start the application via https://certificaat.kpn.com/aanvragen/beroepscertificaten/. This form contains an extensive explanation.
The above does not apply to those recognized professions as mentioned in the Act of 11 November 1993, governing occupations in the field of individual healthcare.
The information requested for the subscriber registration is:

- the name of the subscriber;
- contact details.

The application for a PKIoverheid Recognized Profession Certificate must be signed by the Subscriber. By signing, the Subscriber confirms that the certificate request was completed correctly, fully and truthfully, and that the subscriber agrees to the KPN Special Terms.

The signature must be a valid signature, so it must be a handwritten or electronic signature. The electronic signature must comply with Regulation (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT (eIDAS)

The application for a PKIoverheid Recognized Profession Certificate shall provide proof that the certificate holder is authorized to exercise the Recognized Profession. This evidence must be authentic. As authentic evidence to exert a Recognized Profession is only Considered:

- either a valid certificate of registration in an approved (profession) register where disciplinary actions are legally regulated;
- or a valid nomination by the Minister;
- or a valid (e.g., a license) compliance with the legal requirements for exercising the profession.

A valid certificate means that certificate has not expired or (provisionally) revoked.
For a limited number of professional groups (notaries and bailiffs) KPN itself will check the registers maintained by the professional groups in question.

In Addition, the application for PKIoverheid Recognized Profession Certificates shall be accompanied by a copy of the ID of the Certificate holder. This identification must meet the requirements of the Wid (Dutch Identification Act). The identification is used to compare the data of the certificate with the details of the evidence for exercising the Recognized Profession. It also will be used to compare the signature on the application with the signature on the ID. The ID must still be valid at least six weeks after submission of the application.

KPN will receive the application form and supporting documents and will assess the completeness and correctness by, among other things, consulting other external sources. Segregation of duties is applied between he / she that assesses (Check) and he / she that approves (Decision). Only if the form is complete and correct, KPN will approve the form, proceed to registration, assign a subscriber number and inform the Subscriber. The subscriber number should always be used in the communication between subscriber and KPN. Only if an organization is registered as a subscriber with KPN it may apply for certificates from KPN.

If changes Occur in the data provided by the Subscriber to KPN, the Subscriber is obliged to inform KPN in an early stage. Early means at least 10 working days before the change becomes effective. Changes cannot be made retrospectively.

Changes which must be communicated are for example the departure of the Authorized Representative or contact or change in the contact of the Subscriber. For the communication of these changes forms available on the site (https://certificaat.kpn.com/wijzigenregistratie/). These forms are also provided with a detailed explanation. Here too, KPN will review the changes for completeness and accuracy and that the Subscriber will be informed on making changes in the subscriber registration.

3.2.3 Authentication of individual identity

If a subscriber wants to apply for a certificate, it must complete a specially developed electronic application form and send it to KPN. These forms:

- Request PKIoverheid Personal Certificates;
- Request PKIoverheid Profession Certificates;
- Request PKIoverheid Group Certificates;
- Request PKIoverheid eSeal Certificates (Self Service Portal only);
- Request PKIoverheid Server Certificates.

The application form (electronic) is shall be signed by the Subscriber. By signing the form, the Certificate holder or Certificate Administrator are authorized to receive the requested certificate on behalf of the Subscriber and to use and / or manage it.

KPN offers customers the ability to use a self-service portal. After registration Authorized Representatives and Contact persons of the subscriber can use the portal. The login is based on a PKIoverheid personal certificate. The portal gives users access to the main subscriber data and an overview of the certificates already issued. It also offers the opportunity to apply for certificates with reuse of already recorded data.

When applying for a certificate the Subscriber has (if requested) to enclose a photocopy of the identity of each Certificate holder for which a certificate is requested.

The identification must meet the requirements of the Wid (Dutch law on Identification). At the time of establishing the identity, the relevant ID must not be expired.

The identification is carried out on an agreed time and place by a member of AMP.

3.2.3.1 Authentication for certificates for natural persons (Individuals)

Certificates for natural persons are requests for either Occupational Certificates or Personal Certificates. On the application form for such a certificate the following data must be filled in.

Of the Subscriber:

- subscriber number
- name Contact person (only for Personal Certificates).

Of the Certificate at least:

- full names;
- other data required for identification like Nationality, gender, date of birth and - place;

the delivery address (business or private postal address), for sending the smartcard /usb token and PIN-mail respectively. If the choice has been made for the issuance of a mobile smart card for the delivery of the installation instruction and PUK code.
Other data, such as:

- if once before a certificate is issued to the certificate holder (in that case the earlier obtained subject serial number must be included in the application);
- Universal principal name (UPN, general Windows login name);
- the Desired product.

3.2.3.2 Authentication for the purpose of a Services Certificate

Services Certificates must be managed by a Certificate Manager specially designated and authorized by the Subscriber. In principle Certificate Managers can manage multiple Services Certificates.

Intended Certificate Managers, who are not yet registered, can be included in the application for a services certificate by the Subscriber as a new Certificate Manager.
The application form must then contain the following information of the Certificate Manager:

- full names;
- data needed for identification like date of birth and - place;
- the name of the organization where the Certificate Manager is employed
- e-mail address and telephone number;
- delivery address (postal address).

KPN will review this data for completeness and accuracy while handling the Services Certificate application. Segregation of duties is applied between he / she that assesses (Check) and he / she that approves (Decision). Only if the data are complete and accurate, KPN will register the Certificate Manager and as a result can act as a Certificate manager of a Services Certificate.

KPN will inform the subscriber about the registration by e-mail.

3.2.3.3 Authentication for the purpose of a Group Certificate

The Certificate Request for a Group Certificate must be completed with the following information.

Of the subscriber's organization:

- the subscriber number.

Of the Contact Person:

- last name;
- date of birth

Of a new Certificate Manager:

- full names;
- data needed for identification such as date of birth and - place;
- the name of the organization where the Certificate Manager is employed;
- e-mail address and telephone number;
- delivery address (postal address).

Of an existing Certificate Manager:

- last name;
- e-mail address;
- Registration number.

Other data, such as:

- If an organization wants to participate in the digital government services, such as Digikoppeling and Digipoort: the Government Identification number (for government organisations) or Chamber of Commerce number (for private sector organizations);
- Universal principal name (UPN, general Windows login name);
- if once before a certificate is issued to the certificate holder;
- the desired product.

KPN will review the Certificate Application for completeness and accuracy, including the signature and submitted evidence. Segregation of duties is applied between he / she that assesses (Check) and he / she that approves (Decision). Only if the Certificate Application is complete and correct, KPN will approve the Certificate Application.

KPN will inform the Subscriber in writing or by e-mail on approval of the Certificate Application.

3.2.3.4 Authentication for the purpose of an eSeal Certificate

In the Self Service Portal the request for an eSeal Certificate must be completed with the following information (some fields are pre-filled):

Of the subscriber's organization:

- the subscriber number.

Of the Contact Person:

- last name;
- date of birth

Of a new Certificate Manager:

- full names;
- data needed for identification such as date of birth and - place;
- the name of the organization where the Certificate Manager is employed;
- e-mail address and telephone number;
- delivery address (postal address).

Of an existing Certificate Manager:

- last name;
- e-mail address;
- Registration number.

Other data, such as:

- if once before a certificate is issued to the certificate holder;
- the desired product.

KPN will review the Certificate Application for completeness and accuracy, including the signature and submitted evidence. Segregation of duties is applied between he / she that assesses (Check) and he / she that approves (Decision). Only if the Certificate Application is complete and correct, KPN will approve the Certificate Application.

KPN will inform the Subscriber in writing or by e-mail on approval of the Certificate Application.

3.2.3.5 Authentication for the purpose of Server Certificate

The Certificate Request for a Server Certificate must be completed with the following information.
Of the subscriber's organization:

- the subscriber number.

Of the Contact Person:

- the subscriber number and last name;
- date of birth.

Of a new Certificate Manager:

- full names;
- data needed for identification like date of birth and - place;
- the name of the organization where the Certificate Manager is employed;
- e-mail address and telephone number;
- delivery address (postal address).

Of an existing Certificate Manager:

- last name;
- e-mail address;
- Registration No.

Of the Certificate Holder at least:

- Certificate Signing Request data from the server;
- (primary) identifier or name of the server,the primary name of the server will be included in the Subject.commonName and in the SubjectAltName.dNSName of the certificate;
- Optional additional identifier 's or names of the server can be specified, additional names are in addition to the primary name included in the SubjectAltName.dNSName of the certificate, in the order as provided in the application.

Other data such as:

- country name and country code in accordance with ISO 3166;
- If an organization wants to participate in the digital government services, such as Digikoppeling and Digipoort: the Government Identification number (for government organisations) or Chamber of Commerce number (for private sector organizations);

The subscriber must demonstrate entitlement to use the organization's primary and additional names that identify the server or service. The primary and additional names of the server MUST be referred to as "fully qualified domain name" (FQDN, see definitions). In this field, a Plurality or FQDN "s MAY be used.

KPN will review the Certificate Application for completeness and accuracy, including the signature and submitted evidence. Segregation of duties is applied between he / she that assesses (Check) and he / she that approves (Decision). Only if the Certificate Application is complete and correct, KPN will approve the Certificate Application.

KPN will inform the Subscriber by e-mail on approval of the Certificate Application.

3.2.3.6 Authentication for the purpose of a Private Services server certificate

3.2.3.6.1 Authentication of a Certificate Manager

Private Services Server certificates must be managed by a Certificate Manager explicitly designated and authorised by the Subscriber. In principle, Certificate Managers can manage several certificates. Because this is a very common practice, the identification and authentication of the Certificate Manager is disconnected from the certificate request of the Private Services Server certificate itself. KPN has implemented the following working method.

Certificate managers must be registered separately by the Subscriber, for each Subscriber for whom he/she is or will be working. A registration form is available for this purpose. The following information must be entered on the registration form for Certificate Managers.

From the Contact Person:

- Subscriber number and name;
- name and contact details.

From the Certificate Manager:

- Full names;
- data required for identification as nationality, sex, date and place of birth;
- the name of the organisation for which the Certificate Manager is working (only if the Certificate Manager is not working for the Subscriber);
- e-mail address and telephone number;
- delivery address (postal address).

This evidence must not be older than 13 months otherwise the data must be resubmitted and verified unless the agreement with the subscriber explicitly provides that the certificate manager retains his or her authorisation until such time as it is reviewed by the subscriber or until the agreement expires or is terminated. KPN will receive the registration form and assess it for completeness and accuracy, including the signature and evidence provided. In doing so, a separation of functions is applied between the person who assesses (checks) and the person who decides (has). Only if the registration form is complete and correct will KPN register the Certificate Manager and a Private Services Server certificate can be requested.

KPN will inform the Subscriber by e-mail on approval of the Certificate Application.

3.2.3.6.2 Authentication for the purpose of a Private Services server certificate

On the Certificate request for a Private Services Server certificate, the following information must be provided:

From the subscriber organization:

- The subscriber number.

From the Contact Person:

- Subscriber number and name;
- name and contact details.

From the Certificate Administrator:

- Full names;
- telephone number;
- Registration number.

Other information such as:

- whether it is an initial application or a replacement;
- Country name and country code according to ISO 3166.

The subscriber must demonstrate that the organization may use the primary and additional names identifying the server or service. The primary and additional server names MUST be listed as fully-qualified domain names (FQDN, see definitions). Multiple FQDNs are used in this field MUST be used. These FQDNs MUST come from the same domain name range. (e.g. www.logius.nl, application.logius.nl, secure.logius.nl etc.).

KPN will receive the Certificate Application and assess it for completeness and correctness, including the signature and evidence provided. In this case, a segregation of duties is applied between the person who assesses and the person who decides. KPN will only approve the Certificate Application if the Certificate Application is complete and correct.

KPN will inform the Subscriber of the approval of the Certificate Application by e-mail.

3.2.4 Non-verified subscriber information

All information in the certificate is verified.

3.2.5 Validation of the authority

KPN validates the applicant’s legal status (described in section 3.2.2 and 3.2.3) by:

- checking the Chamber of Commerce registry for organisational applicants;
- checking the individual identity of the applicant in the face-to-face check;
- checking the authorization for the profession (Recognized Profession Certificates only);
- where the applicant has been authorised by the legal representative of an organisation, authorisation must be completed, or there must be a completed authorisation available.

The authorization of the Certificate Holder to receive and use a certificate from the organization is demonstrated by signing the certificate application by or on behalf of the subscriber.
In case of a Server Certificate, the Subscriber must supply proof of the identifier of the device or system, so that reference can be made to it.

The KPN special conditions stipulates that the Subscriber has the obligation, if relevant changes occur in the relationship between the subscriber and Certificate Holder, to revoke the certificate immediately. Significant changes in this regard may include suspension or termination of employment or professional practice.

3.2.6 Criteria for interoperation

No stipulation. KPN has no interoperation or cross-certification.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

KPN does not allow for renewal of certified keys. A request for renewal will be treated as an application for a new certificate.

3.3.2 Identification and authentication for re-key after revocation

No stipulation. KPN does not allow for renewal after revocation.

3.4 Identification and authentication for revocation request

In Section 4.9 Revocation and suspension of certificates is described who may submit a request for revocation.

Only the Subscriber or the Certificate holder, or in the case of the Services Certificate, the Certificate Manager, may submit a request to revoke a certificate. This can be done Electronically / online through the KPN website (https://certificaat.kpn.com/intrekken/).
In order to revoke the Certificate. The Certificate Holder/ Certificate Manager is required to make use of a revocation pass code.

The revocation code for Profession Certificates, and Personal certificates is sent to the Certificate Holder or the Certificate Manager (PIN-mail). The revocation code for Services Certificates and Server and Private services server certificates is sent to the Certificate Manager. In case of a server certificate the revocation code can also be sent by encrypted e-mail.

In some cases, the Subscriber is obliged to revoke its certificate (see the KPN Special Conditions). In the event that the Certificate Holder / Certificate Manager fails to do this, the subscriber needs to be able to do this. For this purpose, the Certificate / Certificate Administrator must provide the revocation code to the Subscriber or The Subscriber must obtain the revocation code from the Certificate Holder / Certificate Manager immediately after issuing and record carefully this carefully.

For non-urgent revocations the Subscriber and / or the Certificate Holder / Certificate Manager can submit a revocation request using the form "Request Revocation Certificates.

On the form " Certificates Revocation Request ", the following information must be completed.

Of the Contact person:

- Subscriber number and –name;
- name en contact data.

Of the Certificate:

- name in the Certificate;
- subject serial number in the Certificate;
- certificate type;

- serial number(s) the Certificate (s)
- revocation code;
- reason for revocation.

The form "Certificate Revocation Request" will be accepted by KPN and reviewed for completeness and accuracy. If the application is complete and accurate KPN will execute the revocation. With this segregation of duties is applied between he / she that assesses (Check) and he / she that approves (Decision). This revocation will be executed within four hours after the receipt of the revocation request.

The Subscriber and the Certificate Holder / Certificate Manager will be informed by e-mail concerning the outcome of the revocation request.

If KPN has good cause to doubt the authenticity of a revocation request, KPN can require that he /she who submitted the request will produce proof of Identity to KPN before the revocation is executed.

KPN is also entitled to revoke certificates independently if: (see Section 4.9.2):

- Subscriber acts Contrary to the conditions Imposed on him for use, as defined in this CPS and in the Special Conditions or;
- the Private Key of the KPN CA or from the State of the Netherlands, is stolen or otherwise compromised or;
- The algorithm used is compromised, or is liable to be compromised or, in general, becomes too weak for the purpose for which it is used.

KPN is able to revoke a certificate without the revocation code.

A relying party may report a subscriber who does not or does not fully comply with the conditions imposed. This can be done using the contact form https://certificaat.kpn.com/intrekken/.
In the field ‘Betreft’ (subject) option ’10. Melding omstandigheid intrekking Certificates’ should be chosen. (eng:"10. Notification conditions that can lead to revocation”).
This form can contain the following: details of the reporter such as his name, organization name and contact information;

- data of the condition, such as a description and date and time of the notification;
- details of the relevant certificate such as the name and subject serial number of the Certificate holder, the Certificate type and serial number.

KPN will receive the notification, review the form for completeness and accuracy, and possibly try to collect additional information and decide whether to proceed with revocation. With this segregation of duties is applied between he / she that assesses (Check) and he / she that approves (Decision).
Revocation will be executed within four hours after the decision to do so.
The detector, the Subscriber, Certificate holder/ Certificate Manager in question will be informed by e-mail about the notification and its handling.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application?

In principle, only the Authorized Representative of the Subscriber can apply for a subscriber registration. By signing the subscriber registration, the Authorized Representative authorizes one or more contacts mentioned in the form to apply for, install, manage and revoke certificates and to Authorize other contacts and Certificate Managers, on behalf of the Subscriber.

4.1.2 Enrolment process and responsibilities

4.1.2.1 Enrolment process

The processes defined by KPN for the realization of its certification service are in general divided two parts, based on the principle of segregation of duties. The first part is the assessment and the second part is the execution. In the assessment the receipt of the application is recorded, the completeness of the application and the presence of supporting documents are determined(acceptance) and evaluated on accuracy. Last part of this section is to take a decision on the application. The second part, the execution, is to implement the decision and informing stakeholders about it. In the following sections, the processes will be described in more detail.

The duties and responsibilities of those involved, KPN, Subscriber, Certificate Holder / Certificate Manager and Relying Party are described in the KPN Special Conditions.

4.1.2.2 Responsibilities and obligations of the TSP

KPN is responsible for all certification services and guarantees Subscribers, Certificate Holders and Relying Parties that it will abide by the Special Conditions, the CPS and the applicable CPs. KPN is obviously responsible for outsourcing (parts of) services to other parties. An example of this is the outsourcing to AMP of the identification of Certificate Holders and Certificate Managers. But KPN has outsourced multiple services. As final responsible Trust Service Provider, as an outsourcer of services, KPN ensures the quality of the outsourced services by applying (forms of) management, coordination, supervision and mutual assurance. The implementation will depend on the specific situation.
If a subcontracting reaches a certain extent, the outsourcing will be described in an appendix to this CPS.

4.1.2.3 Responsibilities and obligations of the Subscriber

The Subscriber is responsible for the correctness of all data required for the creation and delivery of certificates and for the proper use of those certificates. Subscriber warrants to KPN and Relying Parties that it will abide by the Special Conditions, the CPS and the applicable CPs.

4.1.2.4 Responsibilities and obligations of the Certificate Holder

The Certificate Holder (including, in the case of a server certificate or Group Certificate, the Certificate Manager), as holder of the certificate that is requested on behalf of the Subscriber of the Certificate Holder is also responsible for the correct delivery of all data needed for creating and delivering certificates and the proper use of those certificates. The Certificate Holder warrants to KPN, the

Subscriber and Relying Parties that he / she will abide by the Special Conditions, the CPS and the applicable CPs.

4.1.2.5 Responsibilities and obligations of the Relying Party

Relying Party is responsible for correctly Relying on a certificate and Warrants to KPN, the Subscriber and the Certificate Holder that it will abide by the Special Conditions, the CPS and the applicable CPs.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Organizations must, before being able to apply for certificates, register as a subscriber of the certification services from KPN. This can be done by completing a web form “PKIoverheid Subscriber Registration”, attach the required evidence (see Section 3.2.2) and send all by mail to KPN. Detailed instructions for using the form are attached to this form. Other forms are available for maintaining the data supplied to KPN. See the website https://certificaat.kpn.com/wijzigenregistratie/

Part of the registration of a subscriber, is the authorization of one or more contact persons. These contact persons need to be authorized to apply for certificates, to authorize other contact persons and to be allowed to revoke certificates. The authorization is done by signing the form “Abonnee Registratie (subscriber registration)” by the Authorized Representative of the subscriber (see Section 3.2.2).

KPN will receive the forms and assess the completeness and accuracy of the forms. A registration form must be complete in order to be accepted and to proceed to assess the accuracy. In case of deficiencies the subscriber that submitted the PKIoverheid Subscriber Registration web form will be contacted.

If the subscriber registration has been approved, the subscriber is registered and can request for certificates. The Subscriber will be informed in writing and by e-mail of approval or disapproval.

In addition to registering the organization as a Subscriber, also Certificate Managers of Services Certificates can be registered. Certificate Managers can manage multiple certificates in principle but must first be registered to do so. This can be done during the application for a Services Certificate by adding a not yet registered Certificate Manager. This can also be accomplished by filling out the form Registration Certificate Managers, attach the requested evidence (see section 3.2.3.2) and send all by mail or Electronically to KPN. Detailed instructions for using the form are attached to the form. There are also forms available for maintaining the data supplied to KPN.

Also for registering Certificate Managers it applies that KPN will accept the application for registration of a Certificate Manager, assess the completeness and accuracy and will come to an approval or disapproval. The Subscriber will be informed by e-mail of the decision.
Part of the registration of the Certificate Manager is his personal identification. This is handled in the same way as for Certificate Holders, by AMP (see also section 4.2.2).

Once a Certificate Manager is identified and registered, applications for Server and Group Certificates can be handled as described in section 4.2.

If the Certificate Manager’s personal details changes, the Contact Person must pass this modified data to KPN using the form: “Wijziging gegevens Certificaatbeheerder (Change information Certificate Manager)” (see Electronic storage), and if a Certificate Manager is no longer able to manage the assigned certificates, the Subscriber has to report this by means of the form “Verwijdering Certificaatbeheerders(Removal of Certificate Manager)”. KPN will review this form for completeness and accuracy. After a positive decision KPN will remove the Certificate Manager from the corresponding registration. Prerequisite for that removal is that the management of the certificates is transferred to another registered Certificate Manager.

4.2.2 Approval or rejection of certificate applications

There are different procedures for different types of applications:

- Applications for Personal Certificates, Profession Certificates and Group Certificates on a Smartcard or USB token, whereby the key pair is created by KPN;
- Applications for Profession Certificates and profession Certificates in the form of a Mobile smartcard (HSM) where the key pair is created in the HSM by the App of Ubiqu by means of a smart phone.
- Requesting Server Certificates, where the key pair is created by the Subscriber in the Subscriber's Safe Environment.
- Requesting Private Services Server Certificates, where the key pair is created by the Subscriber in the Subscriber's Safe Environment.

4.2.2.1 Application for Certificates on a Smartcard or USB token

The following steps must be taken by default for applying for a Personal, Professional, Group or eSeal Certificate on a smartcard or USB token.

Contactperson(s) authorised by the Authorised Representative and who have a PKIoverheid personal certificate for access to the Self Service Portal are authorised to request qualified certificates for electronic seals (eSeal).

1. The Subscriber fills out a certificate application form for a (prospective) Certificate Holder (or a Certificate Manager for the latter) and hereby declares that he agrees with the Special Terms and Conditions. Further instructions on how to use the form are enclosed with the form.
2. The Subscriber signs the application form and sends it to KPN.
3. KPN receives the Certificate Application, evaluates the completeness and correctness of the Certificate Application and makes a decision on it. Among other things, it is checked at recognised registries such as Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA) whether Subscriber is the owner of the domain name, as it forms part of the e-mail address.
4. In the case of profession certificates, the authenticity of the proof of exercise of the Recognised Profession is verified.
5. AMP identifies the Certificate Holder, makes a copy of his identity document (with shielding the passport photo and BSN) and sends this copy together with the signed identification electronically to KPN. If KPN can rely on an identification previously carried out by KPN, this identification does not need to be repeated. KPN can rely for Certificate Managers on an identification previously carried out by or on behalf of KPN if the identity document used is used again in the new application, it is not registered as stolen or missing and it is still valid until six weeks after submission of the application. The date of receipt of the application by KPN is the decisive factor.
6. If KPN approves the Certificate Application, the key material in the QSCD will be generated and the Certificate generated. KPN also generates the secret PIN and PUK code for the QSCD and the revocation code for the Certificates.
7. The smartcard/token containing the certificates is sent by post to the delivery address of the Certificate Holder/Certificate Manager. The smartcard/token is accompanied by an acknowledgement of receipt notification with a code. The Certificate Holder/Certificate Manager must confirm receipt of the smartcard/token via a link in the email using this code. AMP identifies

the Certificate Holder, makes a copy of his identity document, sends this copy to KPN electronically together with the signed identification.
8. Upon receipt of the electronic AMP confirmation, KPN will send the document containing the secret PIN and PUK codes for the QSCD/SUD and the certificate revocation code for the Certificates by post to the specified delivery address of the Certificate Holder.

KPN will continue to offer the possibility of allowing identification and issuance at a time/location to be agreed upon.

4.2.2.2 Application for Certificates as Mobile Certificates

For the application of a Mobile Certificate, in principle the same steps (1 to 6) are followed as for the physical Smart Card or USB token. See 4.2.2.1.
The validation of the data and identification take place in exactly the same way. However, no physical product is received in the form of a smart card or token.

7. A PINmailer is sent in which the PUK code of the certificate is included.
8. KPN sends an order to Ubiqu to generate the key pairs.
9. KPN sends a registration and activation code by email and the corresponding CSR to the customer by letter.
10. The customer installs the app with the obtained registration and activation code and chooses a pin code.
11. With the chosen PIN code, the certificate holder confirms the creation of the certificate.

4.2.2.3 Application for Server Certificates

CAA DNS records.
The CAA record is a DNS record that gives domain owners extra control over TLS certificates issued for their domains - you use it to indicate which CA may issue certificates for your domains. The CAA record already became a recognised standard in 2013. Although it is often used, it was not compulsory. As of September 2017, it is mandatory for Certificate Authorities to check the CAA record of a domain name as part of the issuance of a certificate. Domain owners are not obliged to fill the record.

What is a CAA DNS Record?
A Certificate Authority Authorization record, or a CAA DNS record, is designed to allow domain owners to indicate which CA root certificate can be used to sign certificates for the domain in question. Because this certificate belongs to a certain certificate authority, it can effectively indicate which certificates may be issued for a domain. This prevents the issuing of a certificate by another CA that the selected CA.

KPN identifies itself as KPN.COM. If a domain owner wants KPN to be able to issue certificates for its domain, this identification must be included in the CAA record.

Example: IN CAA 0 issue "kpn.com".

KPN is therefore entitled to issue certificates for a certain domain if:

- The DNS of the domain in question does not contain a CAA record.
- The applicant has entered the identification "kpn.com" in the CAA record for the domain concerned.

In all other cases, KPN cannot issue the certificate and will contact the certificate applicant.

The Certificate Application for a Server Certificate largely follows the same procedure as mentioned under 4.2.2.1, considering the following difference.

1. The Certificate Administrator creates the key pair (length is 2048 bits) in the Subscriber's Safe Environment and sends a Certificate Signing Request (CSR) containing the Public Key. Subscriber completes the electronic application form PKIoverheid Server Certificates for a (future) Certificate Holder. This form can be found on the KPN website (https://certificaat.kpn.com/aanvragen/servercertificaten/). This site also contains further instructions on how to use the form.
2. KPN receives the Certificate Application and assesses the completeness and correctness of the Application. Among other things, it is checked at recognised registries such as Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA) whether Subscriber is the owner of the domain name.
   KPN has 3 permitted methods for domain validation according to the Baseline Requirements of the CA/BROWSER forum. (https://cabforum.org/) It concerns the methods:

   NB. The numbers below are the corresponding section numbers from the Baseline Requirements of the CABforum, where these requirements are described.

   a) 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact
      In the Whois application the administrative contact is determined and the administrative contact is asked by email for approval to use the domain in question
      If the whois data is not available (or if no answer is received from the administrative contact) an email is sent (method b) to the contact person who submitted the application for the certificate containing a code, with the request to put this code in a certain directory on the site (/.well-known/pki-validation) or in a TXT field of the DNS registration of the domain in question (method c);
   b) 3.2.2.4.7 DNS Change;
   c) 3.2.2.4.18 Agreed-Upon Change to Website v2.

3. KPN will determine whether there is a CAA DNS record for the domain (s) involved and if this occurs whether KPN has been included through its identification kpn.com as a permitted certificate issuer for these domain (s). If this is not the case, KPN will contact the applicant and reject the relevant certificate application.
4. In addition, it is also assess whether there is url-spoofing or phishing, therefore https://www.phishtank.com or similar will be consulted to see if the domain name does not appear on a spam and/or phishing blacklist. If KPN suspects phishing or other possible abuse, KPN will report this suspicion to https://www.phishtank.com.
5. Subscriber's KvK data are read in real time from the Chamber of Commerce systems. An OIN is generated automatically from the data of the Chamber of Commerce.
6. If KPN approves the Certificate Application, the Certificate is created and sent to the Certificate Manager by e-mail.

4.2.2.4 Distinction in Public and Private Services Server certificates

A PKIoverheid services server certificate comes in two types, a Public Root and a Private Root server certificate. Server certificates are suitable for securing traffic between systems and traffic to/from websites. Both types of certificates meet the requirements of PKIoverheid, are securely managed and audited by a third, independent party. However, the certificates differ in two respects, the validity period and the applicability of the certificate.

A Public Root certificate is valid for approximately 1 year and 1 month (397 days max). This applies to new certificates to be issued with effect of November 1, 2019. Certificates already issued retain their validity period. This type of certificate is registered with software suppliers and is automatically trusted by web browsers.

A Private Root certificate is valid for 3 years. This type of certificate is not registered with software suppliers and is not automatically trusted by browsers. However, this is not an obstacle if the certificate is used for messaging between systems.

The Certificate request for a Private Services Server certificate is essentially similar to the request for a server certificate. See 4.2.2.3.

4.2.3 Time to process certificate applications

In principle, KPN uses a period of 10 working days to process a Certificate Application. In principle, because this deadline also depends on the quality of the application submitted.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

4.3.1.1 Issuance of Personal, Professional, Group and eSeal Certificates

AMP informs KPN about the result of the identification. After a positive message, KPN sends out the document containing the access codes for the smart card and the revocation codes of the certificates.

In the event that the certificate holder fails to identify himself, he will be reminded of this after 3 weeks. If after 6 weeks the identification has not taken place, the certificate applications will be revoked without further notice.

If the Certificate Holder / Certificate Manager has not confirmed receipt within 3 weeks, KPN will send a reminder. If the Certificate Holder / Certificate Manager has not confirmed receipt within 6 weeks, KPN will revoke the Certificates concerned without further notice.

KPN shall confirm the issuance of the Certificate in writing or by e-mail to the Subscriber.

4.3.1.2 Issuance of all types of Server Certificates

For applications from registered Certificate Managers, KPN sends the created Certificates by e-mail to the specified e-mail address of the Certificate Manager and to the requesting Contact Person.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Immediately after the generation of the Certificate, completion can be seen via Directory Service. However, because the physical transfer to Subscriber takes place at a later time, this has limited value.

The Certificate Holder shall be explicitly informed of the production by physical transmission of the smartcard, including the certificate produced. The Certificate Manager is explicitly informed of the production by sending the Server Certificate by e-mail to the specified e-mail address.

In the case of a Mobile Smart Card no physical Smartcard is sent. Only a PINmailer is sent containing the PUKcode of the certificate.

The Subscriber (not applicable to Profession Certificates) will be informed by e-mail or post of the creation and transmission of the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

Professional, Personal, Group and eSeal Certificates
The Professional, Personal, Group or eSeal Certificate is deemed to have been issued and accepted as soon as it is received by the (Subscriber/) Certificate holder or Certificate Manager. He/she shall acknowledge receipt via the link provided by e-mail with the code supplied with the smart Card.

The following applies to the Mobile certificate: The customer installs an app with the obtained registration and activation code and chooses a PIN code. With the chosen PIN code, the creation of the certificate is confirmed by the certificate holder.

Server Certificates
The Server Certificate is deemed to have been issued and accepted as soon as the Certificate Manager uses the Server Certificate obtained. The Certificate Manager must check the content of the certificate for completeness and correctness before installing and using it.

In the specific case of municipalities that are likely to arise (see section 3.2.2), the Certificate Manager must explicitly and as soon as possible confirm receipt of the Server Certificate to KPN. The Certificate Manager ultimately has 6 weeks to do so. KPN will remind the Certificate Manager of its obligation after 3 weeks if KPN has not received the acknowledgement of receipt within this period. If the confirmation of receipt has not been received by KPN within 6 weeks, the relevant Server Certificate will be revoked without further notice. KPN will inform the Subscriber about the revocation of the Server Certificate. However, the payment obligation shall remain in full force and effect.

4.4.2 Publication of the Certificate by the CA

After the Certificate has been issued, it will be included directly in the Directory service.

4.4.3 Notification of certificate issuance by the CA to other entities

KPN does not notify other entities of the issuance of a certificate. Relying parties are able to enquire certificate statuses via the CRL and the OCSP.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

The responsibilities and in particular the associated obligations of the Subscriber and the Certificate Holder/Certificate Manager are described in the Special Terms and Conditions. By signing the various forms or by relying on them, the parties concerned agree to these Special Terms and Conditions.
In addition, it is important for them to take note of the Programme of Requirements of PKIoverheid in general and the applicable CP in particular. The CP sets out all the requirements to which all parties involved in the certification service delivery must comply.

4.5.2 Relying party public key and certificate usage

Before relying on a Certificate, it is particularly important for relying parties to first check the validity of the entire chain from the Certificate to the Root Certificate.

Furthermore, the validity of a Certificate should not be confused with the authority of the Certificate Holder to perform a certain action on behalf of an organization or on the grounds of his/her profession. PKIoverheid does not regulate authorisation. The trustee must convince himself/herself of the authorisation of the Certificate Holder in another way.

4.6 Certificate renewal

KPN does not offer any possibility to renew PKIoverheid Certificates. A request for renewal shall be treated as a request for a new certificate.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other

No stipulation.

4.7 Certificate re-key

Keys of Certificate Holders shall not be reused after expiry of the validity period or after the corresponding Certificates have been revoked.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other

No stipulation.

4.8 Certificate modification

KPN does not offer any possibility to modify the content of PKIoverheid Certificates. If the information in the Certificate no longer corresponds to the actual situation, the Subscriber is obliged to revoke the Certificate in question immediately. If desired, the Subscriber can then apply for a new Certificate.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 *Conduct constituting acceptance of modified certificate*

No stipulation.

4.8.6 *Publication of the modified certificate by the CA*

No stipulation.

4.8.7 *Notification of certificate issuance by the CA to other*

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 *Circumstances for revocation*

In the following cases, the Subscriber and/or the Certificate Holder is obliged to submit a request to KPN to revoke the Certificate immediately and without delay:

- loss, theft or compromise of the Certificate, the private key, the QSCD/SUD, the PIN code and/or PUK code;
- errors in the content of the Certificate;
- changes in the information contained in the Certificate (name, e-mail, etc.);
- changes in the particulars necessary for the reliability of the Certificate, such as termination of employment or professional activity;
- death of the Certificate Holder (in the case of Personal or Profession Certificates);
- Termination or bankruptcy of the organization of the Subscriber (in the case of Organization-related Certificates);

In addition, certificates will be revoked in the following cases if:

- the subscriber indicates that the original request for a certificate was not allowed and the subscriber does not give his consent with retroactive effect.
- KPN possesses sufficient evidence:
  - that the subscriber's private key (corresponding to the public key in the certificate) is affected, and/or
  - a suspicion of compromise, and/or
  - an inherent security weakness, and/or
  - that the certificate has been misused in some other way.

  A key shall be considered impaired in the event of unauthorized access or suspected unauthorized access to the private key, lost or suspected lost private key or QSCD/SUD, stolen or suspected stolen key or QSCD/SUD or destroyed key or QSCD/SUD.
- A subscriber does not fulfil his obligations as set out in
  - this CP and/or
  - KPN's corresponding CPS and/or
  - the agreement that KPN has concluded with the subscriber.
- KPN is informed or otherwise becomes aware of a material change in the information contained in the certificate. An example of this is: a change in the name of the certificate holder.
- KPN determines that the certificate has not been issued in accordance with this CP or KPN's CPS or the agreement entered into by KPN with the subscriber.
- KPN determines that information in the certificate is not correct or misleading.

- KPN ceases to operate and the CRL and OCSP services are not taken over by another Trust Service Provider.

Note: In addition, certificates may be revoked as a measure to prevent or combat a disaster.
The compromise or alleged compromise of KPN's private key, with which certificates are signed, is certainly considered to be a disaster.
Also, if the algorithm used has been compromised, threatens to be compromised or in general becomes too weak for the purpose for which it is used, revocation can be applied where appropriate.

For server certificates also the following reasons apply:

- KPN is informed or becomes aware that the use of the domain name in the certificate is no longer legally permitted (e. g. by a court order).
- The Subscriber uses a "code signing" certificate to digitally sign "hostile code" (including spyware, malware, trojans etc.).
- The PKIoverheid Policy Authority or Agentschap Telecom (supervisory body for eIDAS in the Netherlands) concludes that the technical content of the certificate poses an irresponsible risk to subscribers, relying parties and third parties (such as browser parties) and requests KPN to revoke the certificate.

If a Server certificate has been revoked or if the validity of the Server certificate has expired, it is no longer permitted to use the private key, which is part of the public key of the relevant services server certificate.

Server Certificates issued to a municipality involved in a municipal reclassification need not be revoked immediately as long as the names of the certificate holders concerned do not change. The same applies to ministries involved in redeployment/merger of ministries. If the name of the certificate holder changes in connection with the municipal redivision or merger, the certificate concerned shall be revoked.

Certificates can be revoked by KPN without further intervention if the Subscriber, the Certificate Holder and/or the Certificate Administrator do not comply with the obligations in the Special Terms and Conditions. The reason for each revocation independently carried out by KPN is registered by the company.

In the Mobile certificate application, if the "profile" on the smartphone is deleted, this will be detected by Ubiqu and reported to KPN. This is the signal for KPN to revoke the certificate. The certificate holder will be informed of this revocation.

KPN ensures that the date and time of revocation of (Services) Certificates can be determined precisely. In case of doubt, the time set by KPN will be considered as the moment of revocation.

If a (Services) Certificate has been revoked, it cannot be made valid again.

4.9.2 Who can request revocation?

KPN will revoke a Certificate following a request to do so from the Subscriber, the Certificate Holder, the Certification Manager or the Policy Authority of PKIoverheid. KPN itself may also initiate a revocation request.
A Relying Party may not request a revocation, but may indicate the suspicion of a circumstance that may give grounds for revocation of a Certificate. KPN will investigate such a report and, if there is reason to do so, will revoke the Certificate.

4.9.3 Procedure for revocation request

A request for revocation or notification of a circumstance that may lead to the revocation of a Certificate may be made by email or online (Self Service Portal) at:

https://certificaat.kpn.com/intrekken/

It should be stressed that if the revocation serves an urgent interest, this should be done via the procedure described in section 1.5.2.

KPN ensures that the date and time of revocation of Certificates can be determined precisely. In case of doubt, the time set by KPN will be considered as the moment of revocation.

If a Certificate has been revoked, it cannot be made valid again.

If the "profile" on the smartphone is deleted with the Mobile certificate, this will be detected by Ubiqu and automatically notified to KPN, which will treat it as an automatic revocation request. See 4.9.1

4.9.4 Revocation Request Grace Period

As indicated, if the revocation has an urgent interest, this should be done electronically via the online revocation pages. There is no grace period for online revocation requests.
Requests for revocation by letter shall be considered only on the following working day at the earliest.

4.9.5 Time within which CA must process the Revocation Request

KPN processes the revocation of certificates within four (4) hours after receiving the request.

4.9.6 Revocation checking requirement for Relying Parties

Relying Parties shall be obliged to verify the current status of a Certificate (revoked/not revoked) against the date stated in the Certificate by the end of validity date and by reference to the Certificate Status Information, linked to the time when the Certificate is/will be used. Certification status information can be obtained by consulting the CRL, OCSP or Directory Service. Relying Parties are also obliged to check the Electronic Signature with which the CRL has been signed, including the associated certification path.

Revoked Certificates shall remain on the CRL until their original validity date has expired. Thereafter, Relying Parties can only verify the status of that Certificate through via KPN's online Directory Service or through OCSP.

If a Relying Party wishes to rely on a certificate that he/she has received from a Court Bailiff (a member of the Royal Netherlands Bailiffs Association), he/she must, in addition to the above mentioned inspections, also check whether the Bailiffs mentioned in the certificate mentioned on the date of use of the certificate by the Court Bailiffs, are listed in the register to which the URL mentioned in the certificate (www.registergerechtsdeurwaarders.nl) refers.
If the Court Bailiff has been suspended on the date of use of the certificate by the Court Bailiff, the relevant certificate cannot and may not be relied on.
If the register is not available, the Relying Party should independently obtain information from the Royal Netherlands Bailiffs Association (dutch: Koninklijke Beroepsorganisatie van

Gerechtsdeurwaarders) in order to determine whether the Bailiffs are listed in the register kept by the Royal Bailiffs Association.

4.9.7 CRL issuance frequency

The update of the CRL is initiated every 60 minutes, after the CRL has been generated, the CRL is published. A CRL is valid for 24 hours.

After the expiry date of the issuing CA the last CRL will be published for at least 1 month.

4.9.8 Maximum latency for CRLs

The maximum latency for the CRL is 10 seconds.

4.9.9 On-line revocation status checking availability

In addition to the publication of CRLs, KPN also provides certificate status information via the so-called OCSP. The OCSP configuration is in accordance with IETF RFC 6960.

OCSP validation is an online validation method whereby KPN sends an electronically signed message (OCSP response) to the trustee after the trustee has sent a specific request for status information (OCSP request) to the OCSP service (OCSP responder) of KPN.
The requested OCSP response shows the status of the relevant certificate.

The status can contain the following values: good, revoked or unknown. If an OCSP response is not received for any reason, no conclusion can be drawn regarding the status of the certificate. The URL of the OCSP responder with which the revocation status of a Certificate can be validated is shown in the AuthorityInfoAccess.uniformResourceIndicator attribute of the certificate.

An OCSP response is always sent and signed by the OCSP responder. A Relying Party shall verify the signature in the OCSP response with the system certificate included in the OCSP response. This system certificate has been issued by the same Certification Authority (CA) as the CA that issued the Certificate whose status is being requested.

After the validity date of the issuing CA, the OCSP validation facility will be discontinued.

4.9.10 On-line revocation checking requirements

Relying parties are responsible for checking the certificate status and CRL. Relying parties that fail to check the status of the certificate cannot legitimately rely on the certificate.
KPN supports an OCSP capability using the HTTP GET method for certificates issued in accordance with the Baseline Requirements. The KPN OCSP Responders will respond to a request for the status of a certificate serial number that is “unused” with an "unknown" status.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements related to key compromise

Revocation of a domain or a TSP certificate (or distrust in case of a root certificate) will be considered if the signing key belonging to the certificate is compromised or suspected to be compromised.

Indicators of private key compromise may include:

- Theft or loss of device holding a private key;
- Audit findings indicating private key compromise;
- CT Log findings indicating unauthorized certificate signing;
- Incidents reported to Logius by third parties which may indicate key compromise.

All indicators are registered, analyzed, and followed up accordingly.

4.9.13 Circumstances for suspension

No stipulation. KPN does not perform suspension of certificates

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate Status Services

The CRL is part of a CA system. This system is available 24 /7 hours a week.

Also, in the event of system failures, service activities or other factors beyond KPN's reach, KPN will ensure that for revocation requests submitted online a new CRL is issued within four hours after this submission. For this purpose, a fall-back location and scenario has been designed, among other things, which is regularly tested in combination with redundant data processing and storage.

In addition to consulting the certificate status via CRL and OCSP, it is also possible to request this via the Directory Service.

4.11 End of subscription

If a Subscriber wishes to terminate the subscription with KPN, a form entitled' Opzeggen abonnement (Eng: Subscription cancellation)' can be used. Before KPN can terminate the subscription, all Subscriber's Certificates must be revoked.

Those municipalities that cease to exist because of a municipal reclassification or those ministries that cease to exist because of a ministerial reclassification should not terminate their subscription to KPN immediately but ultimately should terminate their subscription. Not directly because in those cases the rights and obligations of the old organization are taken over by the new organization. But in the end, it is because the old organization formally ceases to exist.

KPN will take receipt of the form, assess its completeness and accuracy and decide on it. Part of this assessment is whether the Subscriber has revoked all Certificates issued to Subscriber. KPN informs the Subscriber about the decision.

Suspension of Certificates is not supported by KPN.

4.12 Key Escrow and Recovery

By default, there is no Escrow of Private Keys. There is no possibility to include Private keys related to Signature Certificates and Authenticity Certificates in Escrow.

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. Facility, Management, and Operational Controls

KPN's certification service provider business unit is certified against ISO9001:2015, ISO27001:2013, ETSI EN 319 411-1 and ETSI EN 319 411-2. Both the Quality Management System and the Information Security Management System are continuously focused on improving these systems through the PDCA cycle.

5.1 Physical controls

5.1.1 Site location and construction

The certification services are managed in and delivered from a highly secure environment within KPN's computing centre in Apeldoorn. This environment complies with the laws and regulations in force for the government, including the Wet Bescherming Staatsgeheimen 1951 (Eng: Act on the Protection of State Secrets).

KPN's secure environment offers standard up to at least five physical barriers to the production environment. For non-production (offline) storage of cryptographic hardware and material, for example, six levels apply.

Improper access to the secure environment requires compromising multiple systems. Depending on the space, this can be a combination of knowledge, QSCD/SUD, biometric data, access guidance and visual inspection. Additional measures include intrusion detection and video recordings. The different access control systems are separated from each other and monitor access to the secure environment. The segregation of duties in combination with five or six physical barriers prevents one individual from gaining access to KPN's critical equipment.

KPN has taken numerous measures to prevent emergencies in the secure environment and/or limit damage. Examples are

- Lightning rod;
- Air conditioning facilities
- Backup of electricity supply by means of an own electrical device;
- Constructional measures (fire resistance, drainage, etc.);
- Fire prevention by means of automatic and manual fire alarm devices. This in combination with targeted, automated fire extinguishing.

The measures are tested on a regular basis. In exceptional cases, an escalation plan shall take effect. The police and fire brigade are familiar with the specific situation regarding KPN's secure environment.

5.1.2 Physical Access

Physical access to the secure environment is achieved through a combination of procedural and technical and constructional measures. Access to the building and the secure environment is monitored by electronic (biometric) and visual means. The entrance system of the building records the entry and exit of staff and visitors. The building is monitored by a security company for 7*24 hours.

The security systems automatically detect attempts at (un)authorized access. The technical measures are supported by various procedures, including movement sensors that monitor persons and materials (for cryptographic key management). The technical infrastructure, including the security systems, is located in protected areas with a designated manager. Access to these areas is registered for audit purposes.

Domestic regulations are in force for the registration and supervision of visitors and service personnel of third parties. Arrangements have been made with service companies for access to certain rooms. In addition, the building management department checks the incoming and outgoing goods (based on accompanying documents).

5.1.3 Power and Air Conditions

See section 5.1.1.

5.1.4 Water Exposures

See section 5.1.1.

5.1.5 Fire Prevention and Protection

See section 5.1.1.

5.1.6 Media storage

Storage media from systems used for PKIoverheid Certificates are handled safely within the building to protect them from unauthorized access, damage and theft. Storage media are meticulously removed when no longer needed.

5.1.7 Waste disposal

KPN has signed an agreement with a professional waste disposal company for the safe disposal of waste, used paper and the like. KPN's staff are obliged to dispose of all waste paper in the closed paper containers throughout the building.

5.1.8 Off-site backup

Media containing data and software are also stored in another KPN building, with as a minimum an equivalent level of security.

5.2 Procedural Controls

5.2.1 Trusted Roles

KPN has implemented a Trusted Employee Policy. Among other things, this policy describes the job categories and roles for which the status "trusted" is described. This mainly concerns positions involved in the management of certificates and key material, positions involved in system development, management and maintenance and positions in security management, quality management and auditing. See also 5.3.2. Background check procedures.

5.2.2 Number of persons required per task

Multiple employees are required to carry out certain pre-defined activities in the areas of key, certificate management, system development, maintenance and management. The need to have a certain activity with several people is enforced by means of technical facilities, authorisations in combination with identification/authentication and additional procedures.

5.2.3 Identification and authentication for each role

All employees are verified and authenticated, including face-to-face checks and identification checks based on government issued identity documents.

5.2.4 Roles requiring separation of duties

KPN uses a segregation of duties between executive, decisive and controlling tasks. In addition, there is also a segregation of functions between system management and operation of the systems used for PKIoverheid Certificates, as well as between Security Officer (s), System auditor (s), System administrator (s) and operator (s).

Security duties and responsibilities, including confidential functions, are documented in job descriptions. These have been drawn up based on the segregation of duties and powers and in which the sensitivity of the function has been established. Where applicable, a distinction has been made in the job descriptions between general functions and specific TSP functions.

Procedures have been drawn up and implemented for all confidential and administrative tasks that affect the provision of Certification Services.

Authorisation of the TSP staff takes place based on the need-to-know principle.

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

KPN deploys personnel with sufficient expertise, experience and qualifications to deliver PKIoverheid Certificates.

KPN has determined which knowledge and experience is required for each function to be fulfilled properly. This is maintained, because developments in the field of expertise follow one another quickly. In addition, each employee's knowledge and experience is registered.
A training plan is drawn up each year as part of the Planning & Control cycle and, once approved, the budget required to implement the plan is made available. The implementation of the plan is monitored and recorded. Where necessary, the training courses are made compulsory and, where possible, stimulated. Employees are also trained on the job. Employees are trained and trained as widely as possible, on the one hand to be able to use them as widely as possible and, on the other hand, to offer them as much variation in the range of tasks as possible.

The employees are followed by a Performance Management (PPM) cycle consisting of objectives interview, a functioning interview and an assessment interview.

5.3.2 Background check procedures

KPN has drawn up and implemented a Trusted Employee Policy for its certification services. In formulating and maintaining this policy, the possibilities and impossibilities of generally applicable legislation and regulations such as the Dutch Civil Code, the Wbp and the European eIDAS Regulation and (customer) specific legislation and regulations from, for example, De Nederlandse

Bank, the Pension and Insurance Chamber and the PKIoverheid have been carefully considered. This Policy describes in detail how, for example, a pre-employment screening (mandatory for those employees involved in the certification service provision), the issuing of a Statement of Conduct (VOG) pursuant to the Wji (also mandatory) and the conduct of security screening by services such as the General Intelligence and Security Service or the Military Intelligence and Security Service in order to obtain a Statement of No Objections (VGB). The policy also includes the options available to management if an employee or future employee does not wish to cooperate or if the outcome of the investigation is not positive.

Other provisions from the TEP are:

- Personnel who are not employed by KPN can under no circumstances perform any function or role with the status of "familiar" without direct supervision;
- A Trusted function/role may only be performed if the corresponding investigation has been completed, no objections have arisen and the employee has been formally appointed by management.
- Assessing the safety risks during employment is a responsibility of the direct supervisor as part of the PPM cycle.

5.3.3 Training requirements

All employees must complete an e-learning programme on security and legal compliance at the start of employment. Depending on the position, additional specific e-learning training modules are mandatory.

5.3.4 Retraining frequency and requirements

All employees are required to take regular e-learning awareness training. KPN maintains records of these training and monitors the timely attendance to ensure that employees maintain a skill level that enables them to perform.

5.3.5 Job rotation frequency and sequence

KPN does not use this method.

5.3.6 Sanctions for unauthorized actions

KPN has a disciplinary procedure. In the event of unauthorised employee actions, the procedure will be followed. Disciplinary action can result in termination of employment and/or legal action where applicable.

5.3.7 Independent contractor requirements

KPN employs contractors from preferred suppliers. Preferred suppliers are bound by the rules of KPN.

5.3.8 Documentation supplied to personnel

KPN employees are provided with a contract of employment, a defined job role and the KPN Company code. In addition, the Trusted Employees involved in the certificate service are provided with the specific security handbook.

5.4 Audit logging procedures

5.4.1 Types of events recorded

KPN maintains records for audit purposes of the following:

- Creation of accounts;
- Installation of new software or software updates;
- date and time and other descriptive information concerning backups;
- date and time of all hardware changes;
- Date and time of audit log dumps;
- Closing and (re)start of systems.

Logging takes place at a minimum:

- Routers, firewalls and network system components;
- Database activities and events;
- Transactions;
- Operating systems;
- Access control systems;
- Mail servers.

KPN keeps track of the following events manually or automatically

- Life cycle events with respect to the CA key, including:
  - generation of keys, backup, storage, recovery, archiving and destruction;
  - Cryptographic device life cycle events.
- Life cycle events regarding the management of certificates, including:
  - applications for certificates, issue and revocation;
  - successful or unsuccessful processing of applications;
  - generating and issuing Certificates and CRLs.
- Threats, including:
  - successful and unsuccessful attempts to gain access to the system
  - PKI and security activities undertaken by personnel;
  - reading, writing or deleting security-sensitive files or records;
  - Changes to the security profile;
  - system crashes, hardware failure, and other irregularities;
  - firewall and router activities;
  - Entering and leaving the space of the CA.

The log files contain at least the following data:

- source addresses (IP addresses if available);
- Target addresses (if available);
- Time and date;
- User IDs (if available);
- Name of the event;
- Description of the event.

5.4.2 Frequency of processing log

Monitoring procedures are in place to ensure the completeness and integrity of the audit log.

5.4.3 Retention period for audit log

The log files are retained for at least 24 months.
The consolidated (electronic) audit logs, as well as the manual registrations during the period of validity of the Certificate, are retained for a period of at least seven years from the date of expiry of the Certificate.

5.4.4 Protection of the audit Log

Events recorded electronically are recorded in audit logs. This is achieved through an appropriate combination of different types of security measures, including, inter alia, encryption and segregation of duties, protected against unauthorized inspection, alteration, deletion or other undesirable modifications.

Events recorded manually are recorded in files. These files are stored in fire-safe cabinets in a physically safe environment with appropriate access measures.

5.4.5 Audit log back up procedures

Incremental backups of audit logs are created daily, in an automated way, complete backups are created on a weekly basis and are also archived at a remote location.

5.4.6 Audit collection system (internal vs. external)

Actual log data is consolidated on a central log server for the PKI infrastructure.

5.4.7 Notification to event-causing subject

KPN does not notify people of their actions creating an event.

5.4.8 Vulnerability assessments

KPN performs an annual risk assessment to maintain the risk register. In case of significant changes, a risk assessment for the significant change is performed and if necessary, the risk register is updated. Countermeasures are taken and maintained on the basis of the risk assessment.

External and internal vulnerability scans are carried out monthly. Penetration tests are carried out at least annually. External penetration tests are also carried out by the Dutch Government agencies.

5.5 Records Archival

5.5.1 Types of records archived

KPN records all relevant registration information, including at least

- the certificate application form;
- the details of/over the identity document presented by the Certificate Holder or Certificate Administrator;
- the findings and decision on the application;
- the identity of the validation officer who processed or approved the Certificate Application;
- the method of validating identity documents and establishing identities;
- proof of identification and receipt.

5.5.2 Retention period for archive

KPN retains all relevant documentation and information relating to a Certificate during its term of validity and for a period of at least seven years from the date of expiry of the Certificate.

5.5.3 Protection of archive

KPN takes care of the archiving itself. It ensures the integrity and accessibility of the archived data during the retention period.
All equipment and software necessary for accessing the information shall be kept for the same period.
KPN ensures a careful and secure way of storage and archiving.

5.5.4 Archive back-up procedure

No stipulation.

5.5.5 Requirements for time-stamping of records

The precise date and time of relevant events in the life cycle of certificates and keys are recorded. This also applies to important events in the life cycle of the systems used for or supporting certification service delivery.

5.5.6 Archive collection system (internal or external)

The internal archive collection system is in the the data centre as described in section 5.1.1.

5.5.7 Procedures to obtain and verify archive information

Archive data access is strictly limited. Only specific authorised employees have access. KPN will further only release information from the archive upon a legal court order to do so.

5.6 Key Changeover

The keys of a CA Certificate are renewed at the same time as renewing that CA Certificate.
The old keys of the expired CA will be destructed. Old HSMs are destroyed after the end of their lifetime and - if applicable- the associated archiving period.

Keys of Certificate Holders shall not be reused after the expiry of the validity period or after revocation of the associated Certificates.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

KPN has implemented procedures to minimise the consequences of any disaster as much as possible. These measures include a contingency plan and a disaster recovery scenario.
KPN will inform the stakeholders immediately about the risks, dangers or events that can directly or indirectly threaten or influence the security of the services and/or the image of the PKIoverheid.

5.7.2 Computing resources, software, and/or data are corrupted

See section 5.7.3.

5.7.3 Entity private key compromise procedures

Compromise of KPN's Private Key is considered to be a disaster. KPN will inform Relying Parties, Subscribers, Certificate Holders and Certificate Managers as soon as possible of the compromise of KPN's Private Key by publishing information about this on its website (see Electronic Storage Site). KPN will also send an e-mail to Subscribers, Certificate Holders and Certificate Managers and inform the Government Policy Authority immediately.

5.7.4 Business continuity capabilities after a disaster

KPN has set up a complete fallback for its CRL and the online revocation facility. The back-up device is always fully identical to the production environment in terms of software and data and, for example, in the event of a disaster, it can be switched to the back-up device. This switchover is regularly tested. The alternate location is another KPN location (Almere) and has an equivalent level of security.

A contingency scenario was realised for the remaining parts of the CA system. This scenario provides for the realization of a contingency within 24 hours. This scenario is maintained and tested annually.

5.8 CA or RA termination

If KPN terminates the certification service delivery, this will be done in accordance with a controlled process as further described in the KPN CA Termination Plan. This termination may be voluntary or involuntary, and the activities to be carried out will depend on it.

Parts of the plan upon termination include the plan:

- Stop issuing new Certificates immediately;
- rewriting, supplementing and publishing the CPS;
- Maintain the revocation status service (CRL/OCSP) for up to 6 months after the expiry date of the last certificate issued has expired or has been terminated by revocation;
- Destroy or permanently deactivate all private keys used for the service provision in question and permanently destroy all private keys used for that purpose;
- termination and destruction of systems, procedures and non-relevant data;
- an inventory of the data to be retained, necessary in order to provide legal proof of certification;
- Realisation of provisions relating to the transfer of the obligations to other Trust Service Providers, insofar as this is reasonably possible.

KPN has taken out adequate insurance cover for all common business risks to cover the costs of operations under the CA Termination Plan. KPN has established a guarantee institution to cover these costs in the event of bankruptcy.

5.8.1 Involuntary termination

Involuntary termination may be due to the following:

- Bankruptcy;
- Wide loss of confidence in the service, for example due to a major security incident;

- Termination of Agentschap Telecom (AT) registration due to sanction following enforcement or change of legal entity.

Currently, there is limited willingness for TSPs registered with AT to take over (parts of) the certification service from TSPs who involuntarily terminate their TSP service. For this reason, the transfer will consist of the legally required limited service (6 months of CRL/OCSP publication and 7 years of archiving validation files) to another TSP registered with AT. This limited transfer will result in the revocation of all relevant end-user and CA certificates.

5.8.2 Voluntary Termination

In case of voluntary termination, the following activities will also be carried out:

- At least three months in advance, Subscribers, Certificate Holders and Certificate Managers shall be informed of the termination and the manner in which the termination will take place;
- Where reasonably possible, take measures to limit damage that may be caused to Subscribers and Certificate Holders as a result of the termination of the service.

6. Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

When generating CA key pairs, KPN uses reliable procedures that are performed within a secure environment that meets objective and internationally recognised standards.

The key generation of KPN CAs used for PKIoverheid Certificates has taken place in an EAL4+ certified HSM, in accordance with ISO 15408 (' Cryptographic module for CSP Signing Operations').
The SHA-1 root (domain Government/Businesses) is based on the signature algorithm' SHA1RSA'. Key pairs keys are 2048 bits asymmetric RSA and the used hashing algorithm is' SHA-1'.
and the SHA-2 root (domain organization) is based on the signature algorithm' SHA2RSA'. The keys of the key pairs are 4096 bits of asymmetric RSA and the used hashing algorithm is' SHA-2'.

The key generation for Personal Certificates and eSeal Certificates takes place in QSCDs. The key generation for Group Certificates takes place in SUDs. The SHA-2 root (domain organization) uses the signature algorithm' SHA256RSA'. The keys of the key pairs are 2048 bits or higher asymmetric RSA and the used hashing algorithm is' SHA-2'.’

For mobile Smartcard certificates, the key pair is not located on the Smartcard (QSCD), but on an HSM in a specially secured environment of a KPN Datacenter. The app on the certificate holder's phone guarantees that the certificate holder has sole control over the use of the electronic signature.

The Server Certificates must be generated by and under the responsibility of the Subscriber in a Secure Environment.
KPN monitors the QSCD certification status until the end of the certificate's validity period and will take appropriate action in the event of a change in this status, for example by the expiry of the certification validity period or the premature revocation of this certification.
As a first step, the KPN Policy Management Authority (PMA) will be informed of this status change and the PMA will implement any further measures based on the situation found at that time.

When handling and processing applications for a certificate KPN uses secure resources and trustworthy systems generating key pairs and certificates for End Users. These trustworthy systems are provided with a positive CEN TS 419 241 or CEN TS 419 261 audit report.

All Certificates, except for Server Certificates, are generated by a trustworthy system in an QSCD (for personal, professional and eSeal certificates) or SUD (for Group Certificates). Multiple Certificates can be stored on the QSCD and SUD.

6.1.2 Private key delivery to subscriber

Personal, Professional, Group or eSeal Certificates are transferred to the Certificate Holder in the following manner: sending the QSCD or SUD, including the Private Keys created by KPN via a commercial mail company, where the necessary PIN for the QSCD or SUD is issued separately to the Certificate Holder (' out of band'). The Certificate Holder signs for receipt of the QSCD or SUD before he/she is sent the PIN.

The key pair for which the Public Key is provided with a Server Certificate by KPN is generated by the Subscriber in the Subscriber's Safe Environment. The Private Key remains in that Safe Environment, so it is not transferred.

6.1.3 Public key delivery to certificate issuer

The key pairs of Personal, Professional and Group Certificates are generated by KPN and are therefore not transferred by the Subscriber to KPN.

The Subscriber does send the Public Key to KPN to have it provided with a Server Certificate. This Public Key is attached to an electronic application form and is linked to a unique Certificate Signing Request number (CSR number). The Public Key link to CSR number is used, after the Public Key has been provided with a Server Certificate, to return the Public Key provided with a Server Certificate by e-mail to the e-mail address mentioned in the Subscriber's Certificate Application request.

6.1.4 CA public key delivery to relying parties

KPN's Public Keys used for PKIoverheid Certificates are made available to Relying Parties via KPN's Directory Service (see Electronic Storage Site).

6.1.5 Key sizes

The key size of a Certificate is at least 1024 bits RSA. However, from 01-01-01-2011, only Certificates with 2048 bits are issued. The key size of a SHA-1 CA Certificate is 2048 bits RSA and of a SHA-2 CA Certificate is 4096 bits.

6.1.6 Public key parameters generation and quality checking

KPN has pre-issuance Regular Expression validation checks for most of the certificate request fields. In addition, KPN uses ZLint and RSA Key Validator to verify compliance to X.509 RFCs and ETSI standards.

The certificate issuance process will abort if any non-conformities to the requirements is detected.

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

The Certificates, including the associated key pairs, are only intended for the purposes described in this CPS and which are included in (the extensions of) the Certificate (field: Key Usage).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

In the development and use of cryptographic components, KPN ensures that these components meet all the requirements that can be set in terms of security, reliability, application range and mitigation of the susceptibility to interference. The applicable procedures may be assessed based on internationally recognised standards.

6.2.1 Cryptographic module standards and controls

For operational use, the cryptographic data is stored in an HSM. The HSM is EAL4+ certified.
The HSM that is used with the Mobile certificate has an FIPS 140-2 level 3 certification.

The HSMs are supplied by the supplier in tamper-evident bags, which are packaging that make any form of corruption visible. Each consignment shall be checked immediately after its arrival based on the corresponding list sent out-of-band.

KPN applies Key Management procedures to install, activate, backup and restore the Private Keys of KPN CAs, which sign (Services) Certificates and CRLs. These actions are performed simultaneously by at least two employees.

KPN CA Private Keys will be destroyed when this product is decommissioned.

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

The Private Keys associated with KPN's CA Certificates are in principle not readable in one piece. In addition, the cryptographic hardware modules on which they are stored are protected in such a way that multiple persons are required to access them, and they are stored in a secure environment. This Safe Environment is equipped with several layers of security measures of different type (technical, physical and organizational) and nature (preventive, detective, etc.). In order to be able to pass through the security layers, several employees of several departments are required.

6.2.3 Private key escrow

By default, there is no Escrow of Private Keys. If desired, a Subscriber can submit a request to Escrow for Private Keys of Confidentiality (encryption) Certificates and can make agreements about this.

If the Private Key of a Confidentiality Certificate is not taken in escrow, the loss, destruction or other unusability of the Private Key will result in the fact that the data previously encrypted with this certificate can no longer be decoded.

There is no possibility of Escrow of Private Keys related to Signature Certificates and Authentication Certificates.

6.2.4 Private key backup

A backup is made of the Private Keys associated with KPN's CA Certificates. The backup is stored in encrypted form in cryptographic modules and associated storage devices.

No backup will be made of the Private Keys associated with subject Certificates.

6.2.5 Private key archival

Private keys of Certificates are not archived.

6.2.6 Private key transfer into or from a cryptographic module

For the Private Keys belonging to KPN CA Certificates, which are stored in a cryptographic hardware module, access protection is used to ensure that the keys cannot be used outside the module. See 6.2.2.

6.2.7 Private key storage on cryptographic module

CA-Private Keys are stored encrypted in hardware cryptographic modules.

6.2.8 Method of activating private key

The Private Keys associated with KPN CA Certificates are activated by means of a key ceremony in the presence of the therefore necessary officers.

6.2.9 Method of deactivating private key

Under specific circumstances, KPN may determine that the Private Keys are deactivated, subject to the safeguards applicable to them for the sake of due care.

If an QSCD or SUD is lost by the Certificate Holder and returned to KPN by a finder, this QSCD or SUD will be destroyed by KPN, including the Private Key included therein. KPN will then also check whether the relevant Certificates have been revoked and if not, it will do so immediately.

In the case of the mobile certificate, the certificate holder will have to report the loss of his telephone to KPN on basis of which KPN will revoke the certificates.

6.2.10 Method of destroying private key

The Private Keys with which Certificates are signed can no longer be used after the end of their life cycle. KPN ensures adequate destruction, avoiding the possibility of tracing the destroyed keys from the remains. If such keys are destroyed, those activities will be logged.

6.2.11 Cryptographic Module Rating

For those certificates issued on smart cards, i.e. personal certificates, profession certificates and group certificates, the smart cards are certified by CWA 14169 at the EAL4+ level.

In the case of Server Certificates, use is made of the possibility offered by PKIoverheid to protect the keys of a Server Certificate by means of software. This means that the environment in which the keys are generated and stored must be as secure as if they were generated and stored in a SUD. That same level of security can be achieved by a combination of appropriate compensatory measures in and for that environment.

Compensatory measures must be of such a quality that it is practically impossible to steal or copy the keys unnoticed. Compensatory measures include a combination of physical access security, logical access security, logging and audit and separation of functions.

When applying for a Server Certificate, the Subscriber declares that the environment in which the keys are generated and stored is sufficiently secure, as described above.

The Special Terms and Conditions stipulate that KPN has the right to carry out an audit of the measures taken.

For mobile certificates, secure storage takes place by means of a secure device in the form of an HSM in the secure environment of a KPN data center, whereby the HSM is certified against FIPS 140.

6.3 Other aspects of Key Pair Management

All aspects of key pair management performed by KPN are subject to careful procedures that are consistent with the intended purpose.

6.3.1 Public key archival

Public Keys are archived by KPN for at least seven years after the original validity period of a Certificate has expired. Archiving will take place in a physically secure environment.

6.3.2 Certificate operational periods and key pair usage periods

Professional, Group and eSeal Certificates can be selected for a period of 3 or 5 years.

For Standard Server Certificates, the maximum validity period is 397 days.

For the mobile certificate, the maximum validity period is 1 year.

For the private services server certificate, the maximum validity period is 3 years.

KPN will inform the Subscriber of the expiry of the Certificates issued at his request at least 4 weeks before the expiry of the validity period.

6.4 Activation Data

6.4.1 Activation data generation and installation

The QSCD or SUD, in which the Key pair and its Certificate are stored, is provided with activation data. These PIN and PUK code are generated by a trustworthy system, consists of five characters and is printed on a PIN-mail. After acceptance of the PIN-mail, the system will destroy the PIN and PUK codes. In the time between generation and acceptance, the codes are encrypted by the trustworthy system.

6.4.2 Activation data protection

The PIN-mail, with the PIN and PUK code printed on it, is sent to the Certificate Holder/Certificate Manager only after the Certificate Holder/Certificate Manager has acknowledged receipt of the QSCD via a Link to KPN. Upon receipt of the PIN and PUK codes, the Certificate Holder/Certificate Manager shall be solely responsible for their protection and confidentiality.

6.4.3 Other aspects of activation data

In order to gain access to the Key Material and Certificate, the Certificate Holder must use the PIN code obtained, belonging to the QSCD or SUD. If the PIN code has been entered incorrectly three times (5 attempts for the mobile certificate), the QSCD or SUD is automatically blocked. In that case, the QSCD or SUD can only be unlocked with the PUK code.

If the PUK code is entered incorrectly three times, the QSCD or SUD will be permanently blocked and will therefore become unusable. For the mobile certificate this is 10 attempts. After that, the mobile certificate is definitively blocked.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

KPN appropriately safeguards the computer systems used for PKIoverheid Certificates against unauthorized access and other threats, including through multi-factor authentication.

The integrity of CSP systems and information is protected against viruses, malicious and unauthorized software and other possible sources that could lead to service disruption, by means of an appropriate set of physical, logical and organizational measures. These measures are preventive, detective, repressive and corrective in nature. Examples of measures include: logging, firewalls, intrusion detection and redundancy of systems, system components and network components.

The Directory Service is adequately protected against manipulation and is accessible online. Information about the revocation status can be consulted 24 hours a day and seven days a week.

6.5.2 Computer security rating

KPN classifies the resources used based on a risk assessment.

6.6 Life cycle technical controls

6.6.1 System development controls

KPN also develops, in part, its own Card Management System (CMS). Although the CMS is obtained from a specialist supplier, it consists of many different, small modules, which can be combined in different order and composition into a working CMS using a system supplied by the supplier. Several developers have been trained in this system, where necessary supported by the supplier.

In the management of the CMS, a separation of functions has been made between the development, user and management organization. This separation of functions has continued in the separate production, testing and development environments. The transition from development, to testing and production environment is managed using the existing change management procedure. This change management procedure includes maintaining and recording versions, changes and emergency repairs of all operational software.

The other CA systems are obtained from reliable suppliers and, like the CMS, are equipped with a CEN TS 419 261 audit report or equivalent.

KPN's systems use a trusted source of time.

The capacity utilization is tracked, and forecasts are made of the capacity required in the future to provide sufficient processing power and storage capacity in the future.

6.6.2 Security Management controls

Suppliers' software delivery is surrounded by control measures that can be used to determine the integrity and authenticity of the software. A measure used in addition to the measures mentioned in section 6.6.1 is the use of hashes.

6.6.3 Life cycle security controls

Change control procedures are in place for releases, modifications and emergency fixes of any operational software and hardware.

Based on the KPN security policy internal security procedures ensures that:

- security patches are applied within a reasonable time after they come available;
- security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them. The reason for not applying any security patch is documented.

6.7 Network Security Controls

KPN takes appropriate measures to ensure the stability, reliability and security of the network. This includes, for example, measures to regulate data traffic and to identify and prevent unwanted data traffic, as well as the installation of firewalls to ensure the integrity and exclusivity of the network. These measures are preventive, detective, repressive and corrective in nature. They also include the regular (at least monthly) security scan and (at least annually) a penetration test.

The network security measures conforms to the CA/Browser Forum Network Security Controls as well as the network security requirements from Regulation (EU) No. 910/2014, ETSI EN 319 411-1/411-2 and Program of Requirements PKIoverheid.

6.8 Time-stamping

No stipulation. KPN does not provide time-stamping services.

7. Certificate, CRL and OCSP profiles

7.1 Certificate profile

7.1.1 Version number(s)

The PKIoverheid Certificates are structured according to the PKI X.509 v3 standard. Signature certificates are structured according to the EESSI/ETSI Qualified Certificate Profile. Any extensions within this framework shall also be included in the other Certificates.

External and internal vulnerability scans are carried out monthly. Penetration tests are carried out at least annually. External penetration tests are also carried out by the Dutch Government agencies.

7.1.2 Certificate extensions

All certificates are configured per Baseline Requirements, Regulation (EU) No. 910/2014, ETSI EN 319 411-1/411-2 and/or Program of Requirements PKIoverheid. All other fields and extensions in the certificates are set in accordance with RFC 5280. See Appendix 3.

7.1.3 Algorithm object identifiers

KPN uses RSA encryption with SHA-2 algorithm and keys having the length at least of 2048 bits.

7.1.4 Name forms

Each Certificate includes a serial number that is unique to the Issuing CA and is output from a CSPRNG, greater than zero (0). The length of the SerialNumber is for the following products:

- Personal, Professional and Group Certificates
  - from 1-04-2016 64 bits
  - from 5-03-2019 96 bits
  - from 23-05-2019 160 bits
- eSeal Cerificates
  - 160 bits
- Server Certificates
  - 160 bits

7.1.5 Name constraints

All certificates are configured to meet the applicable requirements, including Baseline Requirements, Regulation (EU) No. 910/2014, ETSI EN 319 411-1/411-2 and Program of Requirements PKIoverheid.

7.1.6 Certificate policy object identifier

The applicable Certificate Policies can be identified through the following OIDs:

Personal, Professional, Group and eSeal Certificates:

Domein Organisatie Persoon (Domain Organization Person)	
2.16.528.1.1003.1.2.5.1	Authentication certificate
2.16.528.1.1003.1.2.5.2	Signing certificate

2.16.528.1.1003.1.2.5.3	Confidentiality certificate
Domein Organisatie Services (Domain Organization Services)	
2.16.528.1.1003.1.2.5.4	Authentication certificate
2.16.528.1.1003.1.2.5.5	Confidentiality certificate
2.16.528.1.1003.1.2.5.7	Certificate for electronic seal

Server certificates:

Domein Organisatie Services (Domain Organization Services)	
2.16.528.1.1003.1.2.5.9	Server certificate (under EV Root)

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

KPN issues certificates with a policy qualifier within the Certificate Policies extension. This extension contains a CPS pointer qualifier that points to the CPS.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL-profile

7.2.1 Version number(s)

KPN issues X.509 version 2 CRLs. The CRLs (or more recent status information) used for the PKIoverheid Certificates is structured in such a way that it can easily be the subject of validation processes.

KPN may adjust the CRLs layout and format, as well as the principle underlying the CRL, in accordance with the interests of the parties involved.

7.2.2 CRL and CRL entry extensions

See Appendix 3.

7.3 OCSP profile

7.3.1 Version number(s)

The OCSP Responder conforms to RFC 6960.

7.3.2 OCSP extensions

See Appendix 3.

8. Compliance Audit and Other Assessment

Since November 1, 2002, KPN B. V. (one of its predecessors) has been certified by KPMG Certification b. v. against the' TTP. NL Scheme for management system certification of Trust Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key Certificates, Website Certificates and / or Time-stamp tokens' against ETSI TS 101 456 and thus fulfilled the requirements of the dutch law for Electronic Signatures. The ETSI TS 101 456 Certificate was extended on the same date in the years 2005,2008,2011 and 2014 by the certification body BSI Management Systems.
Since 2014, KPN has also been certified against ETSI TS 102 042.
Among other things, the Scheme specifies the frequency with which the audit is carried out, the requirements that the certifying body must meet and how non-conformities are dealt with. A certifying body must be accredited by the Accreditation Board before it can certify.

eIDAS
On July 1, 2016, the European Regulation (REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC) entered into force.
This decree replaces the Dutch Electronic Signature Act.
Because this regulation sets out the requirements regarding the frequency of the audit and accreditation, the afore mentioned TTP. NL Scheme lapses on that date.

In February 2016, the previous ETSI certifications ETSI TS 101 456 and ETSI TS 102 042 were also replaced by ETSI certifications ETSI EN 319 411-2 and ETSI EN 319 411-1 respectively.
KPN also complies with the relevant parts of PKIoverheid Programme of Requirements as stated in the Programme of Requirements (see https://www.logius.nl/english/pkioverheid). This is demonstrated by means of an audit report issued by BSI Group The Netherlands. A copy of the ETSI EN 319 411-2 and ETSI EN 319 411-1 certificate can be found on the KPN site (see Electronic Storage Site).

With effect from 10 March 2017, the Netherlands Radiocommunications Agency (hereinafter AT) has been designated as statutory supervisor of the eIDAS ordinance.
KPN is registered as a Qualified Trust Service Provider (QTSP) by the Netherlands Radiocommunications Agency.

8.1 Frequency or circumstances of assessment

As a qualified Trust Service Provider in The Netherlands, KPN is annually audited to assess compliance with ETSI EN 319411-1, ETSI EN 319411-2/eIDAS, CA/Browser Forum – Baseline Requirements, CA/Browser Forum - Network and Certificate System Security Requirements, Program of Requirements PKIoverheid, ISO 9001, ISO 22301, ISO 27001 and national law & regulations.

8.2 Identity/qualifications of assessor

KPN is annually audited by DNV GL Business Assurance B.V for the ISO certifications and by BSI Group The Netherlands for the ETSI certifications and related requirements.

8.3 Assessor's relationship to assessed entity

External auditors are independent and have no business interests in KPN. No external auditor has any business affiliation with KPN.

8.4 Topics covered by assessment

The scope of the audit covers all requirements from the standards for the Trust Service Provider component services:

- Registration Service
- Certificate Generation Service
- Dissemination Service
- Revocation Management Service
- Revocation Status Service
- Subject Device Provision Service

with subjects as:

- Organisation and Compliance
- Risk assessment
- Policies, Practices, Terms and Conditions
- Key Management and Cryptographic Controls
- Trustworthy Systems and Device Certifications
- Logical Access Control
- Network and System Security
- Logging and Monitoring
- Asset management, Change Management, Incident management
- Human Resource Security
- Physical Security
- Business Continuity and TSP Termination

8.5 Actions taken as a result of deficiency

In case of a deficiency, KPN addresses this nonconformity in a Corrective Action Plan (CAP) in accordance with the Trust Service Provider Conformity Assessment requirements ETSI EN 319 403. In the CAP the actions and planning are documented to resolve the nonconformity.

9. Other Business and Legal Matters

KPN is the ultimately responsible Trust Service Provider. KPN is also responsible for those parts that are outsourced to other organizations. See section 1.3.5

9.1 Fees

9.1.1 Certificate issuance or renewal fees

All fees are published on the KPN website: https://certificaat.kpn.com/pkioverheidcertificaten/tarieven/

9.1.2 Certificate access fees

There are no certificate access fees.

9.1.3 Revocation or status information access fees

There are no revocation or status information access fees.

9.1.4 Fees for other services

See section 9.1.1.

9.1.5 Refund policy

KPN does not have a refund policy.

9.2 Financial Responsibility

9.2.1 Insurance coverage

KPN has put in place adequate arrangements, including insurance, to cover liabilities related to the provision of the service in question. In addition, KPN has the financial stability and resources necessary for sound business operations.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of Business Information

The financial statements of KPN B.V. are integrated in the financial statements of Koninklijke KPN N.V. As a publicly listed company, it is the Royal KPN N.V. not allowed to provide financial data outside the regular reports and official channels.

9.3.1 Scope of confidential information

The following shall be regarded as confidential, inter alia:

- agreements with, inter alia, Subscriber' s;
- Internal procedures for handling and processing Subscription, Certificate applications and revocation requests;
- data on systems and infrastructures;
- PIN, PUK and revocation codes;
- Internal security procedures and measures;
- audit reports;
- Private keys.

For personal data, see section 9.4.2.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

KPN has formulated a policy for all information relating to security issues (see, for example, 9.3.1.). This policy states, among other things, that this information is confidential and is only made available based on the need-to-know principle. This also means that, in principle, this information is only made available for inspection to third parties within the KPN building, but only to the extent that there is a clear need for this (for example an audit) and always under strict confidentiality.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

KPN complies to the applicable local privacy laws and regulations including the Council Directive 95/46/EC of the European Parliament. KPN undergoes regular internal and external audits to verify its privacy compliance.

KPN has formulated a privacy statement for, among other things, its certification services. The statement describes how KPN deals with personal data. The privacy statement is made available via KPN's website (see Repository).

9.4.2 Information treated as private

The following personal data are considered confidential and will not be provided to third parties:

- Subscriber details;
- certificate application details and certificate application treatment details;

- certificate application processing data;
- certificate revocation details;
- notifications of circumstances which may lead to revocation.

KPN will provide the Subscriber and/or Certificate Manager or Certificate Holder with the personal data concerning him/her, upon request. Upon request, KPN provides the Subscriber with personal data of a Certificate Manager or Certificate Holder who has received a Certificate on behalf of the Subscriber.

9.4.3 Information not deemed private

The published data of certificates is publicly available. The information that is made available in respect of published and revoked certificates is limited to the limits set out in Chapter 7 ' Certificate, CRL and OCSP profiles' of this CPS.

Information on revocation of certificates is available through the CRL. This information provided only concerns the certificate number, the moment of revocation and status (valid/revoked) of the certificate.

9.4.4 Responsibility to protect private information

KPN will not publish, disclose or otherwise make personal data available for unauthorised view/use. KPN has implemented appropriate technical and organizational security measures to protect personal data.

9.4.5 Notice and consent to use private information

The Certificate Holder, the Certificate Manager and Subscriber grant permission for publication of certificate data by consent to the General Conditions KPN and Special Terms and Conditions PKIoverheid. The completion of an application procedure by the Certificate Holder is considered by KPN as permission for the publication of the data in the Certificate.

9.4.6 Disclosure pursuant to judicial or administrative process

KPN does not provide confidential data to investigating officers, except insofar as Dutch legislation and regulations require KPN to do so and only upon presentation of a legally valid summons.

The Certificate and the information supplied with the Certificate Application shall continue to be stored for a further period specified to the Subscriber and/or Certificate Holder and insofar as necessary to provide proof of certification in the legal process. Confidential data will only be provided to parties other than the Subscriber and the Certificate Holder for the purpose of evidence, with the prior written consent of the Subscriber or the Certificate Holder.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

All information regarding conditions pertaining to intellectual property rights can be found in the General Conditions KPN and Special Terms and Conditions PKIoverheid.

9.6 Representations and warranties

9.6.1 CA representations and warranties

KPN declares that:

- KPN has followed the procedures in this CPS at the time of certificate issuance
- KPN maintains a 24 x 7 publicly accessible repository available for checking certificate status.
- KPN will revoke a certificate for reasons as described in this CPS.

9.6.2 RA representations and warranties

KPN operate the RA functions. For representations and warranties see section 9.6.1.

9.6.3 Subscriber representations and warranties

In the General Conditions KPN and Special Terms and Conditions PKIoverheid certificates, the manner in which KPN and the parties involved must deal with obligations and guarantees is set out.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

KPN provides no warranties concerning certificates other than the warranties which have been explicitly provided under 9.6.1 above. Any implied warranties, including merchantability and fitness for a particular purpose, are explicitly disclaimed to the extent permitted under applicable law.

9.8 Limitations of Liability

KPN accepts liability for PKIoverheid Certificates as set out in the General Conditions KPN and Special Terms and Conditions PKIoverheid certificates.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments to this CPS are effective when published in the Repository and remain in effect until replaced with a newer version.
This CPS applies for as long as any certificate issued by KPN under this CPS remains valid.

9.10.2 Termination

This CPS will remain applicable to the KPN PKIoverheid certificate services if services are still offered by KPN. If KPN cease to issue PKIoverheid certificates this document will cease to be relevant.

9.10.3 Effect of termination and survival

The provisions within this CPS terminate in the event of termination by KPN of its provision of PKIoverheid certificates.

9.11 Individual notices and communications with participants

KPN communicates with stakeholders in various ways. This is done verbally (telephone), mainly through the employees of the Validation department who, among other things, process and handle the Certificate applications. This department can be reached by calling +31 (0)88 661 05 00.

Communication also takes place via this CPS and for example the certificate application forms used, all of which are accompanied by a detailed explanation. There is also the possibility of raising questions or other matters via e-mail address pkivalidation@kpn.com

The listed documents and many other information are available in the Electronic Storage.

9.12 Amendments

9.12.1 Procedure for amendment

KPN has the right to amend or supplement the CPS. The operation of the current CPS is assessed at least annually by KPN's PMA. Subscribers, Certificate Holders, Certificate Managers and Relying Parties may comment on the content of the CPS and submit it to KPN's PMA, see section 1.5.2. If, based on this, it is determined that changes to the CPS are necessary, the PMA will implement these changes in accordance with the change management process set up for this purpose.

Amendments to the CPS are approved by KPN's PMA. Changes of an editorial nature or obvious clerical and/or spelling errors can enter into force without prior notice and are recognizable by increasing the version number by 0.1 (1.1 > 1.2). In the event of major changes, a new version will be produced, recognizable by increasing the version number by 1 (1.0 > 2.0).

9.12.2 Notification mechanism and period

Amendments to the CPS are announced on KPN's website (see Electronic Storage Recordings). This is done two weeks before the CPS's starting date of validity. This starting date of validity is stated on the cover page of this CPS.

9.12.3 Circumstances under which OID must be changed

OIDs used within PKIoverheid certificates are determined by the PKIoverheid Policy Authority. KPN does not control the circumstances for those changes.

9.13 Dispute Resolution Procedures

Complaints are dealt with by means of a Complaint procedure. These complaints can be reported by telephone and by e-mail to the Service Desk. A web form is available on the website for this purpose, which can be used to submit a complaint, among other things.
https://certificaat.kpn.com/contactformulier/

Telephone: 088-6610621 (working days from 9:00 to 17:00
E-mail: pkio.servicedesk@kpn.com

KPN makes every effort to provide you with the best possible service. However, it is possible that you are not satisfied with our services. In that case, there is a possibility to appeal about the handling of your complaint. You can reach this procedure via : https://www.kpn.com/zakelijk/service/klacht-indienen-over-kpn-zakelijk.htm

9.14 Governing Law

The eIDAS regulation governs KPN's certification services within the PKIoverheid, insofar as it concerns the Qualified Certificates (non-repudiation).

KPN's services are also governed exclusively by Dutch law.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

Appendix 1 Definitions

Advanced Electronic Signature: an Electronic Signature that meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it makes it possible to identify the signatory;
(c) it is established by means which the signatory can maintain under his sole control;
(d) it shall be linked to the electronic file to which it relates in such a way that any subsequent alteration of the data can be detected.

Applicant: a natural person (Recognized Profession Certificates) or legal entity (Organisation-linked Certificates) who submits a Certificate Application for the issuance of a Certificate to KPN. The Applicant does not have to be the same party as the Subscriber or the Certificate Holder, but is one of both.

Asymmetric Key Pair: a Public Key and Private Key within the public key cryptography that are mathematically connected in such a way that the Public Key and the Private Key are each other's counterparts. If one key is used to encrypt, the other key must be used to decrypt and vice versa.

Authentication: (1) Checking an identity prior to transmission of information; (2) verifying the accuracy of a message or sender.

Authenticity certificate: Certificate certifying the Public Key of the key pair used for identification and authentication services.

Authorised representative: A natural person authorised to represent an organisation. The power of representation may derive from the law or from a power of attorney. There may also be several natural persons, e. g. a board of an association, who are authorised to represent an organisation.

CA Certificate: a Certificate of a Certification Authority.

CA Key: the key pair, Private and Public Key of a Certification Authority.

Certificate: the Public Key of an End User, together with additional information. A Certificate is enciphered with the Private Key of the Certification Authority that issued the Public Key, making the Certificate unalterable.
Certificates can be grouped in different ways. Firstly, there is the distinction between Organizational Certificates and Profession Certificates. Certificates for Organisation-linked Certificates are requested by an organisational entity, which is a Subscriber at KPN, for a Certificate Holder who is part of or has a relationship with that organisational entity. The Certificate Holder shall use the Certificate on behalf of the organisation.
For Profession Certificates, they are applied for by a practitioner of a Recognised Appeal, who in that capacity is a Subscriber himself or herself, but at the same time also a Certificate Holder. The Certificate Holder shall use the Certificate on account of his profession.
The Organisation-specific Certificates are subdivided into Personal Certificates and Services Certificates. The Services Certificates can in turn be divided into Group and Server Certificates.

Certificate Application: the request submitted by an Applicant for the issue of a Certificate by KPN.

Certificate Administrator: (Certificate Manager) a natural person who is authorized to apply for, install, manage and/or revoke a Server Certificate or Group Certificate on behalf of the Subscriber and for the benefit of the Certificate Holder. The certificate administrator carries out actions that the certificate holder himself is not capable of doing.

Certificate Holder: an entity that is identified in a Certificate as the holder of the Private Key belonging to the Public Key given in the Certificate.
In principle, there are two types of Certificate Holders: the organisation-specific Certificate Holder and the professionally related Certificate Holder. The organisation-specific Certificate Holder is part of an organisational entity in which the organisational entity is the Subscriber who applies for Certificates for the Certificate Holder and in which the Certificate Holder may use these Certificates on behalf of the Subscriber. The profession certificate holder is a practitioner of a recognized profession, who in that capacity becomes a Subscriber at KPN and applies for Certificates for himself. In the case of the profession Certificates, the Subscriber is the Certificate Holder, the Subscriber and the Certificate Holder are the same person.

Certificate Profile: a description of the content of a Certificate. Each type of Certificate (signature, confidentiality, etc.) has its own interpretation and thus its own description - in which there are, for example, agreements on naming and the like.

Certificate Policy (CP): a named set of rules indicating the applicability of a Certificate for a particular community and/or application class with common security requirements. Using a CP, Subscribers and Relying Parties can determine how much confidence they can place in the relationship between the Public Key and the identity of the Public Key holder. The applicable CP’s are included in the PKIoverheid Programme of Requirements (PoR). This concerns the part 3a Certificate Policy - Domain Government/Businesses and Organisation and the part 3b Certificate Policy - Services, appendix to CP Domain Government/Businesses and Organisation.

Certificate Revocation List: (CRL): a publicly accessible and consultable list of revoked Certificates, signed and made available by the issuing TSP

Certification Authority (CA): an organisation that generates and revokes Certificates. The functioning as CA is a partial activity carried out under the responsibility of the TSP. In this respect, KPN therefore both operates as a CA and a TSP (CSP)

Certification services: the issuing, management and revocation of Certificates by Trust Service Providers.

Certification Practice Statement (CPS): a document describing the procedures followed and measures taken by a CSP in relation to all aspects of the service provision. The CPS describes how the CSP(TSP) meets the requirements as stated in the applicable CP.

Certification Practice Statement PKIoverheid (CPS PKIoverheid: the CPS in question, as applicable to the issue by KPN of PKIoverheid Certificates and their use.

Certification Service Provider: a natural or legal person whose function is to provide and manage Certificates and key information, including the associated media (QSCD, SUD). The Certification Service Provider also has the final responsibility for providing the Certification Services, whether it carries out the actual activities itself or subcontracts them to others.

Confidentiality certificate: Certificate certifying the Public Key of the key pair used for confidentiality services.

Country code TopLevelDomain (ccTLD) code
The ccTLD (country code Top Level Domain) is the domain name extension for a country or independent territory. A ccTLD consists of the 2-letter country code defined according to the ISO 3166-1 standard. For instance: .nl .be .de.

Data for the creation of Electronic Signatures: see Signature Creation Data.

Data for verifying an Electronic Signature: see Signature Verification Data.

Digital Signature: see Advanced Electronic Signature.

Directory Service: a service from (or with the cooperation of) a CSP that makes Certificates issued by the CA available and accessible online for the benefit of consulting or trusting parties.

End User: a natural or legal person who performs one or more of the following roles within the PKIoverheid: Subscriber, Certificate Holder or Relying Party. In view of the limited distinctive character of this term, it is not used in the CPS, except in so far as it concerns the prescribed structure of the document (i.e. headings, etc.).

Electronic Signature: electronic data that are attached to or logically associated with other electronic data and are used as a means of authentication. The Electronic Signature is used to ensure that electronic correspondence and transactions can compete on two important points with the time-honoured "signature on paper". By placing an Electronic Signature, it is certain that someone who claims to have signed a document has actually done so.

Electronic Storage: location where relevant information regarding KPN's services can be found. See: https://certificaat.kpn.com/elektronische-opslagplaats/.

Escrow (Key-Escrow): A method to generate a copy of the Private Key for the purpose of access to encrypted data by authorised parties during the issuance of a Certificate and its secure storage.

Fully Qualified Domain Name (FQDN)
A Fully Qualified Domain Name (FQDN) as defined by PKIoverheid is a full name registered in the Internet Domain Name System (DNS) with which a server on the Internet is unique to identify and address. With this definition, an FQDN includes all DNS nodes up to and including the name of the relevant Top-Level Domain (TLD) and an FQDN is registered in the Internet DNS under a DNS Resource Record (RR) of type' IN A' and/or' IN AAAA' and/or' IN CNAME'.

Examples of FQDNs are
www.logius.nl
webmail. com. nl
local. logius. nl
server1. local. local. logius. nl
Logius. nl (subject to registration under a DNS RR of type' IN A' and/or' IN AAAA' and/or' IN CNAME').

Generic TopLevelDomain (gTLD):The gTLD is a generic top-level domain (generic Top Level Domain), a domain name extension that does not belong to a particular country and that can be registered in principle by anyone anywhere in the world.

Government: Within the context of PKIoverheid, government is/are considered to be government or government organisations:

- all of the national government, the provinces, the municipalities, the partnerships based on the Act on Common Regulations and the Water Boards;
- implementing organisations and services such as inspections, benefits and expenditure services and police services;
- Judiciary;
- independent administrative bodies as listed in the ZBO register

GovernmentCA: a CA that is the RootCA within the hierarchy of PKIoverheid. In a technical sense, it is the central point of trust within the hierarchy and is controlled by the Government Policy Authority.

Government Identification Number (dutch: OverheidsIdentificatieNr OIN): Identification number from the Digikoppeling Service Register. This is a register for government organisations. If governmental organizations want to participate in Digikoppeling, a government facility for improving electronic communication between governmental organizations, they must, when applying for a Server Certificate, prove their existence with an extract from the Digikoppeling Service Register and the OIN is included in their Server Certificate.

Government Policy Authority: the highest policy-making authority within the hierarchy of PKIoverheid that controls the Government-CCA.

Group Certificate: a combination of two Non-Qualified Certificates, stored on a SUD, which together support the functions of confidentiality and authenticity and fulfil the following requirements:
(a) they have been spent on a service or function, forming part of the Subscriber (organisational entity); and
(b) they have been issued on the basis of the Certificate Policy Services in force within PKIoverheid (PoR Part 3b)

Hardware Security Module: The peripherals used on the server side to accelerate cryptographic processes. The creation of keys should be considered in particular.

KPN Special Terms and Conditions PKIoverheid Certificates: the Special Terms and Conditions, which, in addition to the General Conditions KPN, apply to all parties involved in the issue and use of PKIoverheid Certificates.

Mobile Certificate: The means by which KPN provides an eIDAS qualified signature certificate and an authentication certificate that is under "sole control" of the certificate holder using his mobile phone. The key material is securely stored on systems managed by KPN in a secure environment. As a result, the certificate holder no longer needs a Smartcard or USB token to sign documents with a qualified signature, but a mobile phone with an activated Mobile certificate and an application that is connected to the corresponding signing service.

Non-qualified Certificate: a Certificate that does not meet the requirements for a Qualified Certificate.

Object Identifier (OID): A sequence of numbers that uniquely and permanently identifies an object.

Online Certificate Status Protocol (OCSP): a method to check the validity of Certificates online (and in real time). This method may be used as an alternative to consulting the CRL.

Organization-specific certificates
There are two different types of organisational certificates:
1. for persons;
2. for services.

Ad. 1
In the case of organisation-specific certificates for persons, the certificate holder is part of an organisational entity. The certificate holder has the power to make a particular transaction on behalf of that organisational entity.

Ad. 2
In the case of organisation-specific certificates for services, the certificate holder is :

- an apparatus or a system (non-natural person), operated by or on behalf of an organisational entity; or
- a function of an organisational entity.

Personal certificates:
The certificate holder will be a natural person in the case of personal certificates. The certificate holder is either part of an organisational entity for which a subscriber is the contracting party (organisational certificate holder), or the person practising a recognised profession and in that capacity itself a subscriber and thus the contracting party (profession certificate holder) or a citizen and, in that capacity, a subscriber and thus the contracting party.

PKIoverheid, the Public Key Infrastructure of the State of the Netherlands (also known as PKIoverheid): a system of agreements that allows generic and large-scale use of the Electronic Signature, and also facilitates remote and remote identification.
Confidential communication. The arrangement system is owned by the Minister of the Interior and Kingdom Relations and is managed by the Policy Authority PKIoverheid.

PKIoverheid Certificate: a Certificate issued by KPN under the PKIoverheid certificate.

Policy Management Authority: the organisational entity within KPN responsible for developing, maintaining and formally establishing service-related documents, including the CPS.

Private IP address: An Internet Protocol address (IP address) is an identification number assigned to each device (e. g. computer, printer) participating in a computer network that uses the Internet Protocol (TCP/IP) for communication purposes.
Private IP addresses are not routable on the internet and are reserved for private networks. The IPv4's IPv4 address range reserved or kept available for private use is (see RFC 1918):

- 10.0.0.0 – 10.255.255.255;
- 172.16.0.0 – 172.31.255.255;
- 192.168.0.0 – 192.168.255.255;

In addition, the 169.254.0.0.0 -169.254.255.255.255 series is reserved for Automatic Private IP Addressing (APIPA). These IP addresses may not be used on the Internet.

The IPv6 is the IP address range reserved or kept available for private use (see RFC 4193):
fc00: /7

In addition, the series of fe80: /10 is reserved for Automatic Private IP Addressing (APIPA). These IP addresses may not be used on the Internet.

Private Key: the key of an asymmetric key pair that should only be known to its holder and kept strictly secret. Within the framework of the PKIoverheid, the Private Key is used by the Certificate Holder to identify himself electronically, to place his Electronic Signature or to decipher an encrypted message.

Profession Certificate: a combination of two Non-Qualified Certificates stored on an QSCD, which together support the functions of authenticity and confidentiality, as well as a Qualified Certificate that supports the function of non-repudiation, and which are issued exclusively to a practitioner of a Recognised Profession.

The Certificates shall comply with the following requirements:

a. they have been issued to a natural person, who uses the Certificate or is going to use it for his or her profession; and
b. they have been issued on the basis of the Certificate Policy Domain of Government/Businesses and Organisation Certificate (PoR Part 3a) applicable within PKIoverheid.

Public IP address: Public IP addresses are unique worldwide and can be routable, visible and accessible from the Internet.

Public Key Infrastructure (PKI): the organisation, procedures and technology required to issue, use and manage Certificates.

Public Key: the key of an asymmetric key pair that can become public
published. The Public Key is used to check the identity of the owner of the asymmetric key pair, to check the Electronic Signature of the owner of the asymmetric key pair and to encrypt information for a third party.

Qualified Certificate: A Certificate that meets the requirements set out in REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT (eIDAS) and has been issued by a Trust Service Provider that meets the requirements set out in this Regulation. The Certificate must also apply to the application of the Qualified Electronic Signature.

Qualified Certificate for Electronic Signature: an Electronic Signature that meets the following requirements:

a. it is uniquely linked to the signatory;
b. it makes it possible to identify the signatory;
c. it is established by means which the signatory can maintain under his sole control;
d. it shall be linked to the electronic file to which it relates in such a way that any subsequent alteration of the data can be detected;
e. it is based on a Qualified Certificate as referred to in REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT (eIDAS);
f. it has been generated by a secure means for the creation of Electronic Signatures as referred to in REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT (eIDAS).

Qualified Certificate for electronic Seal (eSeal): means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal, and meets the requirements of REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT (eIDAS).

Qualified Signature Creation Device (QSCD): a means for the creation of Electronic Signatures that meets the requirements of REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT (eIDAS). An QSCD is used for personal and profession certificates. An QSCD can be a smart card or a USB token, for example.

Recognised profession: Profession certificate holders must exercise a recognised profession in order to apply for Certificates within PKIoverheid. In this context, a recognised profession is a profession which is mentioned in the program of PKIoverheid requirements as a Recognised profession.

Relying Party: the natural or legal person who is the recipient of a Certificate and who acts in confidence in that Certificate.

Root: the central part of a (PKI) hierarchy from which the entire hierarchy and its level of reliability are displayed.

Root certificate: the Root-CA Certificate. This is the Certificate belonging to the place where trust in all Certificates issued within PKIoverheid originates. There is no higher CA from which confidence is derived. This Certificate is signed by the Certificate Holder (within PKIoverheid this is the GovernmentCA) itself. All underlying Certificates are issued by the holder of the Stam Certificate.

Root Certification Authority (Root-CA): a CA which is the centre of common trust in a PKI hierarchy. The Certificate of the Root-CA (the Root-CA (the Root Certificate of Stam Certificate) is self-signed, as a result of which it is not possible to authenticate the source of the signature on this Certificate, only the integrity of the content of the Certificate. However, the Root-CA is trusted based on, for example, CP and other documents. The Root-CA does not necessarily have to be positioned at the top of a hierarchy.

Secure User Device (SUD): a means that contains the users private key (s), protects this key (s) from compromise and performs authentication or decryption on behalf of the user. A QSCD is used for service certificates. Also, a QSCD can be a smart card or a USB token.

A smart card or USB token is called QSCD if it can be used to create electronic signatures, i. e. if it carries qualified certificates. If a smart card or USB token service contains certificates, it is called a SUD.

Server Certificate: A Non-qualified Certificate stored within the Subscriber's Secure Environment that supports the functions of authenticity and confidentiality and meets the following requirements:

a. it has been issued to a server, being part of the Subscriber (organisational entity); and
b. it has been issued based on the Certificate Policy Services in force within PKIoverheid (PoR Part 3b).

Services Certificate: A certificate that links a function or device, such as a server, to a legal entity or other organisation. A Services Certificate can be a Server Certificate, if a device is linked to an organization, or a Group Certificate, if a function is linked to an organization.

Secure Means of Creating Electronic Signatures: see Secure Signature Creation Device.

Secure Environment: The environment of the system that contains server certificate keys. Within this environment it is permitted to protect the keys in software, rather than in a SUD. Compensatory measures for this must be of such a quality that it is practically impossible to steal or copy the keys unnoticed. Compensatory measures include a combination of physical access security, logical access security, logging, audit and separation of functions.

Signature Creation Data: unique data, such as codes or private cryptographic keys, used by the signatory to create an Electronic Signature.

Signature Creation Device: configured software or hardware used to implement the data for the creation of Electronic Signatures.

Signature creation tool: see Signature Creation Device.

Signature Verification Data: data, such as codes or cryptographic Public Keys, used to verify an Electronic Signature.

Subscriber: the natural person (Recognized Profession Certificates or legal entity (Organisation related Certificates) who enters into an agreement with KPN to effectuate the issue of PKIoverheid Certificates to Certificates to Certificates Holders designated by the Subscriber.

Trust service provider (TSP): Provider of trust services. Since the European Regulation eIDAS the common name for CSP.
see Certification Service Provider.

Non-repudiation: the property of a message to demonstrate that certain events or actions have taken place, such as sending and receiving electronic documents.

X. 509: an ISO standard that defines a basis for the electronic format of Certificates.

Appendix 2 Abbreviations

Abbreviation	Meaning
AT	Agentschap Telecom (supervisory body for eIDAS in the Netherlands)
CA	Certificatie Autoriteit (Certification Authority)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificates Revocation Lijst
EESSI	European Electronic Signature Standardization Initiative
eSeal	Qualified Certificates for electronic Seals
ETSI	European Telecommunication Standardisation Institute
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Personal Unlock Code number (Dutch: Kengetal)
PoR	PKIoverheid Program of Requiremenst (Dutch: Programma van Eisen)
RA	Registration Authority
QSCD	Qualified Signature Creation Device
SUD	Secure User Device
TSP	Trust Service Provider
Wid	Wet op de identificatieplicht (Dutch Identification Act)

Appendix 3 Certificate, CRL and OCSP profiles

3.1 Certificates profiles

3.1.1 Personal certificates and Profession Certificates

Basic attributes

Field	Value
Version	2 (X.509v3)
SerialNumber	Unique serial number within the CA
Signature	The used algorithm under the SHA-1 root (domain Government /Companies) is sha1WithRSAEncryption. The used algorithm under the SHA-2 root (domain Organization) sha256WithRSAEncryption.
Issuer	Contains the name of the CA concerned and is represented by the following attributes: CommonName, OrganizationName en CountryName. There have been / are several CA certificates in use. • CA-Certificate with OrganizationName 'PinkRoccade Infrastructure Services BV'. The CommonName contains 'PinkRoccade CSP - Overheid – 'and the designation 'Onweerlegbaarheid CA' of 'Vertrouwelijkheid CA' of 'Authenticiteit CA', depending on the type of certificaat. The CountryName is 'NL'. • CA-Certificate with OrganizationName 'Getronics PinkRoccade Nederland B.V.'. The CommonName contains 'Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie'. The CountryName is 'NL'. • CA-Certificate with OrganizationName 'Getronics Nederland BV'. De CommonName contains 'Getronics CSP Organisatie CA – G2. the CountryName is 'NL'. • CA-certificate with OrganizationName 'KPN Corporate Market B.V.', the Common name contains 'KPN Corporate Market CSP Organisatie CA - G2'. The CountryName is 'NL'; • CA-certificate with OrganizationName 'KPN Corporate Market B.V.', the Common name contains 'KPN Corporate Market PKIoverheid CA-Overheid en Bedrijven' The CountryName is 'NL'. • CA-certificate with OrganizationName 'KPN B.V.', the Common name contains 'KPN PKIoverheid CA-Overheid en Bedrijven' The CountryName is 'NL'. • CA-certificate with OrganizationName 'KPN B.V.', the Common name contains 'KPN BV PKIOverheid Organisatie Persoon CA - G3' with organizationIdentifier = NTRNL-27124701' and CountryName 'NL'
Validity	see 6.3.2.
Subject	The subject's name is displayed as a Distinguished Name (DN), and is represented by at least the following attributes: • CountryName; • CommonName; • OrganizationName; • Title • SerialNumber (subjectSerialnumber). The attributes used to describe the subject name it in a unique way.

	The CountryName attribute is set to a two-letter country code according to ISO 3166. The Title attribute shall only be filled with the Recognised Profession title of the Certificate Holder if a Profession Certificate has been applied for.
subjectPublicKeyInfo	Contains the PublicKey of the Subject

Standard extensions

Field	Critical	Value
AuthorityKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash
SubjectKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash
KeyUsage	Yes	The digital signature bit is included in Authenticity Certificates. The keyEncipherment, dataEncipherment and keyAgreement bits are included in Confidentiality Certificates. In Signing Certificates, the non-Repudiation bit is included.
BasicConstraints	Yes	The CA bit is set to ‘False’ en pathLenConstraint to ‘none’
CertificatePolicies	No	Domain Government/Companies Authhentication certificates contain the OID 2.16.528.1.1003.1.2.2.1. Signing certificates contain the OID 2.16.528.1.1003.1.2.2.2. Confidentiality Certificates contain the OID 2.16.528.1.1003.1.2.2.3. Domain Organization Authhentication certificates contain the OID 2.16.528.1.1003.1.2.5.1. Signing certificates contain the OID 2.16.528.1.1003.1.2.5.2. Confidentiality Certificates contain the OID 2.16.528.1.1003.1.2.5.3. All types of Certificates contain a link to the CPS and a user text. The user memo contains a message that in case the <job_title> field is filled with a Recognised Profession is a Profession Certificate. When using his certificates, the Certificate Holder shall act on account of his profession. This with reference to this CPS. In the case of a profession certificate issued to a member of the Royal Netherlands Bailiffs Association, the following URL is mentioned here: www.registergerechtsdeurwaarders.nl. This URL refers to the bailiff's register. This register must be consulted before relying on the certificate received.

SubjectAltName	No	This includes • the subject's e-mail address; • the OID of the CA concerned; • The subject serial number of the Certificate Holder. The OID of the concerning CA is one of the following: • PinkRoccade CSP CA belonging to the Certificate type; - Authentication 2.16.528.1.1003.1.3.2.2.1, - Signing 2.16.528.1.1003.1.3.2.2.2, - confidentiality 2.16.528.1.1003.1.3.2.2.3 • or the Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie CA; 2.16.528.1.1003.1.3.2.2.5 • or the Getronics CSP Organisatie CA – G2; 2.16.528.1.1003.1.3.5.4.1. • or the KPN CSP Overheid/Bedrijven CA: 2.16.528.1.1003.1.3.2.7.1 • or the KPN CSP Organisatie CA – G2; 2.16.528.1.1003.1.3.5.9.1 In addition, in the authentication certificate, an 'othername' MAY be included for use with Single Sign On (SSO).
CrlDistributionPoints	No	Contains the URI value from which the CRL belonging to the Certificate type can be retrieved.
ExtendedKeyUsage	No	Authentication certificates can contain this extension. This extension makes it possible to use the Certificate for Windows Smartcard Logon, among other things.
AuthorityInfoAccess	No	Contains the URI value of the OCSP responder, which belongs to the certificate type. The OCSP response allows real-time status information about the relevant Certificate to be requested.

Private extensions

Field	Critical	Value
QCStatements	No	Certificates for the electronic signature MUST indicate that they are issued as qualified certificates complying with annex I of EU regulation 910/2014. This compliance is indicated by including the id-etsi-qcsQcCompliance statement in this extension.

3.1.2 Group certificates

Basic Attributes

Field	Value
Version	2 (X.509v3)
SerialNumber	Unique serial number within the CA
Signature	The used algorithm under the SHA-1 root (domain Government /Companies) is sha1WithRSAEncryption. The used algorithm under the SHA-2 root (domain Organization) sha256WithRSAEncryption.
Issuer	Contains the name of the CA concerned and is represented by the following attributes: CommonName, OrganizationName en CountryName. There have been / are several CA certificates in use. • CA-Certificate with OrganizationName 'PinkRoccade Infrastructure Services BV'. The CommonName contains 'PinkRoccade CSP - Overheid – 'and the designation 'Onweerlegbaarheid CA' of 'Vertrouwelijkheid CA' of 'Authenticiteit CA', depending on the type of certificaat. The CountryName is 'NL'. • CA-Certificate with OrganizationName 'Getronics PinkRoccade Nederland B.V.'. The CommonName contains 'Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie'. The CountryName is 'NL'. • CA-Certificate with OrganizationName 'Getronics Nederland BV'. De CommonName contains 'Getronics CSP Organisatie CA – G2. the CountryName is 'NL'. • CA-certificate with OrganizationName 'KPN Corporate Market B.V.', the Common name contains 'KPN Corporate Market CSP Organisatie CA - G2'. The CountryName is 'NL'; • CA-certificate with OrganizationName 'KPN Corporate Market B.V.', the Common name contains 'KPN Corporate Market PKIoverheid CA-Overheid en Bedrijven' The CountryName is 'NL'. • CA-certificate with OrganizationName 'KPN B.V.', the Common name contains 'KPN PKIoverheid CA-Overheid en Bedrijven' The CountryName is 'NL'. • CA-certificate with OrganizationName 'KPN B.V.', the Common name contains 'KPN BV PKIoverheid Organisatie Services CA - G3' with organizationIdentifier = NTRNL-27124701' and CountryName 'NL'
Validity	see 6.3.2.
Subject	The subject's name is displayed as a Distinguished Name (DN), and is represented by at least the following attributes: • CountryName; • CommonName; • OrganizationName; • SerialNumber (subject serial number); • State; • Locality. The attribute OrganizationUnit can also be included as an option.

	The CommonName contains the name of the Service, for example a DNS or group name. The attributes describe the subject name in a unique way. The CountryName attribute is set to a two-letter country code according to ISO 3166.
subjectPublicKeyInfo	Public Key of the Subject

Standard Extensions

Field	Critical	Value
AuthorityKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash
SubjectKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash
KeyUsage	Yes	The digital signature bit is included in Authenticity Certificates. The keyEncipherment, dataEncipherment and keyAgreement bits are included in Confidentiality Certificates.
BasicConstraints	Yes	The CA bit is set to ‘False’ and pathLenConstraint to ‘none’
CertificatePolicies	No	Domain Government/Companies • Authentication certificates contain the OID 2.16.528.1.1003.1.2.2.4. • Confidentiality Certificates contain the OID 2.16.528.1.1003.1.2.2.5). Domain Organization • Authentication certificates contain the OID 2.16.528.1.1003.1.2.4.4. • Confidentiality Certificates contain the OID 2.16.528.1.1003.1.2.4.5). All types of certificates contain a link to the CPS and a user text.
SubjectAltName	No	Herein the OID of the CA: • PinkRoccade CSP Services CA; 2.16.528.1.1003.1.3.2.2.4; • of de Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie CA; 2.16.528.1.1003.1.3.2.2.5; • of de Getronics CSP Organisatie CA – G2; 2.16.528.1.1003.1.3.5.4.1 and the Subject number of the Certificate Holder are stated. Confidentiality Certificates and Authentication Certificates also include the Subject's e-mail address.
CrlDistributionPoints	No	Contains the URI value of the relevant CRL, which belongs to the certificate type, can be retrieved.

ExtendedKeyUsage	No	Group Certificates can contain this extension, which makes it possible to use the Certificate for Windows Smartcard Logon and Codesigning among others.
AuthorityInfoAccess	No	Contains the URI value of the OCSP responder, which belongs to the certificate type. The OCSP response allows real-time status information about the relevant Certificate to be requested.

3.1.3 eSeal certificates

Basic Attributes

Field	Value
Version	2 (X.509v3)
SerialNumber	Unique serial number within the CA
Signature	sha256WithRSAEncryption.

Issuer	CN = KPN BV PKIoverheid Organisatie Services CA - G3
	organizationIdentifier = NTRNL-27124701
	O = KPN B.V.
	C = NL

Validity	see 6.3.2.
Subject	The subject's name is displayed as a Distinguished Name (DN), and is represented by at least the following attributes: • CountryName; • CommonName; • OrganizationName; • OrganizationIdentifier.
subjectPublicKeyInfo	Public Key of the Subject

Standard Extensions

Field	Critical	Value
AuthorityKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash
SubjectKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash
KeyUsage	Yes	nonRepudiation
BasicConstraints	Yes	The CA bit is set to 'False' and pathLenConstraint to 'none'
CertificatePolicies	No	Policy identifier: 2.16.528.1.1003.1.2.5.7 Policy identifier: 0.4.0.194112.1.3 (qcp-l-qscd) policyQualified: 1.3.6.1.5.5.7.2.1 (id-qt-cps) policyQualified: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) All types of certificates contain a link to the CPS and a user text.
SubjectAltName	No	The OID of the CA
CrlDistributionPoints	No	Contains the URI value of the relevant CRL, which belongs to the certificate type, can be retrieved.

ExtendedKeyUsage	No	eSeal Certificates can contain this extension, which makes it possible to use the Certificate for Codesigning among others.
AuthorityInfoAccess	No	Contains the URI value of the OCSP responder, which belongs to the certificate type. The OCSP response allows real-time status information about the relevant Certificate to be requested.
QcStatement	No	Certificates for the electronic seals MUST indicate: - that they are issued as qualified certificates complying with annex III of EU regulation 910/2014. This compliance is indicated by including the id-etsi-qcs-QcCompliance statement in this extension. - that the certified public key resides in a QSCD. This compliance is indicated by including the id-etsi-qcs-QcSSCD. - that they are issued for the purpose of electronic seal. This compliance is indicated by including the id-etsi-qcs-QcType 2. - the location of the PDS. This compliance is indicated by including the id-etsi-qcs-QcPDS.
QcStatement-2	No	Certificates for the electronic seals MUST indicate the semantic of the OrganizationIdentifier. This compliance is indicated by including the id-etsi-qcs-SemanticsId-Legal.

3.1.4 (Standard) Server certificates

Basic Attributes

Field	Value
Version	2 (X.509v3)
SerialNumber	Unique serial number within the CA
Signature	The used algorithm under the SHA-1 root (domain Government /Companies) is sha1WithRSAEncryption. The used algorithm under the SHA-2 root (domain Organization) sha256WithRSAEncryption.
Issuer	Contains the name of the CA concerned and is represented by the following attributes: CommonName, OrganizationName and CountryName. There are/(have been) several CA certificates in use. • CA-Certificate with OrganizationName ‘PinkRoccade Infrastructure Services BV’. The CommonName contains ‘PinkRoccade CSP - Overheid – ‘ and the designation ‘Onweerlegbaarheid CA’ of ‘Vertrouwelijkheid CA’ of ‘Authenticiteit CA’, depending on the type of certificate. The CountryName is set to ‘NL’. • CA-Certificate with OrganizationName ‘Getronics PinkRoccade Nederland B.V.’. The CommonName contains ‘Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie’. The CountryName is set to ‘NL’.

	- CA-Certificate with OrganizationName 'Getronics Nederland BV'. The CommonName contains 'Getronics CSP Organisatie CA – G2. The CountryName is set to 'NL' - CA-certificate with OrganizationName 'KPN Corporate Market B.V.', The Common name contains 'KPN Corporate Market CSP Organisatie CA - G2' and the CountryName is set to 'NL'; - CA-certificate with OrganizationName 'KPN Corporate Market B.V.', the Common name contains 'KPN Corporate Market PKIoverheid CA-Overheid en Bedrijven' and the CountryName is set to 'NL'. - CA-certificate with OrganizationName 'KPN B.V.', the Common name contains 'KPN PKIoverheid CA-Overheid en Bedrijven' and the CountryName is set to 'NL'. - CA-certificate with OrganizationName 'KPN B.V.', the Common name contains 'KPN BV PKIoverheid Organisatie Server CA - G3' with organizationIdentifier ' NTRNL-27124701' and the CountryName 'NL' - CA-certificate with OrganizationName 'KPN B.V.', the Common name contains 'KPN PKIoverheid Server CA 2020' and the CountryName 'NL'
Validity	see 6.3.2.

Subject	CN = < *FQDN* >
	SERIALNUMBER = < *subjectserialnumber* > (optional)
	OU = < *part of subscriber's organization* > (optional)
	L = < *city* >
	O = < *subscriber's organization* >
	C = < *country code* >
	The CountryName attribute is set to a two-letter country code according to ISO 3166.

subjectPublicKeyInfo	Contains the Public Key of the Subject

Standard extensions

Field	Critical	Value
AuthorityKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash
SubjectKeyIdentifier	No	KeyIdentifier is set to 160 bit SHA-1 hash
KeyUsage	Yes	n/a
CertificatePolicies	No	- Server certificates contain the OID 2.16.528.1.1003.1.2.5.9. (under EV Root) - CAB/Forum OID for OV 2.23.140.1.2.2. All types of certificates contain a link to the CPS and a user text.
SubjectAltName	No	This field contains the OID of the CA of either - PinkRoccade CSP Services CA; - or the Getronics PinkRoccade PKIoverheid CA - Government/Businesses and Organization CA; - or the Getronics CSP Organization CA - G2; - or KPN BV PKIoverheid Organization Server CA - G3'; - or KPN PKIoverheid Server CA 2020

		and the subject number of the certificate holder. In server certificates, the primary name of the service and, if applicable, the additional names of the service are included in SubjectAltname. dNSName.
CrlDistributionPoints	No	Contains the URI value where the CRL, belonging to this type of Certificate, can be retrieved
ExtendedKeyUsage	No	Server certificates may contain this extension, which makes it possible to use the Certificate for server and client authentication as well as email security.
AuthorityInfoAccess	No	Contains the URI value of the OCSP responder, which belongs to the certificate type. The OCSP response allows you to request real-time status information about the relevant Certificate.

3.1.5 Private Services Server certificates

Basic attributes

Field	Value
Version	2 (X.509v3)
SerialNumber	Unique serial number within the CA

Issuer	CN = KPN PKIoverheid Private Services CA – G1
	O = KPN B.V.
	C = NL

Validity	see 6.3.2.

Subject	CN = <FQDN>
	SERIALNUMBER = <KvK nummer>
	O = <organisatienaam>
	OU =
	L = <plaats>
	S = <provincie>
	C = <landcode>
	1.3.6.1.4.1.311.60.2.1.3 = NL2
	2.5.4.15 = <businessCategory>

Standard extensions

Field	Essential	Value
AuthorityKeyIdentifier	No	160-bit SHA-1 Hash value of the KPN Private Services Server CA
SubjectKeyIdentifier	No	160-bit SHA-1 Hash value of the certificate
KeyUsage	Yes	n/a
BasicConstraints	Yes	The CA bit is set to ‘False’ and pathLenConstraint to ‘none’

CertificatePolicies	No	2.16.528.1.1003.1.2.8.6 (Private Services CP) https://certificaat.kpn.com/elektronische-opslagplaats
SubjectAltName	No	dNSName CN = <FQDN> Multiple FQDNs may be used in this field. These FQDNs MUST all come from the same domain name range.
CrlDistributionPoints	No	Contains the URI value where the CRL, belonging to this type of Certificate, can be retrieved
ExtendedKeyUsage	No	serverAuth OID id-kp 1 Set (1.3.6.1.5.5.7.3.1) clientAuth OID id-kp 2 Set (1.3.6.1.5.5.7.3.2)
AuthorityInfoAccess	No	Contains the URI value of the OCSP responder, which belongs to the certificate type. The OCSP response allows you to request real-time status information about the relevant Certificate.

3.2 CRL profiles

3.2.1 CRL profile Personal certificates and Profession Certificates

Attributes

Field	Value
Version	1 (X.509 version 2)
signatureAlgorithm	The algorithm used is under the SHA-1 root (Domain Government / Businesses) sha-1 WithRSAEncryption. The algorithm used is under the SHA-2 root (domain Organization) sha-2 WithRSAEncryption.
Issuer	Contains the name of the CA concerned and is represented by the following attributes: CommonName, OrganizationName and CountryName. There are/(have been) several CA certificates in use. • CA-Certificate with OrganizationName ‘PinkRoccade Infrastructure Services BV’. The CommonName contains ‘PinkRoccade CSP - Overheid – ‘ and the designation ‘Onweerlegbaarheid CA’ of ‘Vertrouwelijkheid CA’ of ‘Authenticiteit CA’, depending on the type of certificate. The CountryName is set to ‘NL’. • CA-Certificate with OrganizationName ‘Getronics PinkRoccade Nederland B.V.’. The CommonName contains ‘Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie’. The CountryName is set to ‘NL’. • CA-Certificate with OrganizationName ‘Getronics Nederland BV’. The CommonName contains ‘Getronics CSP Organisatie CA – G2. The CountryName is set to ‘NL’. • CA-certificate with OrganizationName ‘KPN Corporate Market B.V.’, the Common name contains ‘KPN Corporate Market CSP Organisatie CA - G2’ and the CountryName is set to ‘NL’; • CA-certificate with OrganizationName ‘KPN Corporate Market B.V.’, The Common name contains ‘KPN Corporate Market PKIoverheid CA-Overheid en Bedrijven’ and the CountryName is set to ‘NL’.

	• CA-certificate with OrganizationName ‘KPN B.V.’, The Common name contains ‘KPN PKIoverheid CA-Overheid en Bedrijven’ and the CountryName is set to ‘NL’. • CA-certificate with OrganizationName ‘KPN B.V.’, The Common name contains ‘KPN BV PKIoverheid Organisatie Persoon CA - G3’ met organizationIdentifier = NTRNL-27124701’ and the CountryName is set to ‘NL’
effective date	date of issuance
next update	This is the date of issue plus 24 hours, the CRL update is initiated every 60 minutes and published after generation.
revoked certificates	The revoked certificates with certificate serial number and date of revocation and possible reason for revocation.

Extensions

Field	Critical	Value
AuthorityKeyIdentifier	No	contains 160-bit SHA-1 hash

3.2.2 CRL profile Group certificates

Attributes

Field	Value
Version	V2
Issuer	Contains the name of the CA concerned and is represented by the following attributes: CommonName, OrganizationName and CountryName. There are/(have been) several CA certificates in use. • CA-Certificate with OrganizationName ‘PinkRoccade Infrastructure Services BV’. The CommonName contains ‘PinkRoccade CSP - Overheid – ‘ and the designation ‘Onweerlegbaarheid CA’ of ‘Vertrouwelijkheid CA’ or ‘Authenticiteit CA’, depending on the type of certificate. The CountryName is set to ‘NL’. • CA-Certificate with OrganizationName ‘Getronics PinkRoccade Nederland B.V.’. The CommonName contains ‘Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie’. The CountryName is set to ‘NL’. • CA-Certificate with OrganizationName ‘Getronics Nederland BV’. The CommonName contains ‘Getronics CSP Organisatie CA – G2. The CountryName is set to ‘NL’. • CA-certificate with OrganizationName ‘KPN Corporate Market B.V.’, the Common name contains ‘KPN Corporate Market CSP Organisatie CA - G2’. The CountryName is set to ‘NL’; • CA-certificate with OrganizationName ‘KPN Corporate Market B.V.’, The Common name contains ‘KPN Corporate Market PKIoverheid CA-Overheid en Bedrijven’. The CountryName is set to ‘NL’. • CA-certificate with OrganizationName ‘KPN B.V.’, The Common name contains ‘KPN PKIoverheid CA-Overheid en Bedrijven’. The CountryName is set to ‘NL’. • CA-certificate with OrganizationName ‘KPN B.V.’, The Common name contains ‘KPN BV PKIoverheid Organisatie Services CA - G3’ with organizationIdentifier = NTRNL-27124701’. The CountryName is set to ‘NL’

effective date	Date of issuance
next update	This is the date of issue plus 24 hours, the CRL update is initiated every 60 minutes and published after generation.
signatureAlgorithm	The algorithm used is under the SHA-1 root (Domain Government / Businesses) sha-1 With RSAEncryption. The algorithm used is under the SHA-2 root (domain Organization) sha-2 With RSAEncryption.

CRL extensions

Field	Value
AuthorityKeyIdentifier	Contains160 bit sha-1 hash of the Public Key of the CA.
CRL Number	Contains an integer indicating the sequence number of the relevant CRL.

Revocation List entry fields

Field	Value
Serial Number	Contains certificate serial number of the revoked certificate.
Revocation Date	Contains date and time of revocation.

3.2.3 CRL profile Server certificates

Attributes

Field	Value
Version	V2
Issuer	Contains the name of the CA concerned and is represented by the following attributes: CommonName, OrganizationName and CountryName. There are/(have been) several CA certificates in use. ● CA-Certificate with OrganizationName 'PinkRoccade Infrastructure Services BV'. The CommonName contains 'PinkRoccade CSP - Overheid – ' and the designation 'Onweerlegbaarheid CA' or 'Vertrouwelijkheid CA' or 'Authenticiteit CA', depending on the type of certificate. The CountryName is set to 'NL'. ● CA-Certificate with OrganizationName 'Getronics PinkRoccade Nederland B.V.'. The CommonName contains 'Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie'. The CountryName is set to 'NL'. ● CA-Certificate with OrganizationName 'Getronics Nederland BV'. The CommonName contains 'Getronics CSP Organisatie CA – G2. The CountryName is set to 'NL'. ● CA-certificate with OrganizationName 'KPN Corporate Market B.V.', The Common name contains 'KPN Corporate Market CSP Organisatie CA - G2'. The CountryName is set to 'NL'; ● CA-certificate with OrganizationName 'KPN Corporate Market B.V.', The Common name contains 'KPN Corporate Market PKIoverheid CA-Overheid en Bedrijven'. The CountryName is set to 'NL'. ● CA-certificate with OrganizationName 'KPN B.V.', The Common name contains 'KPN PKIoverheid CA-Overheid en Bedrijven'. The CountryName is set to 'NL'.

	• CA-certificate with OrganizationName 'KPN B.V.', The Common name contains 'KPN BV PKIoverheid Organisatie Server CA - G3' with organizationIdentifier = NTRNL-27124701'. The CountryName is set to 'NL' • CA-certificate with OrganizationName 'KPN B.V.', The Common name contains 'KPN PKIoverheid Server CA 2020'. The CountryName is set to 'NL'
effective date	Date of issuance
next update	This is the date of issue plus 24 hours, the CRL update is initiated every 60 minutes and published after generation.
signatureAlgorithm	The algorithm used is under the SHA-1 root (Domain Government / Business) sha1WithRSAEncryption. The algorithm used is under the SHA-2 root (domain Organization) sha256WithRSAEncryption.

CRL extensions

Field	Value
AuthorityKeyIdentifier	Contains 160-bit sha-1 hash of the Public Key of the CA.
CRL Number	Contains an integer indicating the sequence number of the relevant CRL.

Revocation List entry fields

Field	Value
Serial Number	Contains the certificate serial number of the revoked certificate.
Revocation Date	Contains date and time of revocation.

3.2.4 CRL profile Private Services Server certificates

Attributes

Field	Value
Version	V2

Issuer	CN = KPN PKIoverheid Private Services CA – G1
	O = KPN B.V.
	C = NL

effective date	Date of issuance
next update	This is the date of issue plus 24 hours, the CRL update is initiated every 60 minutes and published after generation.
signatureAlgorithm	The algorithm used is under de SHA-2 root (domain Organisatie) sha256WithRSAEncryption.

CRL extensions

Field	Value
AuthorityKeyIdentifier	Contains 160-bit sha-1 hash of the Public Key of the CA
CRL Number	Contains an integer indicating the sequence number of the relevant CRL.

Revocation List entry fields

Field	Value
Serial Number	Contains the certificate serial number of the revoked certificate.
Revocation Date	Contains date and time of revocation.

3.3 OCSP profile

Basic attributes

Field	Value
Version	V2
serial number	SHA1 hash of public key

Issuer DN	C=NL
	O=KPN B.V.
	CN=KPN PKIoverheid Server CA 2020

Subject DN	C=NL
	O=KPN B.V.
	CN= KPN PKIoverheid Server CA 2020 OCSP **n-1**
	(**n**= 1, 2, 3, 4), (**1**=tracking number)

notBefore	**yymmdd**000000Z **(Date of Key Ceremony)**
notAfter	**yymmdd**000000Z **(397 days)**
Public Key Algorithm	Sha256withRSAEncryption (1 2 840 113549 1 1 11)
Public Key Length	2048

Standard Extensions

Field	OID	Include	Critical	Value
basicConstraints	{id-ce 19}	x	Yes	n/a
cA				**Clear**
pathLenConstraint				n/a
keyUsage	{id-ce 15}	x	Yes	n/a
digitalSignature				**Set**
certificatePolicies	{id-ce 32}	x	No	n/a
policyIdentifiers				**2.16.528.1.1003.1.2.5.9**
policyQualifiers				N/A
policyQualifierID				1.3.6.1.5.5.7.2.1
Qualifier				https://certificaat.kpn.com/pkioverheid/cps
policyQualifiers				N/A
policyQualifierID				1.3.6.1.5.5.7.2.2
Qualifier				This certificate is subject to KPN's PKIoverheid CPS.
SubjectKeyIdentifier	{id-ce 14}	x	No	n/a
KeyIdentifier				Method-1

AuthorityKeyIdentifier	{id-ce 35}	x	No	n/a
KeyIdentifier				Hash of public key of Issuing CA
CrlDistributionPoints	{id-ce 31}	x	No	n/a
DistributionPoint				n/a
Full Name (URI)				http://crl.managedpki.com/KPNPKIoverheidServerCA2020/LatestCRL.crl
extendedKeyUsage	{id-ce 37 }	x	Yes	n/a
Key Purpose				1.3.6.1.5.5.7.3.9

Private Extensions

Field	OID	Include	Critical	Value
id-pkix-ocsp-nocheck	1.3.6.1.5.5.7.48.1.5	x	FALSE	**05 00** (Null)