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 October 17th, 2017
Versie version 4.29

Inhoudsopgave

1 Introduction to the Certification Practice Statement

The PKI for the government, shortly PKI government, 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 (Logius).

Within the PKI government, KPN BV operates as Trust Service Provider (or 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 PKI government 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 a number of 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 http://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 the PKI government. The CPS contains, among other things, a description of the procedures that KPN applies to the creation, issuance and revocation of PKI Government 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 PKI Government . This CP, Certificate Policy - Programme of Requirements Organization (G2) and Organization Person(G3) Domains, has been established and is maintained by the Policy Authority of the PKI for the government and is part (part 3a, 3b, and 3e) of the Program of Requirements of the PKI for the government (http: // www. logius.nl/pkioverheid).

The CPS describes how KPN fulfills these requirements and meets these requirements.

1.1.4 Positioning of the CPS

All types of Certificates issued by the KPN have the same level of trust, in accordance with Program of Requirements within the PKI Government. For this reason, the CPS applies to all Certificates.

KPN also delivers PKI government EV SSL certificates (Part 3f Program of Requirements). This service requires a separate CPS. This concerns the CPS PKIoverheid Extended Validation SSL Certificates.
In addition, KPN also issues certificates under the private root of PKI government. A separate CPS is also required for this service. This concerns the CPS: KPN PKI Government CPS Private Services.

1.1.5 Status

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).

1.2 Documentname 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.

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

1.3 User community

The user community within the Organization domain consists, on the one hand, of Trust Service Providers and, on the other hand, of Subscribers, organizational entities in government and business, Certification Holders, Certificate Managers and Relying Parties. There are also individuals working in a recognized profession who are both Subscriber and Certificate Holder. For a description of these concepts, see paragraph 1.7 Definitions and abbreviations.

The Program of Requirements within PKI for the Government (Part 3a, 3b and 3e) applies to this user community. In addition, the KPN Special Terms and Conditions PKI Overheid Certificates (further: Special Terms) apply. Please refer to the Repository of KPN https://certificaat.kpn.com/elektronische-opslagplaats/ .

KPN also delivers PKI government EV SSL certificates (Part 3f Program of Requirements). This service requires a separate CPS. This concerns the CPS PKIoverheid Extended Validation SSL Certificates.
In addition, KPN also issues certificates under the private root of PKI government. A separate CPS is also required for this service. This concerns the CPS: KPN PKI Government CPS Private Services.

The KPN PKI Government Special Terms and Conditions are binding for all parties involved in the certification service. In case of conflict between the CPS and the Special Conditions, the latter will prevail.

KPN conforms to the current version of the Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates as published at http://www.cabforum.org. Should there be an inconsistency between the PKI Government 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.

1.4 Certificate use

The certificates issued by KPN are issued in accordance with the Program of Requirements PKI Government (sections 3a, 3b and 3e).

1.4.1 Certificate use (Program of Requirements PKI Government part 3a)

Within the domain Organization (g2) and Organization Person (g3), Program of Requirements PKI Government 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 concernes:

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 Goverment / Business OID 2.16.528.1.1003.1.2.2.2, 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 which has been created by a Secure Signature Creation Device (SSCD), 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 Government / Business 2.16.528.1.1003.1.2.2.1 OID, OID 2.16.528.1.1003.1.2.5.1 domain Organization]. 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 Governement / Business 2.16.528.1.1003.1.2.2.3 OID, 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). For definitions see Definitions and abbreviations.

1.4.2 Certificate use (Program of Requirements PKI Government part 3b)

Within the domain of Government / Companies (g1) and Organization (g2), PvE PKIoverheid part 3b, KPN issues two 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;

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 / Business OID 2.16.528.1.1003.1.2.2.4, 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 Government / Business OID 2.16.528.1.1003.1.2.2.5, domain Organization OID 2.16.528.1.1003.1.2.5.5].

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

1.4.3 Certificate use (Program of Requirements PKI Government part 3e)

Within the domain of Government / Business (g1) and Organization (g2), PvE PKIoverheid part 3e, 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 Government / Business OID 2.16.528.1.1003.1.2.2.6 , Domain Organization OID 2.16.528.1.1003.1.2.5.6]. 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

1.4.4 Qualified Seals and Qualified Web Certificates (eIDAS)

Kpn does not issue qualified Seals and web certificates.

1.5 CA-model

In the hierarchy of PKI government, the State of the Netherlands Root CA is the highest CA. This CA is owned by PKI Government and is a self-signed CA. Under this SHA-1 Root CA, two domain CAs are positioned, these are the domain CAs for the Burger domain and the Government / Business domain. Under the SHA-2 Root CA, 3 domain CAs are positioned. These are the Burger domain, the Organization domain and the Autonomous Devices domain.
The domain CAs are signed by the Root CA. The Domain CA's signs the CAs of the TSP operating in that domain, including those of KPN.

The foregoing statement is fully described in PKI Government Program of Requirements (Part 1, of Programme of Requirements - Introduction). Both the Root CAs and the CAs are managed by PKI government. A description of the management of these CAs can be found in the CPS Policy Authority for certificates issued by the Policy Authority PKI Government. Both documents can be found on http://www.logius.nl/producten/toegang/pkioverheid .

1.6 Management of the CPS

The KPN CPS is managed by a dedicated Policy Management Authority (PMA). Information regarding this CPS and comments can be directed to:

KPN
Attn. KPN Securtiy Services, Policy Management Authority
PO Box 9105
7300 HN Apeldoorn
Pkisupport@kpn.com

Other documents related to the service of PKI Government Certificates from KPN can be found in the Repository. (dutch: Elektronische opslagplaats) on https://certificaat.kpn.com/downloads/

The PKI Government Certificates are a service of KPN. For more information about KPN, refer to the Electronic Storage.

1.7 Cooperation with the Ministry of Security and Justice (dutch: Ministerie van Veiligheid en Justitie)

KPN concluded a cooperation agreement on certification services with the Ministry of Security and Justice (further: the Ministry). Within that agreement, KPN outsourced the RA activities to the Ministry for applications for certificates, submitted by or on behalf of the Ministry. The Ministry has set up a RA office. In short, the Ministry has handled the certificate applications submitted by or on behalf of the Ministry. The Ministry received the applications, registered them, assessed the accuracy and completeness of the application and decided on the application. KPN continued to perform the CA operations, KPN produced the certificates, placed them on SSCD / SUDs, if applicable, and sent the certificates to the Ministry. The Ministry took care of the issuance of certificates, including the identification of certificate managers and certificate holders. After notification of receipt of the SSCD / SUDs at the RA office, KPN provided the shipment of inter alia the revocation data.

The Ministry has not extended this original cooperation agreement by the end of the agreement, June 8, 2015. Cooperation will continue in limited form. The services from June 8, 2015 are briefly described as follows.

- No new certificates will be issued anymore.
- All certificates issued under section 3A were revoked.
- This also applies to the Services Certificates (Group Certificates).
- The Server Certificates are / are not revoked.
- The revocation service and revocation status service will remain available.

1.8 Cooperation with Multi-Post Services b.v.

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

- Stock management of SSCDs / SUDs.
- Generating key pairs for the SSCDs / SUDs and the insertion of keys in the SSCDs / SUDs.
- Generate activation and revocation code and print that data on a PIN mailer
- Archiving and personalizing SSCDs / SUDs;
- Hand over the SSCDs / SUDs and PINs to the distribution channel.

1.9 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.

1.10 Definitions and abbreviations

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repository

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

2.2 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.

2.3 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.

2.4 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 is renewed 1x per 4 hours.

2.5 Access to published information

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 reacheble 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 can not 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 Certificates comply with the X.501 name recommandation. The names consist of the following parts:

Attribuut	Waarde
Country (C)	NL
Organization (O)	Name of the subscriber
Common Name (CN)	full name of the Certificate holder
Subjectserienummer (SN)	Subjectserialnumber of the Certificate holder

The names used in Server certificates and Group certificates comply with the X.501 name recommandation. The names consist of the following parts:

Attribuut	Waarde
Country (C)	NL
Organization (O)	Name of the subscriber
Common Name (CN)	(group) roll name of the Certificate holder (server) FQDN
State or Province (S)	Province where the Subscriber is located
Locality (L)	Place where the Subscriber is located
Optional:	
Organizational Unit (OU)	Department of the subscribers organization

3.1.2 Need for names to be meaningful

No further stipulations

3.1.3 Anonymity or pseudonymity of subscribers

The use of pseudonyms is not allowed within the PKI government.

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 case of a Server Certificate, the CSR number is used for this purpose.

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

3.1.6 Dispute resolution on name claims

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.

3.1.7 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 has to sign fort his 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 PKI Overheid Subscriber Registration. This form contains an extensive explanation. With this form the Subscriber must send along a number of 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 and
- 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.

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 Law on 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 has to fill in the appropriate web form Request PKI government recognized profession Certificates (dutch: webformulier Aanvraag PKIoverheid Beroepsgebonden Certificaten). 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
http://certificaat.kpn.com/pkioverheidcertificaten/beroepscertificaten/beroepscertificaten-aanvragen/
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 PKI government 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 PKI government 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 an 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 (eg, a license) compliance with the legal requirements for exercising the profession.

A validate a 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 PKI government 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 law concerning Identification). 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 can not 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/formulieren/). 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 Occupational Certificates;
- Request PKIoverheid Group Certificates;
- PKIoverheid Application 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 Contactpersons 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 Recognized Profession 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;
- both the business and the private postal address (if present) , respectively, for the forwarding of the PIN-mail, and the smart card.

Other data, such as:
- if once before a certificate is issued to the certificate holder (in that case the earlier obtained subject serial number has to 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

3.2.3.2.1 Authentication of the Certificate Manager

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;
- Business 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 in writing or by e-mail.

3.2.3.2.2 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 Certficate Manager is employed ;
- e-mail address and telephone number;
- business 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:
- province name ;
- 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 organisaties) 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 reffered 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 in writing or by e-mail on approval of the Certificate Application.

3.2.3.2.3 Authentication for the purpose of Group 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:
- 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 Certficate Manager is employed ;
- e-mail address and telephone number;
- business 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 organisaties) 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.

3.2.4 Authorization of the Certificate Holder

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 has to 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.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Currently KPN does not allow for renewal of certified keys.

3.3.2 Identification en Authentication for routine re-key of the CA certificate

The CA Certificate is not routinely renewed. The CA Certificate (If Desired) renewed around three or five years before the end of his life. That will be on March 23, 2017. Renewal of the CA certificate will be subject to a strict procedure in consultation and in cooperation with the Policy Authority of PKIoverheid.

KPN offers no possibility for routine renewal of PKIoverheid Certificates. A request for renewal will be treated as an application for a new certificate

3.3.3 Identification and authentication for re-key after revocation

Currently KPN does not allow for renewal of certified keys

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/pkioverheidcertificaten/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 Recognized Profession Certificates, and Personal is sent to the Certificate Holder. or the Certificate Manager (PIN-mail). The revocation code for Services Certificates and 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 CertificateHolder / 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 Contactperson:

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

Of the Certificate

- name in the Certificate;
- subject serial nummer in the Certificate;

- certificate type;
- serial nummer(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 in writing or 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/support/intrekken/
In the field ‘Betreft’ (subject) option ’10. Melding omstandigheid intrekking Certificaten’ 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 or not 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 in writing or by e-mail about the notification and its handling.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can apply for a certificate

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 Responsibilities and obligations

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

4.1.2.1 Responsibilities and obligations of the CSP

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.

4.1.2.2 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.

4.1.2.3 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.

4.1.2.4 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.

4.1.3 The proces

The processes defined by KPN for the realization of its certification service are in general divided two parts, based on the principle of seggregation 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.

4.2 Certificate application processing

4.2.1 Registration of Subscriber and Certficate Manager

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/support/opzeggen-en-wijzigen-registratie

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 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 in writing 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 Certficate application

There are different procedures for different types of applications:

- Applications for Personal Certificates and Group Certificates, whereby the key pair is created by KPN;
- Applications for Professional Certificates where the key pair is also created by KPN. This group is dealt with separately because for the Professional Certificates, the Subscriber and the Certificate Holder are the same person;
- Requesting Server Certificates, where the key pair is created by the Subscriber in the Subscriber's Safe Environment.

4.2.2.1 Application for Personal Certificates and Group Certificates

NB. Group certificates are not available on a temporary basis (since 1 July 2017). For current information, please visit https://certificaat.kpn.com/pkioverheidcertificaten/groepcertificaten/

The following steps must be taken by default for applying for a Personal Certificate or Group Certificate.

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. If KPN approves the Certificate Application, the key material in the SSCD/SUD will be generated and the Certificate generated. KPN also generates the secret PIN and PUK code for the SSCD/SUD and the withdrawal code for the Certificates.
5. The smart card containing the certificates is sent by post to the home address of the Certificate Holder/Certificate Manager. A request for notification / acknowledgement of receipt is attached to this smart card. The Certificate Holder/Certificate Administrator must be identified by AMP, if he or

she has not previously been identified by KPN. If KPN can rely on an identification previously carried out by KPN, this identification need not be repeated. The Certificate Holder/Certificate Administrator will then receive an acknowledgement of receipt with the smart card and a separate email. The Certificate Holder/Certificate Administrator must confirm the receipt via a link indicated in the email. KPN may rely on an identification previously made by or on behalf of KPN for Certificate Manager if the identity document used for this purpose is used again at the time of the new application, if it is not registered as stolen or missing and if it is still valid until six weeks after the application has been submitted. The date of receipt of the application by KPN will be the determining factor.

6. AMP identifies the Certificate Holder, makes a copy of his identity document, sends this copy to KPN electronically together with the signed identification.
7. Upon receipt of the electronic AMP confirmation, KPN will send the document containing the secret PIN and PUK codes for the SSCD/SUD and the certificate revocation code for the Certificates by post to the business 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 Professional Certificates

The following steps must be followed in order to apply for a Professional Certificate.

1. The Subscriber/Certificate Holder fills in a Application for Professional Certificates and declares that he agrees with the Special Terms and Conditions, among other things. Further instructions on how to use the form are enclosed with the form.
2. The Certificate Holder signs the application form, accompanies it with a copy of his/her identity document and the proof of exercising a Recognised Appeal (see 3.2.2 Subscriber's Authentication) and sends it to KPN jointly.
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 whether the proof of exercising the Recognised Profession is authentic.
4. If KPN approves the Certificate Application, the key material in the SSCD is generated and the Certificate is generated. KPN also generates the secret PIN and PUK codes for the SSCD and the withdrawal code for the Certificates.
5. The smart card containing the certificates is sent by post to the home address of the certificate holder. The certificate holder receives an acknowledgement of receipt with the smart card and a separate email. The Certificate Holder must confirm the receipt by means of a link indicated in the email.
6. If it concerns an application that will replace a previously issued professional certificate and the application for the new professional certificate is electronically signed with the to be replaced certificate, issued by KPN, no identification need be carried. (only for first replacement).
7. 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 AMP electronic confirmation, KPN will send the document containing the secret PIN and PUK codes for the SSCD and the certificate revocation code for the Certificates by post to the business address of the Certificate Holder. If a business address has not been provided, this will be sent to the private address of the Certificate Holder.

KPN will continue to offer the possibility, at an additional charge, of allowing the identification to take place at a time/location to be agreed upon.

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 SSL 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, taking into account 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 (http://certificaat.kpn.com). 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:
   a. 3.2.2.4.1 Validating the Applicant as a Domain Contact
   b. 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact
   c. 3.2.2.4.5 Domain Authorization Document

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 http://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 http://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.

4.2.3 Application processing time for the certificate

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 Issuance of Personal Certificates and Group Certificates

The smartcard containing the certificates issued and the document containing the access codes (PIN and PUK code, also known as activation data) and the revocation code of the certificates are issued at different times and via different channels. In the first instance, the smart card will be sent by post to the home address of the certificate holder. This smart card is accompanied by a receipt confirmation code, which is entered online by the certificate holder. AMP executes the personal identification.

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 withdrawn 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.

4.3.2 Issuance of Proffesional Certificates

The smartcard with the certificates issued and the document containing the access codes associated with the smart card and the revocation code of the certificates are issued at different times and, if possible, by different means. In the first instance, the smart card will be sent by post to the home address of the certificate holder.

This smart card is accompanied by a receipt confirmation code, which is entered online by the certificate holder. AMP executes the personal identification.

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 certain cases, it is possible that the certificate holder may no longer have to be identified, for example in the case of a replacement application.
If the certificate holder has not confirmed receipt within 3 weeks, KPN will remind him of this fact. If the Certificate Holder has not confirmed receipt within 6 weeks, KPN shall revoke the Certificates concerned without further notice.

4.3.3 Issuance of Server Certificates

In the case of applications for registered Certificate Managers, KPN will send the Certificates created by e-mail to the Certificate Manager's stated address.

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

4.3.4 Notification of certificate issuance to the Certificate Holder or Manager

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

4.4 Certificate Acceptance

4.4.1 Acceptance of Professional, Personal and Group Certificaten

The Professional, Personal or Group 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.

4.4.2 Acceptance of 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.

4.4.3 Publication of the Certificate by the CA

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

4.5 Key Pair 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.

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. The PKI government 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.

4.7 Certificate rekey

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

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.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances leading to 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 SSCD, the 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 Professional Certificates);
- Termination or bankruptcy of the organization of the Subscriber (in the case of Organization-related Certificates);

In addition, certificates will be withdrawn 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 suspectedly lost private key or SSCD/SUD, stolen or suspected stolen key or SSCD/SUD or destroyed key or SSCD/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 an 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 de 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 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.

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 may make a request for 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 a request for revocation

A request for revocation or notification of a circumstance that may lead to the revocation of a Certificate may be made by the following means:

In writing: KPN B.V.
t.a.v. Afdeling Validatie, PKIoverheid Certificaten
Postbus 9105
7300 HN Apeldoorn

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

It should be stressed that if the revocation serves an urgent interest, this should be done via the online / real time revocation pages. This form of revocation is available 24 hours a day, seven days a week.

For submitting requests for revocation in writing the contact form can be used which can be found on the website . https://certificaat.kpn.com/support/intrekken/

In the field ‘Betreft’ (subject) option ’10. Melding omstandigheid intrekking Certificaten’ should be chosen. (eng:"10. Notification conditions that can lead to revocation”).

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

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

4.9.4 Duration for processing revocation request

As indicated, if the revocation has an urgent interest, this should be done electronically via the online / real time revocation pages.
Requests for revocation by letter shall be considered only on the following working day at the earliest and processed within four hours after receipt.

4.9.5 Verification conditions when consulting certificate status information

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 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 (http://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 (nl: Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders) in order to determine whether the Bailiffs are listed in the register kept by the Royal Bailiffs Association.

4.9.6 CRL issuance frequency

The update of the CRL is initiated every 15 minutes, after the CRL has been generated, the CRL is published. A CRL is valid for 24 hours.

4.9.7 Maximum delay for CRL issuance

KPN will revoke the (Services) Certificate no more than four hours after an authorised online revocation request has been received.

4.9.8 Online revocation status check

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 with regard to 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.

4.9.9 Certificate Status Service

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.

4.9.10 Termination of the 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.

4.9.11 Other notices of revocation

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

4.9.12 Certificate Suspension.

Suspension of Certificates is not supported by KPN

4.10 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.

5 Management, operational and physical security measures

KPN's certification service provider business unit is certified against ISO9001:2000, 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 Fysieke beveiliging

5.1.1 Location, construction and physical protection

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) .

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).

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, SSCD/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 Security Certificate Holders/Managers

No further provisions in the case of Professional Certificates, Personal Certificates or Group Certificates.

If a Server certificate is involved, then the key material must have been generated in a Safe Environment and the Private Key must be permanently accommodated therein. For further explanation, see the definition of Safe Environment (Section 1.6).

5.1.3 Storage of media

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.

5.1.4 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.

5.1.5 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

Security duties and responsibilities, including confidential functions, are documented in job descriptions. These have been drawn up on the basis of 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 on the basis of the need-to-know principle.

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. Trusted Employee Policy.

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 System Administration Controls

KPN ensures procedural security through the application of ITIL management processes. ITIL is a methodology for standardizing IT management processes with the aim of bringing, maintaining and where possible improving the quality of these processes to a defined level.

KPN has separate systems for development, testing, acceptance and production. These systems are managed using the ITIL procedures referred to above.
The transfer of software from one environment to another is controlled using the change management procedure. This procedure includes,among other things, maintaining and recording of versions, making changes and emergency repairs to all operational software.

The integrity of all systems and information used for PKIoverheid Certificates is protected against viruses, malicious software and other possible disruptions to service provision through an appropriate combination of physical, logical and organizational measures. These measures are preventive, repressive and corrective in nature. Examples of measures taken include: logging, firewalls, intrusion detection and system redundancy.

KPN has provided for timely and coordinated action to respond quickly to incidents and to limit the impact of security breaches. All incidents shall be reported as soon as possible after they occur.

If an incident or other event in any way could threaten or affect the reliability of the certification service and/or the image of the PKI for the government, this will be reported immediately to the PKIOverheid Policy Authority.

5.2.4 Seggregation 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).

5.3 Personnel Security Controls

5.3.1 Expertise, experience and qualifications

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 Trusted Employee Policy

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.

5.4 Audit Logging Procedures

5.4.1 Event logging

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 with regard to 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.

Audit logs are regularly reviewed to see if there have been significant security or operational events that may require further action.

5.4.2 Audit log Retention period

The log files are stored for at least 18 months and then deleted.
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.

5.4.3 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 seggregation 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.

5.4.4 Audit log back up procedures

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

5.5 Records Archival

5.5.1 Archival of events and documents

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 Archive retention period

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 Archive protection

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 further stipulations

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.

5.6 Key Changeover

The keys of a CA Certificate are renewed at the same time as renewing that CA Certificate.
Old keys remain on the token if the new ones are placed on it. Old tokens are destroyed after the end of their lifetime and the associated archiving period (zeroising).

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

5.7 Compromise and Disaster Recovery

5.7.1 Disaster management

KPN has implemented procedures to minimise the consequences of any disasters as much as possible. These measures include a contingency plan and an disaster recovery scenario. 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.

5.7.2 Business Continuity

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 CSPs registered with AT to take over (parts of) the certification service from CSPs who involuntarily terminate their CSP 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 CSP 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 Generation and installation of key pairs

6.1.1 Generation of key pairs

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 PKI government 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 takes place in SSCDs/SUDs. 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'.

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 CWA 14167-1 audit report.

All Certificates, with the exception of Server Certificates, are generated by a trustworthy system in an SSCD (for personal and professional certificates) or SUD (for Group Certificates). Multiple Certificates can be stored on the SSCD and SUD. For the Server Certificates, these must be generated by and under the responsibility of the Subscriber in a Safe Environment.

6.1.2 Transfer of Private Key and SSCD to Subscriber

Personal, Professional Certificates or Group Certificates are transferred to the Certificate Holder in the following manner: sending the SSCD or SUD, including the Private Keys created by KPN via a commercial mail company, where the necessary PIN for the SSCD or SUD is issued separately to the Certificate Holder (' out of band'). The Certificate Holder signs for receipt of the SSCD 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 Transfer of Subscriber Public Key

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 Transfer of the Public Key from TSP to Confidential 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 Size

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 an SHA-1 CA Certificate is 2048 bits RSA and of an SHA-2 CA Certificate is 4096 bits.

6.1.6 Generation of Public Key parameters

No Stipulations.

6.1.7 Key pair usage

For the use of key usage extensions, see section 7.1.4. Certificate Profiles overview.

6.1.8 The purpose of key usage (as defined in X. 509 v3)

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 on the basis of internationally recognised standards.

6.2.1 Standards required for the cryptografische module

For operational use, the cryptographic data is stored in an HSM. The HSM is EAL4+ certified.

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 on the basis of 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 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 Escrow of Private keys of Certificate Holders

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 Back-up of private keys

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 Certificates.

6.2.5 Archiving of Private Keys

Private keys of Certificates are not archived.

6.2.6 Acces to Private Keys in the cryptografic 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 Storage of Private Keys in the cryptografic module

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

6.2.8 Activation of Private Keys

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 Deactivation of Private Keys

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 SSCD or SUD is lost by the Certificate Holder and returned to KPN by a finder, this SSCD 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.

6.2.10 Methods for destruction of Private Keys

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 Requirements for safe means of storage and use of certificates

For those certificates issued on smart cards, i. e. personal 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.

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 Archiving of van Public Keys

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 Period of use for Certificates, Public Key and Private Keys

For SHA-2 certificates, a term of validity of 3 years (standard) or 5 years can be chosen. However, this does not apply to server certificates; the PKI government's IPU allows a maximum validity period of 3 years for server certificates.
For the SHA-1 Server Certificates issued in 2011, the lifespan was limited to 31 December 2011. For those SHA-1 Server Certificates, issued in December 2011 with PKI government permission, which can still be issued until 31 December 2013, a fixed date of validity of 31 December 2013 applies.

On 7 September 2017, the Netherlands Radiocommunications Agency(Agentschap Telecom), as supervisor under the European eIDAS Regulation, decided to grant qualified status to the new trust service based on the KPN G3 CA.

Under this CA server certificates can be issued with a validity period of 2 or 3 years. Personal, Professional and Group Certificates can be selected for a period of 3 or 5 years.

KPN will inform the Subscriber of the expiry of this period of validity at least two months before the expiry date of the Certificates issued upon request.

6.4 Activation Data

6.4.1 Generation and Installation of activation data

The SSCD or SUD, in which the Key pair and its Certificate are stored, is provided with activation data. This PIN and PUK code is 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 Protection of activation data

The PIN-mail, with the PIN and PUK code printed on it, is sent to the Certificate Holder/Certificate Manager via a different route and at a different time, i. e. separated from SSCD or SUD. 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 Functioning of the activation data

In order to be able to access the Key Material and Certificate, the Certificate Holder must use the PIN code obtained for the SSCD or SUD. If the PIN code is entered incorrectly three times, the SSCD or SUD is automatically blocked. In that case, SSCD or SUD can only be unlocked with the PUK code.

If the PUK code is entered incorrectly three times, the SSCD or SUD is permanently blocked and therefore becomes unusable.

6.5 Computer Security Controls

6.5.1 Specific technical requirements for computer security

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 Security Rating

KPN classifies the resources used on the basis of a risk assessment.

6.6 Life Cycle Security Controls

6.6.1 Controls for system development

KPN also develops, in part, its own CardManagementSystem (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 CWA 14167-1 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 6.6.1 is the use of hashes.

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.

6.8 Time-stamping

KPN does not provide time-stamping services.

7 Certificaat-, CRL- en OCSP-profiles

7.1 Certificate profiles

7.1.1 CP OID

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

Personal and Professional Certificates:

Domein Overheid/Bedrijven (Domain Government/Companies)	
2.16.528.1.1003.1.2.2.1	Authentication certificate
2.16.528.1.1003.1.2.2.2	Signing certificate
2.16.528.1.1003.1.2.2.3	Confidentiality certificate
Domein Organisatie (Domain Organization)	
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

Server certificates:

Domein Overheid/Bedrijven(Domain Government/Companies)	
2.16.528.1.1003.1.2.2.6	Server certificate.
Domein Organisatie(Domain Organization)	
2.16.528.1.1003.1.2.5.6	Server certificate.

Groupcertificates:

Domein Overheid/Bedrijven(Domain Government/Companies)	
2.16.528.1.1003.1.2.2.4	Authentication certificate.
2.16.528.1.1003.1.2.2.5	Confidentiality certificate.
Domein Organisatie(Domain Organization)	
2.16.528.1.1003.1.2.5.4	Authentication certificate.
2.16.528.1.1003.1.2.5.5	Confidentiality certificate.

7.1.2 Overview Certificate Profiles

The PKIoverheid Certificates are structured according to the PKIX X. 509 v3 standard, whereby extensions can be used.

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.
Certificate profiles are drawn up in accordance with Part 3 of the PKI government's Programme of Requirements, in accordance with the Certificate Profile of the Certificate for the Domain Government/Companies and Organization.

7.1.2.1 Personal certificates and Recognized Profession Certificates

Basic attributes

Field	value
Version	2 (X.509v3)
SerialNumber	Unique 128 bits long serialnumber
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	The validity period of the Personal or Professional Certificate is by choice either 3 or 5 years.
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 Appeal of the Certificate Holder if a Professional 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 Professional 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 professional 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 extensies

Veld	Critical	Value
QCStatements	Nee	Certificates for the electronic signature MUST indicate that they are issued as qualified certificates complying with annex I of EU regulation 920/2014. This compliance is indicated by including the id-etsi-qcsQcCompliance statement in this extension.

7.1.2.2 Groupcertificates

Basic Attributes

field	value
Version	2 (X.509v3)

SerialNumber	Unique 128 bits long Certificate number
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	The validity period of the Group certificate is standard 3 years, but a validity period of 5 years can be chosen.
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	Bevat de PublicKey van de 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	Ja	Het CA bit is ingesteld op 'False' en pathLenConstraint op 'none'
CertificatePolicies	No	Domain Government/Companies • Authhentication 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 • Authhentication 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 Certificaat 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.

7.1.2.3 Servercertificates

Field	Value
Version	2 (X.509v3)
SerialNumber	Unique 128 bits long Certificate number
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 ingesteld op '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' met organizationIdentifier ' NTRNL-27124701' and the CountryName 'NL'
Validity	The validity period of the Server Certificate is optional 2 or 3 years.
Subject	CN = < *FQDN* > SERIALNUMBER = < *subjectserialnumber* > (optional) OU = < *part of subscriber's organization* > (optional) L = < *city* > ST = < *province* > O = < *subscriber's organiztion* > C = < *conytry code* > The CountryName attribute is set to a two letter country code according to

	ISO 3166.
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	n/a
CertificatePolicies	No	Domain Organization • Server certificates contain the OID 2.16.528.1.1003.1.2.5.6. 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' 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.

7.2 CRL-profiles

The CRL (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 CRL's layout and format, as well as the principle underlying the CRL, in accordance with the interests of the parties involved.

7.2.1 Personal certificates and Recognized Profession Certificates

Attributes

Field	Value
Version	1 (X.509 versie 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 15 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

7.2.2 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 15 minutes and published after generation.
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.

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.

7.2.3 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'
effective date	Date of issuance
next update	This is the date of issue plus 24 hours, the CRL update is initiated every 15 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 velden

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

7.3 OCSP-profiles

The OCSP Responder conforms to RFC 6960.

7.3.1 OCSP-profiel Servercertificaten G3

Base Certificate				**Value**
Version				2
serial number				SHA1 hash of public key
Issuer DN				C=NL O=KPN B.V. OI=NTRNL-27124701 CN=KPN BV PKIoverheid Organisatie Server CA - G3
Subject DN				C=NL O=KPN B.V. CN= KPN BV PKIoverheid Organisatie Server CA - G3 OCSP **n-1** (**n**= 1, 2, 3), (**1**=volgnummer)
notBefore				**yymmdd**000000Z **(Date of Key Ceremony)**
notAfter				**2001dd**235959Z **(3 years)** **(yymmdd)**
Public Key Algorithm				Sha256withRSAEncryption (1 2 840 113549 1 1 11)
Public Key Length				2048
Standard Extensions	**OID**	**Include**	**Criticality**	**Value**
basicConstraints	{id-ce 19}	x	TRUE	n/a
cA				**Clear**
pathLenConstraint				n/a
keyUsage	{id-ce 15}	x	TRUE	n/a
digitalSignature				**Set**
certificatePolicies	{id-ce 32}	x	FALSE	n/a
policyIdentifiers				**2.16.528.1.1003.1.2.5.6**
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				**Op dit certificaat is de PKIoverheid CPS van KPN van toepassing. (eng = This certificate is subject to KPN's PKIoverheid CPS.)**
SubjectKeyIdentifier	{id-ce 14}	x	FALSE	n/a
KeyIdentifier				**Method-1**
AuthorityKeyIdentifier	{id-ce 35}	x	FALSE	n/a
KeyIdentifier				**Hash of public key of Issuing CA**
CrlDistributionPoints	{id-ce 31}	x	FALSE	n/a
DistributionPoint				n/a

Full Name (URI)				http://crl.managedpki.com/KPNBVPKIoverheidOrganisatiePersoonCAG3/LatestCRL.crl
extendedKeyUsage	{id-ce 37 }	x	TRUE	n/a
Key Purpose				**1.3.6.1.5.5.7.3.9**
Private Extensions	**OID**	**Include**	**Criticality**	**Value**
id-pkix-ocsp-nocheck	**1.3.6.1.5.5.7.48.1.5**	x	FALSE	**05 00** (Null)

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 aforementioned TTP. NL Scheme lapses on that date.

In February 2016, the previous ETSI certifications ETSI 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 the PKI government's Programme of Requirements as stated in the Programme of Requirements (see http://www.logius.nl/producten/toegang/pkioverheid/).
This can be demonstrated by means of an audit report issued by BSI Management Systems b. v,
A copy of the ETSI EN 319 411-2 and ETSI TS 102 042 certificate can be found on the KPN site (see Electronic Storage Site). The audit reports drawn up by the auditors concerned are secret from a security point of view. They are not made available to third parties and can only be viewed on request and under strict confidentiality.

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 Trust Service Provider (TSP) with the Netherlands Radiocommunications Agency, as a certified publisher of Qualified Certificates to the public.

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.

KPN has outsourced the identification of certificate holders and certificate managers to AMP B. V.

9.1 Fees

No further stipulations.

9.2 Financial Responsibility

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.

9.3 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 Listing of information considered confidential

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 9.4.2 Confidential personal data.

9.3.2 List of information considered as non-confidential

No further stipulations.

9.3.3 Responsibility not to provide data

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 on the basis of 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

KPN complies with the requirements of the Wbp (dutch Act on Privacy). KPN has registered with the Dutch Data Protection Authority (College Bescherming Persoonsgegevens) as being responsible for processing personal data for the purpose of certification services.

9.4.1 Privacy Statement

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 Confidential personal data

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;

9.4.3 Non-confidential data

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 Keys

KPN is responsible for protecting private CA keys.

The responsibility for protecting the Private Key of the Certificate Holder and thus for the SSCD/SUD on which it is stored lies up to and including transfer of the SSCD/SUD with KPN and after transfer with the Certificate Holder/Certificate Manager. As a result, the responsibility for protecting the PIN and PUK codes that secure the smart card also lies with KPN up to and including the transfer of the PIN mail with KPN and after transfer with the Certificate Holder/Certificate Manager.

The Subscriber creates the key pair for which he requests a server certificate. The Subscriber is responsible for creating and storing the relevant Private Key in his or her Safe Environment, the Subscriber is also responsible for the Safe Environment itself.

9.4.5 Notification of use and consent to the use of personal data

The Certificate Holder, the Certificate Manager and Subscriber grant permission for publication of certificate data by consent to the Special Terms and Conditions. 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 Provision of information as a result of a legally valid summons

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.

9.4.7 Provision of private law evidence

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.

9.4.8 Provision of information at the request of the owner

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.
KPN is entitled to charge an appropriate fee for each provision.

9.4.9 Disclosure of information with respect to revocation of a certificate

Information on revocation of Certificates is available through the CRL. The information given there only concerns the Certificate number and the moment of revocation.

9.4.10 Other circumstances which may lead to the provision of information

No further Stipulations.

9.5 Intellectual property rights

The intellectual property rights of this CPS are vested in KPN.

Property rights relating to the Certificate, SSCD and SUD shall also remain vested in KPN and its licensors after issuance, including intellectual property rights. The same applies to documentation provided by KPN's services, including this CPS.

9.6 Obligations and Warranties

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

9.7 Restrictions on warranties

In the Special Terms and Conditions, the manner in which KPN and the parties involved must deal with the restrictions in guarantees is included.

9.8 Liability

9.8.1 Liability of KPN

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

9.8.2 Limitations of Liability to the relying Party

KPN's liability to Relying Parties is limited in the manner described in the Special Terms and Conditions.

9.9 Indemnities

No further stipulations.

9.10 Term and Termination

The special conditions include the manner in which KPN deals with termination.

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 in writing 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 Amendment procedure

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 Confidential Parties may comment on the content of the CPS and submit it to KPN's PMA (pkisupport@kpn.com). If, on the basis of 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 of amendments

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.

9.13 Dispute Resolution Procedures

KPN has a complaints procedure. Complaints may be addressed to the Director of KPN.

Disputes will be resolved as described in the Special Terms and Conditions.

9.14 Governing Law

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

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

9.15 Compliance with Applicable Law

No further stipulations

9.16 Miscellaneous Provisions

No further stipulations

Appendix 1 Practices Ministry of Security and Justice

This Ministry of Security and Justice (hereinafter referred to as the Ministry) appendix is part of KPN B.V.'s General Certification Practice Statement[1] (from here: CPS). This Annex contains the specific supplement to the CPS for the PKI service for the Ministry. The chapter layout is fully in line with the chapter layout of the CPS. In the event of any conflict between the CPS and this Annex, the additions made by the Ministry in this Annex shall prevail.

1 Introduction

The Ministry makes use of a Public Key Infrastructure (PKI) within the PKI government's system of agreements. The Ministry uses the PKI to provide information exchange services between the departments of the Ministry, between the Ministry and its chain partners and for logical access to information and applications of the Ministry. In addition, PKI server certificates are used to establish secure connections between systems and to authenticate systems. The PKI service provides qualified certificates to members of the Ministerial staff. KPN acts as Certification Service Provider and the Ministry as Registration Authority (RA) within the PKI service provision.

1.1 Overview

The structure of the PKI consists of various organisational units that are shown in Figure 1.

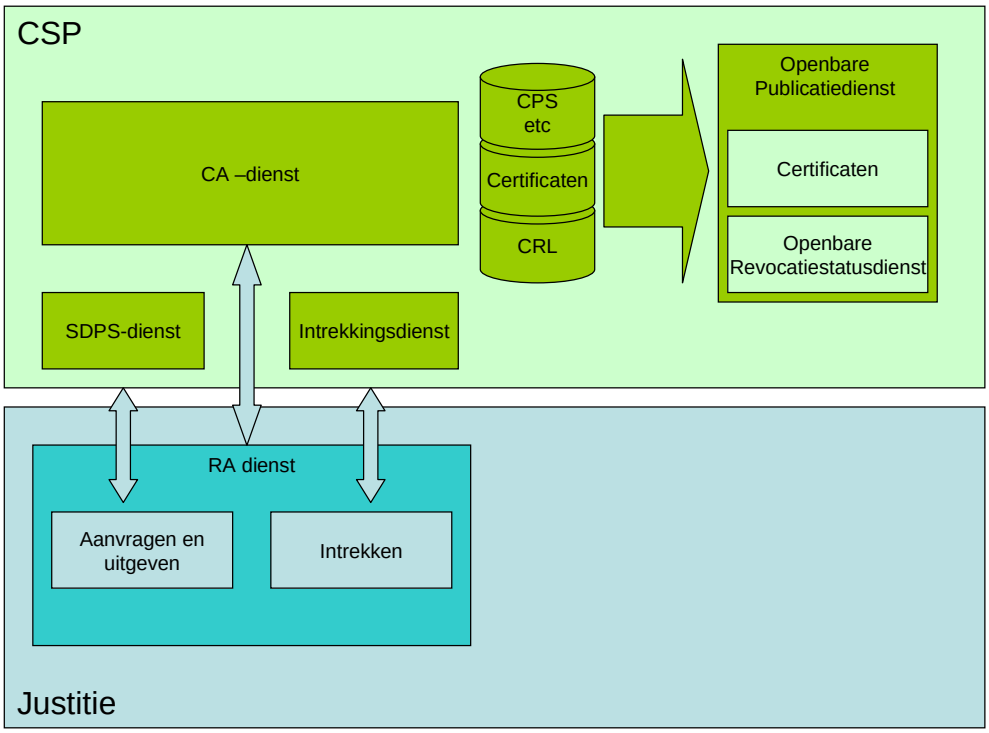

Figure 1: PKI organisational units

CSP

The Certification Service Provider is the service provider that issues certificates under PKI government. The CSP provides and manages certificates and key information including the data carriers provided for this purpose (tokens: smartcard and USB token). The CSP also has the ultimate

responsibility for providing certification services even though the CSP does not carry out the actual work itself.

CA DIENST
The Certification Authority (CA) signs the certificates upon request of the RA and places the personal certificate on the token. The CA also delivers server and group certificates at the request of the RA. In addition, the CA is responsible for signing the Certificate Revocation List (CRL) and its publication.

PUBLISHING SERVICE
The Publication Service is a service that distributes certificates to subscribers and, with the consent of subscribers, to trusted parties. The service also distributes the Certificate Policies (CP) and Certification Practice Statements (CPS) to certificate holders, subscribers and trusted parties.

REVOCATION MANAGEMENT SERVICE
The Revocation Service is responsible for processing requests relating to the revocation of certificates. The status information of revoked certificates shall be made available for publication through the Public Publications Service.

REVOCATION STATUS SERVICE
The status information is disseminated through the Revocation Status Service. This is a service that provides the revocation status to relying parties. This service may be a real-time service (OCSP - Online Certificate Status Protocol), but may also be based on revocation status information updated at regular intervals (CRL publication).

SDPS SERVICE (SUBJECT DEVICE PROVISIONING SERVICE)
The Subject Device Provisioning Service prepares the delivery of Secure Signature Creation Devices (SSCDs or token) and executes it and delivers the tokens (on which the private keys are placed) to the certificate holders. This is done in such a way that the confidentiality of the private keys is not compromised and the issuing to the intended Certficate Holders is guaranteed. In the case of personal or group certificates, the token will have to meet the requirements for an SSCD. For the server certificates, other requirements are imposed on the token: it must meet the requirements for a Secure User Device (SUD). The requirements for SSCD and SUD apply to both the smart card and USB tokens.

RA SERVICE (REGISTRATION AUTHORITY)
A Registration Authority (RA) handles the processing of certificate applications and all associated tasks, the most important of which is the verification of the identity of the certificate holder. The RA has a clear relationship with the CA: after verifying the completeness and correctness of the application, the RA commissions the CA to produce tokens with the relevant certificates.

1.3 User community
The Ministry has signed a contract with KPN for the PKI service. KPN Special Terms and Conditions PKIoverheid Certificates (Special Terms and Conditions) do not apply.

1.4.1 Certificate use (PvE PKIoverheid part 3a, 3b and 3e)
The Ministry does not use Recognized Profession Certificates.

The following types of certificates are available within the PKI service:
- Personal certificate;
- Services certificate
    - Server certificate;
    - Group certificate.

The personal certificates consist of two unqualified certificates, one of which performs the function of identification and authentication and the other supports the function of confidentiality. In addition, there is the qualified certificate that supports the function of non-repudiation. A personal certificate is issued to one person (the certificate holder). The intention is that only the certificate holder has access to the certificate.

A server certificate is an unqualified certificate stored within the Ministry's Safe Environment that supports the functions of authenticity/confidentiality. The server certificate is issued to a server that is used by independent contracting authorities and affiliated public-law institutions of the Ministry.

A group certificate consists of two unqualified certificates that support the functions of identification/authentication and confidentiality. A group certificate is issued to a department or group of employees of the Ministry. The difference between the certificates is that with a personal certificate one can provide electronic messages with a qualified electronic signature. This cannot be done with server or group certificates. For the obligations attached to the certificates, see the relevant conditions of use.

1.6 Management of the CPS
Information regarding the RA service can be obtained from:

Judicial Information Service
PKI department
Egbert Gorterstraat 6
7607 GB Almelo

Post box 695
7600 AR Almelo

For information and/or support, please contact us via e-mail: certificatenpki@justid.nl or by telephone to the front office of the Judicial Information Service under number: 088 99 89 000.
The Judicial Information Service has its own complaints procedure. This regulation prescribes what the Judicial Information Service must do if a person has lodged a written complaint. For more information, see www.justid.nl.
3.2.1 Method of demonstrating Private Key possession
The key pair, of which the Public Key is certified, is created for the Server Certificates in the Ministry's Safe Subscriber Environment and entered into the Ministry's CMS.

3.2.2 Authentication of the Subscriber
Within the PKI service provision, the Ministry is the only Subscriber. The Ministry does not use' AMP' and' DigiKoppeling' within the PKI service provision.

3.2.3 Authentication of personal identity
Within the PKI service provision, the Ministry has appointed qualified applicants who are entitled to submit applications from prospective certificate holders. The authorised applicant knows the intended certificate holder from his or her responsibility and is responsible for the complete and correct submission of the certificate application. The applications for certificates are registered and validated by the RA employees.

3.2.3.1 Authentication for personal Certificates
Employees of the Ministry must apply for a certificate via an authorised applicant. An overview of the active authorised applicants is available at the RA. The authorised applicant checks the employee's

identity by means of the employee's identity document (face-to-face check) and sends the application to the RA, including a copy of the identity document.

3.2.3.2 Authentication for the purposes of Services Certificate
Services certificates are requested by certificate managers. Upon receipt of the application, the RA employee checks whether the relevant certificate manager is still active in the CMS and whether the data in the application is correct.

3.2.3.2.1 Authentication of the Certificate Manager
Employees of the Ministry who are appointed as certificate manager must submit an application via an authorised applicant. The authorised applicant checks the employee's identity by means of the employee's identity document (face-to-face check) and sends the application to the RA, including a copy of the identity document. An overview of the active authorised applicants and certificate managers is available at the RA.

3.2.3.2.2 Authentication for the purpose of server certificate
Server certificates are requested by certificate managers. Administrators of certificates must have been applied for by the competent applicant and must be active in the CMS. Upon receipt of the application, the RA employee checks whether the certificate manager is still active in the CMS. In addition, the RA employee checks whether the data in the application is correct.

3.2.3.2.3 Authentication for the purposes of Group Certificate
Group certificates are applied for by certificate managers. Administrators of certificates must have been applied for by the competent applicant and must be active in the CMS. Upon receipt of the application, the RA employee checks whether the certificate manager is still active in the CMS. In addition, the RA employee checks whether the data in the application is correct.

3.2.4 Authorisation of the Certificate Holder
Employees of the Ministry must apply for a certificate via an authorised applicant. An overview of the active authorised applicants is available at the RA. The authorised applicant checks the identity of the employee on the basis of the employee's identity document (face-to-face check) and sends the application to the RA, including a copy of the identity document. The RA employee checks whether the data in the application is correct.

3.4 Identification and Authentication of requests for revocation
Within the PKI service provision, the terms PIN-mail and PINmailer have the same meaning.
An application for revocation can be submitted by the certificate holder via a KPN self-service portal, by the certificate holder and the authorised applicant via the RA-PKI counter (via telephone or personal appearance) or in writing to the RA of the Judicial Information Service.
If a revocation request is made directly to the RA by telephone, the data is checked by a number of identifying questions and then called back for verification. The reason for revocation will be asked.
In case of a revocation request directly to the RA by e-mail, the data of the certificate holder mentioned on the e-mail message will be checked and if necessary a request will be returned by e-mail for additional data. Subsequently, a call back by telephone is made for verification. The reason for revoking the certificate is asked.

In the event of a request for revocation is made in person to the RA, the identity document will be used to verify the identity of the person. The reason for revoking the certificate is asked.

KPN may also initiate a revocation request (see Chapter 4.9.2 of the CPS).

The tokens handed in, with revoked or expired certificates, are handed over to the Security Officer and destroyed in accordance with the destruction scheme applicable within the Judicial Information Service.

4.2.1 Registration of Subscriber and Certificate Manager
The Ministry is initially registered as a Subscriber with KPN. The Ministry has appointed Certificate Managers responsible for managing server and group certificates within the Ministry. Employees of the Ministry who are appointed as certificate manager must submit an application via an authorised applicant. An overview of the active authorised applicants is available at the RA. The authorised applicant checks the identity of the employee on the basis of the employee's identity document (face-to-face check) and sends the application to the RA, including a copy of the identity document.

4.2.2 Applications for licences and certificates
The Ministry does not use Recognized Profession Certificates.

The various types of certificates (see the Ministry's supplement to Chapter 1.4.1 of this appendix) are applied for by qualified applicants from the Ministry and submitted by KPN RA employees for the purpose of issuing certificates. An authorised applicant may be appointed by an authorised signer. The RA employee checks whether the authorised signer has a mandate and whether the authorised applicant appears on the list or in the collection of approved applications for the function authorised applicant.

4.2.2.1 Application for personal Certificates and Group Certificates
The procedure of the CPS mentioned in section 4.2.2.1 does not apply.

The generic application procedure for personal and group certificates within the PKI service provision is as follows:
1. The application procedure starts with filling in the form "application form for personal or group certificate" by (intended) certificate holder/administrator and is submitted to the competent applicant of the Ministry.
2. The competent applicant will sign the application and send it to the RA.
3. The RA employee checks the application for completeness and accuracy and approves or rejects it.
4. The RA employee records the application data in the Card Management System (CMS).
5. The RA employee (validator) finally approves the application in the CMS.

4.2.2.2 Application Professional Certificates
The Ministry does not make use Recognized Profession Certificates.

4.2.2.3 Application for server certificates and group certificates
The application procedure for server certificates within the PKI service is as follows:
1. The application procedure starts with filling in the form "application for server certificate" by the certificate administrator and is submitted to RA.
2. The RA employee checks the application for completeness and accuracy and approves or rejects it.
3. The RA employee records the application data in the CMS.
4. The RA employee (validator) finally approves the application in the CMS.

4.2.3 Licence processing time
The Ministry has set up its own RA within its organisation.

The processing of applications for certificates by the RA is one working day after receipt of the application for a certificate. The total processing time for processing a certificate application, including KPN's processing time, is a maximum of fifteen working days.

4.3.1 Issuance of Personal Certificates and Group Certificates
The Ministry has set up its own RA within its organisation.
After KPN has created the personal/group certificate and put the required data on the token, the certificate will be delivered to the RA of the Ministry. The RA of the Ministry issues the certificates after verifying the identity of the certificate manager/ certificate holder. During this check, the certificate manager / certificate holder must be in possession of the PINmailer and the identity document with which the application has been submitted. Only then can the certificate be issued.

4.3.2 Issuance of Professional Certificates
The Ministry does not use Recognized profession Certificates.

4.3.3 Issuance of Server Certificates
In the case of applications made by registered certificate managers, KPN will make the created Certificates available to the RA of the Ministry. The RA employee forwards the relevant certificate to the certificate manager.

4.3.4 Notification of certificate production to the Certificate Holder or Manager
The Certificate Holder or the Certificate Manager is informed by KPN via email of the production of the Certificate.

4.4.1 Acceptance of Recognized profession certificates, Personal and Group Certificates
The Ministry does not use Recognized profession Certificates.
The Ministry RA issues the certificates.

4.4.2 Acceptance of Server Certificates
After final approval of the application in the CMS, the server certificate will be generated and KPN will make the server certificate available in the CMS so that it can be issued by the RA to the certificate manager who submitted the application.

In the case of a server certificate, a PINmailer with a revocation code is only created for the revocation. KPN sends the PINmailer to the RA in a secure manner. KPN takes care of this process. KPN will inform the certificate manager by email:
That the PINmailer is sent to the RA; that the certificate manager must make an appointment to receive the PINmailer.

4.9.2 Who may make a request for revocation?
The following entities are authorised to apply for revocation:
The Certificate holder;
The Subscriber;
The authorized applicant;
The certificate manager;
The Trust Service Provider TSP (KPN B. V.).

All authorised signatory managers at the Ministry are qualified applicants. In addition, authorised signatory managers may appoint other employees as authorised applicants. For this purpose, a process has been set up whereby RA employees can check the identity of the authorised applicant and verify whether the relevant authorised applicant has been registered by an authorised signatory manager.

4.9.3 Procedure for a request for revocation

A request for revocation or notification of a circumstance that may lead to the revocation of a Certificate must be made within the PKI service provider by the following means:

Online: https://minjus-portal.managedpki.nl

Written: Judicial Information Service
PKI department
Post box 695
7600 AR Almelo

The entity requesting the revocation of a certificate shall do so by means of
KPN URL's self-service portal: https://minjus-portal.managedpki.nl (and by means of the revocation code) or
the revocation form for revoking certificates either
by telephone or in person to/with the RA of the Ministry.

The applicant's authority to revoke certificates is verified by the RA.
In case of a revocation request directly to the RA by telephone, the data is checked by a number of identifying questions and then called back for verification. The reason for revocation of the certificate shall be asked.
In the event of a revocation request being made directly to the RA by e-mail, the details of the certificate holder will be stated on the e-mail and, if necessary, a request will be returned by e-mail for additional information. Subsequently, a call back by phone is made for verification. The reason for revocation of the certificate shall be asked.

In the event of a request for revocation made in person to the RA, the identity document will be used to verify the identity of the person. The reason for revocation of the certificate shall be asked.

Emergency procedure
In the event of serious disruptions to the RA station and the self-service portal, KPN can manually revoke certificates on the Ministry's CA.
If necessary, a Certificate Holder and/or an RA employee can contact an authorised person who may start the emergency procedure for KPN. The authorised person instructs the revocation by means of a signed email (legally valid digital signature) giving first names, surname, email address and common name of the passport holder and passport number. KPN has been informed of the persons authorised by the Ministry.
This emergency procedure is not intended to be used during maintenance moments on equipment of the Ministry. It is expected that during maintenance backup systems will be available to allow revocation to remain possible.

4.9.4 Duration for processing revocation request

The revocation by the certificate holder should preferably take place via KPN's self-service portal. This is subject to a maximum processing time of four hours.

Other revocation options are also available:
- Written or by e-mail to RA of the minsterie;
- Telephone call to RA of the Ministry;
- Personally with RA ven the Ministry.

These reports are processed on the basis of best effort.

5 Management, operational and physical security measures

The physical, procedural and personal security measures of the RA division of the Ministry are detailed in more detail in the IdM Information Security Plan[3] of the Judicial Information Service.

5.1.1 Location, construction and physical protection

The Ministry shall ensure adequate physical protection to minimise the risks of loss, damage and compromise of the RA service provision. This applies in particular to the RA environment, where the certificates are issued and managed.
The physical security measures comply with the Baseline Information Security[4] of the Ministry and have been determined based on a risk analysis of the RA service provision. These security measures are included in the Information Security Plan IdM[3].

5.1.4 Waste disposal

The Ministry has taken measures to securely destroy confidential data in accordance with the general procedures of the Ministry[4].

5.2 Procedural security procedure

The procedural security measures are further detailed in the Information Security Plan IdM[3].

5.2.1 Confidential functions

The staff security measures are further detailed in the Information Security Plan IdM[3].

5.2.4 Separation of functions

The organisational security measures are detailed in the Information Security Plan IdM[3] and the internal procedures for applying for and issuing certificates[2].

5.2.5 Professional knowledge, experience and qualifications

The Judicial Information Service has determined for RA employees what knowledge and experience is required for a good implementation. This is laid down in the job descriptions of the RA functions.

5.2.6 Trusted Employee Policy

All ministry officials take an oath or promise. The RA employees are also in possession of a VOG. This VOG is not older than six months on employment and is re-applied every three years.

5.4.3 Protection of archives

The RA of the Ministry archives application and revocation forms, copies of Wid documents and other relevant information. These documents are safely stored in a safe. See also the Ministry's Information Security Plan IdM[3] and the Ministry's internal procedures[2].

5.8 TSP termination

Upon expiry of the current agreement or premature termination of the agreement, both parties shall, in consultation with each other and under the ultimate responsibility of KPN, carry out those activities that are necessary to terminate the service provision in an appropriate manner, in accordance with the relevant legislation and regulations. In the implementation of these activities, it will be important which party will terminate its services and what their respective roles will be. As a minimum, the following activities will have to be carried out:

- Aligning and assessing, with due observance of appropriate deadlines, how the agreement should be adapted and continued in order, for example, to continue to provide services or to carry out the transfer and appropriate archiving of relevant data.
- Analysis, coordination, planning and implementation of appropriate communication to all parties involved, including, but not limited to, Certificate Holders, Relying Parties and the Certifying Institutions.

- The (potentially) revocation of all certificates, with attention for the moment and the manner in which they were issued. The maintenance of the CRL and the CA keys up to at least the legal term set for them and then their dismantling, the archiving and possible transfer of certificate creation and revocation data.
- Withdrawal of authorisations, dismantling of the existing CMS application (and associated infrastructure), making the desired number of copies of application software, relevant data and documentation, possibly transferring them to the other party and then cleaning the media used. This is done by drawing up an official report.
- Termination of agreements with suppliers.
- Collecting, if necessary, by compiling a report, transferring and archiving application files in an appropriate manner.
- Analysis, collection, archiving and, if necessary, transmission of all documents that can demonstrate that the management system has functioned appropriately during the years of the stopping party's operation.
- Change and publish the CPS during (and after) the termination period.

6.1.2 Transfer of Private Key and SSCD to Subscriber

The certificate holder agrees with the terms of use and signs them on the date of issue.
RA employee checks data on token with the identity of certificate holder.
RA employee issues token to certificate holder with, if applicable, the card reader.
The RA employee archives the signed user conditions.

6.1.5 Key lengths

The key length of a Certificate shall be at least 2048 bits RSA. The key length of a CA certificate is 4096 bits RSA.

The algorithms and key lengths used meet the requirements as defined in ETSI TS 102 176-1 standard[5]. The lengths of the public and private keys within the PKI Services are:

Type of certificate	Keylength	Hash method
CA certificates	RSA 4096	SHA 256
Personal certificates	RSA 2048	SHA 256
Group certificates	RSA 2048	SHA 256
Server certificates	CSR 2048	SHA 256

6.4 Activation data

6.4.1 Generating and installing activation data

The PINmailer (PIN-mail) is generated by KPN's CMS system.

7 Certificate, CRL and OCSP

7.1 Certification Profiles

7.1.1 CP OID

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

Personal Certificates:

2.16.528.1.1003.1.2.5.1	Authenticity certificate

2.16.528.1.1003.1.2.5.2	Non repudiation certificate
2.16.528.1.1003.1.2.5.3	Confidentiality certificate

Server certificates:

2.16.528.1.1003.1.2.5.6	Server certificate

Group certificates:

2.16.528.1.1003.1.2.5.4	Authenticity certificate
2.16.528.1.1003.1.2.5.5	Confidentiality certificate

7.1.2 Overview Certificate Profiles
The PKIoverheid Certificates are structured according to the PKIX X. 509 v3 standard, whereby extensions can be used.

Signature certificates are built up according to the EESSI/ETSI Qualified Certificate Profile. Any extensions within this framework shall also be included in the other Certificates.
Certificate Profiles have been drawn up in accordance with Part 3 of the PKI government's Programme of Requirements, in accordance with the Certificate Profile of the Certificate for the Domain Organisation.

7.1.2.1 Personal certificates

Basic attributes

Field	Value
Version	2 (X.509v3)
SerialNumber	Unique 128 bits long serial number
Signature	The used algorithm is sha256WithRSAEncryption
Issuer	Contains the name of the CA concerned and is represented by the following attributes: CommonName, OrganizationName en CountryName. There are/have been several CA certificates in use. • 'Getronics CSP Justitie CA - G2 '. The OrganizationName contains 'Getronics Nederland BV'. The CountryName is set to 'NL'. • 'KPN CSP Justitie CA – G2'. The OrganizationName contains 'KPN Corporate Market BV'. The CountryName is set to 'NL'.
Validity	De geldigheidsperiode van het Certificaat is ingesteld op 5 jaar.
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 (subjectserienummer). The attributes used to describe the subject name the subject in a unique way. The CountryName attribute is set to a two-letter country code according to

	ISO 3166. The CommonName is filled in as stated in the WID document that is submitted with the identification of the subject.
subjectPublicKeyInfo	Contains the Subject's PublicKey

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 Signature Certificates, the non-Repudiation bit is uniquely included.
BasicConstraints	Yes	The CA bit is set to 'False' en pathLenConstraint to 'none'
CertificatePolicies	No	Authenticity certificates contain the OID: 2.16.528.1.1003.1.2.5.1. Signature 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.
SubjectAltName	No	This includes • the subject's e-mail address; • the OID of the CA concerned; • The subject serial number of the Certificate Holder. Thee OID's of the concerning CA's are: • de KPN CSP Organisatie CA tbv Ministerie van Justitie en Veiligheid – G2; 2.16.528.1.1003.1.3.5.9.2 • of de Getronics CSP Organisatie CA tbv Ministerie van Justitie en Veiligheid – G2; 2.16.528.1.1003.1.3.5.4.2 Authenticity certificates may also contain a UPN for Windows Smartcard Logon.
CrlDistributionPoints	No	Contains the URI value from which the CRL belonging to the Certificate type can be retrieved.
ExtendedKeyUsage	No	Authenticity 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 on the relevant Certificate to be retrieved with the OCSP response.

Private extensions

Field	Critical	Value
QCStatements	No	Signature certificates contain the indication that they have been issued in accordance with European Directive 99/93/EC.

7.1.2.2 Server- & Group certificates

Basic attributes

Field	Value
Version	2 (X.509v3)
SerialNumber	Unique 128-bit long Certificate number
Signature	The used algorithm is sha256WithRSAEncryption
Issuer	Contains the name of the CA concerned and is represented by the following attributes: CommonName, OrganizationName en CountryName. There are/ have been several CA certificates in use • 'Getronics CSP Justitie CA - G2 '. The OrganizationName contains 'Getronics Nederland BV'. The CountryName is set to 'NL'. • 'KPN CSP Justitie CA – G2'. The OrganizationName contains 'KPN Corporate Market BV'. The CountryName is set to 'NL'.
Validity	The validity period of the Services Certificate is set to 3 years.
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 (subjectserienummer); • Locality; • State. Optionally, the attribute OrganizationUnit can also be included. The CommonName contains the primary name of the Service, for example a DNS or group name. 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.
subjectPublicKeyInfo	Contains the PublicKey van de Subject

Standaard 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 server certificates, the digital signature, keyAgreement and Key Encipherment bits are included in a unique way.
BasicConstraints	Yes	The CA bit is set to 'False' en pathLenConstraint to 'none'
CertificatePolicies	No	• Authenticity certificates contain the OID 2.16.528.1.1003.1.2.5.4. • Confidentiality certificates contain the OID 2.16.528.1.1003.1.2.2.5.5. • Confidentiality certificates of server connections contain the OID 2.16.528.1.1003.1.2.2.5.6. All types of certificates contain a link to the CPS and a user text.
SubjectAltName	No	This includes the OID of the CA: • 2.16.528.1.1003.1.3.5.4.2 and the subject number of the certificate holder. Confidentiality Certificates and Authenticity 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. Server certificates can contain this extension. This makes it possible to use the Certificate for systems that require the use of this extension.
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.

7.2 CRL-profiles

The CRL (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 CRL's layout and format, as well as the principle underlying the CRL, in accordance with the interests of the parties involved.

7.2.1 Personal certificates

Attributes

Field	Value
Version	1 (X.509 versie 2)
signatureAlgorithm	Sha256WithRSAEncryption

Issuer	Contains the name of the CA concerned and is represented by the following attributes: CommonName, OrganizationName en CountryName. There are/have been several CA certificates in use. • 'Getronics CSP Justitie CA - G2 '. The OrganizationName contains 'Getronics Nederland BV'. The CountryName is set to 'NL'. • 'KPN CSP Justitie CA – G2'. The OrganizationName is set to 'KPN Corporate Market BV'. 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 15 minutes and published after generation.
revoked certificates	the revoked certificates with certificate serial number and date of revocation and possible reason for revocation.

CRL extensions

Field	Value
AuthorityKeyIdentifier	Contains a160 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

Veld	Waarde
Serial Number	Contains the certificate serial number of the revoked certificate.
Revocation Date	Contains dat and time of revocation.

7.2.2 Server certificates en Group certificates

The design and format of the CRL for server certificates and group certificates are the same as for personal certificates.

7.3 OCSP-profiles

7.3.1 OCSP-profiles

The OCSP Responder conforms to RFC 6960.

7.3.2 OCSP fields

KPN does not use a unique time indication (nonce) in its OCSP response that optionally demonstrates the freshness of the response, even if the OCSP request contains such a time indication. However, the user system can use its local system clock to check the freshness of the OCSP response.

8 Conformity assessment

For the RA function of the minsterie, a partial certificate has been issued by BSI Group The Netherlands B. V. The scope of this RA audit concerns the processes that are necessary to fulfil the RA function of the PKI Service Provision by the Ministry and is laid down in the Overview of Applicabillity[6].

9 General and legal provisions

The Ministry does not use AMP services.

9.4 Confidentiality of personal data

At the Ministry, the measures with regard to confidentiality of personal data are further detailed in the document Baseline information security[4].

9.4.1 Privacy Statement
The measures with regard to the confidentiality of personal data are detailed in more detail in the document Baseline Information Security[4].

9.4.6 Transmission of data as a result of a legally valid summons
In the case of the Ministry, confidential information will not be disclosed unless there is a legal obligation to do so.

9.4.7 Provision of private law evidence
In the case of the Ministry, confidential information will not be disclosed unless there is a legal obligation to do so.

9.4.8 Distribution at the request of the owner
KPN does not provide any personal data. Within the PKI service, the personal data is managed by RA of the Ministry.

9.13 Dispute resolution
Complaints concerning the RA service provision can be submitted to the RA service provider as described in chapter 1.6 of this Annex.

Ministerie van Veiligheid en Justitie APPENDIX 1: List with references

[1]	KPN B.V., Certification Practice Statement PKIoverheid, versie 4.23, d.d. 1 april 2014.
[2]	Ministerie van Veiligheid en Justitie, RA-PKI-DI-RA Processen en procedures Certificaten, versie 1.1.
[3]	Ministerie van Veiligheid en Justitie, Informatiebeveiligingsplan IdM, versie 1.1.
[4]	Ministerie van Veiligheid en Justitie, Baseline Informatiebeveiliging Rijksdienst, versie 1.0 d.d.1 december 2012.
[5]	ETSI TS 107-176-1, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, V2.0.0., d.d. November 2007.
[6]	KPN Corporate Market B.V., OoA KPN-Justid versie 4.1, v1.0, 17 november 2015

Appendix 2 Practices Multi-Post

5.1 Physical protection

5.1.1 Location, construction and physical protection

The work outsourced to Multi-Post will be carried out from the secure premises of Multi-Post in Dordrecht. Physical access to this property is achieved through an appropriate combination of organisational, procedural and technical measures.

Internal regulations are in force, including for registering and supervising visitors and service personnel of third parties and a clean desk policy.

Appendix 3 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 Professional 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 Professional 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: 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 professional 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 professional 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 Confidential 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 (PvE). 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 withdrawal 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 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 (SSCD, 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 Confidential 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: http://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 Certificaate 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 the PKI government. 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 the PKI government 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 fulfill 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 the PKI government (PvE 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 apply to all parties involved in the issue and use of PKIoverheid Certificates.

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 (professional certificate holder) or a citizen and, in that capacity, a subscriber and thus the contracting party.

PKI for the government, the Public Key Infrastructure of the State of the Netherlands (also known as the PKI government): 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 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 a encrypted message.

Professional Certificate: a combination of two Non-Qualified Certificates stored on an SSCD, which together support the functions of authenticity and confidentiality, as well as a Qualified Certificate that

supports the function of Unrepudiation, 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 (PvE Part 3a) applicable within the PKI government.

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 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).

Recognised profession: Professional certificate holders must exercise a recognised profession in order to apply for Certificates within the PKI government. In this context, a recognised profession is a profession which is mentioned in the program of PKI government 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 the PKI government originates. There is no higher CA from which confidence is derived. This Certificate is signed by the Certificate Holder (within the PKI government 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 on the basis of, for example, CP and other documents. The Root-CA does not necessarily have to be positioned at the top of a hierarchy.

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

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 SUD is used for service certificates. Also and SUD can be a smart card or a USB token.

A smart card or USB token is called SSCD 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 an 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 on the basis of the Certificate Policy Services in force within the PKI government (PvE 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 (Organisationrelated 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.

Unrepudiation: 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 4 Abbrevations

Abbrevation	Meaning
CA	Certificatie Autoriteit (Certification Authority)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificaten Revocatie Lijst
CSP	Certification Service Provider ofwel Certificatiedienstverlener
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunication Standardisation Institute
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OPTA	Onafhankelijke Post- en Telecommunicatie Autoriteit
PIN	Persoonlijk Identificatie Nummer
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Persoonlijk Unlock Kengetal
PvE	(PKIoverheid) Programma van Eisen
RA	Registratie Autoriteit (Registration Authority)
SSCD	Secure Signature Creation Device
SUD	Secure User Device
Wji	Wet justitiële informatie
Wbp	Wet bescherming persoonsgegevens (Dutch Personal Data Protection Act)
Wid	Wet op de identificatieplicht (Dutch Compulsory Identification Act)