Registration Authority Practices Statement

certSIGN OV TLS certificates

KPN B.V.

KPN BV
Postbus 46
6800 AA Arnhem
www.kpn.com
K.v.K. ‘s Gravenhage nr. 27124701
NL009292056B01

Datum 3-11-2026
Versie version 2.4

Publication date 6-11-2026

Version history

Version	Document date	Changes
0.8	02-11-2022	Initial version for internal review
0.9	18-11-2022	Updated based on internal review
1.0	09-01-2023	Approved by PMA
2.0	18-12-2023	Change issuing root from ‘certSIGN ROOT CA’ to ‘certSIGN ROOT CA G2’
2.1	12-12-2024	Annual review
2.2	19-03-2025	Added training requirements Validation Specialists, changed servicedesk emailadress, Revocation Request processing time, monitoring systems and networks and minor cleanups
2.3	06-01-2026	Annual review. Clarify the processing of Revocation Requests and minor cleanups.
2.4	03-11-2026	Conformity Assessment Body transfer from BSI to Attestic, several URL changes, clarification of the different roles and minor cleanups based on observations during ETSI-audit. Location updated due to move from Apeldoorn to Arnhem.

Table of contents

1. Introduction 8

1.1 Overview 8
1.2 Document name and identification 8
1.3 PKI participants 8
1.3.1 Certification authorities 8
1.3.2 Registration authorities 8
1.3.3 Subscribers 8
1.3.4 Relying parties 9
1.3.5 Other participants 9
1.4 Certificate usage 9
1.4.1 Appropriate Certificate Uses 9
1.4.2 Prohibited certificate uses 9
1.5 Policy administration 9
1.5.1 Organisation administering the document 9
1.5.2 Contact Person 9
1.5.3 Person Determining RPS suitability for the policy 10
1.5.4 RPS Approval Procedures 10
1.6 Definitions and acronyms 10

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 11

2.1 Repositories 11
2.2 Publication of certification information 11
2.3 Time or frequency of publication 11
2.4 Access controls on repositories 11

3. Identification and authentication 12

3.1 Naming 12
3.1.1 Types of names 12
3.1.2 Need for names to be meaningful 12
3.1.3 Anonymity or pseudonymity of subscribers 12
3.1.4 Rules for interpreting various name forms 12
3.1.5 Uniqueness of names 12
3.1.6 Recognition, authentication, and role of trademarks 12
3.2 Initial identity validation 13
3.2.1 Method to prove possession of private key 13
3.2.2 Authentication of organization identity (Subscriber authentication) 13
3.2.3 Authentication of individual identity 14
3.2.4 Non-verified subscriber information 15
3.2.5 Validation of the authority 15
3.2.6 Criteria for interoperation 15
3.3 Identification and authentication for re-key requests 15
3.3.1 Identification and authentication for routine re-key 15
3.3.2 Identification and authentication for re-key after revocation 15
3.4 Identification and authentication for revocation request 15

4. Certificate Life-Cycle Operational Requirements 17

4.1 Certificate application 17
4.1.1 Who can submit a certificate application? 17
4.1.2 Enrolment process and responsibilities 17
4.2 Certificate application processing 17
4.2.1 Performing identification and authentication functions 17

4.2.2 Approval or rejection of certificate applications 17
4.2.3 Time to process certificate applications 18
4.3 Certificate Issuance 18
4.3.1 CA actions during certificate issuance 18
4.3.2 Notification to subscriber by the CA of issuance of certificate 18
4.4 Certificate Acceptance 18
4.4.1 Conduct constituting certificate acceptance 18
4.4.2 Publication of the Certificate by the CA 18
4.4.3 Notification of certificate issuance by the CA to other entities 18
4.5 Key Pair and Certificate Usage 19
4.5.1 Subscriber private key and certificate usage 19
4.5.2 Relying party public key and certificate usage 19
4.6 Certificate renewal 19
4.6.1 Circumstance for certificate renewal 19
4.6.2 Who may request renewal 19
4.6.3 Processing certificate renewal requests 19
4.6.4 Notification of new certificate issuance to subscriber 19
4.6.5 Conduct constituting acceptance of a renewal certificate 19
4.6.6 Publication of the renewal certificate by the CA 19
4.6.7 Notification of certificate issuance by the CA to other 19
4.7 Certificate re-key 19
4.7.1 Circumstance for certificate re-key 20
4.7.2 Who may request certification of a new public key 20
4.7.3 Processing certificate re-keying requests 20
4.7.4 Notification of new certificate issuance to subscriber 20
4.7.5 Conduct constituting acceptance of a re-keyed certificate 20
4.7.6 Publication of the re-keyed certificate by the CA 20
4.7.7 Notification of certificate issuance by the CA to other 20
4.8 Certificate modification 20
4.8.1 Circumstance for certificate modification 20
4.8.2 Who may request certificate modification 20
4.8.3 Processing certificate modification requests 20
4.8.4 Notification of new certificate issuance to subscriber 20
4.8.5 Conduct constituting acceptance of modified certificate 21
4.8.6 Publication of the modified certificate by the CA 21
4.8.7 Notification of certificate issuance by the CA to other 21
4.9 Certificate Revocation and Suspension 21
4.9.1 Circumstances for revocation 21
4.9.2 Who can request revocation? 22
4.9.3 Procedure for revocation request 22
4.9.4 Revocation Request Grace Period 22
4.9.5 Time within which RA processes the Revocation Request 22
4.9.6 Revocation checking requirement for Relying Parties 22
4.9.7 CRL Issuance Frequency 22
4.9.8 Maximum Latency for CRLs 23
4.9.9 On-line revocation status checking availability 23
4.9.10 On-line Revocation Checking Requirements 23
4.9.11 Other forms of revocation advertisements available 23
4.9.12 Special requirements related to key compromise 23
4.9.13 Circumstances for suspension 23
4.9.14 Who can request suspension 23
4.9.15 Procedure for suspension request 23
4.9.16 Limits on suspension period 23

4.10 Certificate Status Services 23
4.11 End of subscription 23
4.12 Key Escrow and Recovery 24
4.12.1 Key escrow and recovery policy and practices 24
4.12.2 Session key encapsulation and recovery policy and practices 24

5. Facility, Management, and Operational Controls 25

5.1 Physical controls 25
5.1.1 Site location and construction 25
5.1.2 Physical Access 25
5.1.3 Power and Air Conditions 26
5.1.4 Water Exposures 26
5.1.5 Fire Prevention and Protection 26
5.1.6 Media storage 26
5.1.7 Waste disposal 26
5.1.8 Off-site backup 26
5.2 Procedural Controls 26
5.2.1 Trusted Roles 26
5.2.2 Number of persons required per task 26
5.2.3 Identification and authentication for each role 27
5.2.4 Roles requiring separation of duties 27
5.3 Personnel Controls 27
5.3.1 Qualifications, experience, and clearance requirements 27
5.3.2 Background check procedures 27
5.3.3 Training requirements 28
5.3.4 Retraining frequency and requirements 28
5.3.5 Job rotation frequency and sequence 28
5.3.6 Sanctions for unauthorized actions 28
5.3.7 Independent contractor requirements 28
5.3.8 Documentation supplied to personnel 28
5.4 Audit logging procedures 28
5.4.1 Types of events recorded 28
5.4.2 Frequency of processing log 29
5.4.3 Retention period for audit log 29
5.4.4 Protection of the audit Log 29
5.4.5 Audit log back up procedures 29
5.4.6 Audit collection system (internal vs. external) 29
5.4.7 Notification to event-causing subject 30
5.4.8 Vulnerability assessments 30
5.5 Records Archival 30
5.5.1 Types of records archived 30
5.5.2 Retention period for archive 30
5.5.3 Protection of archive 30
5.5.4 Archive back-up procedure 30
5.5.5 Requirements for time-stamping of records 30
5.5.6 Archive collection system (internal or external) 30
5.5.7 Procedures to obtain and verify archive information 31
5.6 Key Changeover 31
5.7 Compromise and Disaster Recovery 31
5.7.1 Incident and compromise handling procedures 31
5.7.2 Computing resources, software, and/or data are corrupted 31
5.7.3 Entity private key compromise procedures 31
5.7.4 Business continuity capabilities after a disaster 31

5.8 RA termination 31
6. Technical Security Controls 32
6.1 Key pair generation and installation 32
6.1.1 Key pair generation 32
6.1.2 Private key delivery to subscriber 32
6.1.3 Public key delivery to certificate issuer 32
6.1.4 CA public key delivery to relying parties 32
6.1.5 Key sizes 32
6.1.6 Public key parameters generation and quality checking 32
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 32
6.2 Private Key Protection and Cryptographic Module Engineering Controls 32
6.2.1 Cryptographic module standards and controls 32
6.2.2 Private key (n out of m) multi-person control 32
6.2.3 Private key escrow 33
6.2.4 Private key backup 33
6.2.5 Private key archival 33
6.2.6 Private key transfer into or from a cryptographic module 33
6.2.7 Private key storage on cryptographic module 33
6.2.8 Method of activating private key 33
6.2.9 Method of deactivating private key 33
6.2.10 Method of destroying private key 33
6.2.11 Cryptographic Module Rating 33
6.3 Other aspects of Key Pair Management 33
6.3.1 Public key archival 33
6.3.2 Certificate operational periods and key pair usage periods 33
6.4 Activation Data 34
6.4.1 Activation data generation and installation 34
6.4.2 Activation data protection 34
6.4.3 Other aspects of activation data 34
6.5 Computer security controls 34
6.5.1 Specific computer security technical requirements 34
6.5.2 Computer security rating 34
6.6 Life cycle technical controls 34
6.6.1 System development controls 34
6.6.2 Security Management controls 35
6.6.3 Life cycle security controls 35
6.7 Network Security Controls 35
6.8 Time-stamping 35
7. Certificate, CRL and OCSP profiles 36
7.1 Certificate profile 36
7.1.1 Version number(s) 36
7.1.2 Certificate extensions 36
7.1.3 Algorithm object identifiers 36
7.1.4 Name forms 36
7.1.5 Name constraints 36
7.1.6 Certificate policy object identifier 36
7.1.7 Usage of Policy Constraints extension 36
7.1.8 Policy qualifiers syntax and semantics 36
7.1.9 Processing semantics for the critical Certificate Policies extension 36
7.2 CRL-profile 36
7.3 OCSP profile 36

8. Compliance Audit and Other Assessment 37

8.1 Frequency or circumstances of assessment 37
8.2 Identity/qualifications of assessor 37
8.3 Assessor's relationship to assessed entity 37
8.4 Topics covered by assessment 37
8.5 Actions taken as a result of deficiency 37
8.6 Communication of Results 38
8.7 Self-Audits 38

9. Other Business and Legal Matters 39

9.1 Fees 39
9.2 Financial Responsibility 39
9.3 As specified in the certSIGN Web CA OV - CPS.Confidentiality of Business Information 39
9.3.1 Scope of confidential information 39
9.3.2 Information not within the scope of confidential information 39
9.3.3 Responsibility to protect confidential information 39
9.4 Privacy of Personal Information 40
9.4.1 Privacy plan 40
9.4.2 Information treated as private 40
9.4.3 Information not deemed private 40
9.4.4 Responsibility to protect private information 40
9.4.5 Notice and consent to use private information 40
9.4.6 Disclosure pursuant to judicial or administrative process 40
9.4.7 Other information disclosure circumstances 40
9.5 Intellectual property rights 41
9.6 Representations and warranties 41
9.6.1 CA representations and warranties 41
9.6.2 RA representations and warranties 41
9.6.3 Subscriber representations and warranties 41
9.6.4 Relying party representations and warranties 41
9.6.5 Representations and warranties of other participants 41
9.7 Disclaimers of warranties 41
9.8 Limitations of Liability 42
9.9 Indemnities 42
9.10 Term and Termination 42
9.10.1 Term 42
9.10.2 Termination 42
9.10.3 Effect of termination and survival 42
9.11 Individual notices and communications with participants 42
9.12 Amendments 42
9.12.1 Procedure for amendment 42
9.12.2 Notification mechanism and period 42
9.12.3 Circumstances under which OID must be changed 43
9.13 Dispute Resolution Procedures 43
9.14 Governing Law 43
9.15 Compliance with Applicable Law 43
9.16 Miscellaneous Provisions 43
9.17 Other Provisions 43

Appendix 1 Definitions 44

Appendix 2 Abbreviations 47

1. Introduction

1.1 Overview

KPN B.V. is a Registration Authority (RA) for issuing of certSIGN OV TLS Certificates certificates. This Registration Practices Statement (RPS) outlines the procedures that KPN follows to comply with the certSIGN ROOT CA G2 – Certification Practice Statement and certSIGN Web CA for OV SSL Certificates – Certification Practice Statement (Web CA OV - CPS) as published on https://www.certsign.ro/en/repository/.

If any inconsistency exists between this RPS and the certSIGN CPSs, the certSIGN CPSs takes precedence.

1.2 Document name and identification

This document is the KPN B.V. Registration Practices Statement (RPS).

Formally this document is referred to as Registration Practices Statement certSIGN OV TLS certificates. In the context of this document, it is also referred to as 'RPS certSIGN', but usually shortly as 'RPS'. Where this abbreviation is concerned, this document is intended.

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

1.3 PKI participants

1.3.1 Certification authorities

certSIGN is the Certificate Authority (CA) for the ROOT CA G2 and subordinate Web CA.

1.3.2 Registration authorities

KPN is the Registration Authority (RA) and performs the validation and identity verification of the applicant when requesting a certificate. The domain validation is performed by the CA. Once the Registration Authority has provided approval, then the CA can issue the certificate to the applicant. Once the certificate is issued, the applicant becomes the Subscriber.

1.3.3 Subscribers

The Subscriber is the organisation stated in the subject field of the Certificate.

Subscribers are required to act in accordance with this RPS, certSIGN Web CA OV - CPS and General Conditions KPN.

1.3.4 Relying parties

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

1.3.5 Other participants

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

1.4 Certificate usage

A digital certificate (or certificate) is formatted data that cryptographically binds an identified subscriber with a Public Key.
Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate was issued.

1.4.1 Appropriate Certificate Uses

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. This server must belong to the organizational entity named as the Subscriber in the certificate.

1.4.2 Prohibited certificate uses

Certificates validated under this RPS may not be used other than as described in the certSIGN Web CA OV - CPS.

1.5 Policy administration

1.5.1 Organisation administering the document

This RPS is managed by a dedicated Policy Management Authority (PMA) within KPN.

1.5.2 Contact Person

Information regarding this RPS and comments can be directed to:

KPN Identity services
Attn. Policy Management Authority
PO Box 46
6800 AA Arnhem

To notify KPN of a service outage or report a suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter

related to certificates, please contact:
pki.servicedesk@kpn.com

To request an urgent certificate revocation outside office hours (Mon-Fri, 9h-17h), please contact the servicedesk:
+31 88 – 661 06 21 (only for a revocation request)
esd.cic@kpn.com

For the revocation you need the following information:

- Common name
- Subject serial number
- Challenge phrase
- E-mail address

1.5.3 Person Determining RPS suitability for the policy

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

1.5.4 RPS Approval Procedures

Changes to the KPN RPS are approved by the CA certSIGN and the PMA within KPN, after consultation with the relevant stakeholders.

1.6 Definitions and acronyms

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

This RPS is published by KPN in the Repository on https://certificaat.kpn.com/support/downloads/repository/. All other repository responsibilities are the domain of the CA, see https://www.certsign.ro/en/repository/.

2.2 Publication of certification information

Not applicable.

2.3 Time or frequency of publication

Not applicable.

2.4 Access controls on repositories

Not applicable.

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

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards for subjectName. KPN will provide name elements pertaining to subscribers in accordance with the Web CA OV - CPS.

3.1.2 Need for names to be meaningful

The structure of the Distinctive Name is approved / designated and checked by by KPN as stipulated in the Web CA OV - CPS.

3.1.3 Anonymity or pseudonymity of subscribers

The use of pseudonyms is not allowed.

3.1.4 Rules for interpreting various name forms

As stipulated in the Web CA OV - CPS.

3.1.5 Uniqueness of names

As stipulated in the Web CA OV - CPS.

3.1.6 Recognition, authentication, and role of trademarks

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

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

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

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

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The server certificate key pair is created by or on behalf of the Subscriber in the Subscriber's Secure Environment and entered on the (HTTPS) website of KPN. To ensure that that has indeed happened, the Subscriber must sign for this on the Certificate Request form for the Server Certificate.

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 Subscriber Registration. This form contains an extensive explanation. With this form the Subscriber must send along several supporting documents.

The information requested is:

- The Chamber of Commerce number;
- Name of the subscriber. The Subscriber may, if desired, use a trade name, provided that it is registered;
- Subscriber contact information;
- Name and function of his authorized representative;
- Billing data;
- Data of the contact to be authorized, such as name and contact details;
- Copy of the identity of the (Delegated) Authorized Representative(s) that meets the requirements of the Dutch Identification Act (hereafter Wid).

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

- to have filled in the Subscriber Registration application completely and truthfully, agreeing to the Special Conditions,
- that the Delegated Authorized Representative(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) 910/2014 of the European Parliament amended by Regulation (EU) 2024/1183 (eIDAS).

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

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

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

Changes which must be communicated are for example the departure of the Authorized Representative or contact or change in the contact of the Subscriber. For the communication of these changes forms available on the site (https://kpnpkio.managedpki.com/wijzigregistratie/ and https://kpnpkio.managedpki.com/wijzigcertbeheerder/). 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

KPN offers customers the ability to use a self-service portal. After registration (Delegated) Authorized Representatives can use the portal. The login is based on a 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.

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

Of the subscriber's organization:

- the subscriber number.

Of the (Delegated) Authorized Representatieve:

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

Of a new Certificate Manager:

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

Of an existing Certificate Manager:

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

Of the Certificate Signing Requets (CSR) at least:

- 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.
- locality and state/province;
- country name and country code in accordance with ISO 3166.

Validation of Domain Authorization or Control is performed by certSIGN as stipulated in the Web CA OV - CPS.

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

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

3.2.4 Non-verified subscriber information

The contact details represent non-verified subscriber information.

3.2.5 Validation of the authority

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

- checking the Chamber of Commerce registry for organisational applicants;
- where the applicant has been authorised by the legal representative of an organisation, authorisation must be completed, or there must be a completed authorisation available.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

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

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

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

Only the the Certificate Manager may submit a request to revoke a certificate. This can be done the Self Service Portal (https://www.kpn.com/zakelijk/pki-certificaten/intrekken).

The following information must be completed.

Of the (Delegated) Authorized Representative:

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

Of the Certificate:

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

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

The form "Certificate Revocation Request" will be accepted by KPN and reviewed for completeness and accuracy. If the application is complete and accurate, KPN sends the revocation request to certSIGN. This revocation will be executed within twenty four (24) hours after the receipt of the revocation request.

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

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application?

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

4.1.2 Enrolment process and responsibilities

To request a Server Certificate, you need a CSR (Certificate Signing Request) generated on your server. The CSR should be uploaded in the web Certificate Application form during the request.

The enrollment process, for a Certificate Applicant, includes the following:
• Completing the Certificate Application form;
• Uploading the CSR;
• Responding to authentication requests in a timely manner.

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 certSIGN Special Conditions, CPS and CP.

KPN is responsible for the registration services and guarantees Subscribers and Relying Parties that it will abide by the certSIGN Special Conditions, CPS and CP. KPN is responsible for the outsourcing to AMP regarding the identification of Certificate Managers.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

After receiving a certificate application, KPN verifies the application information and other information in accordance with Section 3.2. KPN creates and maintains records to establish that it has performed its required verification tasks and communicate the completion of such performance to certSIGN. Then certSIGN performs the domain validation as stipulated in the Web CA OV - CPS.

4.2.2 Approval or rejection of certificate applications

The Certificate Application for a Server Certificate is as follows:

1. The Certificate Manager creates the key pair (length is RSA 2048 bits or RSA 4096 bits) in the Subscriber's Safe Environment and sends a Certificate Signing Request (CSR) containing the Public Key. Subscriber completes the electronic application form certSIGN OV TLS Certificates. This form can be found on the KPN website (https://www.kpn.com/zakelijk/pki-certificaten/certsign-ov/aanvragen). This site also contains further instructions on how to use the form.

3. KPN receives the Certificate Application and assesses the completeness and correctness of the Application. If this is not the case, KPN will contact the applicant and reject the relevant certificate application.
4. In addition, it is also assessed whether there is url-spoofing or phishing, therefore https://www.phishtank.com or similar will be consulted to see if the domain name does not appear on a spam and/or phishing blacklist. If KPN suspects phishing or other possible abuse, KPN will report this suspicion to https://www.phishtank.com.
5. KPN performs a pre-check on the CAA DNS record. certSIGN identifies itself as certSIGN.ro. If a domain owner wants KPN to be able to issue certificates for its domain, this identification must be included in the CAA record. certSIGN performs the final domain validation according to the permitted methods as described in the certSIGN CPS.
6. If KPN approves the Certificate Application, the Certificate is created and sent to the Certificate Manager by e-mail.

4.2.3 Time to process certificate applications

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

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

No stipulation.

4.3.2 Notification to subscriber by the CA of issuance of certificate

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

The Certificate Manager is explicitly informed of the production by sending the Server Certificate by e-mail to the specified e-mail address.

The Subscriber will be informed by e-mail or post of the creation and transmission of the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

Subscribers are required to protect their Private Keys from unauthorized use or disclosure, must discontinue using a Private Key after the expiration of all associated certificates or revocation of any associated certificates, and use Private Keys only as specified in the key usage extension.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

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

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other

Not applicable.

4.7 Certificate re-key

Subscriber keys shall not be reused after expiry of the validity period or after the corresponding Certificates have been revoked.

4.7.1 Circumstance for certificate re-key

Not applicable.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other

Not applicable.

4.8 Certificate modification

KPN does not offer any possibility to modification of OV TLS Certificates. A request for modification shall be treated as a request for a new certificate.

4.8.1 Circumstance for certificate modification

Not applicable.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

In the following cases, the Subscriber 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 PIN code and/or PUK code;
- errors in the content of the Certificate;
- changes in the information contained in the Certificate;
- Termination or bankruptcy of the organization of the Subscriber;

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

- the subscriber indicates that the original request for a certificate was not allowed and the subscriber does not give his consent with retroactive effect.
- KPN (or certSIGN) 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.
- A subscriber does not fulfil his obligations as set out in
  - the certSIGN CP and/or
  - corresponding CPS and/or
  - the agreement that KPN has concluded with the subscriber.
- KPN (or certSIGN) is informed or otherwise becomes aware of a material change in the information contained in the certificate.
- KPN (or certSIGN) determines that the certificate has not been issued in accordance with the certSIGN CP or CPS or the agreement entered into by KPN with the subscriber.
- KPN (or certSIGN) determines that information in the certificate is not correct or misleading.
- KPN (or certSIGN) is informed or becomes aware that the use of the domain name in the certificate is no longer legally permitted.

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.

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

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

4.9.2 Who can request revocation?

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

4.9.3 Procedure for revocation request

A request for revocation or notification of a circumstance that may lead to the revocation of a Certificate may be made online (Self Service Portal). The instruction is available at:
https://www.kpn.com/zakelijk/pki-certificaten/intrekken

It should be stressed that if the revocation serves an urgent interest or if the Self Service facility is unavailable, the revocation request should be done via the procedure described in section 1.5.2.

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

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

4.9.4 Revocation Request Grace Period

As specified in the certSIGNWeb CA OV - CPS.

4.9.5 Time within which RA processes the Revocation Request

KPN processes Revocation Requests via the Self Service Portal automatically and the urgent Revocation Requests manually in accordance with Section 4.9.3.

All Revocations are executed by certSIGN as specified in the certSIGN Web CA OV – CPS.

KPN, in collaboration with certSIGN, processes the revocation of certificates within twenty four (24) hours after receiving the request.

4.9.6 Revocation checking requirement for Relying Parties

As specified in the certSIGN Web CA OV - CPS.

4.9.7 CRL Issuance Frequency

As specified in the certSIGN Web CA OV - CPS.

4.9.8 Maximum Latency for CRLs

As specified in the certSIGN CA OV - CPS.

4.9.9 On-line revocation status checking availability

As specified in the certSIGN Web CA OV - CPS.

4.9.10 On-line Revocation Checking Requirements

As specified in the certSIGN Web CA OV - CPS.

4.9.11 Other forms of revocation advertisements available

No Stipulation.

4.9.12 Special requirements related to key compromise

As specified in the certSIGN Web CA OV - CPS.

4.9.13 Circumstances for suspension

Not applicable.

4.9.14 Who can request suspension

Not aplicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate Status Services

As specified in the certSIGN Web CA OV - CPS.

4.11 End of subscription

A Subscriber's subscription service ends if its certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. Facility, Management, and Operational Controls

KPN's Registration Authority business unit is certified against ISO9001:2015 and ISO27001:2013. Both the Quality Management System and the Information Security Management System are continuously focused on improving these systems through the PDCA cycle.

5.1 Physical controls

5.1.1 Site location and construction

The Registration Authority services are managed in and delivered from highly secure environments within data centers in Arnhem and Almere in the Netherlands. These environments complies with the laws and regulations in force for the government.

KPN's secure environment offers standard up to at least five physical barriers to the production environment.

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

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

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

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

5.1.2 Physical Access

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

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

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

5.1.3 Power and Air Conditions

See section 5.1.1.

5.1.4 Water Exposures

See section 5.1.1.

5.1.5 Fire Prevention and Protection

See section 5.1.1.

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site backup

Media containing data and software are also stored in an off-site datacenter, with as a minimum an equivalent level of security.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

5.2.2 Number of persons required per task

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

5.2.3 Identification and authentication for each role

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

5.2.4 Roles requiring separation of duties

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

Security duties and responsibilities, including confidential functions, are documented. These have been drawn up based on the segregation of duties and powers and in which the sensitivity of the function has been established.

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

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

KPN deploys personnel with sufficient expertise, experience and qualifications for performing RA activities.

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.

5.3.2 Background check procedures

KPN has drawn up and implemented a Trusted Employee Policy (TEP) for its RA activities. In formulating and maintaining this policy, the possibilities and impossibilities of generally applicable legislation and regulations such as the Dutch Civil Code, the GDPR and the European eIDAS Regulation.
This TEP includes, among others, a pre-employment screening (mandatory for those employees involved in the RA activities), the issuing of a Statement of Conduct (VOG) and the signing of a non-dislosure statement.
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.

5.3.3 Training requirements

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

Validation Specialist are trained on the job and must pass an exam before performing validation tasks.

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

KPN does not use this method.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

KPN maintains records for audit purposes of the following:

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

Logging takes place at a minimum:

- routers, firewalls and network system components;
- database activities and events;
- transactions;

- operating systems;
- access control systems;
- mail servers.

KPN keeps track of the following events manually or automatically

- Life cycle events regarding the management of certificates, including:
  - applications for certificates and revocation;
  - successful or unsuccessful processing of applications.
- Threats, including:
  - successful and unsuccessful attempts to gain access to the system
  - 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 RA.

The log files contain at least the following data:

- source addresses (IP addresses if available);
- target addresses (if available);
- date and time;
- User IDs (if available);
- name of the event;
- description of the event.

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

The log files are retained for at least 24 months.
The consolidated (electronic) audit logs are retained for a period of at least ten years.

5.4.4 Protection of the audit Log

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

5.4.5 Audit log back up procedures

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

External and internal vulnerability scans are carried out monthly. External and internal penetration tests are carried out at least annually.

5.5 Records Archival

5.5.1 Types of records archived

KPN records all relevant registration information, including at least

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

5.5.2 Retention period for archive

KPN retains all relevant documentation and information relating to a Certificate (revocation) request for a period of at least ten years.

5.5.3 Protection of archive

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

5.5.4 Archive back-up procedure

No stipulation.

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

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

5.5.7 Procedures to obtain and verify archive information

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

5.6 Key Changeover

As stipulated in the certSIGN Web CA OV - CPS.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

As stipulated in the certSIGN Web CA OV - CPS.

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

As stipulated in the certSIGN Web CA OV - CPS.

5.7.3 Entity private key compromise procedures

As stipulated in the certSIGN Web CA OV - CPS.

5.7.4 Business continuity capabilities after a disaster

certSIGN maintains CRL and OCSP access points that KPN in the role of RA and entities relying on the RA can use to access revocation information. In the event that the KPN RA operations is not available, certSIGN Administrators have the ability to directly access the CA systems to revoke certificates.

5.8 RA termination

The termination of the RA activities is subject to the agreements between KPN and certSIGN.

Before KPN terminates RA activities, KPN shall:
1. Provide notice and information about the termination by sending notice by email to its customers and by posting such information on https://www.kpn.com/zakelijk/pki-certificaten; and
2. Transfer all certificate responsibilities to certSIGN.

6. Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The Subscriber generates its key pair by itself. Key pair requirements are defined in the certSIGN Web CA OV - CPS.

6.1.2 Private key delivery to subscriber

The key pair is generated by the Subscriber in the Subscriber's Safe Environment. The Private Key remains in that Safe Environment, so it is not transferred.

6.1.3 Public key delivery to certificate issuer

The Subscriber sends the Public Key to KPN attached to an electronic application form and is linked to a unique Certificate Signing Request number (CSR number). After successful validation, KPN sends the request with the public key to the certificate issuer certSIGN.

6.1.4 CA public key delivery to relying parties

As stipulated in the certSIGN Web CA OV - CPS.

6.1.5 Key sizes

As stipulated in the certSIGN Web CA OV - CPS.

6.1.6 Public key parameters generation and quality checking

As stipulated in the certsSIGN Web CA OV - CPS.

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

As stipulated in the certSIGN Web CA OV - CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

As stipulated in the certSIGN Web CA OV - CPS.

6.2.1 Cryptographic module standards and controls

As stipulated in the certSIGN Web CA OV - CPS.

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

As stipulated in the certSIGN Web CA OV - CPS.

6.2.3 *Private key escrow*

No stipulation.

6.2.4 *Private key backup*

No stipulation.

6.2.5 *Private key archival*

No stipulation.

6.2.6 *Private key transfer into or from a cryptographic module*

No stipulation.

6.2.7 *Private key storage on cryptographic module*

As stipulated in the certSIGN Web CA OV - CPS.

6.2.8 *Method of activating private key*

As stipulated in the certSIGN Web CA OV - CPS.

6.2.9 *Method of deactivating private key*

As stipulated in the certSIGN Web CA OV - CPS.

6.2.10 *Method of destroying private key*

As stipulated in the certSIGN Web CA OV - CPS.

6.2.11 *Cryptographic Module Rating*

As stipulated in the certSIGN Web CA OV – CPS.

6.3 Other aspects of Key Pair Management

As stipulated in the certSIGN Web CA OV - CPS.

6.3.1 *Public key archival*

As stipulated in the certSIGN Web CA OV - CPS.

6.3.2 *Certificate operational periods and key pair usage periods*

As stipulated in the certSIGN Web CA OV - CPS.

6.4 Activation Data

6.4.1 Activation data generation and installation

As stipulated in the certSIGN Web CA OV - CPS.

6.4.2 Activation data protection

As stipulated in the certSIGN Web CA OV – CPS.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

The integrity of the RA 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.

6.5.2 Computer security rating

KPN classifies the resources used based on a risk assessment.

6.6 Life cycle technical controls

6.6.1 System development controls

KPN develops the RA workflow within a Certificate Management System (CMS) obtained from a specialist supplier. This CMS consists of many different, small modules, which can be combined in different order and composition into a working RA system. 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 CMS is obtained from a reliable supplier and is equipped with a CEN TS 419 261 audit report or equivalent.

6.6.2 Security Management controls

All operational systems and networks are real-time monitored, managed and controlled to ensure their correct operation. The integrity of systems is checked every 12 hours. Administrators are alerted to unexpected anomalies.

6.6.3 Life cycle security controls

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

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

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

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.

6.7 Network Security Controls

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

The network and certificate system security measures conforms to requirements from eIDAS Regulation (EU) No. 910/2014 amended by Regulation (EU) No. 2024/1183, ETSI EN 319 401 and ETSI EN 319 411-1.

6.8 Time-stamping

KPN's systems use a trusted source of time.

7. Certificate, CRL and OCSP profiles

7.1 Certificate profile

7.1.1 Version number(s)

As stipulated in the certSIGN Web CA OV - CPS.

7.1.2 Certificate extensions

As stipulated in the certSIGN Web CA OV - CPS.

7.1.3 Algorithm object identifiers

As stipulated in the certSIGN Web CA OV - CPS.

7.1.4 Name forms

As stipulated in the certSIGN Web CA OV - CPS.

7.1.5 Name constraints

Not applicable.

7.1.6 Certificate policy object identifier

As stipulated in the certSIGN Web CA OV - CPS.

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

As stipulated in the CA Web CA OV - CPS.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL-profile

As stipulated in the certSIGN Web CA OV - CPS.

7.3 OCSP profile

As stipulated in the certSIGN Web CA OV - CPS.

8. Compliance Audit and Other Assessment

8.1 Frequency or circumstances of assessment

KPN started on 1-1-2024 as a Registration Authority for certSIGN Web CA OV. Since then, KPN is annually audited to assess compliance with the certSIGN Web CA OV - CPS, eIDAS Regulation (EU) No. 910/2014 amended by Regulation (EU) No. 2024/1183, ETSI EN 319 401, ETSI EN 319 411-1, relevant CA/Browser Forum – Baseline Requirements, ISO 9001, ISO 22301 and ISO 27001.

8.2 Identity/qualifications of assessor

DNV GL Business Assurance B.V is the auditor for the ISO certifications. Attestic is the auditor for eIDAS Regulation (EU) No. 910/2014 amended by Regulation (EU) No. 2024/1183, ETSI EN 319 401, ETSI EN 319 411-1 and the relevant CA/Browser Forum – Baseline Requirements. certSIGN is the auditor for KPN's compliance with the applicable CPS.

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

The scope of the audit covers all requirements from the standards for the Registration Authority component services:

- Registration Service
- Revocation Management Service
- Dissemination Service (partly)

with subjects as:

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

8.5 Actions taken as a result of deficiency

In case of a deficiency, KPN will promptly notify the TSP certSIGN and addresses this nonconformity in a Corrective Action Plan (CAP). In the CAP the actions and planning are documented to resolve the nonconformity.

8.6 Communication of Results

The results of an audit are reported to the TSP certSIGN and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

8.7 Self-Audits

KPN performs regular self-audits to ensure that KPN is in compliance with this RPS. certSIGN performs regular self-audits to ensure that KPN is in compliance with the certSIGN Web CA OV - CPS.

9. Other Business and Legal Matters

9.1 Fees

Certification services fees and the types of services charged are published in the list of fees available at the address https://www.kpn.com/zakelijk/pki-certificaten/tarieven. Prices are set according to the internal price policy

9.2 Financial Responsibility

9.3 As specified in the certSIGN Web CA OV - CPS.Confidentiality of Business Information

9.3.1 Scope of confidential information

KPN shall protect the following as confidential information using a reasonable degree of care:

1. Internal procedures for handling and processing Subscription, Certificate applications and revocation requests;
2. Internal security procedures and measures;
3. Information and data on the RA systems and infrastructure;
4. Business continuity, incident response, contingency, and disaster recovery plans;
5. Information held by KPN as confidential information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports.

For personal data, see section 9.4.2.

9.3.2 Information not within the scope of confidential information

Information not listed as confidential is considered public information. Published certificate and revocation data is considered public information.

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of Personal Information

9.4.1 Privacy plan

KPN complies to the applicable privacy laws and regulations including the GDPR. KPN undergoes regular internal and external audits to verify its privacy compliance.

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

9.4.2 Information treated as private

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

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

9.4.3 Information not deemed private

Information included in Certificates is deemed pubic information and is not subject to protections outlined in section 9.4.2. Information in a certificate is not considered private or privacy act information.

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

Information that is not included in a certificate that is provided during the application or identity verification process is considered confidential. Unless otherwise stated in the certSIGN Web CA OV - CPS or RPS, a party shall only use information considered confidential after obtaining the subject's express written consent. All Subscribers must consent to the global transfer and publication of any personal data contained in a certificate.

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

As stipulated in the ROOT CA G2 certSIGN Web CA OV - CPS.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The CA offers the warranties described in the certSIGN Web CA OV - CPS.

9.6.2 RA representations and warranties

KPN operates the RA functions and complies with the stipulations as described in this RPS and the reference documents certSIGN Web CA OV - CPS, including:

- Performing identify verification of certificate applicants in accordance with Section 3.2.3;
- Maintaining its operations in conformance to the stipulations of the approved RPS;
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate;
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate;
- Ensuring that obligations are imposed on Subscribers, and that Subscribers are informed of the consequences of not complying with those obligations; and
- Revocation services (when applicable) and use of a repository conform to all material requirements of this RPS and the applicable CPS in all material aspects.

9.6.3 Subscriber representations and warranties

Subscribers must sign an agreement containing the requirements the Subscriber shall meet including protection of their private keys and use of the certificates before being issued the certificates.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

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

9.8 Limitations of Liability

KPN accepts liability for certSIGN Certificates as set out in the General Conditions KPN and certSIGN Web CA - Terms and conditions.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This RPS and any amendments to this RPS are effective when approved by the CA certSIGN and the PMA of KPN and remain in effect until replaced with a newer version.

9.10.2 Termination

This RPS and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of termination and survival

KPN shall communicate the conditions and effect of this RPS's termination in a manner mutually agreed to by the CA certSIGN and KPN. At a minimum, all responsibilities related to protecting confidential information will survive termination.

9.11 Individual notices and communications with participants

KPN communicates with individual participants mainly by email or telephone by the staff of the Validation department who, among other things, process and handle the Certificate applications. This department can be reached by +31 (0)88 661 05 00 or pkivalidation@kpn.com.

General communication is done via the service portal https://www.kpn.com/zakelijk/pki-certificaten or via documents available in the Repository https://certificaat.kpn.com/support/downloads/repository/.

9.12 Amendments

9.12.1 Procedure for amendment

This RPS is reviewed annually. Amendments are made by mutual agreement between the CA certSIGN and KPN, and may require ratification by the appropriate PMA.

9.12.2 Notification mechanism and period

Notices of amendments may be provided to the appropriate PMA but are not provided to any other third party.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute Resolution Procedures

As stipulated in the certSIGN Web CA OV - CPS.

9.14 Governing Law

KPN's services are governed by Dutch law. certSIGN Certification services is according to Romanian Law 455/2001.

9.15 Compliance with Applicable Law

The present RPS and provision of KPN services are compliant with relevant and applicable Dutch laws and Regulation EU 910/2014

9.16 Miscellaneous Provisions

No stipulation.

9.17 Other Provisions

No stipulation.

Appendix 1 Definitions

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.

CAA DNS Record: A Certificate Authority Authorization 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.

CA Certificate: a Certificate of a Certification Authority.

Certificate: the Public Key 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.

Certificate Application: the request submitted for the issue of a Certificate.

Certificate Manager: a natural person who is authorized to apply for, install, manage and/or revoke a Server Certificate on behalf of the Subscriber.

Certificate Profile: a description of the content of a Certificate.

Certificate Policy (CP): a named set of rules indicating the applicability of a Certificate for a particular community and/or application class with common security requirements. Using a CP, Subscribers and Relying Parties can determine how much confidence they can place in the relationship between the Public Key and the identity of the Public Key holder.

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, certSIGN therefore both operates as a CA and a TSP.

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

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

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.

Electronic Storage: location where relevant information regarding the services can be found.

For KPN, see: https://certificaat.kpn.com/support/downloads/repository/. For certSIGN, see: https://www.certsign.ro/en/repository/.

FQDN: Fully Qualified Domain 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'.

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.

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

Online Certificate Status Protocol: (OCSP): ainternet protocol used for obtaining the revocation status of an X.509 digital certificate

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

Private Key: the key of an asymmetric key pair that should only be known to its holder and kept strictly secret.

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.

Registration Authority (RA): a Registration Authority receives, checks and approves or rejects the registration and certificate issuance and revocation requests. In this respect, KPN therefore operaties as RA.

Registration Practice Statement (RPS): a document describing the procedures followed and measures taken by the RA in relation to the aspects of the registration and revocation services. The RPS describes how the RA meets the requirements as stated in the applicable CPS.

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 CA 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 originates. There is no higher CA from which confidence is derived.

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 Certificate) is self-signed, as a result of which it is not possible to authenticate the source of the signature on this Certificate, only the integrity of the content of the Certificate. However, the Root-CA is trusted based on, for example, CP and other documents.

Trusted Service Provider (TSP): The organization with the final responsibility for providing the Certification Services, whether it carries out the actual activities itself or subcontracts them to others.

Appendix 2 Abbreviations

Abbreviation	Meaning
CA	Certificatie Autoriteit (Certification Authority)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificates Revocation Lijst
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RPS	Registration Practice Statement
TLD	Top-Level Domain
TSP	Trust Service Provider
Wid	Wet op de identificatieplicht (Dutch Identification Act)