# PKI Disclosure Statement

v 5.4
June 25, 2021

## Contents


1 Summary 2

2 CA contact information 2

3 Type of certificates, validation procedures and certificate usage 2

4 Limitation of the use of the reliability of certificates (Reliance limits) 3

5 Obligations for subscribers 3

6 Obligations of the relying parties for the verification of the certificate status 3

7 Exclusion and liability limitation clauses 4

8 Applicable agreements, certification practice statement, certificate policy 4

9 Data protection directives 4

10 Reimbursement directives 5

11 Governing Law and settlement of disputes clauses 5

12 CA and certificate directory licenses, confidentiality trademarks and audit 5

13 Abbreviations and Terms 5

14 Document Information 6

## 1 Summary

The purpose of this PKI Disclosure Statement is to summarize and present the key points of the KPN PKI Overheid Certificate Practice Statements and specific conditions in a more readable and understandable format for the benefit of Subscribers and Relying Parties.

This PKI Disclosure Statement does not substitute or replace the KPN Certification Practice Statements under which digital certificates are issued.
Reader must read the KPN CPS:

- KPN PKIoverheid Certification Practice Statement

published at (https://certificaat.kpn.com/support/downloads/repository/) before applying for or relying on a certificate issued by KPN.

## 2 CA contact information

Queries regarding this PKI Disclosure Statement shall be directed at:

KPN B.V.
Attn.: KPN Security, Policy Management Authority
Postbus 9105
7300 HN Apeldoorn.
E-mail: pkio.servicedesk@kpn.com.

For general information please visit our website: https://certificaat.kpn.com/

To revoke a certificate, follow the procedures on the self-service portal:
https://certificaat.kpn.com/intrekken/

## 3 Type of certificates, validation procedures and certificate usage

KPN issues 5 types of certificates under the Public Root of PKIoverheid:

1. Personal certificates (Persoonlijke certificaten);
2. Profession bound certificates (Beroepsgebonden certificaten);
3. Group certificates (Groepscertificaten);
4. Server certificates (Servercertificaten);
5. Qualified Electronic Seal Certificates (eSeal certificaten).

And 2 types of certificate under the Private Root of PKI Overheid:
1. Private Services Server certificates;
2. Group certificates (Groepscertificaten).

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

The full description of the types of certificates supported by KPN and their respective validation procedures are covered in the KPN CPS document.

## 4 Limitation of the use of the reliability of certificates (Reliance limits)

KPN does not impose reliance limits for Certificates issued under this policy. Reliance limits may be imposed by other policies, Dutch applicable law or by Relying Party Agreement.
See Section 7 below for limitation of liability.

## 5 Obligations for subscribers

- Submit accurate and complete information to the CA during subject registration in accordance with the requirements of the CP;
- Exercise reasonable care to avoid unauthorized use of the Subject’s Private Key
- If any of the following occurs up to the end of the validity period indicated in the Certificate the subscriber must immediately revoke the certificate:
    - The Subject’s Private Key has been potentially or actually lost, stolen or compromised;
    - Control over the Subject’s Private Key has been lost due to potential or actual compromise of activation data (eg PIN code) or other reasons;
    - Inaccuracy or changes to the Certificate content, as notified to the Subscriber.

  This can be achieved by following the procedures on the KPN self-service portal: https://certificaat.kpn.com/intrekken/
- Ensure that if the Subscriber or Subject generates the Subject’s Key Pair, only the Subject holds the Private Key;
- Generate the Key Pair in a safe environment.

## 6 Obligations of the relying parties for the verification of the certificate status

- Independently assess the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose;
- Utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations, as a condition of relying on a Certificate in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. Relying parties will not rely on a Certificate unless these verification procedures are successful;

- Check the status of the Certificate on which the relying parties wishes to rely, as well as all the Certificates in its Certificate Chain. If any of the Certificates in the Certificate Chain have been revoked, relying parties will not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain;
- In the case of a “beroepsgebonden certificaat” (profession bound certificate) with the profession “gerechtsdeurwaarder” (Bailiff), it is the responsibility of the relying party to check whether this bailiff was registered as a bailiff in the register: http://www.registergerechtsdeurwaarders.nl at the time of usage of the certificate;
- Rely on the Certificate, if all of the checks described in the previous paragraphs are successful, provided that reliance upon the Certificate is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, it is the responsibility of the relying parties to obtain such assurances for such reliance to be deemed reasonable.

## 7 Exclusion and liability limitation clauses

KPN accepts liability for PKIoverheid Certificaten insofar as stated in the “Bijzondere Voorwaarden PKIoverheid certificaten”(special conditions PKIoverheid certificates) in https://certificaat.kpn.com/support/downloads/repository/

## 8 Applicable agreements, certification practice statement, certificate policy

See for applicable agreements and documents the repository:
https://certificaat.kpn.com/support/downloads/repository/

The Subscriber Agreement is submitted with the Subscriber’s Request Form to KPN in order to obtain a valid certificate.

This PKI Disclosure Statement serves as a summary for the certification practice statement (CPS) and refers to other operational documentation for more details concerning request and validation procedures.

## 9 Data protection directives

- KPN is careful with your data. You can rest assured that your details are safe with KPN and that we comply with the law;
- We do not look at the content of communications. We do not monitor calls, do not look at the content of your text messages, e-mails or chats, and do not keep track of which sites you visit;
- We do not sell your information to third parties.

KPN has formulated a privacy statement for all her services including her certificate services. In this statement is written down in which way KPN handles personal data. The privacy statement is made available on: https://certificaat.kpn.com/support/downloads/repository/

## 10 Reimbursement directives

Not applicable.

## 11 Governing Law and settlement of disputes clauses

All services concerning the KPN PKIoverheid certificates are governed exclusively by Dutch law.

## 12 CA and certificate directory licenses, confidentiality trademarks and audit

KPN is subject to a yearly compliance audit by a accredited auditor against the requirements of:

- European Union's (EU) eIDAS regulation;
- The program of requirements PKI Overheid;
- ETSI EN 319 411-1 and ETSI EN 319 411-2.

Proof of successful certification can be found by viewing the BSI certificates of compliance on our website: https://certificaat.kpn.com/support/downloads/repository/

## 13 Abbreviations and Terms

| Abbreviation /Term | Description |
|---|---|
| CA | Certification Authority |
| Certificate | An electronic document that uses a digital signature to bind a public key and an identity. |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| PKI | Public Key Infrastructure. A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). |
| Specific Conditions PKIoverheid certificates | An amendment to KPN's general conditions specific to the use of KPN's PKIoverheid certificates. In Dutch : Bijzondere Voorwaarden PKIoverheid certificaten |
| Subscribers | A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement. |

| Abbreviation /Term | Description |
|---|---|
| Relying Party | Any natural person or Legal Entity that relies on a Certificate by verifying the authenticity of a subscriber based on a certificate of PKIoverheid.<br>A relying party can also be a subscriber. |

## 14 Document Information

Version history

This PKI Disclosure statement has the following revisions:

| Version | Date | Status | Description |
|---|---|---|---|
| 0.90 | 25-09-2016 | Draft | |
| 0.91 | 30-09-2016 | Checked Draft | |
| 0.95 | 05-10-2016 | Pre-approval Draft | |
| 1.0 | 10-10-2016 | Final version | |
| 2.0 | 10-01-2019 | Update 2019 | |
| 5.3 | 01-07-2020 | Update 2020 | Introduction new types of certificates<br>Version numbering brought in line with CPS. |
| 5.4 | 25-06-2021 | Update 2021 | EV SSL en QWAC discontinued<br>Internet links checked and adjusted where necessary. |

-/-