Remote Qualified Signature Creation Device (Remote QSCD) Service 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 7 mei 2026

Versie version 1

Publication date

Version history

Version	Document date	Changes
0.1	26/02/2026	Initiële versie
0.2	03/03/2026	Minor changes based on the feedback from TUV
0.3	30/03/2026	Toegestane identificatie documenten toegevoegd
0.4		Multiple changes
0.5	20/04/2026	Additional changes based on the feedback from TUV
0.6	21/4/2026	Additional changes based on the feedback from TUV
0.7	22/4/2026	Additional changes based on the feedback from TUV
1.0	05/05/2026	Formatted this document to ensure RFC-3647 compliance

Inhoudsopgave

1. Introduction

1.1 Overview

This remote Qualified Signing Service Practice Statement ("rQSSPS") applies to the remote Qualified Signing Service of KPN for remote signatures and seals based on Qualified Certificates in accordance with the eIDAS Regulation.
This document describes KPN's delivery of signing and sealing services and management of the lifecycle of private keys on behalf of Subscribers and aims to comply with the requirements of:

- eIDAS Regulation 910/2024 (articles 29a and 39a) amended by 2025/1183
- ETSI TS 119 431-1

This document is binding between KPN and the Subscriber and/or the Relying Party. For Subscribers, this document becomes effective and binding by accepting the terms and conditions of the Service.
For Relying Parties, this document becomes binding by relying upon a Signature or Certificate from the Service.

This Service Practice Statement describes the practices and procedures of KPN for providing a remote qualified electronic signature and seal creation capability supported by a Remote QSCD and associated components, and any related qualified trust services.

1.2 Document name and identification

This document is KPN's remote Qualified Signing Service Practice Statement.

1.3 PKI participants

Refer to chapter 1.3 'PKI Participants' of the KPN CPS.

1.4 Certificate usage

Refer to chapter 1.4 'Certificate Usage' of the KPN CPS.

1.5 Policy administration

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

Refer to chapter 1.5 'Policy Administration' of the KPN CPS.

1.5 Definitions and Acronyms

Refer to Appendices 1 and 2 of the KPN CPS.

2. Publication and Repository Responsibilities

KPN ensures the availability of relevant information in the Repository:
https://certificaat.kpn.com/support/downloads/repository/

Refer to chapter 2 ‘Publication and Repository Responsibilities’ of the KPN CPS.

3. Identification and Authentication

3.1 Introduction

The Qualified Signing Service enables the creation of Qualified Electronic Signatures (for natural persons) and Qualified Electronic Seals (for legal entities) based on Qualified Certificates in accordance with the eIDAS Regulation.

The Private Keys supporting the Service are stored on a Qualified Signature and Seal Creation Device (QSCD) at KPN, on behalf of the Signer. Refer to Section 6.1.7 ‘Private key storage on cryptographic module’ of the CPS.

The user generates a hash of an electronic file, Data to be Signed (DTBS), with a signing service solution of a third party. The hash is sent to KPN’s rQSCD service to be signed.

During a signing session, the Signature Activation Protocol (SAP) will require data to authorize the signing request using Signature Activation Data (SAD) that takes the data to be signed as Data To Be Signed Representation (DTBS/R) and create a digital signature under signer control.

To ensure (sole) control of the Signer over the Private Key, a mobile application is provided by KPN during enrolment. This mobile application is required to authorize the signatures and generate the Signature Activation Data.

The certification of UBIQU’s QSCD version 2.6 (QSCD-Certificate pursuant to Art. 30 para. 3 lit. b eIDAS, has been described in ‘*VIG-22-037_QSCD-Certificate_Ubiqu_v26_Final_sign-HL.pdf*.

3.2 Acceptable Identity documentation

The AMP Identity Proofing Practice Statement states that only ‘*International Civil Aviation Organization (ICAO)*’ compliant identity documents, per ICAO Doc 9303, are accepted for identification purposes.

KPN follows this principle with the additional distinctions, whereby permitted documentation is defined as follows:

- Dutch driver’s license, ID card and passport
- Dutch residence permit. This is a document stating that the holder is legally in the Netherlands
- European ID’s, only if they are ICAO compliant
- Other passports, only if they are ICAO compliant

3.3 Object Identifier

The KPN Object Identifier for rQSCD EUSPv2: EU SSAS Policy itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4) or in dot notation: OID 0.4.0.19431.1.1.4.

Changes made to a SP which affect its applicability will be reflected in the policy identifier.

3.4 Identity proofing

ETSI TS 119 461 in Appendix C.3 specifies a list of use cases for issuing of qualified certificate according to Article 24.1 of the original eIDAS regulation. The following three use cases are applicable to the KPN rQSCD service.

C.3.1: Use case for identity proofing by physical presence of the applicant. For this use case has an agreement with AMP as the Identity Prover Service Provider refer to their practice statement located here.
To prevent fraud KPN additionally checks BKR's Verificatie Identificatie Systeem (VIS) to determine whether the provided identity documentation is accurate, up-to-date and not reported as missing, or otherwise.

C.3.5: Use case for identity proofing of legal person
Information provided by the Kamer van Koophandel (Chamber of Commerce) is used to verify whether an organization exists. The Chamber of Commerce is nationally (Dutch) approved.

C.3.6: Use case for identity proofing of natural person representing legal person

Refer to chapter 4 of the CPS.

After a successful identification KPN generates the signing key.

4. Certificate and Signing Key Life-Cycle Operational Requitements

4.1 Signing Key Initialization

4.1.1 Signing Key generation

Subscriber Private Keys are generated and used within the following Qualified Signature Creation Device (QSCD) during the lifecycle of the keys:

Name	Qualified Signature and Seal Creation Device (QSCD) Ubiqu's Qualified Remote Signature and Seal Creation Device, version 2.6
Applicant	Ubiqu Access B.V

The QSCD is initialized with technical mechanisms that require at least two operators and operated in accordance with the operating conditions described in the certification documentation.

Time of generation
A Signer's signing key is generated prior to Certificate generation, but as part of the Certificate generation process.

Cryptographic algorithms and key lengths

The SAP provided by Ubiqu provides cryptographic strength mechanisms that protect the authentication factors against compromise by the protocol threats as well as trusted third party impersonation attacks.

Cryptographic Algorithm	RSA
Key Length	2048
Hashing Algorithm	SHA-256

Algorithm parameters
Algorithm parameters for signature and seal creation are chosen that are currently resistant and will remain resistant during the lifetime of the Subject's Certificate.

Key protection
Private keys are stored in an encrypted manner, ensuring confidentiality and integrity, in a Hardware Security Module (HSM) certified against FIPS-140-2 L3.

Trustworthy system (TWS)
KPN uses secure resources and trustworthy systems generating key pairs and certificates for End Users. These trustworthy systems are provided with a positive CEN TS 419 241 audit report.
The SAP provided by Ubiqu is protected against replay, bypass, and forgery attack between signer and the remote SCDev.
Ubiqu has provided documentation to support the safe operation, installation and management of its module.

4.1.2 Electronic identification means linking

KPN provides authentication and remote server signing solutions to customers. The service consists of the ubiqu API, available to partners and/or users. This API is called the Signer Creation application (SCA). Part of the SCA is the signer interface (SI) that enables the user to mark a document for signing, or indicate the intention to authenticate by scanning a QR code

Authenticate app
- KPN Themed app with QR code scan function
- App API as defined by the App API guide and the registration and installation guide.
- Ubiqu will update and enhance the app-API and will keep the API stable for KPN

4.1.3 Certificate linking

The link between Signer's signing keys and the private key is verified before Certificate issuance. The integrity of the link is protected and the signing key cannot be used by the Signer before the public key Certificate is linked.

The signature activation data (SAD) links with a high level of confidence at least the following:
- A given DTBS/R or a set of DTBS/R
- Items to identify the authentication signer, and,
- Default or selected signing keys

Where not legally allowed, it is possible to disable the use of more than one DTBS/R.

4.1.4 Electronic identification means provision

After successful identity proofing an email is sent to the user (natural person or legal representative), containing a QR-code, the following steps are completed:

- The user installs Ubiqu's Authenticator app, which is bound to the user's phone
- The user accepts the Terms and Conditions
- The user chooses a PIN

The key pair is assigned to the user and corresponding certificates are issued.

4.2 Signing key lifecycle operational requirements

4.2.1 Certificate revocation

A certificate can be revoked under certain circumstances.

Refer to chapter 4.9 of the CPS for certificate revocation.

4.2.2 Signing key backup and recovery

For the continuity of the rQSCD service, the keys are stored on multiple HSM's at two different, physically separated, locations. The HSM's have been coupled Active-Active.

The number of copies maintained to ensure the continuity of the rQSCD service will not exceed the minimum, as described above.

4.3 SSASP as a Qualified TSP

For the status of KPN as a Qualified Trust Service Provider, please refer to the eIDAS trusted list.

Based on ETSI TS 119 431-1 KPN operates a Remote QSCD/SCDev under EUSPv2 (Extended Local Identification of the Person - Extended LoIP) and issues certificates accordingly.

4.3.1 Signing key generation

Signer's signing keys are generated in a QSCD, which is operated in accordance with the operating conditions.

4.3.2 Signature activation

Signer's signing keys are used in a QSCD, which is operated in the configuration as described in the certification guidance documentation or in an equivalent configuration which achieves the same security objective.

As described in Ubiqu's service description, the signing key can only be used to sign DTBS/R authorized by the Signature Activation Protocol (SAP).

5. Facility, management, and operational controls

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

Refer to chapter 5 ‘Facility, Management, and Operational Controls’ of the KPN CPS for additional information.

5.1. Physical security controls
Refer to chapter 5.1 ‘Physical controls’ of the KPN CPS

5.2. Procedural controls
Refer to chapter 5.2 ‘Procedural controls’ of the KPN CPS

5.3. Personnel controls
Refer to chapter 5.3 ‘Personnel controls’ of the KPN CPS

5.4. Audit logging procedures
Refer to chapter 5.4 ‘Audit logging procedures’ of the KPN CPS

5.5. Records archival
Refer to chapter 5.5 ‘Records archival’ of the KPN CPS

5.6. Key changeover
Refer to chapter 5.6 ‘Key changeover’ of the KPN CPS

5.7. Compromise and disaster recovery
Refer to chapter 5.7 ‘Compromise and disaster recovery’ of the KPN CPS

5.7.1 Reporting obligations
Refer to communication flow scheme as defined in ’Proces en communicatieflow Security Incidenten’.

6. Technical Security Controls
Refer to chapter 6 ‘Technical Security Controls’ of the KPN CPS

7. Compliance audit and other assessments
Refer to chapter 8 ‘Compliance audit and other assessments’ of the KPN CPS

8. Other business and legal matters
Refer to chapter 9 ‘Other business and legal matters’ of the KPN CPS.

9. Other provisions
No stipulations