Identity Proofing Service Practice Statement

KPN BV

Datum: 7 mei 2026
Versie: 1.0

Publicatie datum:

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

Version history

Version	Document date	Changes
0.1	25/02/2026	Initial Version
0.4	20/04/2026	Changes based on the feedback from TUV
1.0	05/05/2026	Formatted this document to ensure RFC-3647 compliance

Content

1 Introduction

1.1 Overview

This Identity Proofing Service Practice Statement (IPSPS) describes the policies and practices employed by KPN B.V. for identity proofing of natural persons, in alignment with eIDAS and relevant ETSI standards.

1.2 Document Name and Identification

This document is KPN's Identity Proofing Service Practice Statement. It describes the practices the IPSP employs with regards to the Identity Proofing of natural persons. This IPSPS is based on Regulation (EU) 910/2014 (eIDAS)(32014R0910 - EN - EUR-Lex), and ETSI TS 119 461. Any requirements on Identity Proofing for natural persons laid down by the PKIoverheid Programme of Requirements (PoR) or ETSI standards EN 319 411-1 and EN 319 411-2 are also in scope of this document.

1.3 PKI Participants

With respect to AMP Refer to chapter 1.5 ‘Other Participants’ of the KPN CPS.

1.4 Certificate usage

Refer to chapter 1.4 ‘Certificate Usage’ of the KPN CPS.

1.5 Policy administration

This document is managed by a dedicated Policy Management Authority (PMA).

Refer to chapter 1.5 ‘Policy Administration’ of the KPN CPS.

1.6 Definitions and Acronyms

Refer to Appendices 1 and 2 of the KPN CPS.

2 Publication and Repository responsibilities

Refer to chapter 2 ‘Publication and Repository responsibilities’ of the KPN CPS. Connectivity with the Chamber of Commerce, Dutch – Kamer van Koophandel (KvK) is encrypted.

The connection to the KvK is secured through a HTTPS session using a 2048-bit key. KPN has an account with the chamber of commerce allowing for the use of an API to retrieve relevant information.

Communication with another trusted register, registerd accountants, is message-based and therefore encrypted using s/mime.

3 Identification and authentication

Refer to chapter 3 ‘Identification and authentication’ of the KPN CPS.

KPN uses the ‘Extended LoIP’ as defined in ETSI TS 119 431-1. The KPN Level of Identity Proofing (LoiP) additionally uses ENISA’s ‘Identity Proofing Good Practices’ as a guideline for the risk management process. For the KPN service, ‘Fraud risk’ is avoided as KPN performs identity proofing face-to-face and verification of validity of provided identity documentation.

KPN relies on the Identity Proofing service performed by AMP as described in their ‘Identity Proofing Practice Statement’ whereby chapter 17.2 is applicable to the service provided. To prevent fraud, KPN additionally checks Bureau Krediet Registratie’s (BKR) Verificatie Identificatie Systeem to determine whether the provided identity documentation is accurate, up-to-date and not reported as missing, or otherwise.

In situations where a subscriber is not listed in the KvK, KPN will investigate the legitimacy of the legal person by checking the ‘Register van Overheidsorganisaties’ on overheid.nl.

Additional trusted registers include:
- Kamer van Koophandel (KvK): KVK - Kamer van Koophandel | KVK
- Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA): www.nba.nl
- Register van Overheidsorganisaties: www.overheid.nl
- Bureau Krediet Registratie (BKR): www.BKR.nl
- Register Notariaat (KNB): www.knb.nl
- Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders: www.kbvg.nl

4. Facility, Management and Operational Controls

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

5 Identity Proofing Practices

5.1 Identity Proofing Application

5.1.1 Who Can Apply for Identity Proofing

Any natural person at least 18 years of age and in possession of a valid identity document that is supported by KPN can apply for identity proofing. The person has to apply for identity proofing themselves, this cannot be done by a representative.

5.1.2 Enrolment Process and Responsibilities

For additional information refer to chapter 4.3.1.1 ‘Issuance of Personal, Professional, Group and eSeal Certificates’ of the KPN CPS.

5.1.3 Information collected if applicant is a legal person

The following information is collected if an applicant is a legal person
a) full name of the legal person;
b) country of registration of the legal person;
c) unique identifier and type of identifier for the legal person (unless such identifier does not exist).

5.2 Application Processing

5.2.1 Performing Identification and Authentication Functions

Identification and authentication are done as described in chapter 3 ‘Identification and authentication’. KPN does not reuse previously submitted evidence.

5.2.2 Approval or Rejection of Identity Proofing

The IPSPS will approve or reject identity proofing based on the outcome of the steps described in Chapter 3 ‘Identification and authentication’.

As per the AMP Identity Proofing Practice Statement, AMP’s validation tasks are assigned randomly to available registration officers.

5.3 Identity Proofing Completion

5.3.1 Actions During Completion

The process is completed by a registration officer, see chapter 3 ‘Identification and authentication’. It is not technically possible for one person to submit and complete the same application.

5.3.2 Notification to Subscriber of Completion of Identity Proofing

AMP notifies KPN and KPN notifies the subscriber once identity proofing is completed. Refer to the process steps defined in chapter 1.3.2 ‘op locatie’ of the AMP Practice Statement.

5.4 Identity Proofing Aborted

The AMP Practice Statement does not specify how to handle in case of abortion of the identity proofing process.

5.5 Data retention

Refer to chapter 17.2.5 – 3 ‘Opslag en Bewaartermijnen’ of the AMP IPPS.

In addition to the period AMP retains information KPN must keep said information indefinitely to ensure its availability for legal purposes. KPN stores the evidence in the BlueX environment. Access to the BlueX environment is restricted to only those staff allowed to work on BlueX. Retention is documented in KPN’s ‘PKI Privacy Statement’.

The data is stored in a way that ensures the integrity and accessibility of the archived data during the retention period.

The data is stored such that it is easily retrievable.

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

As per the AMP Identity Proofing Practice Statement, the time of completion is part of the evidence maintained.

5.6 Identity Proofing Modification

Identity Proofing results cannot be modified. If the data collected during Identity Proofing is no longer actual, the Subscriber must have their profile deactivated. The Subscriber can apply for reactivation of their profile with new data if desired.

5.7 End of Subscription

During identity proofing, a user can terminate their identity proofing application at any moment of their choosing. After a successful identity proofing application, subscription can be ended by Certificate Revocation.

5.8 Discrepancies and Complaints

If the name supplied by the requestor does not match the name on the identity document the request will be denied. Exceptions are those that are obvious typing mistakes, which may be adjusted based on the provided identity document.

Refer to chapter 9.13 ‘Dispute Resolution Procedures’ of the KPN CPS.

Whether or not a legal person remains a legitimate contact is the responsibility of the customer and has been contractually anchored. KPN relies on the KPN CMS which is considered leading.

The freshness of the legal representative will be reviewed every 3 years whereby the representative will receive a request to acknowledge their role.

5.9 Risk Management

The risk framework is maintained by the KPN compliance team and is documented in KPN’s ‘Risk assessment proces PKIo-Identity-KPN Security’. The risk management process is subject to, at least, a yearly review.

Refer to chapter 5.4.8 of the KPN CPS.

Refer to AMP Practice Statement chapter 4 ‘Risicoanalyse’ for more information regarding AMP’s approach to Risk Management.

The KPN Risk Management process describes ‘External Factors’ including:

- Documentation provided by the ‘Nationaal Coördinator Terrorismebestrijding en Veiligheid’ (NCTV) is used to determine pertinent issues potentially impacting the KPN PKI environment
- Risks identified through threat intelligence are assessed and documented
- Risks, resulting from threats intelligence and requiring training and / or awareness have been addressed in the Risk assessment process
- Vulnerability notifications feed the vulnerability management process
- KPN CERT notifications are sent to appropriate teams to determine applicability, and if applicable, to manage associated risks

Risks associated with the Identity Proofing service provided by AMP have been analyzed and documented in the risk assessment. Identified risks include:

- Human error: mistakes made by the officer performing the physical identification, such as incorrectly validating provided documentation
- Falsified documentation provided and accepted
- Actor influencing the decision of the officer performing the physical identification

Resilience to False Acceptance Rates (FAR) and False Rejection Rates (FRR) of applicants and regular testing of the performance against these goals is described in AMP's Practice Statement.

5.9.1 Crisis Management

KPN's incident management process which, describes when to initiate a crisis such that other teams, depending on the incident, are involved, is covered in internal documents.

6 Compliance Audit and Other Assessments

Refer to chapter 8 'Compliance Audit and Other Assessment' of the KPN CPS.

Compliance is periodically assessed by an independent, accredited conformity assessment body.

7 Other Business and Legal Matters

Refer to chapter 9 'Other Business and Legal Matters' of the KPN CPS.

7.1 Disabilities

To be completed once AMP has updated policy statement.