Identity Proofing Practice Statement

Remote Video Identity Proofing

v1.1

Date: 20 May 2026

Important Notice

Address: 29 A Tudor Vladimirescu Avenue,

AFI Tech Park 1, Bucharest, Romania

Phone: 004-021-31.19.901

Web: www.certsign.ro

Document History

Version	Effective Date[1]	Reason	Responsible
1.0	January 2026	First version publishing	CISO
1.1	20 May 2026	Update with phyisical cases	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
certSIGN	CISO	January 2026

Distribution List

Destination	Date distributed
Public-Internet	January 2026
Public-Internet	May 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	January 2026
1.1	Policies and Procedures Management Body	May 2026

[1] Last day of the month, if not explicit

Content

1 Scope and Purpose

This Identity Proofing Practice Statement (IPPS) describes the identity proofing practices applied in support of trust services provided by certSIGN as QTSP, in accordance with ETSI TS 119 461.

Identity proofing is not a standalone trust service under the eIDAS Regulation. It is performed as a component of a trust service and supports the issuance of certificates by certSIGN.

This IPPS provides transparency regarding identity proofing practices to all parties relying on the outcome of the identity proofing process, including certSIGN, Conformity Assessment Bodies (CABs), and relying parties that place trust in certificates issued following successful identity proofing.

2 Identity Proofing Service Provider Model and Responsibilities

The identity proofing capability described in this IPPS is delivered through a hybrid operational model.

certSIGN acts as the responsible Identity Proofing Service Provider (IPSP) and performs manual identity proofing activities, including manual review and final decision-making. certSIGN remains fully accountable for identity proofing outcomes and certificate issuance.

Automated components supporting the remote video identity proofing process are provided by external solution providers acting as subcontractors under the contractual control and governance of certSIGN. Responsibility for identity proofing outcomes is not transferred to subcontractors.

3 Identity Proofing Contexts and Compliance Claim

3.1 Supported Identity Proofing Contexts

Remote video identification

Identity proofing under this IPPS applies exclusively to natural persons and is performed in a remote environment with:

- unattended operation;
- hybrid processing combining automated and manual activities;
- Extended Level of Identity Proofing (Extended LoIP).

Identity proofing is performed exclusively using physical identity documents, limited to the type of documents originated from the certSIGN list https://www.certsign.ro/en/list-identity-documents-video-identification/

- Passports
- National identity cards.

No trusted registers, proof-of-access mechanisms, supplementary documents, attestations, or electronic identification schemes are used.

Identification by physical presence

Identity proofing under this IPPS applies exclusively to natural persons and is performed in a physical environment with:

- attended operation;
- manual veriifcation of the ID document and binding to applicant by manual face verification;
- Extended Level of Identity Proofing (Extended LoIP).

Identity proofing is performed exclusively using physical identity documents, limited to the type of documents originated from the certSIGN list https://www.certsign.ro/en/list-identity-documents-video-identification/:

- passports;
- national identity cards.

No trusted registers, proof-of-access mechanisms, supplementary documents, attestations, or electronic identification schemes are used

3.2 Compliance Claim for Supported Use Cases

Compliance with ETSI TS 119 461 is claimed for the following use cases:

I.

- Remote unattended identity proofing with Extended Level of Identity Proofing, as specified in clause 9.2.3.1;
- Hybrid identity proofing combining automated and manual operation, as specified in clause 9.2.3.3;
- Identity proofing for issuance of qualified certificates, as specified in Annex C.3.4.

II.

- Identity proofing for issuance of qualified certificates, as specified in Annex C.2.1 & C.3.1.
- Attended identity proofing of a natural person using an identity document with physical presence of the applicant, with manual operation as specified in clause 9.2.1.1 and 9.2.1.2

Compliance is claimed only for the above use cases and only within the scope defined in this IPPS.

4 Collection of Identity Attributes and Evidence

Identity attributes are collected exclusively from the physical identity document presented by the applicant. Identity documents with an embedded chip are treated solely as physical documents.

The means used to collect identity attributes include:

- automated extraction of attributes from the physical identity document (including OCR and machine-readable zones where available);
- manual review and correction by certSIGN's operators where required;
- directly from the applicant by typing in information or otherwise; such information is then validated against the ID document

Only identity attributes necessary to uniquely identify the applicant are collected. No supplementary attributes are collected or validated.

For each supported identity proofing context, the accepted identity documents are limited to passports and national identity cards from https://www.certsign.ro/en/list-identity-documents-video-identification/.

5 Handling of Encoding and Name Representation Differences

Where identity attributes are obtained from different representations of the same physical identity document, predefined and documented rules are applied to resolve differences in encoding, transliteration, and name representation in a consistent and controlled manner.

This is to ensure consistent, accurate, and legally reliable identity matching, despite variations in:

- Character encoding (UTF-8, Latin-based, ICAO transliteration)
- Name structure (ordering, prefixes, compound names)
- Language and script differences (diacritics, non-Latin alphabets)

The machine-readable zone (MRZ), where present, is used as the authoritative source for transliterated name representation.

The certSIGN operators have an internal procedure to use mapping tables for common substitutions based on ICAO-Based Transliteration Handling. In the procedure the operators handle compound names using hyphen normalization or space standardization, and check the exact match after normalization, through a field-by-field comparison (surname, given name, date of birth).

6 General Identity Proofing Process Principles

The identity proofing process establishes the unique identity of the applicant and binds that identity to the person participating in the process.

Physical identity documents are presented by the applicant in real time through a remote video-based interaction or by physical presence to demonstrate possession of the original document.

For remote video identity proofing, the process combines automated mechanisms and manual verification activities and results in one of the following outcomes:

- acceptance of the applicant;
- rejection of the applicant;
- termination of the identity proofing process where reliable identification cannot be achieved.

Where automated and manual verification activities yield conflicting results, the identity proofing process is terminated.

For identity proofing trough physical presence the process is mostly manual with some automatic checks performed by the dediicated ID document scanners.

7 Biometric Performance and Presentation Attack Detection (PAD) Governance

certSIGN as IPSP applies a risk-based identity proofing process in which resilience to false acceptance and false rejection is achieved through conservative decision logic and operational controls, in accordance with ETSI TS 119 461.

At process level, security is prioritized by preventing acceptance of applicants whose identity cannot be reliably established. Suspected impersonation, document fraud, presentation attacks, or insufficient confidence result in termination or escalation of the identity proofing process.

Quality is addressed by combining automated mechanisms with manual review, including controlled handling of encoding and representation differences, in order to avoid unnecessary rejection of legitimate applicants.

7.1 Biometric Performance Objectives

With respect to biometric face matching, the IPSP aims to achieve performance aligned with industry best practice for one-to-one face recognition. This objective is met by relying on biometric solutions whose performance is publicly demonstrated through recognized industry benchmarks, such as the NIST Face Recognition Vendor Test (FRVT).

The IPSP does not independently define or measure False Acceptance Rate (FAR) or False Rejection Rate (FRR) values, but ensures that biometric solutions are operated in their standard, vendor-recommended configuration and that security-relevant decision thresholds are not relaxed.

7.2 Presentation Attack Detection Objectives

Presentation Attack Detection (PAD) capabilities are provided through an ISO/IEC 30107-3 certified PAD component. PAD performance characteristics, including APCER and BPCER, are based on vendor-maintained testing and certification activities.

The adequacy of PAD-related security objectives is periodically reviewed as part of the IPSP threat intelligence and risk management process. Emerging presentation attack techniques do

not lead to relaxation of PAD acceptance criteria, but may result in strengthened operational controls or escalation measures.

8 Remote Video Identity Proofing Risk Management and Security Principles

The identity proofing process is designed taking into account the high attack potential associated with remote and unattended identity proofing scenarios.

certSIGN applies a risk-based approach addressing risks including:

- identity fraud and impersonation;
- presentation, replay and injection attacks;
- manipulation of captured evidence;
- misuse or compromise of identity proofing systems.
- use of authoritative sources of information on document appearance and document validation - Public Register of Authentic Travel and Identity Documents Online (PRADO).

Measures are applied to ensure integrity of evidence capture and to mitigate risks related to replay, injection or manipulation of captured data.

Risk assessments are reviewed periodically and whenever significant changes occur in the identity proofing process or threat environment.

9 Identity proofing trough Physical Presence Risk Management and Security Principles

The process is performed with manual validation of the physical identity document and the registration officer have access to authoritative sources of information on document appearance and document validation - Public Register of Authentic Travel and Identity Documents Online (PRADO).

At least three, different security features of physical identity documents are verified considering an attacker with the relevant attack potential. Security elements can be watermarks, holograms, printing techniques, visual and ultraviolet light patterns, and see-through elements.

The registration officers verify optical and haptic/tactile security features if any. Level 2 security features are verified with UV lamps.

Manual binding of the applicant to an identity document is used. The registration officesr perform a morphological analysis according to a defined feature list, as recommended by the FISWG Facial Comparison Overview and Methodology Guidelines and the corresponding checklist.

10 Organizational and Operational Controls

Identity proofing activities are performed within a controlled operational environment.

certSIGN ensures that:

- roles and responsibilities are clearly defined;
- personnel involved in manual verification activities are trained and competent;
- documented procedures govern identity proofing operations.

Oversight of subcontracted automated components is maintained through contractual requirements, service monitoring, and escalation and fallback procedures.

11 Evidence and Record Management

Evidence related to the identity proofing process is collected and handled in accordance with applicable legal, contractual, and regulatory requirements.

Identity proofing records support traceability and auditability and are protected with respect to integrity and confidentiality. Retention and deletion of evidence are performed in accordance with defined retention requirements.

12 Limitations and Explicit Exclusions

This IPPS explicitly excludes:

- trusted registers;
- proof-of-access mechanisms;
- supplementary documents or attestations;
- identification of legal persons or representation of legal persons;
- reuse or lifecycle management of reference face images.

13 Maintenance of the IPPS

This IPPS is reviewed periodically and updated when significant changes occur in identity proofing practices, applicable standards, threat landscape, or operational arrangements.

Servicie Termination provisions are according to the general certSIGN Termination procedure.