



IN GROUPE DENMARK PS

Identity Proofing Practice Statement

Document information

No of pages: 23	Reference: N/A	Department: IN Groupe Digital Factory	Classification: Public
Creation date: 11/08/2026		Last saved update: 27/08/2026	Version: 1.2

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

TABLE OF CONTENT

Table of Content	2
Version Control and Revision History	5
1 Scope	6
2 Definitions of Terms, Symbols, Abbreviations and Notations	6
3 References	7
4 General Concepts	7
4.1 Identity proofing actors	7
4.2 Identity proofing process	8
4.3 Identity proofing context	8
4.4 Authoritative evidence and supplementary evidence	8
4.5 Consideration of threats	8
4.6 Identity proofing service policy	9
5 Operational Risk Assessment	9
6 Policies and Practices	9
6.1 Identity proofing service practice statement	9
6.2 Information security policy	10
7 Identity Proofing Service Management and Operation	10
7.1 Internal organization	10
7.2 Human resources	10
7.3 Asset management	10
7.4 Access control	10
7.5 Cryptographic controls	10
7.6 Physical and environmental security	11
7.7 Operation security	11
7.8 Network security	11
7.9 Vulnerabilities and incident management	11
7.10 Collection of evidence	11
7.11 Business continuity management	11
7.12 Termination and termination plans	11
7.13 Compliance	12
7.14 Supply chain	12
8 Identity Proofing Service Requirements	12



Identity Proofing Practice Statement

Reference: N/A

Version: 1.2

Creation Date: 11/08/2026

Latest updated: 27/08/2026

8.1	Initiation	12
8.2	Attribute and evidence collection.....	13
8.2.1	General requirements.....	13
8.2.2	Attribute collection	13
8.2.3	Use of physical or digital identity document as evidence	14
8.2.4	Use of existing eID means as evidence	15
8.2.5	Use of existing digital signature means as evidence	15
8.2.6	Use of trusted register as supplementary evidence	15
8.2.7	Use of proof of access as supplementary evidence	15
8.2.8	Use of documents and attestations as supplementary evidence.....	15
8.2.9	Evidence collection for natural person representing legal person	15
8.3	Attribute and evidence validation.....	15
8.3.1	General requirements.....	15
8.3.2	Validation of digital identity document.....	15
8.3.3	Validation of physical identity document	16
8.3.4	Validation of eID means	16
8.3.5	Validation of digital signature with certificate.....	16
8.3.6	Validation of trusted registers	16
8.3.7	Validation of proof of access.....	17
8.3.8	Validation of documents and attestations	17
8.4	Binding to applicant	17
8.4.1	General requirements.....	17
8.4.2	Capture of face image of the applicant	17
8.4.3	Binding to applicant by automated face biometrics	18
8.4.4	Use of existing digital signature means as evidence.....	18
8.4.5	Binding to applicant for legal person and natural person representing a legal person.....	18
8.5	Issuing of proof	19
8.5.1	Result of the identity proofing	19
8.5.2	Evidence of the identity proofing process	19
9	Use cases for identity proofing	20
9.1	Introduction, compliance with the present document, general requirements for all use cases	20
9.2	Use cases for identity proofing of natural person.....	20
9.2.1	Use cases using an identity document with physical presence of the applicant	20
9.2.2	Use cases using an identity document for attended remote identity proofing	20



Identity Proofing Practice Statement

Reference: N/A

Version: 1.2

Creation Date: 11/08/2026

Latest updated: 27/08/2026

9.2.3	Use cases using an identity document for unattended remote identity proofing	20
9.2.4	Use case for identity proofing by authentication using eID means	21
9.2.5	Use case for identity proofing using digital signature with certificate	22
9.3	Use case for identity proofing of legal person	22
9.4	Use case for identity proofing of natural person representing legal person	22
9.5	Use cases for additional identity proofing to enhance an identity proven by use of an eID from Baseline LoIP to Extended LoIP	23
9.5.1	General requirements	23
9.5.2	Use case for enhancing identity proofing to Extended LoIP by a full identity proofing using an identity document	23
9.5.3	Use case for enhancing identity proofing to Extended LoIP by use of a previously captured reference face image	23

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

VERSION CONTROL AND REVISION HISTORY

Version Number	Date of Change	Author/Modifier	Summary of Changes
1.0	28-05-2025	Robert Peter Laursen	First version
1.1	27-06-2025	Robert Peter Laursen	Update after conformity assessment stage 1 review
1.2	27-08-2026	Carl Pedersen	General review and updates to formulation regarding eMRTD.

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

1 SCOPE

IN Groupe Denmark A/S is the provider of the white label Identity Provider platform called "IN ID" and used by trust service providers for identity proofing, authentication, and credential management. The identity proofing component used by IN ID is called "IN ID Verify" and is also provided as a standalone product.

The IN ID practice statement documentation is organised as described below:

- "Identity Proofing Practice Statement" describing that the requirements from ETSI TS 119 461 are met (current document) for "IN ID Verify".
- "Trust Service Practice Statement" [1] describing that the general requirements from eIDAS Regulation (EU) No 910/2014 and ETSI EN 319 401 are met for "IN ID".
- "Authentication and Credential Management Practice Statement" [2] describes that the requirements from Commission Implementing Regulation (EU) 2015/1502 are met in "IN ID".

2 DEFINITIONS OF TERMS, SYMBOLS, ABBREVIATIONS AND NOTATIONS

Term/Acronym	Definition
3DFaceMap	A 3DFaceMap is a digital representation of the three-dimensional geometry of a human face. It is created using specialised technology to capture the unique contours, shape, and depth of an individual's facial features.
Applicant	An individual or entity undergoing an identity proofing and enrolment process to become a subscriber.
Authentication	The process of verifying the identity of a subscriber, as a prerequisite to allowing access to resources. It answers the question "Prove you are who you say you are."
Authenticator	Something the end-user possesses and controls (e.g., a cryptographic key, a password, an OTP device) that is used to authenticate their identity.
Biometrics	Measurable physical characteristics (e.g., fingerprint, facial features) or behavioural traits used for identity verification or authentication.
CSP	Credential Service Provider: An entity responsible for identity proofing individuals and issuing and managing their authenticators. In the context of this document, IN Groupe acts as a CSP for the defined services.
eIDAS	Electronic Identification, Authentication and Trust Services: EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market.
eMRTD	Electronic Machine Readable Travel Document. A machine-readable travel document containing an integrated circuit (chip) in which identity information and the holder's facial image are stored in accordance with ICAO Doc 9303. Examples include electronic passports and compatible electronic identity cards.
End-user	Synonym for subscriber or applicant.
ETSI	The European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit, standardization organization in the field of information and communications technology
FAR	False Acceptance Rate - The probability that the system will accept an imposter's biometric data as the correct, Expected User's data and incorrectly provide access to the imposter.
FRR	False Rejection Rate – The probability that a system will reject the correct User when that User's biometric data is presented to the sensor. This metric is used to measure sensitivity. If the FRR is high, Users will get frustrated with the system because they are prevented from accessing their own accounts.

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

ICAO	International Civil Aviation Organization. In the context of this document, ICAO refers primarily to ICAO Doc 9303, which specifies requirements for Machine Readable Travel Documents (MRTDs), including eMRTDs.
Identification	The process of claiming an identity, typically through a username or other identifier. It answers the question "Who are you?"
Identity Proofing	The process of confirming that an individual is who they claim to be, typically involving the validation of identity evidence.
IdP	Identity Provider: A system that manages and verifies digital identities.
IN ID	A system for electronic identification of natural persons.
IN ID Verify	System for identity proofing of natural persons in accordance with ETSI 119 461
IPSP	Identity Proofing Service Provider is a trusted entity responsible for verifying the identity of a person
KYC	Know Your Customer" (KYC) is a process, where financial institutions and other businesses verify the identity and assess the risk associated with their customers.
LoIP	Level of Identity Proofing (ETSI TS 119 461) aligned with eIDAS regulation.
MFA	Multi-Factor Authentication: An authentication method that requires the user to provide two or more verification factors from different categories (something you know, something you have, something you are).
OIDC	OpenID Connect - A modern, standardised way for applications (RP) to verify who a user is and get basic profile information about them
PIN	Personal Identification Number
Relying Party (RP)	An entity that relies upon a subscriber's authenticated identity and related attributes, as asserted by the CSP.
Subscriber	An individual or entity that has successfully completed the IDV and enrolment process and has been issued authenticator(s) by the CSP.
TSP	Trust Service Provider is a person or company that provides services for verifying the identity of individuals and other entities in electronic transactions.

3 REFERENCES

ID	Version	Description
[1]	1.1.1	Trust Service Practice Statement
[2]	1.2	Authentication and credential Management Practice Statement
[3]	2.1.1	ETSI 119 461 v 2.1.1 (2025-02).

4 GENERAL CONCEPTS

4.1 Identity proofing actors

IN ID Verify may operate as a standalone application, as an integrated component of the IN ID app, or as an SDK integrated into a third-party application.

Regardless of the model, processes and responsibilities are defined for all actors involved (TSP, IPSP and applicant) in accordance with the defined standard.

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

4.2 Identity proofing process

As IPSP our solution is designed to support identity proofing processes, within the scope of automated hybrid and remote identity verification. We have implemented the required elements of the identity proofing process, including initiation, attribute and evidence collection, validation and binding to the applicant, and issuing of proof in a fully automated manner.

The solution is modular, to meet the context-specific requirements, in order to support both Baseline and Extended Level of Identity Proofing (LoIP).

4.3 Identity proofing context

Building on our modular implementation, we recognize that different jurisdictions and trust service use cases may impose specific conditions and/or limitations on the identity proofing process. The solution is designed to accommodate these restrictions through configuration.

Our implementation supports this flexibility by enabling:

- Selection and enforcement of mandatory or optional identity attributes.
- Control over permitted document types and trusted evidence sources.
- Tailored workflows that reflect the requirements for specific LoIP levels.

4.4 Authoritative evidence and supplementary evidence

The solution focuses on identity proofing of natural persons using digital identity documents, such as eMRTDs, and eID means as authoritative evidence.

Where required by the identity proofing context or to strengthen the assurance level, supplementary evidence, such as proof of access mechanisms may be incorporated in conjunction with authoritative sources.

4.5 Consideration of threats

Our identity proofing solution incorporates a risk-aware design, addressing the key threat categories relevant to unattended remote identity proofing such as:

- Presentation attacks, including use of falsified or manipulated documents and biometric spoofing.
- Injection attacks, including deepfakes and other forms of media substitution.
- Impersonation, where genuine evidence is used by someone other than the legitimate holder.

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

The solution uses layered technical control, such as biometric liveness detection, automated document authenticity checks, and secure evidence capture and transmission. These controls are evaluated and updated regularly to maintain effectiveness as the threat landscape evolves.

4.6 Identity proofing service policy

The principles and controls governing our identity proofing service policy are embedded throughout this practice statement. This includes the defined scope of our unattended remote identity proofing service, and support for both Baseline and Extended LoIP.

The current practice statement also outlines, how evidence types, validation and binding methods are applied, as well as how identity proofing contexts are addressed, and threats are mitigated.

These elements form the basis of our identity proofing service policy.

5 OPERATIONAL RISK ASSESSMENT

The IN ID Verify service conducts a comprehensive operational risk assessment as described in the TSP Practice Statement.

The TSP's risk assessment encompasses all risks related to information system security, including those requiring effective threat intelligence procedures.

For the IPSP the assessment includes a focused evaluation of risks related to identity fraud. This assessment is integrated into our secure software development lifecycle (S-SDLC) process which feeds into the overall operational risk assessment.

The risk assessment is reviewed and updated regularly to reflect changes in the threat landscape, operational procedures, and technical environment. Identified risks are managed through our formal risk management processes, ensuring that appropriate controls are implemented and maintained throughout the service lifecycle.

6 POLICIES AND PRACTICES

6.1 Identity proofing service practice statement

General requirements under this clause are addressed in the TSP Practice Statement; the following section covers the IPSP-specific requirements. See "Trust Service Practice Statement" [1].

IN ID Verify complies with the following identity proofing use cases



Identity Proofing Practice Statement

Reference: N/A

Version: 1.2

Creation Date: 11/08/2026

Latest updated: 27/08/2026

- Use cases using an identity document for unattended remote identity proofing, see section 9.2.3
- Use case for identity proofing by authentication using eID means, see section 9.2.4
- Use case for enhancing identity proofing to extended LoIP by a full identity proofing using an identity document, see section 9.5.2

6.2 Information security policy

See "Trust Service Practice Statement" [1].

7 IDENTITY PROOFING SERVICE MANAGEMENT AND OPERATION

7.1 Internal organization

See "Trust Service Practice Statement" [1].

7.2 Human resources

See "Trust Service Practice Statement" [1].

7.3 Asset management

See "Trust Service Practice Statement" [1].

7.4 Access control

See "Trust Service Practice Statement" [1].

7.5 Cryptographic controls

See "Trust Service Practice Statement" [1].

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

7.6 Physical and environmental security

See "Trust Service Practice Statement" [1].

7.7 Operation security

See "Trust Service Practice Statement" [1].

7.8 Network security

General requirements under this clause are addressed in the TSP Practice Statement [1].

The IPSP environment is logically and physically separated from non-critical information systems and is subject to the same network security requirements as IN Groupe's QTSP trust services.

7.9 Vulnerabilities and incident management

General requirements under this clause are addressed in the TSP Practice Statement [1].

The IPSP reporting obligations for network and information security incidents are handled through the processes implemented by the IN Groupe QTSP.

7.10 Collection of evidence

See "Trust Service Practice Statement" [1].

7.11 Business continuity management

See "Trust Service Practice Statement" [1].

7.12 Termination and termination plans

See "Trust Service Practice Statement" [1] excluding obligations regarding public keys or trust service tokens.

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

7.13 Compliance

See "Trust Service Practice Statement" [1]

7.14 Supply chain

See "Trust Service Practice Statement" [1]

8 IDENTITY PROOFING SERVICE REQUIREMENTS

8.1 Initiation

IN ID Verify is designed to inform the applicant (natural persons not acting under a pseudonym) of the identity proofing's purpose.

The applicant may select from the available identity proofing processes, depending on the type of authoritative evidence they are able to provide.

Further, the applicant must accept the 'Terms and Conditions' and the 'Privacy Policy' for IN ID Verify before any identity proofing process can be initiated.

IN ID Verify provides clear, step-by-step guidance throughout the identity proofing process, including an initial overview of the required stages.

During this guidance, the applicant is informed about:

- The identity information collected at each step.
- The evidence that the applicant is required to present e.g., an eMRTD compatible ID document.
- The applicant must grant the app access to functions that are required for the identity proofing process (e.g., camera and NFC access).

The 'Terms and Conditions' and 'Privacy Policy' describe how data collection is minimized, protected in accordance with applicable data protection rules, and the legal basis for processing it.

IN ID Verify is designed with accessibility in mind and aims to comply with applicable legislation for persons with disabilities, such as Directive (EU) 2019/882 within the EU.

To facilitate an accessible identity proofing experience, the app is WCAG-compliant to the extent technically feasible and offers the following features:

- Screen reader compatibility, enabling users to hear instructions and understand the necessary actions.

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

- Voice command control for certain interactions, such as approving steps via swiping.

8.2 Attribute and evidence collection

8.2.1 General requirements

The identity attributes that provide unique identification of the applicant, depend on the chosen identity proofing process:

eMRTD-based Identity Proofing: Presentation of a valid government-issued eMRTD compliant with ICAO Doc 9303, such as an electronic passport or supported electronic identity card. Unique identification is achieved through the combination of the document number and the issuing state, as encoded within the Machine Readable Zone (MRZ). This ensures a globally unique identifier for the travel document.

German Identity Card with Online ID Function (eID): Presentation of a valid government-issued ID card and government validated PIN code (e.g. German Personalausweis). Unique identification relies on the unique serial number securely stored on the chip of the identity card, together with the issuing state.

Other notified eID Schemes: The scheme must provide a unique reference to their identity proofing evidence, which is audit logged in the system as a part of the identity proofing. Unique identification is achieved through a combination of verified personal data such as name, issuing state, date of birth, and birth name, often coupled with validated contact information, like a validated mobile number and/or email address. The specific attributes and verification methods employed by these schemes are designed to meet their national requirements for uniqueness and the assurance level of the eID.

8.2.2 Attribute collection

8.2.2.1 Attribute collection for natural person

Depending on the identity proofing process selected by the applicant, at least following attributes are collected:

eMRTD-based Identity Proofing: The chip of the eMRTD ID contains the applicant's given name(s), surname, date of birth, birth name, nationality and document number, document type, document expiry and issuing state, which are collected as part of the identity proofing. Furthermore, the photography contained within the chip is compared against a 3DFaceMap, generated during the identity proofing process. For verification purposes, the FAR score derived from this comparison is part of the identity proofing attributes, but the original photography and 3DFaceMap are not retained.

German Identity Card with Online ID Function (eID): The applicant's given name(s), surname, address, date of birth, birth name, nationality and document number, document type, document expiry and issuing state, which are collected as part of the identity proofing (see further details in section 9.2.4).

Other notified eID Schemes: The existing eID must provide the required attributes based on an assessment against a comparable assurance level. The provided attributes include but are not limited to the

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

applicant's given name(s), surname, date of birth, birth name, nationality and at least one validated contact info (e.g. mobile number or email address), which are collected as part of the identity proofing (see further details in section 9.2.4).

All identity attributes collected as part of the identity proofing include a validation status and an indication of its source e.g. an ID document. Other attributes like mobile and email address are provided and validated by the end-user.

8.2.2.2 Attribute collection for legal person

Legal persons are not supported by IN ID Verify.

8.2.2.3 Attribute collection for natural person representing legal person

Legal persons are not supported by IN ID Verify.

8.2.3 Use of physical or digital identity document as evidence

The requirement for authoritative evidence to contain a face photo or other information for unique identification and binding to the applicant, is addressed as follows in our identity proofing processes:

Identity proofing processes utilizing an ID document with a Face Photo:

eMRTD-based remote identity validation: The eMRTD-compliant ID document used in this process contains a face photo on the chip, which is used for comparison against the applicant's physical appearance.

Identity proofing process utilizing an ID document without a Face Photo:

When reading the chip of the Personalausweis using the PIN, the chip itself does not contain a face photo. In this case, the PIN serves as a strong knowledge factor to authenticate the legitimate holder of a physical document, that was issued following an in-person application process, where the applicant's identity and photo were verified. The secure delivery of the transport PIN via registered mail, further strengthens this link to the verified individual. While a face photo is not directly compared during this online process, the initial issuance of the authoritative document involved face-to-face verification, fulfilling the binding requirement at the point of issuance.

Identity proofing process implicit utilizing ID document(s):

This identity proofing process "Other notified eID scheme" implicitly relies on a physical or digital identity document that was initially presented and verified within the existing eID scheme. It is the responsibility of the organisation utilizing this identity proofing method to have implemented processes that satisfy the requirement for a face photo or other unique identifiers, and the binding to the applicant during their initial verification. Use of this method assumes validation and approval of both the responsible organisation and the eID scheme, confirming adherence to comparable standards for authoritative evidence.

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

8.2.4 Use of existing eID means as evidence

Ref. above section 8.2.3.

8.2.5 Use of existing digital signature means as evidence

Not supported by IN ID Verify.

8.2.6 Use of trusted register as supplementary evidence

Not supported by IN ID Verify.

8.2.7 Use of proof of access as supplementary evidence

Not supported by IN ID Verify.

8.2.8 Use of documents and attestations as supplementary evidence

Not supported by IN ID Verify.

8.2.9 Evidence collection for natural person representing legal person

Legal persons not supported by IN ID Verify.

8.3 Attribute and evidence validation

8.3.1 General requirements

Ref. below section 8.3.2.

8.3.2 Validation of digital identity document

When an eMRTD compliant with ICAO Doc 9303 is used as authoritative evidence, the authenticity and integrity of the document and the data retrieved from its integrated chip are validated as part of the identity proofing process.



Identity Proofing Practice Statement

Reference: N/A

Version: 1.2

Creation Date: 11/08/2026

Latest updated: 27/08/2026

The validation includes:

Passive Authentication verifies the authenticity and integrity of the data stored on the ePassport chip. This process ensures that the data has not been tampered with and was issued by a legitimate authority.

Active Authentication is an additional security measure used to prevent cloning of the ePassport chip. This ensures that the chip is genuine and not a copy.

Biometric Binding, identity proofing process based on eMRTD must also pass a real-time liveness detection and photo comparison step:

- **Liveness detection** ensures that a real, physical person is performing the identity proofing process.
- **Photo comparison**: The photo read from the ID document is compared with the 3D FaceMap obtained during liveness detection, proving that the person performing the identity proofing is the same as the one in the ID document.

The combination of document validation, liveness detection and biometric comparison establishes that the authoritative evidence is valid and that the applicant is the legitimate holder of the eMRTD.

The Identity proofing processes are completed in a combination of the app and the backend, ensuring control is by the responsible actor (IN ID Verify) and the result of the validation step(s) are stored in the audit log.

8.3.3 Validation of physical identity document

Physical identity documents are not supported.

8.3.4 Validation of eID means

Authentication using an eID within an eIDAS-notified eID scheme is accepted as validation at its specified level of assurance.

The PIN for the German Personalausweis is validated through a trusted and authorised intermediary that provides secure access to the authoritative data and performs real-time checks against official government registers.

Other notified eID schemes for natural persons, issued by other states or organisations, are also accepted as valid if they comply with local legislation and the obtained level of assurance in accordance with eIDAS.

8.3.5 Validation of digital signature with certificate

Digital signatures not supported as evidence.

8.3.6 Validation of trusted registers

When validating the country signing certificates, is it validated against the master list(s) stored in the system.



Identity Proofing Practice Statement

Reference: N/A

Version: 1.2

Creation Date: 11/08/2026

Latest updated: 27/08/2026

The master lists are distributed by trusted organisations, but there currently does not exist a single master list hence multiple sources are used– for instance, not all countries are part of the ICAO Public Key Directory (PKD)¹ or the BSI German CSCA Master List² lists.

8.3.7 Validation of proof of access

Proof of access not supported as evidence.

8.3.8 Validation of documents and attestations

For the supported use case ref. section 8.2.3.

8.4 Binding to applicant

8.4.1 General requirements

For the general requirement for verification that the applicant is the legitimate holder of the authoritative evidence ref. to section 8.3.2 for validation of digital identity document.

For existing eID means, no specific binding requirements are needed, since the applicant can use the eID means in question.

8.4.2 Capture of face image of the applicant

The solution uses FaceTec³, which creates a 3D FaceMap® with a short video-selfie, that provides a frame rate and resolution which support identity proofing with an LoIP baseline and extended, depending of the obtained FAR score. The video stream applies attack detection measures, including detecting artificially generated or manipulated face appearance and employs random light patterns and light reflections on the iris during face scanning. The video is captured during the identity proofing session and does not allow for storing or uploading of previous captures.

FaceTec uses proprietary anti-tampering techniques to ensure that the data payloads are secure and have not been altered or tampered with during transmission. It also includes checks to prevent camera feed injection attacks. This ensures that the video feed being analysed is coming directly from the device's camera and not from a pre-recorded or manipulated source.

Biometric data is encrypted during transmission and storage, ensuring that it cannot be intercepted or altered by unauthorized parties.

¹ <https://www.icao.int/Security/FAL/PKD/Pages/ICAO-Master-List.aspx> - note for governmental use only

² <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/CSCA/GermanMasterList.html>

³ See further details on FaceTec security and certifications at <https://www.facetec.com/>

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

The solution is designed to allow three retries in the same identity proofing session.

The captured facial data is compared to the facial photo read from the validated ICAO compatible ID document, ensuring that the person carrying out the process is the rightful owner of the document.

8.4.3 Binding to applicant by automated face biometrics

The IN ID Verify app installed on the applicant's mobile device is used for the real-time capture of the 3DFaceMap and reading the face photo from the ID-document is controlled by the applicant.

The 3DFaceMap is captured while preventing morphing⁴ and will be compared with the photo read from the ICAO document.

The result of the comparison of the captured 3DFaceMap and the facial photo read from the ICAO ID document is a False Acceptance Rate (FAR) score, which must exceed a defined threshold to be accepted.

The required level for the FAR score for facial recognition follows industry standards and is based on ongoing threat intelligence and is:

LoIP Baseline if the obtained FAR⁵ score is at least 5 corresponding to 1/10.000 at FRR⁵ rate of 1%.

LoIP Extended if the obtained FAR score is at least 7 corresponding to 1 in 500.000, at a FRR rate of 1%.

When an accepted FAR score is obtained, it is verified that the natural person in front of the mobile camera matches the photo stored in the chip. This ensures that the document used for identification is neither lost nor stolen.

8.4.4 Use of existing digital signature means as evidence

Not supported by IN ID Verify.

8.4.5 Binding to applicant for legal person and natural person representing a legal person

Legal persons are not supported by IN ID Verify.

⁴ See further details on https://facetec.com/Catching_Morphs_with_FaceTec_3D_2D_Matching.pdf

⁵ The FRR is considered to be <1% ref. dev.facetec.com/3d-2d-face-portrait to see the different FAR level.

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

8.5 Issuing of proof

8.5.1 Result of the identity proofing

Communication between the IN ID Verify app (where the end-user completes identity proofing) and the backend is protected by TLS, and the payload data is encrypted with an additional layer while in transit.

The result of the identity proofing is audit logged in a consistent and tamper-proof audit log. Protection against tampering is ensured by storing a digest of the data in the log entry that also includes the digest of the previous log entry in the same audit thread.

To ensure the confidentiality of the audit log, access is limited to the end-user and qualified employees (with dedicated permissions). Additionally, any lookup in the audit log is itself audit logged, so it is always documented who accessed it.

The audit log of the identity proofing contains at least the following information:

- Current timestamp
- Nationality
- ID document type
- ID document number
- ID document issuing state
- FAR score (for ICAO ID-documents)
- Document signing certificate
- Error code (in case of failure)

Information to uniquely identify the end-users (i.e. eID created based on a completed identity proofing):

- Link to the identity (UUID)
- ID Document number
- ID document country
- ID document type
- eID source system

Addition, changes, or deletion of identity attributes always require an identity proofing on at least the same level and the current LoIP of the identity.

All audit log entries are stored in the audit log, in accordance with applicable data retention regulations for a configurable period.

8.5.2 Evidence of the identity proofing process

See section 8.5.1

	Identity Proofing Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date: 11/08/2026
		Latest updated: 27/08/2026

9 USE CASES FOR IDENTITY PROOFING

9.1 Introduction, compliance with the present document, general requirements for all use cases

Following use cases on Baseline or Extended Level of Identity Proofing (LoIP) are supported by IN ID Verify:

- 9.2.3 Use cases using an identity document for unattended remote identity proofing
- 9.2.4 Use case for identity proofing by authentication using eID means

Compliance with the above use case is assessed by the independent, accredited Conformity Assessment Body Datenschutz.

9.2 Use cases for identity proofing of natural person

Supported use cases are designed in such a way, that video guidance is provided where necessary, as well as contextual guidance in each step of the flow.

9.2.1 Use cases using an identity document with physical presence of the applicant

Not supported by IN ID Verify.

9.2.2 Use cases using an identity document for attended remote identity proofing

Not supported by IN ID Verify.

9.2.3 Use cases using an identity document for unattended remote identity proofing

Identity proofing by retrieving identity data from an eMRTD compliant with ICAO Doc 9303. During the IDV process, the system validates the end-user against the biometric information retrieved from the eMRTD. If a comparison between these data does not match, the flow is aborted, and the end-user is informed that the identity proofing failed.



Identity Proofing Practice Statement

Reference: N/A

Version: 1.2

Creation Date: 11/08/2026

Latest updated: 27/08/2026

The identity proofing and verification process using an eMRTD is as follows:

1. End-user downloads the IN ID Verify App (or an app with the IN ID Verify SDK embedded) from either Google Play or App Store.
2. End-user opens the downloaded app.
3. End-user selects to complete the identity proofing and verification with a supported eMRTD or ID card.
4. End-user reads and accepts Terms and Conditions and Privacy Policy.
5. End-user takes a short film clip of his/her face with the app. This control verifies that it is a physical person in front of the mobile camera ("liveness detection check") and it generates a 3D FaceMap of the live person, which is submitted to the backend.
6. End-user scans the MRZ code on the passport/ID card – can alternatively be entered manually.
7. Scans the embedded chip using NFC in the ID document by using the data obtained in the previous step. During this process, the authenticity of the ID document is verified (via verification of the used country signing certificate), and clone detection is executed to verify that the chip has not been tampered with. Needed identity data, including the photo of the identity, stored in the Chip, is submitted to the backend.
8. The backend compares the photo read from chip in the ID document with the 3D FaceMap of the person in front of the mobile camera. The result of this control measure is a False Acceptance Rate (FAR) score, which must exceed a certain threshold to successfully complete the identity proofing.
9. Depending on the obtained FAR score the identity proofing is either:
 - a. FAR is below threshold for LoIP Baseline: The identity proofing is failed.
 - b. FAR is equal or higher than the threshold for LoIP Baseline, but below the threshold for LoIP Extended: The result of the identity proofing is Baseline.
 - c. FAR is equal to and higher than the threshold LoIP Extended: The result of the identity proofing level Extended.
10. Once the identity proofing is successful, it is verified that the natural person in front of the mobile camera matches the photo stored in the chip. This ensures that the document used is neither lost nor stolen.

If the identity proofing fails a consecutive number of times, the identity document will not be allowed to be used for identity proofing during a pre-defined quarantine period.

9.2.4 Use case for identity proofing by authentication using eID means

IN ID Verify supports the following identity proofing process based on authentication using eID means.

9.2.4.1 Identity card with online ID function

Identity proofing by retrieving identity data from an ID card using the PIN (e.g. Personalausweis). During the IDV process, the system validates that the end-user enters the correct PIN to access the chip data, which will complete the identity proofing.

The identity proofing and verification process using a national identity card (e.g. German Personalausweis) with an online PIN validation (by a state authority) is:



Identity Proofing Practice Statement

Reference: N/A

Version: 1.2

Creation Date: 11/08/2026

Latest updated: 27/08/2026

1. End-user downloads the IN ID Verify App (or an app with the IN ID Verify SDK embedded) from either Google Play or App Store.
2. End-user opens the downloaded app
3. End-user selects to complete the identity proofing and verification with an Identity Card with PIN
4. End-user reads and accepts the IN ID Verify Terms and Conditions and the Privacy Notice.
5. The app displays certificate and requests permission to retrieve data about the user
6. The ID card is connected to the device via NFC
7. The app requests the user to provide PIN code (6-digit)
8. End-user types in PIN, which is validated by the system
9. System validates PIN code and if correct, requests the user to scan their ID card
10. Data is read from the ID card, and the identity proofing is now completed on assurance level high

Personalausweis is issued on assurance level high and when authenticating with Personalausweis using the PIN, the process involves several security measures to ensure the identity of the ID-cardholder.

9.2.4.2 Other Notified eID Scheme

When identity proofing is performed using another notified eID scheme, such as MitID or ID Austria, the resulting LoIP must not exceed the assurance level supported by the authentication. Note: The individual supported eID schemes implemented are dependent on customer configuration.

9.2.5 Use case for identity proofing using digital signature with certificate

Not supported by IN ID Verify.

9.3 Use case for identity proofing of legal person

Legal persons not supported by IN ID Verify.

9.4 Use case for identity proofing of natural person representing legal person

Legal persons not supported by IN ID Verify.



Identity Proofing Practice Statement

Reference: N/A

Version: 1.2

Creation Date: 11/08/2026

Latest updated: 27/08/2026

9.5 Use cases for additional identity proofing to enhance an identity proven by use of an eID from Baseline LoIP to Extended LoIP

9.5.1 General requirements

Identities proofed at LoIP Baseline can be enhanced to level Extended by completing one of the identity proofing methods and obtain level Extended. It is required that it is the same identity document as for the initial identity proofing used to obtain LoIP Baseline.

9.5.2 Use case for enhancing identity proofing to Extended LoIP by a full identity proofing using an identity document

Enhancement of LoIP is possible using identity proofing method as described in section 9.2.2 and 9.2.4.

9.5.3 Use case for enhancing identity proofing to Extended LoIP by use of a previously captured reference face image

Not supported by IN ID Verify.