Trust Services Policy & Practice Statement

for IN Groupe

Table of Contents

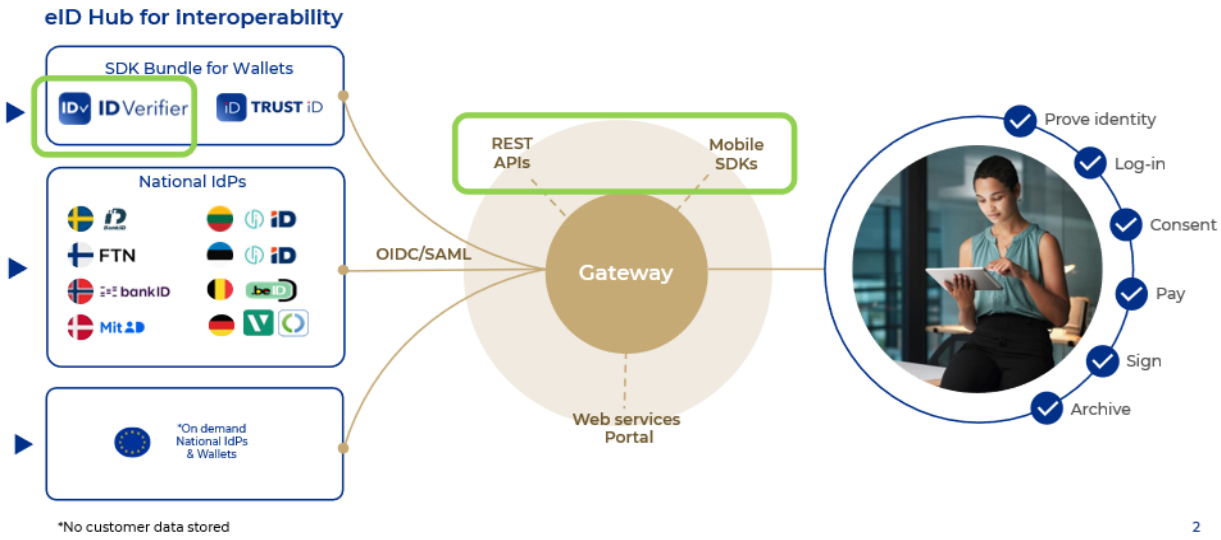
Document Version history

Date:	Change Description:	Version:	Author:
04.01.2022	Document creation/initial draft version	v. 1	Nets Product Management
14.01.2022	Minor changes/management review/1st version approval	v. 1.1	Nets Product Management
14.03.2023	Products rebrand across the whole document (from Passport Reader to ID verifier); picture change; other minor changes / updates/changes on section; 1.2 (applicable regulations); 6,7,8,12; 18.8 (SDK fraud attempts) ; section 18.9 (face match level); 19.3 (LoA and inclusion of audit trail)	v. 2	Nets Product Management
20.03.2023	Management review / 2nd version approval	v. 2.1	Nets Product Management
01.09.2023	Additional specification section 19.3 (audit trail)	v. 2.2	Nets Product Management
20.09.2024	Migration to OTC cloud (section 7)	v. 3.1	IN Groupe Product Management
15.10.2024	App improvements and error messages (section 19.2)	v. 3.2	IN Groupe Product Management
25.09.2025	New IN Groupe branded iOS & Android App release	v. 3.3	IN Groupe Product Management
12.01.2026	New template for CSP	v. 3.4	IN Groupe Product Management

1. Introduction

This document is the Trust Service Practice Statement (TSPS) of the IN Groupe ID Verifier identity verification service. It is not a full Certification Practice Statement (CPS) because IN Groupe IDV only cover the aspects of identity proofing for the issuance of qualified certificates and do not offer other certification services.

The IN Groupe IDV service scans and reads machine-readable identity (ID) documents (passports, driving licenses, and residence cards) with an NFC enabled mobile phone; ensures that the person carrying out the process is the rightful owner of the document using biometrics; ensures that the information is transmitted in a secure manner. The attributes collected uniquely identify the applicant as a natural person in the identity proofing context. Please refer to the illustration below.



For trust services provided by TSPs it is of paramount importance that the user's identity has been established and verified. IN Groupe's ID Verifier service acts as an identity data and document verification technology provider that enables (qualified) TSPs operating under eIDAS to provide their services.

This Trust Services Policy and Practice Statement (TSPS) therefore does not cover the whole set of practices that a TSP covers but focusses on the relevant electronic identification parts that are provided by In Groupe. It focusses on the IN Groupe's solution, that TSPs can use for remote identity data and identity document verification. During the certificate application process of a qualified certificate, IN Groupe's ID Verifier service enables the TSP to effectively and reliably establish the identity of the applicant.

The section headings that do not apply have the statement "Not applicable". Sections that describe actions specific to a single service contain only references to service-specific practice statements. If the subsections are omitted, a single reference applies to all of them.

1.1 OVERVIEW

The purpose of this document is to serve as a base for compliance with eIDAS, the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and the ETSI standards ETSI TS 119 461 [1], ETSI EN 319 401, ETSI EN 319 411-2. The mentioned eIDAS Regulation does not define identity proofing as a trust service on its own. In the present document, identity proofing is defined as a subset of the Trust Service Component "Registration Service" as defined in the ETSI-standard ETSI EN 319411-2. The identity proofing service component can be an integral part of the Trust Service Provider's (TSP) service provisioning, but the service component can also

be the task of a specialized Identity Proofing Service Provider (IPSP) acting as a subcontractor to the TSP.

For IN Groupe IDV, the applicant is a natural person, and the identity proofing process is fully remote and automated
This Trust Services Policy and Trust Services Practice Statement (TSPS) describe the practices and procedures that IN Groupe's ID Verifier employs to support (qualified) TSPs operating under eIDAS to provide their services.
Identity proofing is the process of verifying with the required degree of certainty that the identity of an applicant is correct. IN Groupe has developed a remote identification service, the IN Groupe ID Verifier, for identity proofing of trust service subjects as well as for other purposes such as issuing of electronic identity, onboarding and know-your customers (KYC) processes e.g. for financial services and authentication-based signing.

In particular, IN Groupe verifies the identity of natural persons amongst other methods in accordance with eIDAS, Article 24, paragraph 1 d) by using "other identification methods" which provide equivalent assurance in terms of reliability to physical presence. Conformance with eIDAS at assurance level "High" allows certification service providers to use these services for identity verification in their processes of issuing qualified certificates.
In addition, collaboration with Qualified Trust Service Providers (QTSPs) IN Groupe enables individual users of the contracted partners to electronically sign legally binding contracts using qualified electronic signatures according to the eIDAS regulation. In Groupe's ID Verifier provides identity registration and identity document verification functionality and face verification for (qualified) TSPs operating under eIDAS. IN Groupe ID Verifier is a ready-to-use, client-server white label mobile app that allows identity document verification by scanning the MRZ of the document, reading the NFC chip, and biometric facial verification functionality. Additionally ID Verifier is also available as SDK which can be integrated into customer applications.
ID Verifier is available as an electronic ID (eID) in IN Groupe's E-Ident identity broker service. After configuration, the Customer initiates their End Users authentication by starting a session in IN Groupe's E-Ident specifying passport (and/or other supported ID documents) as the selected eID. The E-Ident service can be presented in two modes: standalone or embedded into an iframe in the Customer's own web UI (User Interface) where we present the End User with:
a QR code to download the ID Verifier application on mobile device (available both in Google Play and Apple App Store). The app default language is English, but it can support multiple languages based on Customers' demand.
A QR or PIN activation code to initiate the in-app authentication process. With each authentication, the End User is presented with a privacy statement.
IN Groupe ID Verifier requires the use of NFC. Devices without NFC hardware will not be able to perform the verification flow, and will display an error message explaining this when opening the app.

1.2 Scope: Identity Proofing Service Policy (IPSP)

The present document (the 'IN Groupe Trust Service Practice Statement') describes the applied practices employed in delivering the IN Groupe ID Verifier service and in meeting the applicable requirements for identity proofing.

More specifically, the practices adopted for fulling the general policy requirements given in ETSI TS 119 461 [1] and describe the policy and security requirements adopted for implementing an
'Identity Proofing Service Component' supporting identity proofing in European and other regulatory framework. This standard has been developed considering the following aspects:
It is based on ETSI EN 319 411-2 v.2.2.2 (2018-04) which contains common requirements for all trust service providers (TSP) implementing best practices for use of selected means and applicable technologies that can be used for identity proofing.
It includes specific requirements for the verification of the identity of natural persons specifying how identity proofing processes can be constructed by combining means to achieve the basic desired outcome of the identity proofing process.
The security requirements of ETSI TS 119 461 [1] cover the most common risks, which fall into two main categories: an applicant falsely claims an identity using forged means of evidence (forged evidence) and an applicant uses valid means of evidence associated with

another person (impersonation). Potential operational risks and social engineering risks are also considered.

To summarize:

• ETSI EN 319 411-2 v.2.2. (2018-04) Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates; - Part 2: Requirements for trust service providers issuing EU qualified certificates, incl. applicable requirements included by reference from ETSI EN 319 401 v2.2.1 and ETSI 319 411-1 v.1.2.2.

• ETSI TR 119 461 v1.1.1 (2021-07): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service sub- jects for the identification method: "IN Groupe ID Verifier", providing unattended remote identity proofing, where the communication with the applicant is automated, specifically: Automated operation.

• (partial) certification of the IN Groupe ID Verifier service provision according to ETSI EN 319 411- 2 (PKI component service: Registration Service).

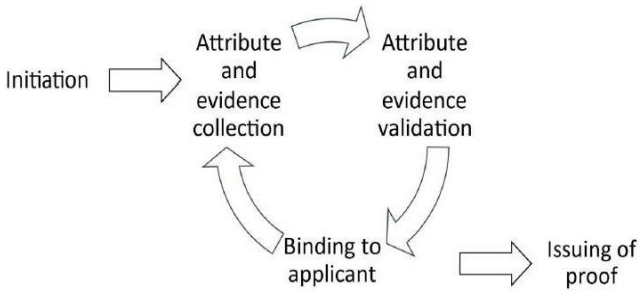
• confirmation of equivalent assurance to physical presence, pursuant to Regulation (EU) 910/2014 (eIDAS) art. 24.1 sub d, of the identification method: "IN Groupe ID Verifier", based on assessment against ETSI TS 119 461 [1] applicable requirements.

• ETSI TS 119 461 [1] applicable requirements are additionally cross-referenced against BITS1 - Requirements for solutions for Secure digital verification of identity (2020-10) for the Norwegian market.

1.3Identity Proofing process

IN Groupe IDV conforms to the following identity proofing service requirements as specified in ETSI TS 119 461 [1], Chapter 8:

- 8.1 (initiation)
- 8.2.1 (attribute and evidence collection general requirements)
- 8.3.1 (attribute and evidence validation general requirements)
- 8.4.1 (binding to applicant general requirements) and
- 8.5 (issuing proof)



1.4 Identity Proofing context

The identity proofing context is the set of external framing conditions that an identity proofing process is subject to and that can impose requirements and restrictions on identity proofing. A core element of the identity proofing context is the regulatory requirements imposed on identity proofing for the defined purpose by the applicable legislation. IN Groupe Customers are responsible for ensuring compliance with local regulations according to their intended identity proofing context. IN Groupe IDV identity proofing context will vary between purposes of identity proofing and be-tween countries in relation to:

- The required level of assurance (eg eIDAS High or Substantial)
- The identity attributes to collect, meaning attributes that are mandatory, prohibited, or optional (eg in Norway, the collection of a national identity number can be mandatory for the identity proofing context, while other countries do not use such numbers).
- The country specific national legislation and government policies on applicable technologies (e.g. certain identity documents like national identity cards from selected countries can be restricted; in some countries, validation of identity attributes against a national population register can be mandatory, while other countries do not have such registers; the means to use for attribute and evidence validation and for binding to applicant, meaning that certain process steps can be mandated or prohibited; in some countries, physical presence can be mandated for certain purposes of identity proofing, or remote identity proofing can be restricted to allow only specific use cases).

When it comes to attribute and evidence collection and validation threats, the following best practices applies to IN Groupe IDV:

- Pending on the identity proofing context, only passports and national ID cards are accepted since the attributes collected in those uniquely identify the person.
- Protection against stolen or revoked identity documents is ensured during the binding to the applicant through biometric; access to authoritative sources of information on document, e.g. TOVE register in Norway/Interpol register internationally, may be supported through IN Groupe but is left at the discretion of IN Groupe Customer.

1.5 Document Name and Identification

This document is identified as: "IN Groupe's Trust Services Policy and Practice Statement"

The Certificate Policies adopted by IN Groupe are aligned with the certificate policies defined in ETSI EN 319 411-1 and ETSI EN 319 411-2 and according to eIDAS Regulation (EU) No 910/2014. The scope of the policies relates to the issuance of qualified certificates for natural persons and IN Groupe's role in this. Since IN Groupe is neither a CA or a TSP, it uses a subset of the above-mentioned policies.

1.6 PKI PARTICIPANTS

The following participants are relevant.

1.6.1 Trust service provider

A party that provides trust services under eIDAS regulation. A TSP is a customer of IN Groupe.

1.6.2 Certificate authorities

Entities that issue certificates.

1.6.3 Registration authorities

Entities that establish enrolment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a Certificate Authority.

1.6.4 Subscribers

Holders of certificates.

1.6.5 Relying parties

A relying party is anyone who acts trusting a certificate issued by a TSP.

1.6.6 Other participants

IN Groupe's ID Verifier provides remote identity document reading and biometric face verification services for TSPs during their CA/RA activities, i.e. enrolment, renewal and reactivation of electronic identities for digital certificates for natural persons.

A public cloud provider is a sub-contractor of IN Groupe and hosts IN Groupe's Server that processes all identity document data and may orchestrate data exchanges. There is contractual agreement between the public cloud provider and IN Groupe. The organizational/contractual and technical security measures provided by the cloud provider meet the relevant requirements laid down by eIDAS and ETSI for TSPs. It is the responsibility of IN Groupe to control and monitor this. Consequently, security requirements in terms of certifications are set for the public cloud provider.

Biometric Verification Provider is an organization offering identity document holder verification services. It does that by providing biometric verification (i.e. facial verification) and liveness detection of the applicant or subscriber. The organizational and technical security measures provided by the biometric verification provider meet the relevant requirements laid down by eIDAS and ETSI for TSPs. Depending on the orchestration model this is the responsibility of either IN Groupe or the TSP. In the first case the biometric verification provider is a sub-contractor of IN Groupe's in the latter case it is a sub-contractor of the TSP.

NFC & MRZ Document Scanning Provider is an organization offering scanning of NFC chip and MRZ in biometric identity documents.

1.7 CERTIFICATE USAGE

Does not apply.

1.8 POLICY ADMINISTRATION

1.8.1 Organisation administration

This IN Groupe's TSPS is administered by IN Groupe's management with contact address mentioned below.

IN Groupe Trust Services ApS NUF
Dronning Eufemias gate 16, 0191 Oslo, Norway
Org.nr:933 127 990
esec-vas-no@ingroupe.com

1.8.2 Time or frequency of publication

The latest version of this TSPS approved by management is available for download on IN Groupe website.

1.8.3 Terms & Conditions

This TSPS becomes effective from the date of publication on the website. Amendments become effective upon publication. This TSPS remains in force until it is replaced by a new version.

Applicable terms and conditions towards IN Groupe Customer for the provision of the IN Groupe IDV service (including e.g. termination, force majeure, dispute resolution, governing law) are regulated in the IN Groupe ID Verifier Service Agreement.

Applicable terms and conditions towards the End user are regulated in the IN Groupe ID Verifier Privacy Notice.

1.9 Definition of Terms and Abbreviations

Term:	Definition:
applicant	person (legal or natural) whose identity is to be proven
(identity) attribute	quality or characteristics ascribed to a person.
Baseline LoA	Level of Assurance (LoA) according to eIDAS Regulation (EU) 910/2014 which distinguished between High, Substantial and Low level.
binding to applicant	part of an identity proofing process that verifies that the applicant is the person identified by the presented evidence.

digital identity document	identity document that is issued in a machine-processable form though NFC (Near Field Communication) enabled technology, that is digitally signed by the issuer, and that is in purely digital form. A digital identity document can be contained in a physical identity document, e.g. an eMRTD contained in a passport or national identity card.
end user	IN Groupe Customer's customer, signatory or other physical person with which IN Groupe Customer has a contractual relationship regarding the IN Groupe ID Verifier service.
(identity) evidence	information or documentation provided by the applicant or obtained from other sources, trusted to prove that claimed identity attributes are correct.
False Acceptance Rate (FAR)	proportion of verification transactions with false biometric claims erroneously accepted according to ISO/IEC 19795-1 [i.17].
False Rejection Rate (FRR)	proportion of verification transactions with true biometric claims erroneously rejected according to ISO/IEC 19795-1 [i.17].
identity	attribute or set of attributes that uniquely identify a person within a given context.
identity document	physical or digital document issued by an authoritative source and attesting to the applicant's identity.
identity proofing context	external requirements affecting the identity proofing process, given by the purpose of the identity proofing, the related regulatory requirements, and the resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself.
identity proofing (process)	process by which the identity of an applicant is verified using evidence attesting to the required identity attributes.
identity proofing policy	set of rules that indicate the applicability of an identity proofing service to a particular community and/or class of application with common security requirements.
Identity proofing practice service statement	Alternative name given in ETSI 119 461 [1], clause 6 for the trust service practice statement defined in ETSI EN 319 401 [1], clause 6.1
Identity proofing service provider	Subcontractor of the trust service provider.
liveness detection	measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture according to ISO/IEC 30107-1 [i.16].
IN Groupe Customer	the legal entity/Company subscribing to the IN Groupe ID Verifier

IN Groupe ID Verifier (Service)	the service provided by IN Groupe which is in scope with this trust service practice statement.
IN Groupe ID Verifier App	the mobile software application(s) as developed by IN Groupe and delivered to IN Groupe Customer.
IN Groupe ID Verifier SDK	IN Groupe IDV Software Development Kit (SDK) provided by IN Groupe to IN Groupe Customer to develop its own application(s).
IN Groupe ID Verifier Privacy Notice	In-app terms and conditions which require consent from the End user.
IN Groupe Security Framework (NSF)	IN Groupe Group primary information security framework. This framework is implemented in all parts of the organization and follows the concepts provided in ISO 27001.
IN Groupe ID Verifier Service Agreement	IN Groupe Customer signed order confirmation for the provision of the IN Groupe ID Verifier Service.
IN Groupe Signing & Identification (SIS) Ser- vices	IN Groupe product portfolio which includes IN Groupe E-Ident broker ser- vice and ID Verifier.
physical identity document	identity document issued in physical and human-readable form.
presentation attack	presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system according to ISO/IEC 30107-1 [i.16].
Presentation Attack Detection (PAD)	automated determination of a presentation attack according to ISO/IEC 30107-1 [i.16].
qualified trust service provider	trust service provider listed in an EU Member State's Trusted List according to eIDAS regulation.
remote identity proofing	identity proofing process where the applicant is physically distant from the location of the identity proofing.
subject	legal or natural person that is enrolled to a trust service
subcontractor	Third-parties that support IN Groupe during delivery of IN Groupe ID Verifier
trust service	electronic service for: • creation, verification, and validation of digital signatures and related certificates; • creation, verification, and validation of time-stamps and related certifi- cates;
trust service component	one part of the overall service of a TSP according to ETSI EN 319 403-1 [i.6].
trust service practice statement	statement of the practices that a TSP employs in providing a trust service.
trust service provider	entity which provides one or more trust services.

validation	part of an identity proofing process that determines whether or not attributes are validated by the presented evidence and whether or not the evidence is genuine, authoritative, and valid.

Abbreviation

DG data group
eID electronic Identification
eMRTD electronic Machine-Readable Travel Document
FAR False Acceptance Rate **FRR**
False Rejection Rate **FML** Face
Match Level
GDPR General Data Protection Regulation **ICAO**
Internation Civil Aviation Organization **IPSP** Identity
Proofing Service Policy
ITIL Information Technology Infrastructure Library
LoA Level of Assurance
MRZ Machine Readable Zone
NFC Near Field Communication **NSF**
IN Groupe Security Framework **PAD**
Presentation Attack Detection **PET**
Privacy Enhancing Technology
QTSP Qualified Trust Service Provider
SIS (IN Groupe) Signing and Identification Services
TLS Transport Layer Security
TSP Trust Service Provider
TSPS Trust Service Practice Statement

2 Publication and Repository Responsibilities

2.1 REPOSITORIES

IN Groupe has an online repository, accessible through ID Verifier | IN Groupe

2.2 PUBLICATION OF INFORMATION

IN Groupe provides public repositories for its TSPS and other important policy documents. The ReadID repository is located at the In Groupe's website ID Verifier | IN Groupe

2.3 TIME AND FREQUENCY OF PUBLICATION

IN Groupe publishes updates of this information in the repository at least once per year or when significant changes are implemented.

2.4 ACCESS CONTROL ON REPOSITORIES

The repository is protected against unauthorized changes. Only authorized employees of IN Groupe have writing/modifying/deleting permissions for the repository.

3 Identification and Authentication

This section describes the identification and authentication processes during initial registration and prolongation. It particularly focusses on remote identification services that are provided by In Groupe ID Verifier to enable a TSP to issue qualified certificates.

NFC-based remote identity verification using In Groupe ID Verifier and face matching provides an alternative for physical verification at the TSP during registration. The document verification is done by reading the chip of government-issued identity documents such as passports, ID-cards, residence permits or driving licenses with a mobile app on a smartphone with NFC capabilities.

3.1 Machine Readable Zone (MRZ) scanning

As a first step, ID Verifier enables the End User to use the inbuilt camera on their mobile device to scan the Machine-Readable Zone (MRZ) of their chosen document using Optical Character Recognition (OCR).
The following is a list of machine-readable official Travel Documents (TD1, TD2 and TD3 size) which are ICAO DOC 9303 compliant:

- passports
- residence cards
- driving licenses

A full document overview per country coverage is available on demand upon request from the Customer.

3.2 Chip reading and verification

As a second step, ID Verifier enables the reading and verification of the contactless chip in the identity document through Near Field Communication (NFC). The reading of the chip is done and assures:

- Basic Access Control security mechanism;
- Passive Authentication security mechanism;
- Active Authentication security mechanism;
- Chip Authentication (EAC-CA_ security mechanism and the reading and interpretation of DG1 with the MRZ information, DG2 with the face image, and DG11 with additional personal information (if present).
- When applicable, Password Authenticated Connection Establishment (PACE) protocol is used to get access to the chip and Chip Authentication for cloning detection.

3.3 Face matching and liveness verification

As a final step, ID Verifier enables the End User to take a video selfie by using the inbuilt camera on their mobile device. The liveness detection and verification service consists of the following security layers:

- 3D Face Map Authentication: measure “perspective distortion” (zoomed and unzoomed video frames) to recreate a three-dimensional user’s face model.
- Liveness Detection: measure up to 50 diverse attributes (including light reflection, pupil dilation, blinking, subtle movements)
- Face verification: compare biometric (3D Face Map) with high resolution picture from document chip to determine a match. False Acceptance Rate (FAR) is the percentage of identification instances in which unauthorised persons are incorrectly accepted. False Rejection Rate (FRR) is the percentage of identification instances in which authorised persons are incorrectly rejected. The highest security level supported by our face matching algorithm is 1/1200000 FAR with under <1% FRR.

3.4 Returned information about the End User

After each successful authentication, a combination of the End User document and biometric data is returned by ID Verifier to the Customer. In accordance with ICAO Doc 9303, there is a set of

minimum requirements to successfully perform an authentication, which are covered by the ID Verifier SDK data minimisation policy (datagroup DG1 with the MRZ information, DG2 with the face image and DG11 with additional personal data). Information about the End User include:

- document type/number and expiration date
- issuing country
- picture
- full name of holder
- nationality
- date of birth
- gender
- optional data (including national identification number, if present)
- facematch level from 1-9:

Level 0 – no match
Level 1 – 1/100 FAR
Level 2 – 1/250 FAR
Level 3 – 1/500 FAR
Level 4 – 1/1000 FAR
Level 5 – 1/10000 FAR
Level 6 – 1/100000 FAR
Level 7 – 1/500000 FAR
Level 8 – 1/950000 FAR
Level 9 – 1/1200000 FAR

4 Technical documentation

The technical documentation for use and implementation of the service is available online. The documentation is continuously updated when the service is modified with new, changed or removed functionality here:
IN Groupe ID Verifier (app and SDK) The documenting includes information on how to integrate against Nets E-Ident API in order to enable ID Verifier in the Customer services/web flow.

Technical Specifications

Android support
ID Verifier supports Android 6 and higher, on smart phones and tablets with NFC. Nets will stop supporting Android versions when this is commercially unreasonable and/or because of security concerns and/or because of technical concerns. Unless there is an urgent technical or security reason that reasonably inhibits the service, dropping support for an Android version will be announced at least one month in advance.
Problems may occur with specific smart phones due to the NFC implementation, or with new Android versions. In that case, if possible and commercially reasonably, ID Verifier will be updated. Examples of problems are phones that do not support NFC-B or do not support extended length application protocol data units (ADPUs). There may be smart phones or tablets in which the application may not function or functions less efficiently.

iOS support
ID Verifier supports iPhone 7 and higher (iOS 13.1 onwards).
There may be iPhones and iPads in which ID Verifier may not function, due to the absence of NFC capability or suitability, including problems with certain types of identity documents.

Supported ID documents
There may be identity documents that are not fully ICAO 9303 standard compliant or otherwise cause problems when scanning, reading or verifying. In that case, Nets will seek to update the ID Verifier within reasonable time.
Some identity documents may not work with certain smart phones or tablets. Nets will upon request, with reasonable effort, provide the Customer with information on what identity document are supported, especially within the EU.

4.1 INITIAL IDENTITY VALIDATION

It is important to understand the key security features incorporated into electronic identity documents:

- Privacy – protects the document holder's personal information through access-control mechanisms and safeguards against eavesdropping.
- Authenticity – ensures that the data stored in the chip has not been forged, altered, or tampered with.
- Clone detection – verifies whether the chip is genuine and identifies attempts to use duplicated or copied chips.

Method to prove possession of private key
Not applicable.

Authentication of organization identity
Not applicable.

Authentication of individual identity
The process involves several steps to ensure the integrity and reliability of the applicant's identity verification.

Document and Data Verification

- Verifying the authenticity of the applicant's identity document to ensure it has not been forged or altered.
- Reading and validating the personal data stored in the document's chip. This includes the applicant's full name, date of birth, unique identifier, document expiry date, document number, nationality (except for electronic driving licences), gender, and the facial image embedded in the chip.

Biometric Verification
In Groupe also performs biometric checks to confirm that the person presenting the document is its rightful holder:

- **Conducting liveness detection** to ensure the facial image captured during registration belongs to a real, live person.
- **Comparing the applicant's live facial image with the image stored in the chip** to confirm a biometric match.

Non-verified subscriber information

In Groupe verifies only the information obtained directly from the applicant's identity documents. It does not validate any additional data that may be required by the TSP during user registration, such as mobile phone number, residential address, email address, or IP address.

Validation of authority
No stipulation.

Criteria for interoperation
No stipulation.

5 Certificate life-cycle operation requirements

5.1 CERTIFICATE APPLICATION

For a certificate application using IN Groupe's ID Verifier, the applicant must present a valid, government-issued electronic identity document (eMRTD or eDL). All applicants are natural persons.

During the application process, before a session begins, the applicant is informed of accepting the terms and conditions within the app and this is controlled by us. The welcome page of the IN

Groupe ID Verifier Mobile Application clearly states that the applicant will undergo identity data, document verification and biometric face verification on behalf of the TSP.

5.2 CERTIFICATE APPLICATION PROCESSING

IN Groupe's ID Verifier performs identity data verification, document authenticity checks, and biometric facial verification as part of the registration process. The results of these procedures are provided to the TSP, who use them to determine whether a certificate application should be approved or refused.

The TSP must, at a minimum, refuse to issue a certificate if:

- The identity data provided in the certificate application does not match the data retrieved from the chip of the identity document.
- The identity data, document validity, or authenticity checks fail.
- The biometric verification or liveness detection fails.

5.3 CERTIFICATE ISSUANCE

Does not apply.

5.4 CERTIFICATE ACCEPTANCE

Does not apply.

5.5 KEY PAIR AND CERTIFICATE USAGE

Does not apply.

5.6 CERTIFICATE RENEWAL

Does not apply.

5.7 CERTFICATE RE-KEY

Does not apply.

TIFICATE MODIFICATION

Does not apply.

5.8 CERTIFICATE REVOCATION AND SUSPENSION

Does not apply.

5.9 CERTIFICATE STATUS SERVICES

Does not apply.

5.10 END OF SUBSCRIPTION

Does not apply.

5.11 KEY ESCROW AND RECOVERY

Does not apply.

6 Management, Operational, and Physical Controls

IN Groupe's management establishes and upholds the security policy that forms the foundation for ensuring consistency and completeness in information security. Management is responsible for approving all policies and practices related to the information security of the IN Groupe's services. In addition, IN Groupe's management ensures that these security policies and procedures are communicated to employees and to all relevant external parties, including TSPs and subcontractors, who are affected by them.

6.1 PHYSICAL SECURITY CONTROLS

6.1.1 Site Location & Construction

All IN Groupe operational facilities are purpose-built for high-security computing environments and are tailored to meet the security requirements applicable to an identity document verification service provider supporting trust service providers. IN Groupe conducts its operations from secure data centers located within Europe. These facilities are protected by comprehensive logical and physical controls that ensure identity verification processes remain inaccessible to non-trusted personnel.

IN Groupe operates under a security policy designed to detect, deter, and prevent any unauthorized access to IN Groupe's operations. The data centers are equipped with prevention and detection mechanisms that address a range of environmental risks, including power outages, communication failures, water exposure, fire, and temperature fluctuations.

6.1.2 Physical and environmental security

The physical and environmental security is in accordance with NSF. This means that proper entry controls, protection against external and environmental threats, cabling security, and maintenance of equipment are in place.

IN Groupe IDV environment runs in data centers, in an active-active set-up, across multiple locations and is subject to strict access and access requirements (four eyes principle) - also including other physical measures such as 24/h security, surveillance, alarms, access cards with code.

6.1.3 Power and Air Conditioning

IN Groupe maintains appropriate heating, ventilation, and air-conditioning systems to ensure stable temperature and humidity levels within its facilities. These environmental controls are designed not only to protect operational equipment but also to support the comfort and well-being of employees working on site.

6.1.4 Fire Prevention and Protection

IN Groupe has implemented appropriate safeguards to prevent, detect, and extinguish fires, as well as to mitigate any potential damage caused by flame or smoke. These measures ensure a secure operating environment and support the continued protection of systems, personnel, and facilities.

6.2 Cryptographic Controls

To ensure consistent and secure management of cryptographic controls, these are always selected and used in accordance with IN Groupe Data Protection and Integrity Guideline.

For IN Groupe IDV communication protocol TLS is used, and data is encrypted during transit. Be- tween frontend and backend IN Groupe Customer: the mobile app connects to the backend. It will send back parameters including a key to encrypt data and a dedicated URL as a destination (backend).

6.3 Operation Security

IN Groupe has implemented the ITIL-processes, including change Management. This ensures that operating procedures are thoroughly documented and kept up to date. Change management is strictly controlled and subject to board-approval. Development, test, and operational environments have been separated.

For IN Groupe IDV, Change Management procedures are documented, and changes are registered in the IT operations tool ServiceNow (note that larger and complicated changes are subject to Change Advisory Board-approval). Patches are implemented in a stages approach: test, staging, pre-production, production. Front-end servers are maintained by other teams (outside of security room). There is a monthly patch routine for these systems. Patches on front-end servers are deployed with the tool Roadrunner.

6.4 Media Storage

Media is stored in on-site safes.

6.5 Waste Disposal

Adequate measures are taken to dispose sensitive information.

6.6 Off-Site Backup

IN Groupe performs routine backups of critical system data, audit log data, and other sensitive information to ensure the continuity, integrity, and recoverability of its services. These backups are executed according to established schedules and are stored in secure, access-controlled environments. Backup processes are regularly tested to confirm that data can be successfully restored when required.

6.7 PROCEDURAL CONTROLS

6.7.1 Trusted Roles

The following trusted roles critical for security are:

Technical Architect: IN Groupe's Technical Architect holds overarching responsibility for the technical design, architectural integrity, and long-term maintainability of IN Groupe's ID Verifier. This role ensures that the system's architecture remains secure, scalable, and aligned with both business objectives and regulatory requirements.

Service Owner: The Service Owner for IN Groupe's ID Verifier holds end-to-end responsibility for the delivery, performance, and continuous improvement of the service. This role ensures that ID Verifier operates reliably, securely, and in alignment with contractual obligations, regulatory requirements, and customer expectations.

Compliance Manager: The Compliance Manager for IN Groupe's ID Verifier holds overarching responsibility for ensuring that the service operates in full alignment with applicable laws, regulations, standards, and internal policies. This role provides independent oversight across the service lifecycle and ensures that compliance requirements are embedded into daily operations, development activities, and strategic decision-making.

Product Manager/ Product Owners: IN Groupe's Product Manager and Product Owners hold overarching responsibility for the development and lifecycle management of IN Groupe's ID Verifier. Their mandate extends beyond day-to-day coordination and includes ensuring that all development activities adhere to established quality standards, security requirements, and regulatory expectations.

Developers: Developers working on IN Groupe's ID Verifier are responsible for implementing high-quality, secure, and maintainable software that aligns with the product's functional, architectural, and regulatory requirements. Their work directly contributes to the reliability, security, and performance of the service delivered to trust service providers.

Network & Operations Team: This team designs, configures, and maintains routers, switches, firewalls, and core connectivity. Also handles day-to-day network operations, monitoring, and troubleshooting

Senior management: Senior Management at IN Groupe holds ultimate responsibility for the strategic direction, governance, and oversight of the ID Verifier service. Their role ensures that the service operates in alignment with the organization's mission, regulatory obligations, and long-term business objectives.

6.7.2 Number of Individuals required per task

IN Groupe ensures that staffing levels are sufficient not only to meet operational demand but also to uphold all security, risk management, and compliance obligations. The organization allocates personnel in a way that supports reliable service delivery while maintaining the rigorous controls required for a secure and compliant operating environment.

6.7.3 Identification & Authentication for Trusted Roles

Employees in Trusted Roles at IN Groupe undergo background screening, and all employees are verified and authenticated through identification checks based on government-issued identity documents. User accounts are created only for personnel whose roles require access to specific systems. Each user must authenticate using their personal account, and administrative commands are restricted to individuals with explicit authorization, with all such actions subject to detailed auditing. Two-factor authentication is mandatory for access to critical systems.

Access to live production data belonging to an IN Groupe customer TSP is strictly limited to exceptional circumstances, such as investigating suspected document fraud or performing debugging activities, and only with the explicit consent of the affected TSP. Any access to such data is fully logged in audit records made available to the TSP, with technical safeguards in place to prevent tampering.

6.7.4 Roles requiring separation of duties

When assigning Trusted Roles, IN Groupe applies the principle of separation of duties. Conflicting responsibilities and areas of potential risk are identified and deliberately segregated to minimize the possibility of unauthorized or unintentional modification, misuse, or compromise of assets. This structured division of responsibilities ensures stronger internal controls and supports the integrity and security of all operations.

6.8 PERSONNEL SECURITY CONTROLS

IN Groupe conducts pre-employment screening for all employees and contractors who have access to IN Groupe source code, cloud services, or who hold senior management positions. These checks are carried out in accordance with contractual and regulatory obligations and include, at a minimum, a criminal background check. Relevant screenings are periodically repeated to ensure ongoing compliance and suitability.

IN Groupe maintains a highly qualified workforce, with employees generally holding advanced education in their respective fields.

IN Groupe employees complete mandatory annual training to ensure they are fully prepared to perform the duties outlined in their employment contracts and job descriptions before undertaking any operational or security-related tasks. This training is continuously reinforced throughout the duration of their employment, ensuring that skills, awareness, and compliance with security and operational requirements remain up to date.

6.8.1 Internal Organisation

The practices, which IN Groupe operates under are non-discriminatory and revolve around segregation of duties. IN Groupe personnel have the necessary education, training, technical knowledge and experience to provide IN Groupe SIS (Signing & Identification) services. Segregation of duties and Identity and Access Management are done accordingly to NSF.

IN Groupe financial and organizational reliability can be attested through publicly available annual reports. Service agreements and internal policies for vendor management, procurement, outsourc- ing and contractual relationships are in place.

- IN Groupe IDV Subcontractors: Inverid/ReadID is used for document scanning and offers own certification as eIDAS module for assurance level High issued by TUV Austria; while the comparison of the high-resolution image from the ID-document with the captured biometric sample is per- formed with a local installation within IN Groupe infrastructure (Norway). Since 2024, this solution has been migrated from previous Amazon Web Services (AWS) instance to a fully European cloud provider, Open Telekom Cloud (OTC).
- IN Groupe IDV applicants/data subject policy: the IN Groupe GDPR web portal is used https://www.IN Groupe.eu/GDPR/dsr/Pages/request.aspx to exercise own rights.

IN Groupe ID Verifier qualifies for eIDAS compliant identity proofing and is certified by a Conform- ity Assessment Body, BSI (The British Standards Institution, BSI Group The Netherlands B.V.) Con- formity certifications against eIDAS Regulation 910/2014, ETSI EN 319411-2 (Trust Service Com- ponent: Registration Service), including ETSI TS 119 461 on Identity Proofing of Trust Service Subjects and BITS are publicly available at: BSI eCertificate Service - Validate eCertificate (bsigroup.com)

6.8.2 Background Check Procedures

IN Groupe HR Onboarding Policy ensures the employment of personnel and, if applicable, subcon- tractors, who possess the necessary expertise, reliability, experience, and qualifications.

IN Groupe Security Academy offers adequate training for security and personal data protection rules as appropriate for the offered services and job function.
Trusted Roles for the IN Groupe IDV service (such as security officer, system administrator/operator) are approved by management and issued to qualified personnel that has access to data center facilities and that can perform system/application configurations.

6.8.3 Training Requirements and Procedures

IN Groupe requires all personnel to complete security training on an annual basis. The content and depth of this training are tailored to each employee's role, ensuring that individuals receive the knowledge and competencies relevant to their responsibilities. Additional specialized training or certifications may be scheduled as part of each employee's personal yearly development plan.

Upon joining the organization, all new employees follow a structured onboarding training program. This includes mandatory security-awareness training as well as function-specific instruction covering areas such as software, hardware, operational procedures, and any other skills required for their role.

IN Groupe maintains detailed records of all completed training activities, including which employees have participated and the level of training achieved, ensuring full traceability and ongoing compliance.

6.8.4 Retraining Frequency and Requirements

All employees are required to attend regular security awareness training sessions.

6.8.5 Sanctions for Unauthorized Actions

IN Groupe employees who fail to comply with this TSPS, whether through negligence or intentional misconduct, are subject to established internal procedures that define appropriate administrative or disciplinary actions. These measures may include corrective actions, formal warnings, suspension, termination of employment, and, where applicable, referral for legal proceedings.

6.8.6 Independent Contractor Controls

IN Groupe employs contractors. Contractors employed in trusted roles at ReadID are background checked per the procedures used for direct personnel.

6.8.7 Documentation Supplied to Personnel

All employees receive an employment contract, a clearly defined job role, and a personnel handbook. Together, these documents outline the employee's responsibilities, rights, and obligations, as well as the laws, policies, and procedures that govern employment at IN Groupe.

6.9 AUDIT LOGGING PROCEDURES

IN Groupe ensures that all relevant information concerning the operation of the Trust Services is recorded to provide evidence for the purpose of legal proceedings.

IN Groupe IDV can return all or a subset of the data to IN Groupe Customer. Each IN Groupe Customer decides on what subset of data is needed according to their identity proofing context. Protected data (e.g. data read from the RFID-chip of a document) is not read according to IN Groupe data minimization policy.

Full list of attributes is available at: eIDs (IN Groupe.eu). Depending on the identity proofing con- text, unique identification can be in the form of an attribute such as a national identity number, or as one or more additional attributes that together with the full name provide unique identification. A country attribute and serial number attribute are e.g. usually required to guarantee unique identity.

6.9.1 Attribute collection for natural person

NFC Technology is used to perform the reading and verification of the contactless chips in identity document that are ICAO Doc 9303 compliant, such as electronic passports, identity cards and resi- dence cards. More specifically, the reading and interpretation of DG1 with the MRZ information, DG2 with the face image, D7 with written signature (if present), DG11 with additional personal in- formation (if present) and DG12 with additional document information (if present).
Sample of data overall processed in IN Groupe IDV:

- document type/number and expiration date

- issuing country
- picture
- full name of holder
- nationality
- date of birth
- gender
- optional data (including national identification number, if present)
- biometric/liveness data (collected during video selfie to prove that a person is a real human being)

6.9.2 Attribute and evidence validation

Optically the identity data is obtained from the Machine Readable Zone (MRZ) with Optical Charac- ter Recognition technology. The MRZ contains amongst others the family name, first name(s) and date of birth of a natural person. This set of attributes corresponds with the minimum data set as specified in eIDAS CIR 2015/1501 to uniquely identify a natural person. Electronically the data is read from the chip via NFC technology. This information has been provided by the issuing country of the identity document, based on strict government identity verification and issuing processes. Besides providing very reliable personal information, another major advantage is that all data is electronically available. There is no manual input required, so there can be no mistakes in the data. If the country has opened DG11, IN Groupe IDV is able to provide latin and non-latin characters. Since the data extracted may differ from its physical representation (e.g country specific/Norwegian character) and to prevent OCR mistakes, so called-checked digits and national characters are encoded as per ICAO DOC 9303 rules.

The validity of a document can be checked by looking at the expiration date of the identity document. The authenticity is checked by validating the digital signature of the data obtained from the chip via NFC against a list of country signing certificates. Several online databases of trustworthy Country Signing Certificates exist. For example, the French, German, Italian, Schengen, Swiss and Spanish CSCA master lists are published by each of these respective countries, specifying which certificates it considers trustworthy.

Protection against stolen or revoked identity documents is ensured during the binding to the applicant through biometric; access to authoritative sources of information on document, e.g. TOVE register in Norway/Interpol register, can be supported through IN Groupe but is left at the discretion of IN Groupe Customer.

6.9.3 Use of digital identity documents as evidence

IN Groupe IDV uses ReadID SDK to read the RFID chip of ICAO compliant documents (including physical passports and ID-cards), meaning that IN Groupe is only using digital identity document properties.

IN Groupe IDV only works with ICAO-compliant documents:

- passports and residence permit that meet the International Civil Aviation Organization (ICAO) specifications for machine-readable travel documents,
- identity cards from an EU or European Economic Area (EEA) country that follow the Council Regulation (EC) No 2252/2004 standards, or,
- EU or EEA driving licenses that follow the European Directive 2006/126/EC.

Note that all these identity documents are government issued with strict identity verification and issuing requirements and, as such, provide an authoritative source for identity proofing and verification.
A full list of available documents per country is available to IN Groupe Customer upon request.

6.9.4 Validation of digital identity documents

ReadID is used for document scanning and offers own certification as eIDAS module for assurance level High issued by TUV Austria. ReadID implements for ICAO 9303 compliant identity documents:

- the Basic Access Control (BAC) security mechanism for getting access to the chip;
- the Passive Authentication security mechanism for verifying the authenticity of the read data;
- the Active Authentication security mechanism for verifying the authenticity of the

chip (e.g. clone detection);
- the Chip Authentication (EAC-CA) security mechanism for clone detection; and
- the reading and interpretation of DG1 with the MRZ information, DG2 with the face image, D7 with written signature (if present), DG11 with additional personal information (if present) and DG12 with additional document information (if present)
- Password Authenticated Connection Establishment (PACE) which is a successor of BAC that uses more modern cryptography to provide an increased level of security. Note that EU mandates the implementation of PACE by its member states for newly issued travel documents. Passports that have support for PACE also support BAC to remain compatible with the ICAO 9303 standard, that requires documents that support PACE to also support the older BAC.

These security features only apply to the supported digital identity documents and do not extend to e.g attestation or additional authoritative sources.

Data in transit is encrypted using standard TLS protocol and data integrity features are in place to safeguard the integrity of stored data. All IN Groupe IDV keys and licenses are stored in the security room. Each key is stored in duplicate at 2 different server locations. Each key is used for one operation/purpose only. Compromised, revoked, lost keys must be discarded immediately according to NSF. A new key must be generated to replace the compromised one. Keys that become inva- lid (corrupt, revoked or lost) can be immediately replaced by new ones without interrupting the ser- vice.

6.10 Binding to applicant

A technical session identifier, also known as transaction identifier (TID), is defined to initiate a se- cure identity proofing process. A visual session identifier is displayed to the applicant in the form of QR code or activation code.

Besides the identity data and document verification functionality, IN Groupe IDV also performs identity document holder verification. This proves that the applicant holding the identity document is indeed the rightful owner of the document.

IN Groupe IDV compares the high-resolution image from the ID-document with the captured bio- metric sample. The face matching algorithm entails:

- Perspective distortion (zoomed and unzoomed video frames): ensures the user's face is three- dimensional.
- Liveness detection: measures up to 50 diverse attributes (light reflection, pupil dilation, blinking, subtle movements etc) to prevent facespoofing attacks. A 3D shape-based face representation is created because of these techniques.

6.11 Capture of face image of the applicant

3D shape-based face representations are reverse engineered from 100+ video frames captured during the 2 second user video selfie, are always encrypted and aren't human viewable. They have been evaluated from 10.000+ devices from 170+ different countries and contain sessions from users with shadows, directional light, glare in glasses, non-neutral expressions, and low-light scenarios.

The technology in use achieved Level 1&2 PAD certifications in sanctioned third-party testing. More specifically, it was the first and only biometric to achieve a Level 1 & 2 rating in the NIST/NVLAP- certified iBeta Presentation Attack Detection (PAD) ISO 30107-3 Certification Test. It works with any camera of 0.3 - 20 megapixels and is much less dependent on the quality of the device than classic 2D engines. Resilience against other specific biometric attacks include extensive documentation against camera/video injections, passport morphing, alteration and anti-tampering.

IN Groupe IDV mobile apps for iOS & Android are stateless/impersonal and only to be used for col- lection of raw data, which is sent encrypted using TLS 1.2 to IN Groupe E-Ident service where the data is processed. Security features related to rooting, hi-jacking, jail in the mobile apps include root detection and certified pinning, manual code for repacking detection, app installation, debugging, logging fraud data and communication with IN Groupe E-Ident backend.

Note that IN Groupe IDV app is impersonal which is why, by design, there is no way for IN

Groupe to control how many fraudulent attempts a user may try. To detect potential fraud, IN Groupe Customers can categorize collected data at the backend per document number/user data in order to seamlessly detect any suspicious user behavior e.g. recurring scanning of a document, or recurring username completing multiple identification processes.

Best practices are typically discussed with IN Groupe Customers during onboarding routine to collect analytics meant to display collected user's data (on top of today's issued ID token and PDf/PAdES). Analytics typically cover type/country of documents, mobile device model used etc. IN Groupe is planning to develop its own post-authentication dashboard as complementary service (2026 roadmap).

6.12 Automated face biometrics

A confident score is returned for each identification as a Face Match Level. IN Groupe IDV face recognition algorithm boasts a real-world false acceptance rate (FAR) of 1/1.200.000 FAR with less than a one-percent false rejection rate (FRR).

6.12.1 Level 9 – 1/1.200.000 FAR
6.12.2 Level 8 – 1/950.000 FAR
6.12.3 Level 7 - 1/500.000 FAR*
6.12.4 Level 6 - 1/100.000 FAR
6.12.5 Level 5 - 1/10.000 FAR
6.12.6 Level 4 - 1/1.000 FAR
6.12.7 Level 3 - 1/500 FAR
6.12.8 Level 2 - 1/250 FAR
6.12.9 Level 1 - 1/100 FAR
6.12.10 Level 0 - Non-match

*This level is the benchmark for eIDAS High configuration as a minimum, according to referenced industry best practices.

Also note that the IN Groupe IDV matching algorithm is expected to improve over time based on continuous testing and refinement.

6.13 Issuing of proof

End user information will be returned in ID Token/SAML assertion to IN Groupe Customers based on OIDC scope and identification parameters. A link to download images is added to the returned ID Token /SAML assertion. The images will be available for a short while after identification is com- plete.
In addition, the calling application can download a signed PDF with all end user info including pic- ture. Example: PAdES.pdf

Pending on the identity proofing context, IN Groupe IDV can support eIDAS High level of assurance (LoA). Configuration parameters are available at section 19.3 (Automated Operation) of this TSPS.

6.14 Evidence of the identity proofing process

All data read from the RFID chip (transaction data), including the high-resolution picture, is availa- ble as ID token and/or PDF/PAdES with a 90 days retention period. Liveness data collected during video selfie to prove that a person is a real human being is only valid for few minutes.

The data is stored in its original form, e.g. it is not decoded, decrypted or transcoded to a different format. The server, and database are both inside a secure computer environment in the security room. The database is integrity protected and only authorized personnel has access to read the da- tabase.

Data is deleted after 90 days, according to the defined retention policy. It is then up to IN Groupe Customer to implement its own retention/archiving policy based on identity proofing context.
For logs and audit trail, image from video sequences can be additionally provided and processing of it is regulated in the app privacy policy/statement. All successful identifications are logged in

statis- tics for invoicing purposes only.

Privacy Enhancing Technologies (PETs) are implemented across the solution.

7 Identity proofing use cases

IN Groupe IDV conforms to the following use cases specified in ETSI TS 119 461 Chapter 8:
- 8.1 (initiation);
- 8.2.1 (attribute and evidence collection general requirements);
- 8.3.1 (attribute and evidence validation general requirements);
- 8.4.1 (binding to applicant general requirements); and
- 8.5 (issuing of proof).

Upon identity proofing context, country specific national legislation and government policies on applicable technology may pose requirement on the above use cases. E.g. in some countries, physical presence can be mandated for certain purposes of identity proofing, or remote identity proofing can be restricted to allow only specific use cases.

7.1 Identity proofing of natural person

IN Groupe IDV does not require:
7.1.1 physical presence
7.1.2 online communication with a human registration officer

The identity proofing process is not hybrid, but fully digital and automated:
7.1.3 remote presence of the applicant with unattended online communication

7.2 Remote identity proofing

The applicant receives automated guidance throughout the identity proofing process. Cross-platform accessibility ensures both desktop and in-app user guidance (assisted flow in terms of next steps). IN Groupe IDV provides both in-app text aid to the end user (reason for failure/try again) while a list of error codes is sent to IN Groupe Customer. A 2nd line support is provided to both the applicants and IN Groupe Customer according to IN Groupe standard contractual terms.

The identity verification process in IN Groupe IDV app is user-friendly and intuitive (incl. video tutorials) and can be fully performed in under two minutes. The end user accepts IN Groupe IDV app privacy policy, inputs a unique activation code, digitally scans the machine-readable zone (MRZ) of the selected document, verifies the chip through near-field communication (NFC) and performs face recognition.

In-app error messages have been added through each step of the process (MRZ scan, NFC read and biometric) for collecting TID (technical identifier) and help users get quick help in case or errors.

Successful verification is dependent on meeting applicable requirements (e.g. usage of supported devices, environmental conditions) according to the identity proofing context (e.g. pass eIDAS High configuration parameters).

Once done with the in-app process, a live update on IN Groupe Customer's controlled webpage in- forms the end user that the identity has been successfully verified or not. IN Groupe Customer can flexibly decide on next steps:
- Failed authentication: please try again (or other - if fraud is detected)
- Successful authentication: congratulations message and next steps (e.g. KYC questionnaire/end-user self-assessment).

7.3 Automated operation

IN Groupe IDV conforms to the following use cases specified in ETSI TS 119461 Chapter 8:

- 8.3.2 (validation of digital identity document);
- 8.4.3 (binding to applicant by automated face biometrics)

Based on feedback from the supervising authorities in the Nordics, IN Groupe has stopped the implementation of a pre-configured eIDAS High profile, as such a "named profile", with subsequent parameters, is up to each national supervisory bodies definition.
As a consequence, IN Groupe does not enforce a pre-configured eIDAS High LoA configuration (set parameters) to Customers purchasing the ID Verifier service, but instead IN Groupe offers a recommended configuration/set of parameters to achieve High LoA in order to comply with the highest security level and/or mitigate risk to its lowest.

IN Groupe ID Verifier eIDAS High configuration is based upon:
- document scanning through NFC with no allowance for expired documents
- no clone detection / passed control of document authenticity
- biometric facematch level: level 7 (1/500.000 FAR with <1% FRR) as a minimum

Overall, The NFC data from the eMRTDs contain a rich set of data packets that can be used to establish proof of authentication. These are: NFC session status (active and passive); NFC data verification status (data integrity); document signer certificate chain; data groups extracted from the travel document.

To return adequate proof of authentication and ensure full traceability, effective from 03/2023, IN Groupe IDV supports a full audit trail functionality accessible e.g. along the issued ID token resulting from an authentication session:

- Chip session authentication results (e.g. BAC succeeded)
- Clone detection status (passed/not passed incl. reason)
- Certificate chain (incl. country signer certificate/key for audit trail evidence against ICAO)
- Face Match Level (now incl. level 0 in case of failed attempt)
- Transaction timestamp (start, end)
- Transaction milestones (docscan, facescan time)
- Device info (OS, version number etc)

7.4 KEY CHANGEOVER
Not applicable.

7.5 COMPROMISE AND DISASTER RECOVERY
IN Groupe has developed a business continuity plan to make disaster recovery possible. Multiple scenarios have been identified, some of which have been simulated during training sessions. Mitigations for each scenario are in place.

7.6 TERMINATION

IN Groupe has developed a termination plan to be executed if a decision is made to terminate IN Groupe ID Verifier Service Agreement. Termination procedures include
- notification of affected entities; and
- where applicable, transferring the TSP's obligations to other parties.

8 Technical Security Controls

8.1 KEY PAIR GENERATION AND INSTALLATION
Not applicable.

8.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS
Not applicable.

8.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT
Not applicable.

8.4 ACTIVATION DATA
Not applicable.

8.5 COMPUTER SECURITY CONTROLS

IN Groupe infrastructure is segmented into security zones protected by multiple firewalls based on the functional, logical and physical relationship between the systems and services. The SIS (Signing & Identification) service of which the IN Groupe IDV environment is part of, is e.g. running on a separate subnetwork for authorized personnel. Penetration tests are performed in different variants and are available upon IN Groupe Customer request.
To ensure consistent and secure management of cryptographic controls, these are always selected and used in accordance with IN Groupe Data Protection and Integrity Guideline.

For IN Groupe IDV communication protocol TLS is used, and data is encrypted during transit. Between frontend and backend IN Groupe Customer: the mobile app connects to the backend. It will send back parameters including a key to encrypt data and a dedicated URL as a destination (backend).

8.5.1 Operational Security Controls

IN Groupe has implemented the ITIL-processes, including change Management. This ensures that operating procedures are thoroughly documented and kept up to date. Change management is strictly controlled and subject to board-approval. Development, test, and operational environments have been separated.
For IN Groupe IDV, Change Management procedures are documented, and changes are registered in the IT operations tool ServiceNow (note that larger and complicated changes are subject to Change Advisory Board-approval). Patches are implemented in a stages approach: test, staging, pre-production, production. Front-end servers are maintained by other teams (outside of security room). There is a monthly patch routine for these systems. Patches on front-end servers are deployed with the tool Roadrunner.

8.6 NETWORK SECURITY CONTROLS

IN Groupe infrastructure is segmented into security zones protected by multiple firewalls based on the functional, logical and physical relationship between the systems and services. The SIS (Signing & Identification) service of which the IN Groupe IDV environment is part of, is e.g. running on a separate subnetwork for authorized personnel. Penetration tests are performed in different variants and are available upon IN Groupe Customer request.

8.7 CERTIFICATE PROFILE

Not applicable.

8.8 CRL PROFILE

Not applicable.

8.9 OCSP PROFILE

Not applicable.

9 Compliance Audit and other Assessment

ASSESSMENT OBJECTIVES

The objectives of the recertification audit are:

- To assess the readiness for renewal of the conformity certificate ETS-092 (Regulation (EU) 910/2014, ETSI EN 319 411-2) (replacing ETS 072 due to a legal entity name change).
- To assess as to whether IN GROUPE TS and trusted services components services provisioning comply with the applicable assessment criteria.
- To provide a conformity assessment report for the purpose of disclosure to the supervisory body in which the trust service provider is registered.
- A corrective action plan is provided separately, if applicable.

The audit was planned and performed in accordance with ETSI EN 319 403-1 v2.3.1 - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.

It was conducted as a hybrid onsite and remote interview-based audit, with oral evidence collected and documented through records or other formats, as well as through visits to the sites of Data Centers operations. During these audit activities, the applicant confirmed that the scope of the audit corresponds to its trust services components provisioning to customers.

The Trust Service component is being provided for the following qualified trust services as defined in Regulation (EU) 910/2014 (eIDAS):

- Provision of qualified certificates for electronic signatures (qualified trust service)
- Provision of qualified certificates for electronic seals (qualified trust service)
- Provision of qualified certificates for website authentication (qualified trust service)

During the audit procedures, evidence was provided and confirmed by the assessor demonstrating that only

the "provision of qualified certificates for electronic signatures (qualified trust service)" applies to IN GROUPE TS.

Being so, the paragraph above will henceforth be written as follows:

The Trust Service component is being provided for the following qualified trust services as defined in Regulation (EU) 910/2014 (eIDAS):

- Provision of qualified certificates for electronic signatures (qualified trust service)

The applicable IN GROUPE TS policies are the following:

- *IN GROUPE TS - Trust Service Practice Statement (TSPS) & Identity Proofing Service Practice Statement (IPSPS)*

version 3.3 25.09.2025

- *IN GROUPE GLOBAL - INFORMATION SECURITY POLICY version 1.4 02.09.2021*

9.1 COMMUNICATION OF RESULTS

Compliance audit reports and their scope can be requested on IN Groupe's website ID Verifier | IN Groupe The audit reports are confidential, and are given to the disposal of national supervisory bodies.