Identity Proofing Service Practice Statement

Ver. 1.6

November 10, 2026

History

ID	Changes	Rev.	Date	Author	Verified	Approved
IPSPS	First version in Italian.	1.0	15/12/25	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Added §3.2.4, §3.3.4, §3.4.7, §3.4.8, §3.4.9	1.1	15/04/26	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Added §3.1.9 (Identity Proofing with EUDIW PID + eMRTD NFC) and §3.1.10 (Unattended Remote Identity Proofing eMRTD); new OIDs 9.7 and 9.8 in table §1.2; alignment with EAAS Practice Statement and EAAS Service Policy v1.0.	1.2	04/06/26	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Added §3.2.4.2 Management Operating Procedure, §3.4.9.1 List of Records and Sources. Modification §3.3.4 Data acquisition methods	1.3	26/06/26	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Amended paragraphs §1.2, §3.1, §3.2, §3.3, §3.4, §3.5, §3.6, §4.4.3	1.4	11/08/26	D.Saccò	F.Barcellini	P.Sironi
IPSPS	Added resolution table in section §3.3.4	1.5	15/10/26	D.Saccò	F.Barcellini	P.Sironi

IPSPS	Revised sections: §1.2, §1.4.3, §3.1, §3.1.3, §3.1.4, §3.1.5, §3.2, §3.2.2, §3.3.1, §3.3.2, §3.3.3, §3.3.4, §3.4.3, §3.4.4, §3.4.6, §3.5.4, §3.5.5, §3.5.6, §3.6.1, §3.6.2, §4.4.3, §4.6.1, §4.6.2, §5.6. New sections: §3.3.3.3, §3.4.6.4, §3.4.6.5, §3.5.7. Removed the FEQ use case (OID 1.3.6.1.4.1.48990.1.1.9.4: §3.1.4, §3.2.2.3, §3.2.3.5, §3.3.2.3, §3.3.3.3, §3.3.4.3, §3.4.3, §3.5.4 of v1.5) and the eMRTD use case (OID 1.3.6.1.4.1.48990.1.1.9.7: §3.1.7, §3.2.2.6, §3.2.3.3, §3.3.4.6, §3.4.6, §3.5.7 of v1.5). Sections renumbered accordingly.	1.6	10/11/26	D.Saccò	F.Barcellini	P.Sironi

Table of Contents

1 INTRODUCTION 8

1.1 Overview 8

1.2 Document name and identification 8

1.3 Level of Identity Proofing 10

1.4 IPSP Participants 10

1.4.1 Intesi Group as an Identity Proofing Service Provider 10

1.4.2 Qualified Trust Service Provider 11

1.4.3 Subject or Applicant 11

1.4.4 Registration Officer 11

1.4.5 Local Registration Authority 11

1.4.6 External Identity Proofing Service Provider (External IPSP) 11

1.4.7 Other participants 12

1.5 Administration of the IPSPS 12

1.6 Definition and acronyms 12

2 PUBLICATION 13

2.1 Published information 13

2.2 Date and frequency of publications 13

2.3 Access 13

3 IDENTITY VERIFICATION 13

3.1 Types of identification (Use cases) 13

3.1.1 In-person (Use Case 9.2.1.2 in [4]) 14

3.1.2 Unattended Remote (Use Case 9.2.3.3 in [4]) 14

3.1.3 Via eID with "high" assurance level (Use Case 9.2.4 in [4]) 15
3.1.4 Legal Entities (Use Case 9.3 in [4]) 15
3.1.5 Individual representing a Legal Entity (Use Case 9.4 in [4]) 16
3.2 Preliminary phase 16
3.2.1 Information and consent 17
3.2.2 Means of identification required 17
3.2.3 Technological tools 19
3.2.4 Accessibility for people with disabilities (eIDAS Art. 15) 19
3.3 Applicant Data Collection 21
3.3.1 Data collected 21
3.3.2 Accepted Proofs of Identity 22
3.3.3 Data acquisition methods 24
3.3.4 Freshness 25
3.4 General data validation 27
3.4.1 Physical or Remote Identification Validation (Use Cases 3.1.1 e 3.1.2) 28
3.4.2 eID Validation (eID Validation 3.1.3) 30
3.4.3 Legal Entity Validation (Use Case 3.1.4) 31
3.4.4 Validation of a Natural Person representing a Legal Person (Use Case 3.1.5) 31
3.4.5 Anti-Fraud Controls (All Use Cases) 31
3.4.6 Validation through trust registers and authoritative sources 32
3.4.7 Validation through Proof of Access of contact details 35
3.4.8 Technological system for the acquisition of evidence and automated controls 36
3.5 Binding to Requester 41

3.5.1 Binding in Presence Identification (Use Case 3.1.1) 41
3.5.2 Binding in Remote Identification (Use Case 3.1.2) 41
3.5.3 Binding via Notified eIDs (Use Case 3.1.3) 42
3.5.4 Legal Entity Binding (Use Case 3.1.4) 42
3.5.5 Binding Natural Person representing Legal Entity (Use Case 3.1.5) 42
3.5.6 Discrepancy management 43
3.5.7 Face comparison by the Registration Officer 43
3.6 Release of the result 44
3.6.1 Type of outcome 44
3.6.2 Collection and storage of evidence 45
4 MANAGEMENT CONTROLS 45
4.1 Operational Risk Assessment 46
4.2 Threat analysis and monitoring 46
4.3 Personnel safety checks 47
4.3.1 Selection and reliability 47
4.3.2 Specialist training 47
4.3.3 Upgrade and retraining 48
4.3.4 Separation of roles 48
4.4 Physical and logical security 48
4.4.1 Physical security 48
4.4.2 Logical security and separation of systems 48
4.4.3 Communications and data protection 49
4.5 Incident and vulnerability management 49

4.5.1 Monitoring and Tracking 50
4.5.2 Vulnerability analysis 50
4.5.3 Reporting obligations 50
4.5.4 Communication to data subjects 50
4.6 Audit Recording and Evidence Retention 50
4.6.1 Type of events and evidence collected 50
4.6.2 Retention period 51
4.6.3 Security and Integrity 51
4.7 Business continuity and termination 52
4.7.1 Business Continuity and Disaster Recovery Plans 52
4.7.2 Termination of Service 52
4.8 Supplier management (Supply-chain) 52
4.8.1 Liability 53
4.8.2 Evaluation and Monitoring 53
4.8.3 Contractual Agreements 53
5 GENERAL TERMS AND CONDITIONS OF SERVICE 53
5.1 Service Fees 53
5.2 Financial responsibility and insurance 53
5.3 Privacy and protection of personal data 54
5.4 Intellectual property rights 54
5.5 Limits of liability 54
5.6 Complaints, dispute resolution and applicable law 54

1 INTRODUCTION

1.1 Overview

This Practice Statement (IPSPS) describes the IG Persona identity proofing service for verifying the identities of natural persons. The service is provided by Intesi Group S.p.A., acting as a Qualified Trust Service Provider, for the purpose of identity proofing service applicants.

In particular, this document describes the technical, security and organizational requirements adopted by Intesi Group S.p.A. to make the solution compliant with Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024, which establishes the European Digital Identity Framework and amends Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

This IPSPS is not intended to constitute a CPS within the meaning of RFC 3647 but adopts this structure as a methodological reference for the description of the *Identity Proofing service*.

This document supplements the operating manual of trust services published on the Intesi Group website:

[1] TSPPS Trust Service Practice Statement

The IG Persona solution meets the requirements of the following standards:

[2] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
[3] ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates.
[4] ETSI TS 119 461 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.
[5] ETSI TS 119 471 Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services

1.2 Document name and identification

This document is titled "Identity Proofing Service Practice Statement."

Name and version are also indicated on the front page.

The Object Identifiers (OIDs) to which the document is associated are listed in the following table, which also contains descriptions of the policies used for each identification method adopted:

Intesi OID (Object Identifier)	**Description**
1.3.6.1.4.1.48990.1.1.9.1	Use case related to the supervised verification of the identity of the applicant by means of a physical document, carried out in the presence of the applicant and assessed by a Operator (RAO), in accordance with the requirements of ETSI TS 119 461 described in paragraph 9.2.1.2.
1.3.6.1.4.1.48990.1.1.9.2	Use cases involving the use of a physical document for unattended remote identity proofing, with hybrid manual and automated operation (Complies with the requirements of ETSI TS 119 461 described in paragraph 9.2.3.3)
1.3.6.1.4.1.48990.1.1.9.3	Use cases involving identification by authentication with electronic identification means (eID) notified with Level of Assurance "High" (SPID Level 3 and CIE). (Complies with the requirements of ETSI TS 119 461 described in paragraph 9.2.4 and Annex C.3.2).
1.3.6.1.4.1.48990.1.1.9.5	Use cases for identity proofing of a legal person for the issuance of qualified certificates for electronic seals, at Extended LoIP (compliant with the requirements of ETSI TS 119 461, clause 9.3 and Annex C, clause C.3.5).
1.3.6.1.4.1.48990.1.1.9.6	Use cases for identity proofing of a natural person representing a legal person for the issuance of qualified certificates for electronic signature with role, at Extended LoIP (compliant with the requirements of ETSI TS 119 461 described in clause 9.4 and Annex C, clause C.3.6)

1.3 Level of Identity Proofing

The level of assurance achieved by the procedures that make up the IG Persona solution is high (Extended LoIP) and is described by the following ETSI Object Identifier:

ETSI OID (Object Identifier)	Warranty Level
0.4.0.19461.1.2	Extended Level of Identity Proofing (Extended LoIP)

1.4 IPSP Participants

Intesi Group S.p.A. is a trust services provider and uses, where applicable, the procedure for verifying the identity of natural persons as described in this IPSPS. These procedures are also used for the issuance of the SPID digital identity.

All services are provided by Intesi Group through infrastructures hosted in high-security data centers. The location and construction characteristics of the facilities hosting the services and equipment are designed to ensure the proper management and protection of sensitive and high-value information.

1.4.1 Intesi Group as an Identity Proofing Service Provider

Intesi Group is an Identity Proofing Service Provider (IPSP), and identifies itself as follows:

Company name: Intesi Group S.p.A.

Registered Office: Via Torino, 48 – 20123 Milan (MI) – ITALY

Legal Representative: Paolo Sironi (Board of Directors)

VAT number and Tax Code: IT02780480964

Phone: +39 02 6760641

ISO Object Identifier (OID): 1.3.6.1.4.1.48990

Company website: http://www.intesigroup.com

Company Email Address: intesi@intesigroup.com

1.4.2 Qualified Trust Service Provider

Intesi Group, acting as a QTSP, is responsible for managing the process and delivering trust services.

1.4.3 Subject or Applicant

The natural person requesting the service and undergoing identity proofing.

In the case of legal persons and of natural persons representing them (§3.1.4 and §3.1.5), the Applicant is the identified natural person, indicated in the authorization form as the delegate or as the person for whom the interested third party requests the certificate. The Signatory the legal representative of the entity or, for the electronic seal, an attorney with signing powers, who signs the authorization form and attaches the document proving their office or powers (§3.2.2). The Signatory is not the Applicant, unless the two persons are the same.

1.4.4 Registration Officer

Trained personnel who perform the identity proofing process, review the validation results, and verify the binding between the person and the submitted identity document. These personnel are either Intesi Group internal staff or employees of a third-party company to which Intesi Group has subcontracted the identity proofing service.

1.4.5 Local Registration Authority

Company employing the Registration Officer, acting as a subcontractor of the identity proofing service. Such companies shall be part of the Intesi Group supply chain.

1.4.6 External Identity Proofing Service Provider (External IPSP)

Intesi Group may use external suppliers that provide identity proofing services within its ICT supply chain. These entities provide technological and operational components for remote identity proofing. In this model, Intesi Group retains full legal and operational responsibility for the entire process towards the supervisory body (AgID) and the CAB.

1.4.7 Other participants

The activities carried out by the QTSP Intesi Group are subject to the supervision of AgID (Agency for Digital Italy).

1.5 Administration of the IPSPS

This IPSPS is drafted, reviewed and updated by Intesi Group S.p.A. personnel and is published only after approval by Intesi Group Management. Requests for information or clarification regarding this IPSPS may be submitted by e-mail to **tsp@intesigroup.com.**

1.6 Definition and acronyms

Acronyms	Definition
eIDAS2	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European Digital Identity Framework.
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
RO	Registration Officer
RFC	Request For Comments
TLS	Transport Layer Security
TSP	Trust Service Provider
TSPP	TSP Policy
IPSPS	IPS Practice Statement
LoA	Level of assurance
MRZ	Machine Readable Zone
OCR	Optical Character Recognition
OID	Object Identifier

Acronyms	Definition
PAD	Presentation Attack Detection
VIZ	Visual Inspection Zone

2 PUBLICATION

2.1 Published information

This document is publicly available on the Intesi Group company website (https://www.intesigroup.com/it/qtsp/documenti/) and is also published on the AgID website (http://www.agid.gov.it/).

2.2 Date and frequency of publications

The frequency of publication and updating of documentation is established by Intesi Group's internal processes. The valid version is the latest version available on the certification service website (www.intesigroup.com) or, where applicable, the one published on the AgID website (www.agid.gov.it).

2.3 Access

Access to documentation is free and does not require authentication.

3 IDENTITY VERIFICATION

In order to enhance the security of identity proofing processes and protect against threats (Presentation Attacks, Injection Attacks, Deepfakes), Intesi Group, leveraging its experience accumulated over recent years, has developed a new identification system called IG Persona.

3.1 Types of identification (Use cases)

The IPSP service implements the identity proofing process, structured into the following five main phases:

- Initiation;

- Data collection;
- Validation;
- Binding to the applicant;
- Issuance of the result.

The identity proofing processes provided by Intesi Group's Identity Proofing service, ensuring the Extended Level of Identity Proofing (LoIP), are described in paragraph 1.2 and detailed in the following sections.

For the use cases of unattended remote identification (§3.1.2), and in-person identification (§3.1.1), the automated management of deviations (e.g., insufficient quality of evidence, discrepancies between sources) and related process abort conditions are governed by §3.4.6.3 (Discrepancy Management), §3.4.8.2 (Remote Capture Session Controls), §6 (Discrepancy Management), and §3.6.1 (Type of Outcome).

3.1.1 In-person (Use Case 9.2.1.2 in [4])

Identity proofing with the physical presence of the applicant, based on:

- examination of the physical identity document presented by the applicant by the Registration Officer, including verification that the applicant is the holder of the document and analysis of the visible security features of the document;
- manual binding of the applicant to the identity document by the Registration Officer;
- integration of supervised verification with automated documentary, biometric and anti-fraud checks provided for by the QTSP procedures.

3.1.2 Unattended Remote (Use Case 9.2.3.3 in [4])

Unattended remote identity proofing (hybrid), based on:

- automated collection of proof of identity;
- real-time video capture;
- biometric attack detection, including Presentation Attack Detection (PAD) and Injection Attack Detection (IAD)
- automated document validation (OCR scanning and AI/machine learning analysis);
- binding of the applicant to the identity document using biometric technologies and manual review.

3.1.3 Via eID with "high" assurance level (Use Case 9.2.4 in [4])

Identity proofing by means of notified electronic identification means pursuant to the eIDAS Regulation, with a "High" level of assurance, based on the following checks:

- authentication of the Applicant through a qualified Identity Provider (IdP), e.g. SPID Level 3;
- alternatively, reading the NFC microchip of the Electronic Identity Card (CIE);
- acquisition of the authentication assertion containing the certified identification attributes;
- verification of the integrity, authenticity and validity of the assertion received;
- unique association between the IPSP session and the authenticated identity.

In the case of identity proofing via the EUDI Wallet, Person Identification Data (PIDs) are acquired through the applicable protocol, verifying that they are associated with a High Level of Assurance (LoA) and meet the applicable validity, authenticity and non-revocation requirements.

Identity proofing through the EUDI Wallet is prepared but is not active as of the date of issue of this document. It will be activated only when PIDs issued by authorised PID Providers become available, subject to the update of this IPSPS and of the related published information (OIDs).

3.1.4 Legal Entities (Use Case 9.3 in [4])

- Identity proofing of a legal person, aimed at the issuance of qualified certificates for electronic seals, at Extended LoIP, based on:collection of evidence of the organization’s identity from authoritative and independent sources (e.g. company registry extract, official public registers, Chamber of Commerce or equivalent registers);
- verification of the legal existence of the organization at the competent official register;
- acquisition and verification of the main identifying attributes of the entity, including at least:
  - full company name;
  - address of the registered office;
  - official registration number of the organization (e.g. VAT number, Tax Code or equivalent identifier);
- verification by the Registration Officer of the consistency and validity of the information collected against the official sources consulted;

- identification of the natural person submitting the request on behalf of the organization, at Extended LoIP, whose identity must be verified through one of the identification methods provided for in sections 3.1.1 to 3.1.3.

The verification of the entity's documentation is carried out by the RAO during the identification of the Applicant.

3.1.5 Individual representing a Legal Entity (Use Case 9.4 in [4])

Verification of the identity of an individual acting on behalf of a legal entity, for the purpose of issuing trust services associated with the organization (e.g., corporate role signature certificates or other qualified certificates), based on:

- identification of the requesting natural person by one of the methods provided for natural persons (paragraphs 3.1.1 to 3.1.3), ensuring a level of reliability in accordance with the Extended Level of Identity Proofing (LoIP);
- acquisition and verification of documentation attesting to the relationship between the natural person and the organization on whose behalf the request is submitted;
- verification of the Applicant's powers of representation or authorization by means of supporting documentation issued by authoritative sources, such as one of the documents listed in §3.3.2;
- verification of the validity, integrity and consistency of the documentation submitted, as well as the persistence of the powers of representation at the time of the request;
- association between the verified identity of the natural person and the organization represented, with recording of the evidence used for audit purposes.

Checks relating to the powers of representation can be carried out through direct consultation of official public registers, when available, or through documentation provided by the applicant and subsequently validated by Intesi Group's authorized personnel.

3.2 Preliminary phase

The preliminary phase is managed by the RAO for in-person identification and by IG Persona for remote identification and for eID. In this phase the Applicant is informed about the identity proofing process, its purpose and the applicable conditions, and must give explicit consent to the terms and conditions before the verification starts. For legal persons and their representatives, the preliminary phase is that of the use case chosen for the identification of the Applicant.

3.2.1 Information and consent

Before starting the identity proofing process, the Applicant is informed about the purpose of the verification and must actively accept the terms and conditions of the service. This section includes the privacy policy in accordance with the GDPR, specifying what information will be collected and the purposes of the processing. In use cases involving face recognition or biometric binding, the Applicant's explicit consent is obtained prior to the processing of biometric data.

3.2.2 Means of identification required

For identification purposes, the Applicant is informed in advance of the means of identification required based on the selected use case.

3.2.2.1 Physical or remote identification

The presentation of an identification document that is:

- valid;
- in original (it is not possible to upload images or videos taken previously);
- owned by the person making the identification.

3.2.2.2 Identification by means of notified eID means with a High Level of Assurance

To initiate identification by means of notified electronic identification with a "high" level of assurance pursuant to Regulation (EU) No. 910/2014 (eIDAS), the Applicant must have:

- a notified electronic identification means with a high level of assurance, issued by a Member State of the European Union;
- valid and active credentials associated with the eID means;
- any authentication tools required by the eID system (e.g. physical device, PIN, dedicated application).

The Applicant must also use a device compatible with the authentication system provided by the eID means and have an active internet connection to complete the process.

Access to the service is subject to successful authentication with the Identity Provider of the notified eID system.

In the event that the identification of the applicant is made through EUDI Wallet, the applicant must have a device on which a Wallet application issued or recognized by a Member State of the European Union is installed. Inside the Wallet there must be Person Identification Data (PID) with a level of assurance (LoA) equal to "High".

Identity proofing through the EUDI Wallet is prepared but is not active as of the date of issue of this document. It will be activated only when PIDs issued by authorised PID Providers become available, subject to the update of this IPSPS and of the related published information (OIDs).

3.2.2.3 Legal Entity Identification

In the case of identification of a legal entity, the Applicant must provide suitable documentation to prove the legal existence of the organization and its identification data.

The Applicant independently uploads to IG Persona the authorization form for the request of the qualified electronic seal, completed and signed by the legal representative of the entity or by a proxy holder with signing powers (Signatory), together with one of the documents listed in §3.3.2.

3.2.2.4 Identification of a natural person representing a legal entity

In the event that the Applicant is acting on behalf of a legal entity, in addition to the means of identification provided for natural persons, appropriate documentation must be provided to demonstrate the relationship between the Applicant and the organization represented.

The Applicant uploads to IG Persona the authorization form, signed and stamped by the legal representative of the entity (Signatory), together with one of the documents listed in §3.3.2. The form declares that the Applicant belongs to or is affiliated with the entity and, if the Title attribute is requested, indicates the Applicant’s role.

3.2.3 Technological tools

The identity proofing process requires the use of technological tools suitable for guaranteeing the reliability and quality of the verification, depending on the identification method selected.

3.2.3.1 Device

The Applicant must have a device (PC, smartphone or tablet) compatible with the service, adequately configured and equipped with the technical requirements necessary for the specific identification method chosen.

3.2.3.2 Image and video acquisition (where applicable)

In cases of physical or remote document-based identification, the device used for identification must be equipped with a camera with a minimum resolution of 1280x720 pixels (HD) and must be able to capture a real-time video stream at a rate of at least 25 fps (frames per second). In addition, the device must support autofocus and ensure image stability to enable proper reading of documents and biometric analysis of the face.

The service does not allow the use of images, recordings or pre-acquired files; where the acquisition of biometric or documentary data is envisaged, it must take place in real time during the identification session.

3.2.3.3 Authentication via notified eID

For identification by means of a notified electronic identification medium with a high assurance level (LoA High), the device must be compatible with the authentication system provided by the eID means used.

3.2.3.4 Connectivity

An active and stable internet connection is required, allowing the process to be completed without interruptions that could affect its validity.

3.2.4 Accessibility for people with disabilities (eIDAS Art. 15)

In accordance with Article 15 of Regulation (EU) No. 910/2014 (eIDAS) and the requirements of ETSI TS 119 461, Intesi Group adopts measures to ensure access to identity proofing services also to Applicants

with disabilities, ensuring the availability of equivalent alternative methods and preventing situations of discrimination.

3.2.4.1 Accessibility of the technological solution

The IG Persona service is based on a technological platform (ref para. § 3.4.8.1), developed considering the principles of the WCAG (Web Content Accessibility Guidelines), with the aim of supporting the accessibility of the main functionalities of the identity proofing process, where technically applicable.

However, some phases of the automated or hybrid identity proofing process (e.g. biometric facial acquisition, correct positioning of the document) may not be fully accessible for specific categories of users (e.g. people with visual or motor disabilities).

3.2.4.2 Management Operation Procedure

If the Applicant is unable to complete one of the identity proofing processes, he/she may request assistance through the support channels made available by Intesi Group.

Support requests are handled through the company's ticketing system.

The Support Staff, upon receiving a report of inaccessibility, follows the following steps:

1. **Analysis (SLA 72h):** the operator identifies the functional barrier encountered (e.g. difficulty in positioning the document or in biometric capture).
2. **Technical Assessment:** it is verified whether the user has the means for an alternative route (e.g. possession of SPID or willingness to go to an LRA).
3. **Resolution:** the operator manually enables the appropriate identification profile among those described in par. 3.2.4.3 and guides the user through the new flow.

3.2.4.3 Alternative methods of identification

In such circumstances, the Applicant may be directed to alternative methods that ensure an equivalent level of reliability, including:

- Identification by means of notified electronic identification with a "high" level of assurance (ref. para. 3.1.3), which enables verification based on already validated digital identity, reducing the need for complex visual interactions;
- Face-to-face identification (assisted face-to-face) (ref. para. 3.1.1), with a Local Registration Authority (LRA), with the support of a Registration Officer.

3.3 Applicant Data Collection

This chapter describes the types of personal and documentary data collected during the Applicant identity proofing process, as well as the ways in which such data are acquired and used for identity proofing purposes.

Data collection is limited to what is strictly necessary to ensure the reliability of the identity proofing process and compliance with applicable regulatory requirements.

3.3.1 Data collected

The Applicant's data that are collected during the identity proofing process may vary depending on the type of identification and document acquired and the related reference model. In the case of requests submitted on behalf of a legal entity, data relating to the organization and the representation relationship may also be collected. The following data listed in the following paragraphs are always required to achieve LoIP High.

3.3.1.1 Personal data

- Name;
- Surname;
- Date and place of birth;
- Nationality
- Tax ID or equivalent identification number based on nationality
- Details of the identity document
- Residential address.

The Tax Code for Italians and the details of the identity document for all identified persons allow the person to be uniquely identified.

3.3.1.2 Contact details

- Telephone number (validated by OTP submission);
- E-mail (validated by OTP submission).

3.3.1.3 Legal entity data (if applicable)

In the case of identification of a legal entity or a request made by an individual acting on behalf of an organization, the following entity data is collected:

- Full company name;
- Address of the registered office;
- Official registration number of the organization (e.g. VAT number, Tax Code or equivalent identifier);
- Country of registration.

3.3.1.4 Representation data (if applicable)

In the event that the Applicant is acting on behalf of a legal entity, information is collected relating to the relationship between the Applicant and the represented organization, such as:

- Applicant's role or qualification in the organization;
- details of the documentation certifying the powers of representation (e.g. chamber of commerce certificate, notarial power of attorney, formal proxy).

3.3.1.5 Evidence

- Physical document data: type of document, nationality, date of issue, expiry date, country of issue, issuing authority;
- eID session data: identity assertion (SAML/JWT) received.

3.3.2 Accepted Proofs of Identity

In accordance with Art. 24 of the eIDAS Regulation and the ETSI TS 119 461 standard, the following tests are accepted.

3.3.2.1 Physical documents

The service only accepts identification documents:

- issued by reputable government authorities;
- containing a photograph of the owner's face.

In particular, the accepted documents are:

- Electronic Identity Card (CIE);
- Passport;
- Driving license (for Italian citizens only).

For Italian citizens only, and limited to LoIP Extended recognitions, the health card is also required, in order to allow verification of the tax code and the validity of the document.

3.3.2.2 eID means

Credentials of digital identity systems notified at EU level (e.g. SPID and CIE in Italy) with a High level of assurance pursuant to the eIDAS Regulation, issued according to procedures compliant with the applicable requirements and providing a level of assurance comparable to Extended LoIP.

3.3.2.3 Legal entity evidence

In the case of identification of a legal person or verification of powers of representation, the service accepts evidence from official public registers or competent authorities, including:

- Articles of association (statuto);
- deed of incorporation;
- notarial power of attorney;
- extract of a notarial deed;
- certificate or extract (visura) from the Chamber of Commerce;
- for public administrations, the law or the act establishing the entity.

The existence of the entity is verified by the RAO against official registers (§3.4.6); the office held or the signing powers of the Signatory are verified on the attached document.

This evidence is used to verify:

- the legal existence of the organization;
- the identification data of the entity;
- the powers of representation of the Applicant.

3.3.3 Data acquisition methods

Depending on the identification method chosen, data collection takes place in the following ways:

3.3.3.1 OCR Scanning and Biometrics (Use Cases) 3.1.1 e 3.1.2)

Image acquisition:

- of the identity document
- of the applicant's face
- of the video session (if any)

aimed at liveness detection and verification of biometric correspondence between the subject and the photograph on the document, it takes place using a camera integrated into the smartphone.

In the case of remote identification, the applicant must be in possession of a smartphone equipped with a working camera, connected to the Internet and compatible with the identification application. In the case of identification in presence, the acquisition is carried out through the device supplied to the Registration Officer.

The device must guarantee a scan quality that allows the correct reading of the document and the biometric analysis of the face (resolution, autofocus, image stability).

Data collection takes place in the following ways:

- OCR scanning: images are scanned via a wizard interface and extracted data via optical character recognition; Uploading pre-existing files (uploads) is prohibited to prevent fraud.
- Selfie: for in-person identification, a photograph of the applicant's face is acquired via mobile device for the purposes of biometric checks following the verification carried out by the Registration Officer. Also in this case it is not possible to upload pre-existing photographs.
- Video interaction: for remote identification, a video stream of the applicant's face is captured for liveness verification and subsequent biometric binding with the document photograph.

3.3.3.2 Digital Authentication (Use Case 3.1.3)

Data acquisition is automated by receiving a SAML (or equivalent) assertion from the Identity Provider following strong authentication by the applicant. This method replaces visual identity document capture.

3.3.3.3 Legal persons and representatives (Use cases 3.1.4 and 3.1.5)

The collection of the Applicant's data as a natural person follows what is described in sections 3.3.3.1 and 3.3.3.2. The authorization form and the attached document (§3.3.2) are uploaded directly by the Applicant to IG Persona.

3.3.4 Freshness

In compliance with the requirements of ETSI TS 119 461, Intesi Group applies a policy of verifying the "freshness" of the evidence collected based on the identity proofing context and the level of reliability (LoIP) required, to ensure that the identifying attributes are current and reliable at the time of identification. For services that require Extended LoIP, more stringent policies are adopted to mitigate the risks associated with adversaries with high attack potential. The following paragraphs describe the specific cases.

IPSP Use Case (§3.1)	Type of Evidence Acquired	Freshness Requirement (LoIP – Baseline)	Freshness Requirement (Extended LoIP)
§3.1.1 In-person (ETSI 9.2.1.2)	Identity document and photograph/selfie of the Applicant	The identity document shall be valid at the time of verification.	Valid identity document, including an assessment of whether the photograph is consistent with the Applicant's age; real-time acquisition of the photograph/selfie.

§3.1.2 Unattended Remote (ETSI 9.2.3.3)	Identity document, Health Insurance Card (Italy only), and biometric video stream/selfie	Valid identity document; video stream/selfie acquired during the identity proofing session.	Valid identity document, including a photograph/age assessment, and Health Insurance Card; real-time video acquisition with Injection Attack Detection (IAD).
§3.1.3 Via Notified eID (ETSI 9.2.4)	eID authentication assertion (SAML/OIDC) or Person Identification Data (PID)	eID assertion generated in real time during the IPSP session.	eID assertion or PID validated upon receipt, including verification of eIDAS High assurance level, authenticity, and absence of revocation or expiry.
§3.1.4 Legal Entities (ETSI 9.3)	Chamber of Commerce extracts and certificates from official public registers	Evidence obtained from authoritative sources shall have been issued no more than 6 months previously.	Evidence obtained from authoritative sources shall have been issued no more than 3 months previously, to ensure that the powers remain current.
§3.1.5 Natural Person Representing a Legal Entity (ETSI 9.4)	Identity of the representative and documentation evidencing the powers of representation	Valid identity evidence and documentation of powers/official register extract issued no more than 6 months previously.	Identity verified at Extended LoIP and documentation evidencing the powers of representation issued no more than 3 months previously.

Note: for the issuance of qualified certificates, only the Extended LoIP requirement applies (ETSI TS 119 461, Annex C, clause C.3). The Baseline requirements are reported for completeness only.

3.3.4.1 Identity documents (Physical or Digital)

LoIP – Baseline: the document must be valid at the time of verification. Expired documents are not accepted.

LoIP – Extended: in addition to the validity check at the time of acquisition, an evaluation of the photograph is carried out with respect to the age of the applicant, in order to prevent the use of obsolete documents.

3.3.4.2 eID digital identities

Regardless of the confidence level, the authentication assertion (SAML or equivalent) performed via eID means must be generated in real time during the identity proofing session. Upon receipt, the assertion is validated by verifying the authenticity of the signature and compliance with the validity time interval.

In the case of Person Identification Data (PID) requested through EUDI Wallet, the data are validated upon receipt, verifying their validity, the absence of revocation or expiration, as well as the correct issuance by an authorized national body.

3.3.4.3 Chamber of Commerce Searches / Official Registers

LoIP – Baseline: evidence from authoritative sources for legal entities must have been issued no more than 6 months ago.

LoIP – Extended: the evidence from authoritative sources for legal entities must have been issued no more than 3 months ago, to ensure the actuality of the powers of representation.

3.3.4.4 Biometric Tests (Selfie/Video)

Regardless of the confidence level, acquisition should occur exclusively in real-time with injection attack detection (IAD). The use of pre-existing files is prohibited.

3.4 General data validation

Intesi Group's identification system (IG Persona) carries out a structured and in-depth validation of all the data collected during the identity proofing process.

This chapter describes the main data verification, control and correlation functionalities, distinguishing the controls applied according to the type of identification.

3.4.1 Physical or Remote Identification Validation (Use Cases 3.1.1 e 3.1.2)

3.4.1.1 Documents

The ID capture and verification service allows you to recognize them among 500 documents issued by 190 different countries.

Through this service are:

- acquired images of the document and verified the main security features (e.g. OVI inks, microwriting, Kinegrams, holograms);
- extracts the Applicant's personal data via OCR;
- extracts personal data from reading the MRZ (Machine Readable Zone) component.

The image of the user's face is also captured via selfie, used for biometric checks to compare it with the photograph in the document.

On the basis of the data acquired, the following checks are carried out:

- verification of the expiry date of the document;
- verification of the user's age;
- verification of the MRZ code checksum;
- consistency between the data captured by OCR with the data captured by MRZ;
- detection of documents photocopied or shown on a video screen;
- detection of attempts to impersonate and alter the printed photo;
- detection of documents generated by artificial intelligence (deepfakes) or digitally manipulated;
- verification of the security elements of the document (holograms, etc.);
- 1:1 biometric comparison between the applicant's scanned face and the photograph in the document.

The solution verifies the image quality (brightness, contrast, noise and reflections) in real time and, in the event of non-compliance with the minimum requirements, provides the user with indications for a new acquisition.

For each physical document acquired remotely, the system systematically checks at least 3 security features, of which at least 2 are OVD (Optically Variable Devices).

- OVD 1: Optically Variable Inks (OVI).
- OVD 2: Ologrammi o Kinegram.
- Feature 3: Machine Readable Zone (MRZ) with ICAO 9303 checksum verification. The effectiveness of these checks is validated by the technical scores (e.g. PrintAttackTest, ReplayAttackTest) returned by the platform.

3.4.1.2 Liveness Detection

The system uses a technology to detect the physical presence of the subject in order to prevent "Presentation (PAD)" and/or "deepfake" attacks. The solution complies with ISO 30107 at levels 1 and 2.

The technology helps Registration Officers prevent the following attacks:

- Presentation attacks.
- Video presentation attacks.
- 3D animation attacks.
- Print attacks.
- Mask / 3D photo-mask attacks.
- Mannequin attacks.

The "liveness detection" technology is subject to continuous evaluation and monitoring of performance, in accordance with the criteria defined in this IPSPS.

For the Active Liveness Detection module, the reference performance requirement is maxAPCER < 1% to BPCER = 5%, with an upper limit of BPCER of 15% in tests performed according to ISO/IEC 19989-3.

For the Passive Liveness Detection module, the reference performance requirement is maxAPCER < 2% at BPCER = 5%.

The viability detection modules are also evaluated according to the ISO/IEC 30107 standard and have iBeta Level 1 and Level 2 certifications.

3.4.1.3 Video Identification (Use Case Only 3.1.2)

During video identification, the system records the Applicant showing the front and back of the identification document in a continuous video stream.

The video captures the face and document simultaneously, ensuring that they are time-synchronized.

This mode allows you to:

- prove the actual possession of the document;
- prevent presentation and injection (IAD) attacks.

3.4.2 eID Validation (eID Validation 3.1.3)

For identifications via eID (SPID/CIE or other notified systems of High level), validation is based on automatic checks carried out on the response provided by the Identity Provider (IdP), by:

1. verification of the digital signature of the SAML assertion (or equivalent) against the certificates published in the official metadata;
2. verifies that the authentication level returned is "High" (eIDAS High), as a minimum requirement for achieving the Extended LoIP;
3. verification of the presence and completeness of all required attributes.

For EUDI Wallet identifications, Person Identification Data (PIDs) are captured by the applicant using the OID4VP protocol. Upon receipt, the QTSP performs the following checks:

1. verification of the signature of the PID issuer with respect to the certificates and information on the Trusted List of the competent Member State;
2. verification of the validity and absence of revocation of the PID;
3. verification of the Key Binding, ensuring that the submitter actually has the keys associated with the Wallet
4. verification of the LoA High assurance level declared in the PID.

Identity proofing through the EUDI Wallet is prepared but is not active as of the date of issue of this document. It will be activated only when PIDs issued by authorised PID Providers become available, subject to the update of this IPSPS and of the related published information (OIDs).

3.4.3 Legal Entity Validation (Use Case 3.1.4)

In the course of verifying the identity of the Applicant, the RAO verifies the documentation relating to the entity:

1. the request form referred to in §3.2.2 is complete and signed by the Signatory;
2. the attached document is among those admitted and meets the freshness requirements;
3. for entities registered in a register, the existence of the entity (and, where reported by the register, its status), name, registered office and identifier result from the consultation of the register (§3.4.6) and match the data provided during identification;
4. the office held or the signing powers of the Signatory result from the attached document.

3.4.4 Validation of a Natural Person representing a Legal Person (Use Case 3.1.5)

The Applicant is identified through one of the use cases 3.1.1, 3.1.2 or 3.1.3 at Extended LoIP. The RAO verifies that the identified person matches the person indicated in the form (name and tax code) and that the Signatory declares that the Applicant is an employee or affiliate of the entity.

3.4.5 Anti-Fraud Controls (All Use Cases)

Intesi Group has developed a proprietary *Anti-fraud detection component* that intervenes in all use cases by integrating documentary, biometric or digital controls with internal and external consistency checks. In addition to what has already been described, for digital flows, the system verifies:

- verification in internal blacklists of:
  - tax code;
  - telephone number.
  - Email address and/or email domain.
  - identification document.
- Unique checks:
  - Couple tax code / e-mail address.

- Couple tax code / telephone number.
- "Scipafi" checks (only for Italian citizens).

3.4.6 Validation through trust registers and authoritative sources

In compliance with the ETSI VAL-8.3.6 requirements, Intesi Group uses access to the "Centralized System for the Prevention of Identity Theft" called SCIPAFI, used for the verification of the validity of identity documents of Italian citizens and for the prevention of identity theft. The use of the sources is limited to the data strictly necessary to complete the identity proofing process.

3.4.6.1 List of Records and Sources

Depending on the context of identification, the following sources are consulted:

Natural person: for the verification of identity documents of Italian citizens and for the prevention of identity theft, access to the "Centralized System for the Prevention of Identity Theft" called SCIPAFI is used.

Legal person: to verify the existence, name, registration identifier and registered office of the entity, the RAO may consult the business register of the State of registration (for Italian entities, the Registro delle Imprese; for other EU Member States, the respective business register).

Public administrations, public service operators and publicly controlled companies: for Italian entities in this category, the RAO consults the Index of digital domiciles of public administrations (IPA, Art. 6-ter of Legislative Decree 82/2005) and verifies existence, name, tax code, registered office and, where reported, the head of the entity.

Office held and powers of the Signatory: the RAO verifies them on the basis of the documentation provided (company registry extract), comparing it with the data found in the registers consulted.

3.4.6.2 Technical validation procedure

Access to trust registers is through secure channels and automatic consistency checks of the data acquired.

In particular:

- Source authentication: the connection to the registers takes place through secure channels (updated TLS protocol) with authentication of the IPSP service at the data provider;
- Data integrity: the system verifies the integrity and authenticity of the responses received through validation of the certificates of the source's servers;
- Attribute matching: Attributes extracted from the logs are automatically compared with data provided by the Applicant or captured from other evidence collected during the identity proofing process.

3.4.6.3 Discrepancy management

For differences in encoding and for those concerning names, §3.4.6.4 and §3.4.6.5 apply

In the event of a discrepancy between the data acquired from authoritative sources by OCR via XPressID, in accordance with the ICAO 9303 standard, and the data provided or subsequently corrected by the Applicant, the RAO operator shall proceed to assess the discrepancy on the basis of the results and scores returned by XPressID.

For the purposes of the assessment, the RAO applies the following criteria:

- Prevalence of the official source: the data acquired from the official source, if correctly collected and consistent with the identity document presented, prevail over the data self-declared by the Applicant. Any changes made to the automatically acquired data must be adequately evaluated by the RAO and may result in the correction of the data or the invalidation of the recognition outcome.
- Attributes critical for the purposes of Extended Level of Identity Proofing: if the discrepancy concerns one or more attributes relevant for the purpose of maintaining the Extended Level of Identity Proofing, the identity proofing process is not concluded on the basis of the automated outcome alone. The RAO shall manually review the discrepancy or, if it is not possible to ascertain with sufficient reliability the correctness of the data, conclude the process with a negative outcome.

In the case of identification carried out in person, in order to ensure the independence of the verification and mitigate the risk of coercion or undue influence on the Applicant, any modification or correction of the data carried out by the RAO is subject to validation by a second RAO operator of Intesi Group with the role of RAO Master.

Validation by the RAO Master constitutes an independent check on the intervention carried out by the RAO and must be completed before the conclusion of the identity proofing process.

3.4.6.4 Handling of encoding differences in identity attributes

An encoding difference occurs when the same identity attribute is represented differently between pieces of evidence (e.g. visual inspection zone and MRZ of the document, document and health insurance card, document and eID assertion) or between a piece of evidence and the data declared by the Applicant, due to different alphabets, diacritical marks, national characters, separators or date formats.

For documents with an MRZ, the acquisition component compares the data of the visual inspection zone with those of the MRZ, which uses only unaccented Latin characters, and recognises as equivalent the differences due to the compilation and transliteration rules defined by ICAO Doc 9303 (e.g. Ü → UE, À → A, removal of apostrophes and hyphens, the "<" symbol, date format). For passports with the visual inspection zone in a non-Latin alphabet, the match is made using the transposition provided for by ICAO Doc 9303. Identity cards are accepted only with the visual inspection zone in Latin alphabet. A difference in the document number or in the date of birth is never considered equivalent.

If the check returns a warning or a non-consistency outcome, the case is assessed by the RAO. If the data cannot be ascertained with sufficient reliability, the process ends with a negative outcome. In in-person identification, every correction made by the RAO is validated by a Master RAO (§3.4.6.3).

3.4.6.5 Handling of differences in name attributes

A difference in name attributes occurs when the first name or surname do not match between pieces of evidence (e.g. identity document, health insurance card, eID assertion, company registry extract) or between a piece of evidence and the data declared by the Applicant, due to missing or additional names (e.g. a middle name), use of initials, truncation due to length limits, prefixes or suffixes (e.g. Dr, Jr), or a change of first name or surname not reported in one of the pieces of evidence.

The comparison tolerates OCR reading errors and spacing differences. A name truncated in the MRZ due to length limits is recognised as equivalent when it matches the initial part of the full name reported in the visual inspection zone.

Other differences are assessed by the RAO. The data reported in the identity document prevail over the data declared by the Applicant (§3.4.6.3). The RAO accepts the difference only if it can be traced back to one of the cases listed above and the name reported in the identity document corresponds

to the declared one. A change of first name or surname not reported in the document is accepted only if it results from official evidence; otherwise, or if the data cannot be ascertained with sufficient reliability, the process ends with a negative outcome. In in-person identification, every correction made by the RAO is validated by a Master RAO (§3.4.6.3).

The outcome of the automatic and manual checks and the operators involved are recorded and retained with the session evidence (§3.6.2, §4.6.2).

3.4.7 Validation through Proof of Access of contact details

In accordance with ETSI TS 119 461, Intesi Group may apply a proof of access procedure to verify that the applicant has control of the means of communication declared during the identity proofing process.

Contact validation is additional evidence to support the identity proofing process and is not used as the only evidence for the purpose of achieving the Extended Level of Identity Proofing.

3.4.7.1 Scope

The *proof of access* procedure is used for the validation of the following contact attributes:

- mobile phone number, by sending an OTP (One-Time Password) code via SMS;
- e-mail address, by sending an OTP code.

The use of these verifications is limited to use cases where contact information is an attribute necessary to complete the identity proofing process or to operationally manage the service.

3.4.7.2 Validation procedure

The *proof of access* procedure involves the automated execution of the following checks:

- Challenge generation: the system generates a unique random code with limited time validity;
- Proof of possession of the address: the Applicant demonstrates control of the means of communication by correctly entering the code received or by selecting the unique verification link;
- Response validation: the system verifies that the generated code corresponds to the response provided by the applicant. The contact detail is considered validated only if the verification is successful.

3.4.7.3 Limitations of use

The proof of access procedure is used exclusively for the validation of the contact details declared by the Applicant.

No proof of access mechanisms related to bank accounts or other financial resources are used as evidence of the identity proofing process.

3.4.8 Technological system for the acquisition of evidence and automated controls

Intesi Group uses an integrated technological system (XPressID VeriDas) for the controlled acquisition of biometric and documentary evidence and for the execution of automated checks on the authenticity and integrity of identity documents presented during identity proofing processes.

The system is used as a component of the identity validation process in use cases that include:

- guided acquisition of the image of the Applicant's face (selfie);
- capture of real-time video streams during remote identification sessions;
- acquisition and analysis of images of the identity document;
- automated verification of the physical and logical characteristics of the document presented.

Specifically, the use cases in which it is used are:

- identification in presence (par. 3.1.1)
- Remote identification via video session (par. 3.1.2)

3.4.8.1 Technology Solution

The document platform called XpressID, provided in Software as a Service (SaaS) mode, provided by Veridas Digital Authentication Solutions, S.L. allows:

- automatic data extraction via OCR and MRZ parsing;
- the verification of the structural consistency of the document and of the visible and logical security features;
- the identification of anomalies compatible with attempts at falsification;
- the guided acquisition of static images (selfies) and real-time video streams for biometric analysis of the face;

- synchronized capture of face and document, ensuring the unbreakable bond between the subject and the evidence presented during the session

The platform supports the analysis of identity documents from a wide number of international jurisdictions.

The technologies used include Machine Learning models and Deep Neural Networks aimed at document recognition and classification of security features.

3.4.8.2 Remote capture session controls

During the remote identification session, the system applies automatic checks on the acquisition parameters in order to ensure sufficient quality of the evidence collected.

During the session, automatic real-time checks are performed for:

- Face lighting
- Image Clarity
- Frame stability
- Document readability

To enable identification of the RAO operator. If the parameters are below the configured thresholds:

- the session can be suspended, or
- The session can be repeated

before the identity proofing process continues.

3.4.8.3 PAD and IAD Detection Mechanisms (TS 18099)

The biometric acquisition system used by Intesi Group integrates automatic detection mechanisms of the main biometric attack classes during remote identification sessions.

These mechanisms are applied as part of the **identity validation** in use cases involving video capture of the Applicant's face (par. 3.1.2).

Specifically, the measures adopted are as follows:

Presentation Attack Detection (PAD)

The system integrates Presentation Attack Detection (PAD) controls compliant with the ISO/IEC 30107 standard aimed at detecting impersonation attempts based on:

- printed photographs;
- images displayed on the screen;
- video playbacks;
- Three-dimensional masks or artifacts.

PAD controls include automatic liveness detection checks based on dynamic analysis of the face captured during the session.

Injection Attack Detection (IAD)

The system integrates **Injection Attack Detection (IAD)** controls aimed at detecting attempts to alter the acquired video stream through:

- Synthetic stream injection
- Using pre-recorded streams
- software manipulations of the device
- techniques that can be traced back to digital spoofing scenarios (e.g. deepfakes)

These checks help to ensure that the biometric evidence used in the identity proofing process is captured in real time by the Applicant's device.

Capture integrity and protection against virtual camera injection

The system applies technical controls aimed at verifying the origin of the captured video stream, with the aim of reducing the risk of using:

- virtual camera;
- video emulators;
- altered capture pipelines.

These controls, as part of the remote identity proofing process, help ensure consistency between:

- device used;
- capture session;

- biometric evidence collected.

Alignment with ETSI TS 18099 requirements

For remote identity proofing processes that require the Extended LoIP level, the PAD and IAD mechanisms adopted are designed in line with the requirements of the TS 18099 standard.

The effectiveness of the controls implemented is subject to periodic monitoring as part of the internal security management processes of the identity proofing service.

Intesi Group defines the following quality objectives for automated processes, in line with the objectives defined by XPressID:

- Biometrics (FAR/FRR): The system sets a performance target of FMR (FAR) ≤ 1×10^{-5} and a target FNMR (FRR) ≤ 0.003 for facial verification (in line with the NIST FRTE 1:1 empirical measurements of April 2025, which report an FNMR of 0.0027 at an FMR of 1×10^{-5} for the Mugshot category), ensuring the highest level of reliability in the identification process and consistency with the service's technical documentation..

- Anti-fraud (APCER/BPCER): For the PAD module, the target is maxAPCER < 1% for active liveness and maxAPCER < 2% for passive liveness, with a target BPCER of 5%. These targets are monitored every two years through tests by accredited laboratories (ISO/IEC 19989-3 and TS 18099)

Intesi Group undertakes to verify, through the acquisition of documentation or special audits, that the suppliers of the biometric engine (e.g. VeriDas) test their algorithms on reference and updated datasets.

Secure transmission of biometric evidence

The biometric evidence collected during the remote identification session is transmitted to the QTSP validation environment, from the point of acquisition to the identity proofing service validation systems, through encrypted communication channels based on TLS protocols.

3.4.8.4 Updating of document models and detection mechanisms

The supplier keeps document models, recognition datasets and anti-fraud analysis algorithms updated in order to include new document formats, incorporate changes to existing documents and mitigate emerging counterfeiting techniques.

The updates include components of document recognition, image integrity analysis and attack detection, taking into account, where applicable, information available through authoritative public sources such as:

- PRADO;
- report ENISA;
- anti-fraud dataset of reference in the sector.

3.4.8.5 Updating the PAD and IAD mechanisms

The platform includes automatic Presentation Attack Detection (PAD) and Image Attack Detection (IAD) mechanisms aimed at detecting:

- Reused images
- photographic reproductions
- Digital manipulations
- Document spoofing attempts

These mechanisms are updated by the supplier based on the evolution of known attack techniques. analysis of emerging vulnerabilities and available threat intelligence activities.

3.4.8.6 Software update management and performance monitoring

Intesi Group monitors the evolution of the platform used and integrates the relevant software updates according to its management process of the critical components of the identity proofing service.

In particular:

- Security updates are applied according to internal vulnerability management policies
- Relevant functional updates are assessed against their impact on the identity proofing process
- System performance is reviewed periodically

The overall review of the effectiveness of the document validation solution is carried out at least annually or in the presence of significant changes in the threat landscape.

3.5 Binding to Requester

This step is intended to verify that the Applicant is the rightful owner of the submitted proof of identity and that such evidence is in its possession at the time of identification.

The service ensures that the face capture process (selfies and videos) takes place in real time, continuously evaluating the quality of the images (lighting, reflections, sharpness), rejecting sessions that do not allow a reliable comparison.

Depending on the type of identification, the binding process is carried out in different ways.

3.5.1 Binding in Presence Identification (Use Case 3.1.1)

In this scenario, the binding between the identity and the applicant is established through supervised verification by the Registration Officer. The Registration Officer performing the comparison between the applicant physically present and the identity document presented shall be specially trained in:

- techniques for recognizing false or altered documents;
- protection of personal data;
- detection of impersonation attempts and attacks.

The Registration Officer is supported by the result of the biometric verification carried out through the XPressID tool.

3.5.2 Binding in Remote Identification (Use Case 3.1.2)

In the absence of physical presence, the process is based on biometric technologies and automated controls with a high level of reliability.

To verify the vitality of the subject, a real-time video stream (minimum 1280x720 pixels and 25 fps) is captured.

The Biometric comparison is automated: an artificial intelligence algorithm compares the face detected in the video with the photograph extracted from the document, in compliance with predefined thresholds of FAR (False Acceptance Rate) and FRR (False Rejection Rate).

The results of the automated binding are subject to verification by a back-office RAO operator who, on the basis of the information acquired, can confirm or reject the recognition before the final release of the result.

3.5.3 Binding via Notified eIDs (Use Case 3.1.3)

The link between the Applicant and the electronic identity is guaranteed by the verification of the identity assertion issued by the Identity Provider:

- strong authentication at the IdP certifies the ownership of the credentials;
- the personal data contained in the assertion are related to the data entered in the request;
- the assertion is automatically verified for integrity, authenticity, and assurance level (eIDAS High).

In the case of using the EUDI Wallet, the following is checked:

1. the authenticity of the issuer by verifying that the signing key belongs to a *PID Provider* authorized by the Member State and present in the Trusted Lists (EUTL).
2. data integrity through cryptographic algorithms to ensure that the data within the PID (name, surname, date of birth, tax code) has not been modified or manipulated after issuance.
3. the validity status (Revocation) by querying the PID Provider's revocation service in real time (or via updated signed lists) to ensure that that specific PID has not been suspended, revoked or expired.
4. proof that the person submitting the PID is the real owner of the device (Holder Binding).

3.5.4 Legal Entity Binding (Use Case 3.1.4)

The binding is positive only if the following are positive: the identification of the Applicant (§3.4.4), its correspondence with the form and the verification of the documentation provided (§3.4.3).

3.5.5 Binding Natural Person representing Legal Entity (Use Case 3.1.5)

The binding is positive only if the following are positive: the identification of the Applicant (§3.4.4), its correspondence with the form and the verification of the documentation provided (§3.4.3).

3.5.6 Discrepancy management

For both in-person and remote identification cases, if the automated and manual comparison results are inconsistent, the process is immediately terminated with a negative outcome and the case is submitted for validation by the Master RAO.

3.5.7 Face comparison by the Registration Officer

In use cases 3.1.1 and 3.1.2, the Registration Officer compares the face shown on the identity document with the appearance of the Applicant, either live or from the video and the images acquired (§3.3.3.1), taking into account the outcomes of the automatic biometric comparison produced by the XPressID system. The automatic outcomes are of support and do not replace the RAO's assessment, which performs a morphological analysis according to the following list of features:

- general face shape;
- forehead and hairline;
- eyebrows;
- eyes (shape, distance, eyelids);
- nose;
- mouth and lips;
- ears, if visible;
- cheeks and facial folds;
- distinctive marks (moles, scars, visible tattoos).

The RAO assesses stable and modifiable features separately (hairstyle, beard, glasses, make-up) and takes into account the age difference between the photograph on the document and the Applicant.

The outcome of the comparison may be: match, no match, or not determinable. The RAO confirms the binding only in the event of a match; in other cases, or if the quality of the image or video does not allow a reliable comparison, the process ends with a negative outcome. In the event of discordant outcomes between the automatic and the manual comparison, §3.5.6 applies.

3.6 Release of the result

The final outcome of the identity proofing process is generated only at the end of all the required checks and in compliance with the reliability and security criteria defined by the service.

This phase concludes the verification process, formalizing the outcome and ensuring the secure storage of evidence for legal and audit purposes.

3.6.1 Type of outcome

The results of the checks carried out as part of the identity proofing process through IG Persona are processed according to the rules defined by the QTSP and determine the management of the file on the basis of the configured reliability thresholds.

The Identification Assurance Level (LoA) is implicitly selected at the start of the identification procedure, depending on the assurance level required for the specific practice. The successful outcome of the identity proofing process confirms the Identification Assurance Level (LoIP) corresponding to the required level. In particular, the outcome of the identification can be Extended; This outcome is stored in the database and in the logs.

Depending on the outcome, the identity proofing process may be successfully completed, rejected, or subject to additional verification by authorized QTSP personnel in accordance with internal procedures.

In the case of remote identification via video session (use case 3.1.2), the results of the automatic checks are subject to evaluation by the Registration Officer before the conclusion of the file.

If the identity proofing outcome is negative, the applicant may repeat the identity proofing process up to a maximum of three attempts in total.

In the case of face-to-face identification (use case 3.1.1), the results of the automatic checks are managed according to the rules defined by the QTSP and may result in the positive closure, rejection of the file or the activation of further checks by Intesi Group staff, who are required to carry out an additional verification of recognition. In such a scenario, the RAO can approve the recognition only following a successful verification by the Intesi Group operators.

For cases relating to legal persons and their representatives, the case is closed by the RAO, with a positive or negative outcome, only after the verification of the identity of the Applicant (§3.4.4) and of the organization's documentation (§3.4.3).

3.6.2 Collection and storage of evidence

For each session, detailed evidence is collected and maintained documenting the entire identity proofing process. These include:

- documentation of the evidence, indicating the issuer or source;
- video recordings or images captured during the binding phase, if required by the use case and regulatory context;
- Session metadata such as date, time, type of identification, outcome of automatic and manual checks, operators involved;
- System logs containing details on the verifications carried out (OCR, biometrics, eID authentication).

The evidence collected is stored in such a way as to be protected against any tampering. Integrity is checked weekly through automated processes. The results of these checks are reported on the Intesi Group monitoring system, so that, in the event of compromises, the staff can be promptly notified and intervene promptly.

The retention period and the deletion are governed by §4.6.2.

4 MANAGEMENT CONTROLS

The management, operational and physical controls applied to the Identity Proofing service (IPSP) are based on maximum consistency with the security framework already certified for Intesi Group's Qualified Trust Services. For anything not expressly detailed in this manual, the procedures defined in the Practice Statements of the QTSP Intesi Group shall apply in full [1], adopted for Qualified Trust Services, in accordance with the requirements of the ETSI EN 319 401 standard and applicable regulations. The IPSP operates as a component of the trust service under the responsibility of the QTSP, ensuring that identity proofing activities are carried out in accordance with the Extended Level of Identity Proofing (Extended LoIP) for the issuance of qualified certificates.

4.1 Operational Risk Assessment

Intesi Group performs and updates annually a risk analysis also applied to the Identity Proofing service, as part of the security management system adopted for Qualified Trust Services.

As regards the IPSP, the risk analysis complements what is already provided for in the *Practice Statements del QTSP Intesi Group* [1], including specific scenarios related to:

- identity fraud, such as attempts to forge documents or impersonate;
- biometric attacks, with reference to presentation attacks (PAD) and injection attacks (IAD).

Because the service is designed to meet the Extended Level of Identity Proofing (Extended LoIP), the risk assessment explicitly considers the system's ability to counter adversaries with *high attack potential*.

4.2 Threat analysis and monitoring

Intesi Group implements and maintains a documented and effective procedure for threat analysis and monitoring, in order to ensure that the Identity Proofing service is constantly updated and protected against emerging risks.

This activity focuses in particular on new identity fraud techniques, including presentation attacks (PAD), injection attacks (IAD) and the use of artificially generated content using artificial intelligence ("deep fakes").

The procedure involves:

- Monitoring of authoritative sources: constant consultation of sectoral information flows, including ENISA reports and PRADO publications on security features and new patterns of falsification of identity documents.
- Technology collaboration: Interacting with vendors to integrate software updates and machine learning models trained on updated datasets for the detection of document and biometric manipulations.
- Analysis of operational data (Anti-Fraud Service): systematic analysis of fraud attempts detected internally, integrating flows from the proprietary anti-fraud service, in order to promptly identify new high-potential attack patterns.

The results of this activity feed into the regular update of the operational risk assessment and guide the planning of training and retraining initiatives specifically for Verification Personnel (RAOs).

4.3 Personnel safety checks

Intesi Group applies to the personnel involved in the Identity Proofing service the selection, reliability, confidentiality and control policies already adopted for the Qualified Trust Services, as defined in the Practice Statements of the QTSP Intesi Group [1].

To ensure the effectiveness of the verification processes, the Registration Officer (RAO) and the service designers are subject to the following specific requirements covering selection, training, updating and segregation of duties.

4.3.1 Selection and reliability

Personnel are selected on the basis of proven experience in managing critical IT services and are subject to periodic reliability checks. At the time of appointment, each employee signs a confidentiality agreement and receives a formal mandate defining their roles and responsibilities.

4.3.2 Specialist training

Before being qualified for operational activities, personnel receive specific training that compulsorily covers:

- eIDAS legislation and Italian legislation.
- techniques for preventing identity fraud and detecting counterfeit or tampered documents;
- recognition of biometric attacks, including presentation attacks (PAD) and injection attacks (IAD);
- management of cases of identification of legal entities and legal representatives, including verification of powers of representation.
- morphological analysis methodologies of the face for the comparison between the Applicant and the document;
- personal data protection legislation (GDPR) and security procedures of the systems used.

4.3.3 Upgrade and retraining

The training of personnel, especially personnel who carry out the validation of physical documents, is a continuous process that is updated at least annually or promptly following new threats identified by threat analysis and monitoring activities (ref. par. 4.2).

4.3.4 Separation of roles

To prevent conflicts of interest and ensure impartiality of judgment, Registration Officers may not hold any other critical roles within QTSP's operations that may compromise its independence.

4.4 Physical and logical security

Intesi Group adopts physical and logical protection measures to ensure the integrity, availability and confidentiality of identity proofing processes, in full compliance with the requirements of the ETSI EN 319 401 and ISO/IEC 27001 standards.

4.4.1 Physical security

With regard to the protection of the premises, access control, environmental monitoring systems (fire, HVAC, redundant power supply) and business continuity measures, the provisions defined in the Practice Statements of the QTSP Intesi Group are fully applied [1].

The systems used for the Identity Proofing service are hosted in protected data centers, shared with qualified trust services (e.g. CA and Time Stamping), and subject to the same physical security controls.

4.4.2 Logical security and separation of systems

The information system that makes the final decision on identity validation is logically or physically separate from non-critical information systems (e.g., corporate networks or office environments).

The network infrastructure applies appropriate security controls, including firewalls, intrusion detection/prevention systems, and anti-malware protections, as required by the QTSP security framework.

4.4.3 Communications and data protection

To ensure the security of the collected data flows, in particular in remote use cases, the following measures are taken:

- Channel encryption: all transmissions of identification data, images and video streams between the Applicant's device and the validation environment take place over channels encrypted using updated TLS protocols, ensuring authenticity, integrity and confidentiality.
- Capture protection (OCR): the system implements measures to prevent the injection of cloned or pre-recorded data, ensuring that the chip or images are read in real time during the identity proofing session.
- All critical systems synchronize their internal clock with Coordinated Universal Time (UTC). Synchronization is constantly monitored; in the event of non-alignment with UTC, special alarms and notifications are generated to the Operations group, which promptly provides for the necessary verification and recovery activities.
- Operational logs and evidence are protected against tampering by means of digital signature mechanisms.

4.5 Incident and vulnerability management

Intesi Group adopts policies and procedures for the management of security incidents and vulnerabilities in accordance with the requirements of the ETSI EN 319 401 standard and the ISO/IEC 27001 certified management system.

For general governance and coordination, the procedures defined in the Intesi Group QTSP Practice Statement apply [1].

The operating methods for managing incidents and vulnerabilities are formalized in the internal document "Procedure for the Management of Information Security Incidents" adopted by Intesi Group as part of its Information Security Management System (ISMS), accessible to authorized personnel through the company document repository.

For the Identity Proofing service, the management framework is extended to address specific digital identity threats.

4.5.1 Monitoring and Tracking

The system constantly monitors the verification processes to identify anomalies attributable to fraud attempts or biometric attacks (PAD/IAD). Particular attention is paid to video streams and the results of liveness detection mechanisms.

4.5.2 Vulnerability analysis

In line with the activity of threat analysis and monitoring (ref. para.4.2), Intesi Group assesses the impact of new vulnerabilities that could compromise the reliability of identification methods, particularly in the presence of high-potential attacks (e.g. advanced deepfakes).

4.5.3 Reporting obligations

In accordance with applicable regulations, Intesi Group communicates with the competent authorities and supervisory bodies as required, taking into account the nature and severity of the incident.

4.5.4 Communication to data subjects

If an incident may have an adverse effect on the personal data or identity of an Applicant, the latter is informed without undue delay, in accordance with the provisions of the legislation on the protection of personal data.

4.6 Audit Recording and Evidence Retention

Intesi Group adopts registration and storage systems that guarantee the immutability, confidentiality and availability of all relevant events related to the Identity Proofing (IPSP) service.

For general logging, log protection, and audit management policies, the provisions of the TSP Practice Statement of the QTSP Intesi Group apply [1], in line with the ETSI EN 319 401 and ISO/IEC 27001 requirements.

4.6.1 Type of events and evidence collected

For each identification session, comprehensive evidence documenting the entire process is kept.

4.6.1.1 Documentation of evidence

Data extracted from the identity document, eID assertions, evidentiary documentation relating to legal entities and legal representatives.

4.6.1.2 Unique session identifiers

Decision tracks, results of biometric checks (PAD/IAD), facial comparison (face matching), any alerts or warning/KO scores.

4.6.1.3 Multimedia recordings

Images and video streams captured during data collection and binding, if required by the regulatory context and use case.

4.6.1.4 Operator tracking

Information about RAO or back-office personnel involved in the review and approval of the process.

This evidence constitutes evidence for audit, event reconstruction and operational accountability.

4.6.2 Retention period

In compliance with the Prime Ministerial Decree of 22 February 2013, eIDAS requirements and audit requirements, Intesi Group retains the identity proofing evidence for 20 years from the issuance of the certificate issued following the identification, in accordance with the DPCM of 22 February 2013, the eIDAS requirements and audit needs. At the end of the retention period, the data will be deleted.

If the identification does not lead to the issuance of a certificate, the documents and evidence collected in the process are deleted within one week of the closure or abandonment of the request. The registration request is retained, to document the process and its outcome.

4.6.3 Security and Integrity

The log and evidence archiving system is subject to automatic consistency and integrity checks that ensure the immutability of the data retained.

Any anomalies or inconsistencies generate alarms on safety monitoring systems.

Access to logs and tests is allowed only to authorized Intesi Group personnel, limited to the roles of systems administration and audit, in compliance with the principles of segregation of duties, traceability of access and minimization of privileges.

4.7 Business continuity and termination

Intesi Group guarantees the resilience, availability and continuity of the Identity Proofing (IPSP) service through formalized Business Continuity and Disaster Recovery plans, in line with the QTSP security framework and with the ETSI EN 319 401 requirements.

4.7.1 Business Continuity and Disaster Recovery Plans

Recovery procedures are designed to minimize the impact of adverse events such as hardware failure, system unavailability, data corruption, or natural disasters.

Constant alignment between the primary and secondary sites (Disaster Recovery) is guaranteed, in order to preserve the integrity of the evidence and the continuity of the service.

Continuity and recovery plans are documented, kept updated and subjected to periodic tests at least annually, with recording of the results and any corrective actions.

4.7.2 Termination of Service

In the event of termination, the termination procedure defined as the internal procedure will be applied. This procedure is reviewed annually by a Conformity Assessment Body (CAB) and is approved by the Italian supervisory body AgID.

4.8 Supplier management (Supply-chain)

In compliance with the requirements and in line with the QTSP procurement management policies, Intesi Group selects, evaluates and monitors its technology partners on the basis of strict criteria of safety, reliability and regulatory compliance.

For the critical components of the IPSP service related to data collection, OCR extraction and biometric validation (liveness detection and face matching), Intesi Group uses qualified suppliers who have obtained certifications of compliance with the ETSI TS 119 461 and ETSI EN 319 401 standards.

Intesi Group imposes on its critical suppliers the obligation to propagate the same security, privacy and operational requirements to its sub-suppliers (supply chain propagation), ensuring that there is no degradation in the level of trust along the supply chain.

4.8.1 Liability

Intesi Group retains full responsibility for the IPSP service and compliance with information security and personal data protection policies, ensuring that suppliers operate in compliance with the GDPR and the technical and organizational requirements defined in this manual.

4.8.2 Evaluation and Monitoring

Critical suppliers are subject to a prior risk assessment and periodic monitoring of performance, security and compliance to ensure that the Extended LoIP level is maintained and the resilience of the supply chain is maintained.

4.8.3 Contractual Agreements

Relationships with technology partners are governed by agreements that require the adoption of physical, logical, and organizational security measures equivalent to those adopted by the QTSP, including confidentiality, auditability, and incident management clauses.

5 GENERAL TERMS AND CONDITIONS OF SERVICE

5.1 Service Fees

The economic conditions of the Identity Proofing service are defined by the commercial area of Intesi Group and negotiated with enterprise customers in specific contractual agreements.

5.2 Financial responsibility and insurance

Intesi Group maintains adequate insurance coverage for civil and professional liability in relation to the provision of trust services and Identity Proofing services, in accordance with the provisions of its company policies and the regulatory requirements applicable to the QTSP.

5.3 Privacy and protection of personal data

The processing of personal data takes place in compliance with Regulation (EU) 2016/679 (GDPR) and applicable national legislation.

- The data collected are limited to what is strictly necessary for the execution of the Identity Proofing process.
- Biometric data are processed in accordance with the legal bases provided for in the applicable legislation and the enhanced security measures provided for special categories of data.
- Retention periods are defined according to the purposes of the service and regulatory and audit obligations.

Intesi Group has conducted adequate privacy assessments for the identity proofing service.

5.4 Intellectual property rights

This manual and the technical processes described are the property of Intesi Group S.p.A. Applicants retain ownership of their personal data and any distinctive signs used in the context of the service.

5.5 Limits of liability

Intesi Group is not liable for damages resulting from improper use of the service or false information provided by the Applicant. The liability of the QTSP is governed by the contractual terms applicable to the reference service.

5.6 Complaints, dispute resolution and applicable law

The handling of complaints and disputes is governed by the Terms and Conditions of Service and the applicable contractual documents.

The procedures for handling complaints and disputes are governed by the General Terms and Conditions of the certification service and by the applicable contractual documents. Subscribers and certificate applicants are invited to refer to Chapter 11 of the "General Terms and Conditions of the certification service" and/or to the "General Terms and Conditions of the time-stamping service", published on the Intesi Group institutional website. All customers or third parties may submit

complaints or reports by sending an email, preferably a PEC (certified email), to tsp@ig-trustmail.com. The email must contain the sender's identification data (first name, last name, address and tax code or VAT number) and a detailed description of the reasons for the complaint or report.