InfoCert: *Identity proofing service practice statement*

Document code	ICERT-INDI-IPSPS
Version	1.1
Date	10/07/2025

tinexta infocert

1 INTRODUCTION

1.1 Overview

InfoCert is a trust service provider that also offers online services for identity verification of natural persons to support the issuance of certificates.

Through identity proofing and qualified certificates services, individual customers can use electronic signatures legally, according to the Regulation n. 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 (hereinafter "eIDAS" or "eIDAS Regulation").

In particular, SelfQ solution verifies the identity of natural persons in accordance with eIDAS, Article 24, paragraph 1 d) by using "other identification methods" recognized under national regulations which provide equivalent assurance in terms of reliability to physical presence.

This document is the Trust Service Practice Statement for SelfQ solution. It is not a full Certification Practice Statement (CPS) according to RFC 3647 because it is only related to the provisioning of identity verification services but does not include other certification services such as certificates issuance or certificate validation services. (See ICERT-INDI-MO for InfoCert certification services [10]).

The purpose of this document is to serve as a base for compliance with eIDAS.

1.2 Document name and identification

This document is entitled "*InfoCert: Identity proofing service practice statement*", having the following document ID: **ICERT-INDI-IPSPS**. For version and release level information, please see the page header.

The document describes policies and procedures set out to manage InfoCert Identity Proofing Service in compliance with eIDAS Regulation [1].

This document is associated with one or more Object Identifiers (OID) described below.
The *Object Identifier* (OID) which identifies InfoCert is 1.3.76.36.

Below are listed the policies for identification method:

Description	*OID*
Use cases using an identity document for unattended remote identity proofing, with hybrid manual and automated operation: SelfQ (*Compliant with ETSI TS 119 461 requirements established in chapter 9.2.3.3 "Use case for hybrid manual and automated operation)*	1.3.76.36.1.1.5000.34
Use cases using an identity document for unattended remote identity proofing, with hybrid manual and automated operation: SelfQ automated (*Compliant with ETSI TS 119 461 requirements established in chapter 9.2.3.4 "Use case for automated operation)*	1.3.76.36.1.1.5000.34

Table 1 – Policies for identity proofing method

1.3 IPSP Participants

IPSP: Identity Proofing Service Provider

Full details of the organisation acting as IPSP are as follows:

Company name	**InfoCert S.p.A. – Società per azioni Company subject to the management and coordination of Tinexta S.p.A.**
Registered office	**Piazzale Flaminio n.1/B, 00196, Rome, Italy**
Operational offices	**Via Fernanda Wittgens n. 2, 20123 Milano (MI)** **Piazza Luigi da Porto n. 3, 35131 Padova (PD)**
Legal Representative	**Danilo Cattaneo as Managing Director**
REA Number	**RM – 1064345**
VAT Number	**07945211006**
Website	**https://www.infocert.it**

TSP/QTSP: the service provider that manages the process and issues certificates. Could be InfoCert acting as QTSP.

Applicant or Subject: the individual undergoing identification.

Back-office Operator: a trained person who follows the instructions from the IPSP, and reviews validation results.

1.4 Policy and Practice Administration

1.4.1 Contacts

InfoCert is responsible for defining, updating and publishing this document. For questions, complaints, comments and requests for clarification regarding this Identity Proofing Practice Statement, please contact:

Company name	**InfoCert – S.p.A** **Head of QTSP** **Piazza Luigi da Porto n. 3, 35131 Padova (PD)**
Telephone number	**+39 06 836691**
Digital signature Contact Center	**https://help.infocert.it/contatti/ for more details**
Website	**https://www.firma.infocert.it,https://www.infocert.it**

E-mail	**firma.digitale@legalmail.it**

Subjects may request a copy of their personal documentation by filling in and sending the form available on https://www.firma.infocert.it and following the given procedure.

1.4.2 Parties responsible for approving this document

This Identity Proofing Service Practice Statement (hereafter IPSPS) has been approved by the Corporate Management following a review by the Head of Security and Policy, the Privacy Officer, the Head of Certification Services, the Head of Legal Department, the Head of Regulatory Affairs Manager.

1.4.3 Approval procedures

Drafting and approval of this document are carried out in accordance with the procedures described in the Company's Quality Management System ISO 9001:2015.

At least once a year, InfoCert checks the compliance of this Identity Proofing Practice Statement with its certification service process.

1.5 Definitions and acronyms

1.5.1 Definitions

Term	*Definition*
Advanced electronic seal	An electronic seal, which meets the requirements set out in Article 36 of eIDAS Regulation (see eIDAS [1])
Advanced electronic signature	An electronic signature which meets the requirements set out in Article 26 of the eIDAS Regulation (see eIDAS [1]) .
Applicant	Person (legal or natural) whose identity is to be proven [6].
Audit log	The set of automatic or manual entries of events provided for in the Technical Requirements.
Binding to applicant	Part of an identity proofing process that verifies that the applicant is the person identified by the presented evidence [6].
Conformity Assessment Body (CAB)	Body accredited under the eIDAS Regulation as competent to assess the conformity of a qualified trust service provider and of the qualified trust services he provides. It is responsible for drafting the CAR.
Conformity Assessment Report (CAR)	Report in which the Conformity Assessment Body confirms that the qualified trust service provider and its trust services comply with the requirements of the Regulation (see eIDAS [1]).
Customer	Subject with whom Infocert has formalized a service supply contract in exchange for compensation.
Digital identity document	Identity document that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form [6]
Electronic document	Any content stored in electronic form, especially text or sound, visual or audio-visual recording (see eIDAS [1]) .

Electronic identification means	A material and/or immaterial unit containing personal identification data, and which is used to access online services (see eIDAS [1]).
Electronic identification	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person (see eIDAS [1]) .
Identity	Attribute or set of attributes that uniquely identify a person within a given context [6].
Identity Document	Physical or digital document issued by an authoritative source and attesting to the applicant's identity [6].
Identity proofing (process)	Process by which the identity of an applicant is verified by the use of evidence attesting to the required identity attributes [6].
Identity Proofing Service Provider	An IPSP (Identity Proofing Service Provider) is a specialized entity that provides identity proofing as a subcontractor to a Trust Service Provider (TSP), delivering a component of the TSP's trust service**.**
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 [6].
Personal identification data	Set of data used to determine the identity of a natural and/or legal person or of a natural person representing a legal person (see eIDAS [1]
Physical presence	Identity proofing where the applicant is required to be physically present at the location of the identity proofing [6].
Presentation attack	Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system [5].
Presentation attack detection	Automated determination of a presentation attack [6].
Qualified electronic signature	An advanced electronic signature which is created by a qualified electronic signature creation device, and that is based on a qualified electronic signature certificate (see eIDAS [1]
Qualified Electronic Signature Certificate	Electronic signature certificate that is issued by a qualified trust service provider and meets the requirements of the Annex I of eIDAS Regulation (see eIDAS [1]).
Qualified trust service	A trust service that meets the applicable requirements laid down in the Regulation (see eIDAS [1]).
Qualified trust service provider	A trust service provider who provides one or more qualified trust services. Its qualified status is granted by the supervisory body (see eIDAS [1]).
Relying Party	A natural or legal person relying on an electronic identification or a trust service (see eIDAS [1]) .
Subject	Legal or natural person that is enrolled to a trust service [6].
Subscriber	legal or natural person bound by an agreement with a trust service provider to any subscriber obligations [6].
Trust service	An electronic service normally provided for remuneration which consists of: a) the creation, verification and validation of electronic signatures, seals or time stamps, certified electronic delivery services and related certificates, or b) the creation, verification and validation of certificates for Website authentication, or c) the preservation of electronic signatures, seals or certificates related to those services (see eIDAS [1]) .
Trust Service Practice Statement	statement of the practices that a TSP employs in providing a trust service [3].
Trust service provider	A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider (see eIDAS [1]) .

Unattended remote identity proofing	Identity proofing process by remote use of identity document where the capture of the identity document (physical or digital document) and the face video of the applicant are performed in an automated, interactive session without human supervision [6].
VIZ	ID document's Visual Inspection Zone consists of a set of area text zones which contain a pre-determined set of basic information.

1.5.2 Acronyms

Acronym	*Meaning*
AgID	Agenzia per l'Italia Digitale: Supervisory Authority for Trust Service Providers
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
DNN	Deep Neural Network
eMRTD	Electronic Machine-Readable Travel Document
EIC	Electronic Identity Card
eIDAS	Electronic Identification, Authentication and Trust Services [1]
eID	Electronic Identity
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation [2]
ISO	International Organization for Standardization: Established in 1946, the ISO is an international organisation made up of national standardisation bodies
IPSP	Identity Proofing Service Provider
IPSPS	Identity Proofing Service Practice Statement
LoA	Level of Assurance
MRZ	Machine Readable Zone
OCR	Optical Character Recognition
OID	Object Identifier: a sequence of numbers registered according to the procedure given in ISO/IEC 6523, and which references a specific object within a hierarchy
PAD	Presentation Attack Detection
PEC	Posta Elettronica Certificata (Certified e-mail)
QTSP	Qualified Trust Service Provider
TSP	Trust Service Provider
VIZ	Visual Inspection Zone

1.6 References

1. 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, consolidated version: 18/10/2024.

2. GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

3. ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

4. ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

5. ETSI EN 319 411-2: "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".

6. 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”.

7. ICAO Doc 9303 part 3: Machine Readable Travel Documents Eighth Edition, 2021 Part 3: Specifications Common to all MRTDs

8. ICAO Doc 9303 part 4: Machine Readable Travel Documents Eighth Edition, 2021 Part4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs

9. ICAO Doc 9303 part 10: "Machine Readable Travel Document - Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)".

10. InfoCert Certificate Policy & Certificate Practice Statement: ICERT-INDI-MO

11. Preservation Manual InfoCert: 01_Preservation_Manual_of_InfoCert_ENG_2023

2 IDENTITY PROOFING PROCESS

2.1 SelfQ Process steps

The Applicant is guided through an end-to-end process providing an unattended identification experience, composed by the following steps:

Data Collection:

The Applicant receives automated guidance throughout the identity proofing process, including the conditions allowing the identity proofing process to be successfully completed.

Please note that only eMRT digital identity documents compliant with ICAO 9303 part 10 [9] are accepted.

- The Applicant captures images of their ID document via a guided mobile app or web interface (uploads are not allowed).
- SelfQ OCR service extracts data from the identity document, allowing the applicant to confirm or correct minor errors.

Identity documents vary depending on geographic regions, versions, and their use. They usually contain information on both the front and the back (there are few cases where information is only present on the front). The ID document can be described in two types of information.

The first one VIZ (**Visual Inspection Zone)**, where the information about the owner of the ID document appears. It contains the following items:

- Face: Photograph of the face of the person identified by that document.
- OCR nodes: They contain the written information of the document such as names, surnames, dates, identification number, support number, addresses, etc.
- Physical security features: Physical security measures such as OVI inks, micro-writing, Kinegrams, etc.

MRZ (**Machine Readable Zone**) is the identity document area in which information adapted to be read by a machine appears. It is generally composed of two lines (passport) or three lines (identity cards). See [7] and [8].

As anticipated above, the categories of data extracted from identity documents can be different from type of document and its reference template. The common data extracted can be resumed as it follows.

- **Name**
- **Surname**

- **Sex**
- **Tax number**
- Date of birth
- Place of birth
- Nationality
- Residence address
- Document number
- Issuing country
- Valid from (date)
- Valid until (date)
- Place of issue

Data Validation:

- The system verifies whether the identity document has been tampered, MRZ and VIZ consistency, and antifraud indicators (based on replay and print attack checks).
- The information from the MRZ is extracted, validated, and compared with the information from the visible part of the identity document.

Binding to the Applicant:

- The Applicant performs a brief video session for liveness detection. During the video session, exclusively performed at the time of the identity proofing process, a video capture is taken. When all the quality features are matched (lightning, position, resolution), the system automatically takes the pictures of the applicant from the video and the software elaborates it in real time, determining the correct alignment of the face.
- Once the picture of applicant's face is extracted, the system compares it with the picture extracted from the identity document previously collected.

The liveness detection phase addresses the need to verify the presence and actual existence of the user, who submits their face for verification against the photo extracted from their identity document. The service allows to:

- Guide the user through the process of framing their face to take a selfie that ensures optimal conditions for:
  - Alignment of the face during the snapshot.
  - Quality of the captured image.
  - Light of the captured image.
- Perform "live" face recognition during the procedure.

The liveness detection module ensures that a real person, not a photo or a streaming video, is in front of the camera. InfoCert guides the entire data collection process and creates a mini video in which pixels are analyzed and processed automatically to prevent fraud attempts. All technology relies on highly sophisticated AI components, which consist of neural networks, properly trained with a set of coefficients that minimize error and can classify incoming data,

which are then used for binding activities.

Specifically, the module can identify spoofing attempts based on the same selfie used for face matching without user participation and employs a method based on the so-called Deep Neural Network (DNN), which examines various elements of the image to detect artifacts that help distinguish between a live person's photo and a so-called "presentation attack".

InfoCert liveness detection component has been evaluated in compliance with ISO/IEC 30107-3:2023 Standard, on "*Information technology - Biometric presentation attack detection*", achieving the level "substantial". Evaluations and tests have been performed for attacks of type 1 (presentation attacks) and type 2 (injection attacks).

Moreover, liveness detection component conforms to the characteristics specified in its security target for the substantial evaluation level as defined in the CEN TS 18099 and the associated CLR Labs test plan at the Substantial level of certification. Tests have been performed on injection attack detection features.

Video-stream is transmitted to an environment that ensures authenticity, integrity, and confidentiality of the element produced.

Once the liveness detection has been concluded, the automated face matching component compares the user's face shown in the selfie with the photo extracted from the identity document.

Optional back-office operators' review ensures additional accuracy.

Release of Identity Proofing Result:

Once all the checks have been performed by the system with a positive result, a qualified certificate can be issued.

Data and evidence are digitally preserved from the QTSP for the period as per the local norm and regulation. If the QTSP is InfoCert, said data and evidence are digitally preserved for 20 (twenty) years.

3 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

InfoCert has implemented an information security system for its trusted services. The security system is divided into three levels:

- A physical level aimed at ensuring the security of environments where TSP manages the service.
- A procedural level of strictly organisational nature.
- A logical level involving provision of hardware and software technology to address the

problems and risks associated with the type of service and the infrastructure used.

This security system is designed to avoid the risks arising from the malfunction of systems, networks and applications, as well as unauthorised interception or data modification.

An excerpt of the InfoCert security policy can be requested by email to *infocert@legalmail.it*.

InfoCert security policies are reviewed no less than on a yearly basis and are updated for any relevant changes. Each review is tracked within the document itself even when no changes have been necessary.

Physical security controls, site management, physical access, flood and fire prevention and protection, storage management and other facility and security operational controls are managed by InfoCert acting as QTSP and described in ICERT-INDI-MO [10].

3.1 Personell procedural controls

3.1.1 Key roles

Key roles are covered by personnel having the necessary experience, professionalism and technical/legal expertise, which are constantly verified through annual assessments.

3.1.2 Qualifications, experience, and clearance requirements

Following the annual Human Resource planning, the Function/Organizational Structure Manager identifies the characteristics and skills of the resource to be inserted (job profile). Subsequently, in conjunction with the Staff Selection Manager, the search and selection process are triggered. Selected candidates participate in the selection process by taking part in an initial cognitive-motivational interview with the Staff Selection Manager and in a subsequent technical interview with the Function/Organizational Structure Manager, in order to check the skills declared by the candidate. Additional verification tools include exercises and tests.

3.1.3 Training requirements

To prevent any person from individually affecting or altering overall system security or performing unauthorized activities, the operational management of the system is entrusted to different resources, each with separate and well-defined tasks. The personnel in charge of Identity proofing service design was selected for his background in the design, implementation and management of IT services and for his characteristics of reliability and confidentiality. Training sessions are planned periodically to raise awareness on assigned tasks. In particular, prior to the inclusion of staff in operating activities, training courses are carried out to provide all the necessary (technical, organizational and procedural) skills to carry out assigned tasks.

3.1.4 Retraining frequency

Every starting of the year, training requirements are analysed to define the training courses to be held during the year. The analysis is based on the following steps:

- Meeting with Corporate management to collect data on the training requirements needed to achieve business objectives.

- Feedback from the area managers to identify the specific training needs from each area.
- Forwarding of collected data to Corporate Management for Training Plan closing and approval.

Once defined, the Training Plan is shared with the employee staff at the beginning of the year.

3.1.5 Sanctions for unauthorized actions

Sanctions are imposed to the employee staff in accordance with the National Employment Contract for Metalworkers and Installation of Private Industrial Plants ("CCNL Metalmeccanici e installazione impianti industria privata").

3.1.6 Checks on non-employee staff

Access to non-employee personnel is governed by a specific corporate policy. They participate to adequate training.

3.1.7 Documentation to be supplied by personnel

Upon recruitment, employees must provide a copy of a valid identity document, as well as a copy of a valid health card and a passport type photo for their access badge. Subsequently, they will be required to complete and sign a written consent to the processing of personal data and a confidentiality agreement, and to review InfoCert's Code of Ethics and Netiquette policy.

4 AUDIT LOGGING PROCEDURES

4.1 Types of Events Logged

Evidence, events and logs of the identity proofing process are gathered and retained in compliance with the chosen identity proofing method. In some case, depending on the context, also the validation proof can be gathered and retained.

Procedures for the management of evidence, events and logs of related to the operation of the identity proofing service are formalized in an internal procedure.

They are collected by means of ad hoc automated procedures.

4.2 Retention period

All the evidence, log and events are retained for at least 5 (five) year even if the identity proofing was rejected at the end of the retention time defined the evidence of the identity proofing process and all personal data on the applicant will be deleted.
The identity proofing provider can keep the evidences and logs for a longer period of time based on specific agreements with the TSP that uses the service.

4.3 How evidence is stored

The evidence of the identity proofing process is stored in a temper-proof way, ensuring the confidentiality of the information.

The aim is to guarantee the possibility to search, retrieve and re-verify the identity proofing results to keep them easily accessible upon request by law enforcement or by the Subject.

The evidence is stored in the InfoCert SAFE LTA archiving system (see 01_Preservation_Manual_of_InfoCert_ENG_2023) [11].

5 OTHER BUSINESS AND LEGAL MATTERS

5.1 Fees

Fees for the identity verification services are subject to contractual agreements between InfoCert IPSP and its business partners.

5.2 Financial responsibility

5.2.1 Insurance coverage

InfoCert IPSP maintains professional liability insurance coverage.

5.3 Personal Information Privacy

Unless expressly permitted, any information acquired by the IPSP during its routine activities is confidential and non-disclosable, except for information specifically intended for public use. Personal data shall be processed by the IPSP in accordance with Legislative Decree No. 196 of 30 June 2003 and with European Regulation 2016/679 (GDPR) effective as from 25 May 2018 [2].

5.3.1 Privacy plan

InfoCert implements personal data protection policies within its ISO 27001 certified information security management system, ensuring continuous improvement.

5.3.2 Personal Information

Personal Data as defined by applicable legislation [2] refers to any information about a **natural** person that can identify them, directly or indirectly, including a personal identification number.

InfoCert employees who handle information are required to protect it from compromise and disclosure to third parties.

They must comply with Italian privacy laws.

5.3.3 Controller of personal data processing

Company name	**InfoCert S.p.A**
Registered office	**Piazzale Flaminio n. 1/B** **00196 Roma**
E-mail	**richieste.privacy@legalmail.it**

5.3.4 Privacy disclosure and consent

InfoCert's privacy policy is available on the website www.infocert.it at the following link:

https://www.infocert.it/informative-privacy.

InfoCert will process data in the manner and form required by law. The processing will be based on an appropriate legal basis as described in the privacy policy.

In cases where identification requires the processing of biometric data, InfoCert will request consent before providing the service.

If the processing is carried out by another legal entity on behalf of InfoCert, the privacy policy will be made available by the third party, who will also be responsible, if necessary, for obtaining consent.

5.3.5 Disclosure pursuant to legal requests

InfoCert must disclose information requested by authorities, following the procedures set forth by the relevant Authority.

5.4 Intellectual property rights

5.5 Representations and Warranties

InfoCert remains responsible for complying with its information security policy, even when certain functions are outsourced to third parties.

The Subject is responsible for the accuracy of the data provided. If the Subject conceals their identity or falsely claims to be someone else through methods such as forgery or document alteration, he or she is responsible for any damages caused to the IPSP and/or third parties and must indemnify the IPSP against any compensation claims.

5.6 Disclaimer of Warranties

No warranties are provided.

5.7 Limitation of Liability

InfoCert is not responsible for monitoring the content, type, or format of documents transmitted by the Subject, nor for ensuring the validity and traceability of the procedure reflecting the Subject's actual intent.

Except in case of wilful misconduct or gross negligence, the InfoCert is not be liable for any direct or indirect damage to the Subjects and/or third parties because of the use or non-use of subscription certificates issued after the Identity proofing process.

InfoCert also disclaims responsability for any direct and/or indirect damages deriving from: (i) loss, (ii) improper storage, (iii) improper use of identification and authentication tools and/or (iv) the Subject's failure to follow recommendations mentioned above.

Moreover, InfoCert is not liable for any damages and/or delays due to system or network malfunctioning during Identity proofing process.

Except in the case of wilful misconduct or gross negligence, InfoCert is not liable for direct or indirect damages to the Subject.

5.8 Indemnities

InfoCert is solely responsible for direct damage, caused intentionally or by negligence, to any individual or entity, due to non-compliance with eIDAS regulations [1] and failure to implement appropriate measures to prevent damage.

Refunds will not be granted if access issue are due to improper use of the certification service, telecommunication network problems or events beyond InfoCert control, such as force majeure strikes, revolts, earthquakes, acts of terrorism, popular riots, organised sabotage, chemical and/or bacteriological events, war, floods, government-imposed measures, hardware and/or software used by the Applicant.

5.9 Term and termination

5.9.1 Terms & Conditions

The Applicant is informed of terms & conditions, which must be accepted before starting the the identity proofing process. The terms and conditions may apply to the use of the trust service for which the identity proofing is conducted.

5.9.2 Termination

The Contract automatically terminates with the interruption of services in cases of non-compliance with the contract terms. Termination occurs by right when one party notifies the other party by PEC or registered letter a.r.,. The Contract's effects remain unaffected until its termination.

The Subject acknowledges that after termination the Service will no longer be available.

If InfoCert decides to discontinue the SelfQ service, customers will be notified within the agreed notice period. The related evidence will, however, be retained by InfoCert for the required period.

5.10 Amendments

The IPSP reserves the right to amend this document for technical reasons or to comply with legal or regulatory changes. Each new version supersedes previous versions.

Increasing document release numbers indicate amendments that do not have a significant impact on relying parties, whereas increasing document version numbers indicate amendments that significantly impact relying parties (such as significant changes affecting operating procedures). In any event, this document will be promptly published and made available in the prescribed ways.

Major changes require an audit by an accredited CAB, submit the certification report (CAR – Conformity Assessment Report) and approval from AgID before publication.

5.10.1 Amendment history

Information	Description
Version/Release:	1.1
Version/Release date (gg/mm/aaaa):	10/07/2025
Description of changes:	Edits on re-wording § 5.9 Edits on Termination of the service
Reasons:	document update

Information	Description
Version/Release:	1.0
Version/Release date (gg/mm/aaaa):	15/03/2025
Description of changes:	
Reasons:	first version

6 ANNEX

6.1 Outsourced technologies

For some process-related components, InfoCert relies on the technologies provided by the following suppliers:

- **VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, S.L.**
  Available at the following link: https://veridas.com/en/.
  Veridas is provider of all the data and evidence collection, extraction and validation components related to the SelfQ identification process.
  To enhance the reliability of the evidence collection and validation process, only eMRT digital identity documents compliant with ICAO 9303 part 10 [9] are accepted by Veridas solution.
  Veridas has obtained the ETSI TS 119 461 and ETSI EN 319 401 certifications, as described at the following link https://veridas.com/en/compliance/

  IDrND
  Available at the following link: https://www.idrnd.ai/.
  InfoCert liveness detection module is made available to InfoCert by the provider ID R&D. Its components are compliant and certified with the ISO 30107-3 Standard, as stated in the iBeta confirmation letter shown below (available at the following link https://www.ibeta.com/wp-content/uploads/2020/10/200930-ID-RD-PAD-Level-2-Confirmation-Letter.pdf).