ENTAKSISOLUTIONS

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
QUALIFIED TRUST SERVICES
ETSI 319 401 | ETSI 319 411-1 and 2 | ETSI 319 421 | ETSI 119 511
ELECTRONIC SIGNATURES AND SEALS - TIME STAMPS
LONG-TERM PRESERVATION

Manual

MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement EN

Entaksi Solutions SpA

Table of contents

Document information

Project	Integrated Management System
Type	Manual
Document ID	MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement EN
Version	1.0.0
Creation Date	25/11/2025
Last Revision	25/11/2025
Author	Alessia Soccio
Status	Released
Classification	Public
Translation	This document is the original version. Italian translation: "MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement".

Paper reproductions of this document are to be considered working copies not registered by the SIG.

Revisions and releases

Date	Version	Name	Role	Action	Release
25/11/2025	0.0.1	Alessia Soccio	IMSM	Draft creation.	Internal
25/11/2025	1.0.0	Alessia Soccio	IMSM	Review and release.	Public

Document approval

Date	Employee	Role	Signature
25/11/2025	Alessandro Geri	SM	*Digitally signed*

1. Introduction

This document is the **Identity Proofing Service Policy and Practice Statement (IPSPPS) of the qualified Certification Authority operated by Entaksi Solutions SpA - Irish Branch** (hereinafter "Entaksi"), a branch of the Italian company with VAT-ID IT01621900479 Entaksi Solutions SpA, operating in Ireland with National Trade Register number 909882.

Entaksi is a **Trust Service Provider** for:

- **The issuance of qualified certificates for electronic signatures**.
- **The issuance of qualified certificates for electronic seals**.
- **The qualified preservation service for qualified electronic signatures**.
- **The qualified preservation service for qualified electronic seals**.
- **The creation of qualified electronic timestamps**.

Entaksi is registered as a Trust Service Provider by the competent national supervisory body in Ireland (currently the Department of the Environment, Climate and Communications – DECC) and is included in the national trusted list in accordance with the eIDAS Regulation.

The purpose of this document is to serve as a basis for demonstrating compliance with EU Regulation 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, as amended by EU Regulation No. 1183/2024 – eIDAS 2 (hereinafter "eIDAS"), and the ETSI standards ETSI TS 119 461, ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2, describing how the Certification Authority (CA) operated by Entaksi, acting as a TSP, provides the Identity Proofing Service (IPS) as a trust service component within the following services:

- **the issuance of qualified certificates for electronic signatures**;
- **the issuance of qualified certificates for electronic seals**;
- **the qualified service for the management of remote qualified electronic signature creation devices**;
- **the qualified service for the management of remote qualified electronic seal creation devices**.

Entaksi issues qualified certificates that require an Identity Proofing Service for the following usages:

- **Qualified certificates for electronic signatures**.
- **Qualified certificates for electronic seals**.

The document also takes into account the "Commission Implementing Regulation (EU) 2025/1566 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for the verification of the identity and attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued".

1.1. Purpose and scope of the document

This document specifies the policies, processes and security requirements applied by Entaksi, acting as the Identity Proofing Service Provider (IPSP), in delivering identity proofing as a trust service component for Entaksi's Trust Services.
It also sets out the policies, processes and procedures followed in the identification and verification of applicants for the Entaksi Certification Authority Public Key Infrastructure.
Moreover, it describes the roles, responsibilities and relationships of the Participants within Entaksi's PKI, and the requirements for the secure, reliable and compliant execution of identity proofing activities in accordance with applicable standards and regulatory frameworks.

The structure of this document is based on the IETF RFC 3647, "Certificate Policy and Certification Practices Framework".

1.2. Document name and identification

This document is identified by the following OID:

Table 1. Document name and identification.

OID	Description	Permanent Link
1.3.6.1.4.1.57823.1.13	MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.13

1.3. IPSPS participants

The participants within the framework of this practice statement are:

- Entaksi as a Trust Service Provider (TSP) requesting the identity proofing and receiving the identity proofing result.
- The Local Registration Authorities in a contractual relationship with Entaksi Certification Authority.
- The Registration Officer, the operator enrolled by Entaksi who performs all or selected parts of the identity proofing process.
- Onfido, as a subcontracted Identity Proofing Service Provider (IPSP), acting as part of the identification process.
- Applicant to the Entaksi services whose identity is to be proven.
- Relying parties.
- Other participants.

These roles participate in, or interact with, identity verification processes that support certificate issuance and other trust-service operations within the Entaksi's services.

Entaksi digital certificates comply with Internet standards X509v3 as set out in IETF RFC 5280.

1.4. Identity Proofing Process

The identity proofing process implemented by Entaksi follows the structure and requirements defined in clause 4.2 and clause 8 of ETSI TS 119 461, and is composed of the following five tasks, which may be performed sequentially, iteratively, or in a hybrid manner depending on the identity proofing use case and the identity proofing context:

1. **Initiation** The applicant is informed of the purpose of the identity proofing, the applicable terms and conditions, the evidence required, and the tools and processes that will be used. The applicant actively accept these conditions before the identity proofing begin by subscribing Entaksi terms and conditions. Guidance is provided to ensure the applicant understands how the process will be conducted and what is expected of them.
2. **Attribute and Evidence Collection** Identity attributes and the corresponding authoritative and/or supplementary evidence are collected from the applicant or from trusted sources. Depending on the use case, evidence may include physical or digital identity documents, trusted registers, proof of access, electronic attestations of attributes, or other permitted evidence sources.
   Collection may be conducted manually by a registration officer, automatically, or through hybrid manual/automated procedures, according to the use cases defined by Entaksi.
3. **Attribute and Evidence Validation** All collected attributes are validated against the evidence to the level of reliability required by the applicable identity proofing context. Validation includes ensuring that:
   - the evidence is genuine, authoritative, and valid;
   - the attributes are consistent across sources;
   - the integrity and authenticity of digital evidence is preserved;
   - any encoding or transcription differences are handled correctly.

   Validation may be performed by automated systems, by registration officers, or by a combination of the two.
4. **Binding to Applicant** Binding ensures that the individual or legal person presenting the evidence is the same entity to whom the identity attributes relate.
   For natural persons, binding typically involves face verification, either manual, automated (biometric), or hybrid. For legal persons or natural persons representing legal persons, binding includes verification of representation rights and validation against trusted registers or equivalent sources.
5. **Issuing of Identity Proofing Result** At the conclusion of the process, Entaksi securely issues the identity proofing to be used within its services.
   The result indicates the Level of Identity Proofing (LoIP) achieved, and may include the validated attributes, the status of the proofing, and any relevant assurance information.

Evidence of the identity proofing process is gathered and retained in accordance with the applicable identity proofing context and legal requirements, as stated in the terms and conditions document.

1.5. Supported Use Cases

Entaksi identifies in this IPSPS the identity proofing use cases for which conformity with ETSI TS 119 461 and with the Commission Implementing Regulation (EU) 2025/1566 is claimed.
The identity proofing service provided by Entaksi supports the use cases defined in clause 9 and Annex C.3 of ETSI TS 119 461, specifically those applicable to the issuing of qualified certificates and qualified electronic attestations of attributes according to Articles 24.1, 24.1a and 24.1b of the amended eIDAS Regulation.

All supported use cases are implemented in accordance with the required Extended Level of Identity Proofing (Extended LoIP) and fulfil the corresponding normative requirements for initiation, attribute and evidence collection, validation, binding to applicant, and issuing of identity proofing result.

1.5.1. Use case for identity proofing by physical presence of the applicant

Supported operational mode:

- Manual operation.

Entaksi performs identity proofing of natural persons physically present before a registration officer, using authoritative identity documents as required for Extended LoIP.

1.5.2. Use case for identity proofing by authentication using eID means

Entaksi supports identity proofing through authentication with eIDAS substantial or high eID means, provided that such eID means comply with the requirements of Annex C.3.2 for Extended LoIP and have been issued on the basis of identity proofing performed through physical presence or an equivalent high-confidence process.

1.5.3. Use case for identity proofing by certificate of qualified electronic signature or qualified electronic seal

Entaksi supports identity proofing by validating a qualified electronic signature (for natural persons) or a qualified electronic seal (for legal persons), ensuring:

- the qualified certificate was issued following identity proofing at an acceptable level;
- the signature or seal is validated in accordance with eIDAS Article 32 and ETSI TS 119 172-4;
- the chain of trust supports Extended LoIP.

1.5.4. Use case for identity proofing by other identification means

Entaksi supports identity proofing by "other identification means" permitted under Articles 24.1a(c) and 24.1b(d) of amended eIDAS, including:

- attended remote identity proofing using identity documents;
- unattended remote identity proofing using identity documents;
- automated, hybrid or post-processed validation workflows.

For Extended LoIP, the applicable sub-use cases in clause 9.2.2 or 9.2.3 are applied according to Annex C.3.4.

1.5.5. Use case for identity proofing of legal person

Entaksi supports identity proofing of legal persons by validating:

- the unique identity of the legal person through trusted registers or authoritative sources;
- supplementary or additional attributes where required;
- registration numbers and legal existence;
- any additional attributes needed for issuance of qualified certificates or qualified electronic attestations of attributes.

All validations are executed in accordance with Extended LoIP requirements.

1.5.6. Use case for identity proofing of natural person representing legal person

Entaksi supports identity proofing of a natural person acting on behalf of a legal person, including:

- identity proofing of the natural person (via one of the supported natural-person use cases);
- verification of the legal person (via the legal-person use case);
- validation of the person's representative role and authority to act, using trusted registers, documents, electronic attestations of attributes, or other authoritative sources.

All requirements of Annex C.3.6 for Extended LoIP are applied.

1.5.7. Registration authorities

The applicant subscribing a service seeking certificates undergo a process of identification and authentication, that can be carried out directly by Entaksi CA staff, or it can be delegated to third parties, known as "Registration Authorities" (RAs) or Local Registration Authority (LRA). This delegation is sanctioned by specific agreements between Entaksi CA and the RAs.

Entaksi's RAs are responsible for the following functions:

- identifying and authenticating certificate applicants;
- approving or rejecting certification requests;
- processing requests from subscribers to revoke, suspend, reactivate, or renew their certificates;
- sending documents, communications, and requests to the CA.

Registration Authoritys, on the other hand, are not responsible for signing or issuing certificates; instead, they are delegated specific tasks on behalf of Entaksi's CA.

The individuals involved in the functions listed above are called "Registration Authority Officer (RAO)", and can perform these tasks only after having received adequate training from Entaksi.
RAOs operate via email or SaaS web services made available by Entaksi to communicate certificates data. These services are subject to the exclusive control of Entaksi.

RAOs that verify the identity shall not be the natural person to whom the certificate is issued to (as a subject).

Operative instructions for RAOs appointed by Entaksi are contained in the document "OI IMS 20231128 Registration Authority Officer".

1.5.8. Subscribers and subjects

A subject is the entity identified in a certificate as the holder of the private key associated with the public key given in the certificate, as stated in ETSI EN 319 411-1.

In the framework of the present document, the subscriber (also known as applicant) can be:

- a natural person;
- a natural person identified in association with a legal person;
- a legal person.

1.5.9. Relying parties

All parties relying on the information within this document or certificates issued by Entaksi CAs are referred as "relying parties". These parties may or may not be a subscriber, but can be individuals and organizations doing business with subscribers in need to verify the certificates issued by Entaksi.

The communication channels between Entaksi and the relying parties are stated in the chapter Contact person.

1.5.10. Other participants

There are no other participants to the identity proofing service, except for national supervisory bodies.

1.6. Certificate usage

All the information about certificate usages is described in "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN".

1.7. Policy administration

1.7.1. Organization administering the document

This Identity Proofing Service Policy and Practice Statement is issued under the responsibility of Entaksi management.

1.7.2. Contact person

The Trust Service Provider can be contacted at the following addresses:

Entaksi Solutions SpA - Irish Branch
Suite 4.01 - Ormond Building 31 36 Ormond Quai Upper - D07F6DC Dublin 7 - Ireland

Entaksi Solutions SpA - Italian Head Office
via la Piana 76, fraz. Pontepetri, 51028 San Marcello Piteglio (PT), Italy

Entaksi Solutions SpA - Operational office
re.working, Viale della Costituzione - Centro Direzionale Isola E2 - 80143 Napoli, Italy

Info: info@entaksi.eu
Help Desk: helpdesk@entaksi.eu
Data Protection Info: privacy@entaksi.eu
Data Protection Officer: dpo@entaksi.eu
Anti-Bribery: antibribery@entaksi.eu
Certification Authority: ca@entaksi.eu

Phone: +39 0573 171 6484
Website: https://www.entaksi.eu/en/

1.7.3. Person determining CPS suitability for the policy

This Identity Proofing Service Policy and Practice Statement has been approved by Entaksi management following a review by internal and external auditors.

1.7.4. CPS approval procedures

Document maintenance

Entaksi has defined a review process for all the internal documents, including policies, statements and practices.

The documents are periodically reviewed under the responsibility of Entaksi management, in order to assess their compliance with national and international requirements, standards, mandatory legislation, regulations in force, particular needs imposed by the technical and technological evolution, evolution of the business context.

The review and any update take place at least once a year, or whenever one of the following circumstances occurs:

- internal organizational changes that impact on the system;
- major changes to the hardware or software architecture;
- regulatory updates;
- changes in procedures, methodologies or business context.

Approval and publication

This document and all the internal policies and practices mentioned in it have been approved by Entaksi's management, published and communicated to employees and, as regards those classified as "public", published on the company website at the following link: https://www.entaksi.eu/en/documentation.html.
The website is available on 24x7 basis.

Entaksi makes available to all customers of trust services and relying parties any update of this document and other relevant documentation as soon as the update is approved and revised on the basis of what is described in the revision procedure.

Entaksi, will communicate any change that might affect the acceptance of the service by the subject, subscriber or relying parties through the communication channel established in the terms and conditions of the service.

1.8. Definitions and acronyms

1.8.1. Definitions

Certificate

Public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it.

Certificate chain

A chain of digital certificates required to validate a holder's digital certificate back through its respective issuing certification authority to the root certification authority.

Certificate renewal

The process of issuing a new certificate duplicating all the identifying information from an old certificate, but with a different validity period.

Certificate Re-key

The process of issuing a new certificate duplication all the identifying information from an old certificate, but with a new public key and a possibly different validity period.

Certificate Revocation List (CRL)

Signed list indicating a set of certificates that have been revoked by the certificate issuer.

Certification

The process of creating a digital certificate for an entity and binding that entity's identity to the digital certificate.

Certification Authority (CA)

Authority responsible for issuing and assigning certificates to one or more users.

Certification Authority Revocation List (CARL)

A Revocation list containing a list of CA-certificates issued to certification authorities that have been revoked by the certificate issuer.

Digital Signature

Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

Digital transmission

The transmission of information in an electronic format.

Identification

The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization.

Issuing certification authority (issuing CA)

In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Participant

An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

Registration Authority (RA)

Entity that is responsible for identification and authentication of subjects of certificates.

Relying party

A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate.

Secure Cryptographic Device

A secure software, device or utility that generates key pairs, stores cryptographic information and performs cryptographic functions.

Subscriber

A subject of a certificate who is issued a certificate.

Validation

The process of identification of certificate applicants.

1.8.2. Acronyms

CA

Certification Authority.

CP

Certificate Policy.

CPS

Certification Practice Statement.

CRL

Certificate Revocation List.

CSA

Certificate Status Authority.

eIDAS

electronic Identification, Authentication and Signature.

ETSI

European Telecommunications Standards Institute.

HSM

Hardware Security Module.

IETF

Internet Engineering Task Force.

ITU

International Telecommunication Union.

ITU-T

ITU Telecommunication Standardization Sector.

LDAP

Lightweight Directory Access Protocol.

OCSP

Online Certificate Status Protocol.

OID

Object Identifier.

PKI

Public Key Infrastructure.

QTSA

Qualified Time-stamping Authority.

QSCD

Qualified Signature Creation Device.

RA

Registration Authority.

TLS

Transport Layer Security.

TSA

Time-Stamping Authority.

TSP

Trust Service Provider.

TSU

Time Stamping Unit.

UTC

Coordinated Universal Time.

1.9. References

1.9.1. Normative references

Entaksi's Integrated Management System, which also oversees the processes described within this document, is certified against the following international standards:

- **ISO 9001:2015**: Quality management systems - Requirements.
- **ISO/IEC 20000-1:2018**: Information technology - Service management - Part 1: Service management system requirements.
- **ISO/IEC 27001:2022**: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- **ISO/IEC 27017:2015**: Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- **ISO/IEC 27018:2019**: Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- **ISO/IEC 27035:2016**: Information technology — Security techniques — Information security incident management.
- **ISO/IEC 22301:2019**: Security and resilience — Business continuity management systems — Requirements.
- **UNI ISO 37001:2016**: Anti-bribery management systems - Requirements with guidance for use.
- **eIDAS Regulation for Qualified Trust Service Providers**:
  - **ETSI EN 319 401 V3.1.1 (2024-06)**: Electronic Signatures and Infrastructures (ESI) - General Policy Requirements for Trust Service Providers.
  - **ETSI EN 319 411-1 V1.5.1 (2025-04)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 1: General requirements.
  - **ETSI EN 319 411-2 V2.6.1 (2025-06)**: 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.
  - **ETSI EN 319 412-1 V1.6.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures.
  - **ETSI EN 319 412-2 V2.4.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons.
  - **ETSI EN 319 412-3 V1.3.1 (2023-09)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 3: Certificate profile for certificates issued to legal persons.
  - **ETSI EN 319 412-5 V2.5.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 5: QCStatements.
  - **ETSI EN 319 421 V1.3.1 (2025-07)**: Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time-stamps.
  - **ETSI EN 319 422 V1.1.1 (2016-03)**: Electronic Signatures and Infrastructures (ESI) - Time-stamping protocol and time-stamp token profiles.

  - **ETSI TS 119 511 V1.2.1 (2025-10)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.
- **CSA STAR**: Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) Level 2.

All the certifications are publicly available at the following link: https://www.entaksi.eu/en/certifications.html.

The Trust Services Management System, a subcomponent of Entaksi's Integrated Management System, complies with the relevant requirements laid down in eIDAS 2 and meets the additional conformity requirements of the following standards:

- ETSI Standards:
  - **ETSI EN 319 102-1 V1.3.1 (2021-11)**: Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 1: Creation and Validation;
  - **ETSI TS 119 102-2 V1.4.1 (2023-06)**: Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 2: Signature Validation Report;
  - **ETSI TS 119 172-4 V1.1.1 (2021-05)**: Electronic Signatures and Infrastructures (ESI) Signature Policies - Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists;
  - **ETSI TS 119 431-1 V1.3.1 (2024-12)**: Electronic Signatures and Trust Infrastructures (ESI) - Policy and security requirements for trust service providers - Part 1: TSP services operating a remote QSCD / SCDev;
  - **ETSI TS 119 441 V1.3.1 (2025-10)**: Electronic Signatures and Trust Infrastructures (ESI) - Policy requirements for TSP providing signature validation services;
  - **ETSI TS 119 442 V1.1.1 (2019-02)**: Electronic Signatures and Infrastructures (ESI) - Protocol profiles for trust service providers providing AdES digital signature validation services;
  - **ETSI TS 119 461 V2.1.1 (2025-02)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service components providing identity proofing of trust service subjects;
  - **ETSI TS 119 495 V1.7.1 (2024-07)**: Electronic Signatures and Trust Infrastructures (ESI) - Sector Specific Requirements - Certificate Profiles and TSP Policy Requirements for Open Banking;
  - **ETSI TS 119 512 V1.2.1 (2023-05)**: Electronic Signatures and Infrastructures (ESI) - Protocols for trust service providers providing long-term data preservation services;
  - **ETSI EN 301 549 V2.1.2 (2018-08)**: Accessibility requirements for ICT products and services;
- ISO Standards:
  - **ISO 14641:2018**: Electronic document management - Design and operation of an information system for the preservation of electronic documents - Specifications;
  - **ISO/IEC 14721:2025**: Space data and information transfer systems - Open archival information system (OAIS) - Reference model;
  - **CEN/TS 18170:2025**: Functional requirements for the electronic archiving services.

The applicable standards for the issuance of qualified certificates for electronic signatures and the issuance of qualified certificates for electronic seals, pursuant to the EU Regulation No. 910/2014 - eIDAS, as amended by EU Regulation No. 1183/2024 – eIDAS 2 and the "Commission Implementing Regulation (EU) n° 2025/2162 of 27 October 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the accreditation of conformity assessment bodies performing the assessment of qualified trust service providers and the qualified trust services they provide, the conformity assessment report and the conformity assessment scheme", are:

- ETSI EN 319 401 V3.1.1 (2024-06).
- ETSI EN 319 411-2 V2.6.1 (2025-06).
- ETSI EN 319 412-1 V1.6.1 (2025-06).
- ETSI EN 319 412-2 V2.4.1 (2025-06).
- ETSI EN 319 412-3 V1.3.1 (2023-09).
- ETSI EN 319 412-5 V2.5.1 (2025-06).
- ETSI TS 119 461 V2.1.1 (2025-02).
- ETSI TS 119 495 V1.7.1 (2024-07)
- ETSI EN 301 549 V2.1.2 (2018-08).

Entaksi does not issue qualified certificates for Payment Service Providers and does not operate a PSD2/Open Banking trust service. Therefore, ETSI TS 119 495 ("Electronic Signatures and Trust Infrastructures (ESI) - Sector Specific Requirements - Certificate Profiles and TSP Policy Requirements for Open Banking") is not applicable to the trust services provided by Entaksi.

1.9.2. Informative references

Entaksi's Certification Authority is supported by the following policies, practice statements and manuals:

Table 2. CA documents name and identification.

OID	Description	Permanent Link
1.3.6.1.4.1.57823.1.9	MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.9
1.3.6.1.4.1.57823.1.10	MAN eIDAS 20230426 PKI Disclosure Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.10
1.3.6.1.4.1.57823.1.13	MAN eIDAS 20251125 Identity Proofing Service Policy and Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.13

All the previous enlisted documents are classified as "public" and disclosed to the relying parties on the company website: https://www.entaksi.eu/en/

2. Publication and repository responsibilities

2.1. Repositories

Entaksi uses selected identity attributes collected and validated during the identity proofing process exclusively for the purpose of generating and managing qualified certificates, in accordance with applicable standards and legal requirements.

Published certificates, the Certificate Revocation List (CRL) and the OCSP service are available on line, 24 hours a day.

Please refer to "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN" for more info about Entaksi's certificates.

2.2. Publication of certification information

Entaksi publishes all the TSP documents in PDF format at the following link: https://www.entaksi.eu/en/documentation.html.

Published documentation includes, but is not limited to:

- Certificate Policies and Practice Statements (CPCPS);
- Certification Practice Statements (CPS);
- Identity Proofing Service Policy and Practice Statement (IPSPS);
- PKI Disclosure Statements;
- Terms and Conditions and other service documentation.

2.3. Time or frequency of publication

Publication's frequency of Entaksi's documents varies to reflect any changes that have occurred.

2.4. Access controls on repositories

Information relating to issued certificates, CRLs, Certificate Policies, Certification Practice Statements, the Identity Proofing Service Policy and Practice Statement, and the PKI Disclosure Statement is publicly available and accessible without restrictions.

Entaksi is the only entity with write access to the repositories, ensuring their integrity, authenticity and availability.

3. Attributes to be collected

The certificate holder (subject) is identified in the certificate by a Distinguished Name (DN) compliant with IETF RFC 5280, ITU-T X.509, ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 412-1,2,3,5.

All identity attributes collected during the IPS process must support the correct population of the certificate subject fields, the semantics identifiers, and the information needed to confirm eligibility at the time of issuance.

3.1. Attributes for natural persons

When the subject is a natural person, the following information shall be collected and validated:

- **Full name**: surname and given name(s), consistent with national identification practices.
- **Date and place of birth**.
- **Unique national identifier**, such as Tax Identification Number (TIN), National ID Number, or equivalent (when applicable in the subject's country).
- **Reference to an authoritative identity document**, including:
  - document type (passport, ID card, residence permit);
  - issuing country;
  - document number;
  - document validity dates.

Biometric data (face image) only if required for the binding process, and processed exclusively under the terms and conditions of the service provided.

These attributes support correct encoding of:

- `countryName`;
- choice of (`givenName` and/or `surname`);
- `serialNumber`; and
- `commonName`.

3.2. Attributes for legal persons

When the subject is a legal person (electronic seal certificate), the following information shall be collected and validated:

- **Full registered legal name**, consistent with national business registers.
- **Organization identifiers**, including at least one of the following:
  - VAT number;
  - Trade Register number;
  - LEI (Legal Entity Identifier), if applicable;
  - other officially recognized identifiers as per national legislation.
- **Legal form**, when required by national practices or by certificate semantics.

These attributes support correct encoding of:

- `organizationName`;
- `organizationIdentifier`.

3.3. Attributes for natural persons identified in association with a legal person

If the certificate is issued to a natural person representing a legal person:

- all attributes required for natural person identity proofing;
- all attributes required for legal person identity proofing;
- documentary evidence of the representative's authority to act, e.g.:
  - power of attorney;

- registry extract listing representation rights;
- corporate delegation documents.

In this case the subject remains the natural person and attributes referring to the represented organization appear as organizational attributes in the DN or certificate extensions.

3.4. Attributes for subscribers when subscriber is not the subject

If the subscriber is not the subject, evidence shall be collected of:

- all attributes for the subscriber;
- a legally valid agreement permitting representation:
  - an explicit agreement when representing a natural person, or
  - an authorization to represent a legal person.

If the subscriber is a legal person, it must be represented by a natural person, whose authorization must also be proved.

3.5. Other information

All subscribers must provide a

- physical address or equivalent contact information;
- phone number;
- email.

These are not included in the certificate, but are necessary for communications during the certificate life-cycle, identity proofing follow-up and security notifications.

3.6. Recording of identity attributes

Entaksi, acting as TSP/IPSP, records:

- the information necessary to verify the subject's identity;
- references to the documentation used (e.g., passport number, business registry reference);
- evidence of validity limits (expiry dates, restrictions);
- any specific attribute that will appear in the certificate;
- records of subscriber and subject agreements.

Entaksi preserves these attributes in comformity to the terms of use.

3.7. Correctness and timeliness of attributes

The attributes included in the certificate:

- must be assessed as correct at the time of issuance;
- must rely on an identity proofing method that is still valid according to current Entaksi policies;
- must not rely on outdated or insecure methods.

3.8. Handling attribute changes

If any certified attribute changes before certificate issuance the corresponding registration information shall be re-verified and recorded and changes shall be approved by the subscriber (and the subject, when different).

Entaksi defines in its "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN" whether certificate re-key or renewal is allowed in cases where certified attributes have changed.

3.9. Non-verified subscriber information

Certain pre-contractual information such as addresses or telephone numbers may not be verified. Entaksi assumes no responsibility for their accuracy.

3.10. Criteria for Interoperation

Entaksi may interoperate with other recognized Trust Service Providers under specific agreements, ensuring consistent interpretation of identity attributes and semantics identifiers.

3.11. Certificate life-cycle

Information related to renewal, revocation, suspension, re-key or termination of certificates is detailed in "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN".

4. Identity Proofing Process

The identity proofing process implemented by Entaksi follows the structure and the normative requirements defined in clause 4.2 and clause 8 of ETSI TS 119 461 and consists of the following phases:

- Initiation
- Attribute and Evidence Collection
- Attribute and Evidence Validation
- Binding to Applicant
- Issuing of the Identity Proofing Result

Each phase contributes to ensuring the correctness, accuracy and uniqueness of the personal or organizational information that will later be included in qualified certificates, following the naming rules of IETF RFC 5280, ITU-T X.509, ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 412-1,2,3,5.

The process is adapted to each supported use case and to the identity proofing context declared by Entaksi, and is executed by a combination of Entaksi Registration Officers (RAOs) and the subcontracted identity proofing service provider Onfido, as applicable.

4.1. Initiation

The identity proofing process begins when the applicant subscribes to one of Entaksi's qualified trust services (qualified certificates for signatures or seals, or management of remote QSCDs).

During the initiation phase:

- the applicant is informed of the purpose of the identity proofing;
- the applicable terms and conditions, privacy notices, and contractual obligations are presented;
- the evidence required for identity proofing is communicated;
- the applicant explicitly accepts the terms and conditions of the service.

The initiation phase concludes once the applicant has provided consent and the identity proofing request has been formally submitted through one of the supported channels.

For more info about Entaksi services subscriptions please refer to "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN".

4.2. Attribute and Evidence Collection

Entaksi collects identity attributes and evidence in accordance with the selected identity proofing use case. Collection may be performed manually, automatically, or using a hybrid manual–automated approach, depending on the operational mode.

The purpose of this phase is to gather the identity attributes and associated evidence necessary to fulfil the Extended LoIP requirements and to populate the Subject field of the resulting qualified certificate.

All the processes fully comply with Extended LoIP requirements.

4.2.1. Physical applicant presence

When the applicant is physically present at an Entaksi Registration Office:

- attributes and evidence (identity document and personal data) are collected directly by an Entaksi RAO;
- only authoritative physical documents are accepted (e.g., passports, ID cards, residence permits);
- the RAO performs visual and technical checks on the identity document and collects the necessary attributes through secure enrolment systems;
- a live face verification is performed in person to bind the applicant to the identity attributes contained in the document.

The process is carried out as follows:

1. Requests the applicant to show a valid identification document, as stipulated in the service contract: National ID card and passport for Italian citizens, and passport for all other applicants.
2. Verifies the authenticity of the identification document or passport by inspecting security features, holograms, and other anti-counterfeiting measures.

3. Compares the photo on the identification document with the physical appearance of the applicant.
4. Verifies, through a cross-reference, the information provided in the request documents with the details on the identification document or passport.
5. Engages in a conversation with the applicant to assess their knowledge of the provided information and ensure they are the legitimate owner of the identity: confirming date and place of birth.
6. Records all observed details using the protocol provided by Entaksi.
7. If the verification is successful, proceed with the certificate issuance process.
8. In case of discrepancies or doubts, suspend the process and consult with the responsible individual at the Certification Authority of Entaksi.

4.2.2. Remote attended applicant presence

When the applicant is remotely identified in attended mode:

- the RAO conducts a live video call with the applicant via a secure virtual registration office;
- the applicant presents their identity document to the RAO;
- automated analysis tools are used for preliminary document validation (document authenticity, MRZ/OCR extraction, security feature verification);
- the RAO performs manual review of the document and conducts a live face verification during the video call;
- attributes are collected through a secure enrolment application, integrating both automated and manual checks.

The process is carried out as follows:

1. The applicant joins a scheduled video-identification session using a secure platform controlled by Entaksi.
2. The RAO requests the applicant to display a valid identification document (National ID card or passport for Italian citizens; passport for all other applicants), ensuring high-resolution visibility.
3. Automated tools process the identity document (OCR/MRZ extraction, format and security-feature checks).
4. The RAO inspects the document manually, reviewing the physical and digital features visible via camera to detect signs of tampering or forgery.
5. The RAO compares the portrait on the document with the applicant's live video image, assessing physical likeness and performing liveness testing (movement, gestures, verbal interaction).
6. The RAO cross-checks the data extracted by automated tools with the data contained in the service request documents.
7. The RAO engages with the applicant to confirm key identity details (e.g., date and place of birth) and evaluate consistency and legitimacy.
8. The RAO records all verification steps and observations using the protocol and audit logging tools provided by Entaksi.
9. If the verification is successful, the RAO approves the identity proofing result and proceeds with the certificate issuance process.
10. In case of inconsistencies, suspicion of fraud, or insufficient video quality, the RAO suspends the process and escalates the case to the responsible officer within the Certification Authority of Entaksi.

4.2.3. Remote unattended applicant presence

For unattended remote identity proofing:

- the applicant enrolls through an automated process managed by the subcontracted IPSP Onfido;
- automated steps include:
  - capture and verification of the identity document;
  - biometric face capture;
  - automated biometric comparison between document portrait and live capture;
  - extraction and normalization of identity attributes.
- after the automated process, an Entaksi RAO performs manual validation of:
- the identity document and extracted attributes;
- biometric matching results;
- evidence authenticity and consistency.

The process is carried out as follows:

1. The applicant accesses the unattended identity proofing workflow via a secure application integrated with Onfido services.

2. The automated system prompts the applicant to capture images of the identity document, ensuring inclusion of holograms, MRZ codes, and security features.
3. Onfido performs automated checks on the document.
4. The applicant performs a biometric face capture (selfie or video), following liveness instructions provided by the system.
5. Automated biometric matching is performed between the document portrait and the applicant's live capture.
6. Identity attributes (given name, surname, date and place of birth, nationality, document number, etc.) are extracted and normalized.
7. An Entaksi RAO receives the automated result and performs full manual validation.
8. The RAO documents all findings, completes the validation protocol, and determines whether the evidence meets the requirements for Extended LoIP.
9. If validation is successful, the identity proofing process continues toward certificate issuance; otherwise, the RAO suspends the procedure and requests additional evidence or initiates escalation to the Certification Authority.

4.3. Attribute and Evidence Validation

For each supported use case, Entaksi validates the following categories of attributes:

- **Core identity attributes**: name, family name, date of birth, place of birth, gender (if applicable), nationality.
- **Document attributes**: document type, issuing authority, issuance/expiry dates, unique document identifier.
- **Biometric attributes**: facial image collected during the session (manual or automated), used exclusively for binding.
- **Legal person attributes (where applicable)**: registered name, registration number, VAT/LEI (if available), registration authority, registered office.

Validation is performed by:

- manual review by trained RAOs;
- automated evidence verification systems;
- hybrid validation combining both approaches.

Validation steps include:

- authenticity and integrity checks on evidence;
- syntax and semantics checks of extracted attributes;
- consistency checks across evidence sources;
- verification of representation powers (for representatives of legal persons).

All validations meet the reliability requirements of Extended LoIP.

4.3.1. Naming and validation of certificate attributes

The identity attributes validated in this phase are described in Attributes to be collected.

The structure of the certificate fields, including applicable limitations, formatting rules, and semantics, is defined in the document "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN".

4.4. Bindiing to Applicant

Binding ensures that the person or legal person presenting the evidence is the subject to whom the identity attributes refer.

For natural persons, binding is based on:

- biometric face verification (manual, automated, or hybrid);
- comparison with the portrait in the identity document;
- cross-checking personal attributes with evidence.

For legal persons, binding includes:

- verification of the legal entity identity through trusted registers;
- ensuring consistency between evidence and authoritative registers.

For natural persons representing legal persons, binding includes:

- identity proofing of the natural person;
- identity proofing of the legal person;

- verification of the representative's authority and role.

4.5. Issuing of Identity Proofing Result

At the end of the identity proofing process Entaksi produces an identity proofing result containing:

- the validated attributes;
- the achieved Extended LoIP level;
- reference to the evidence used and validation outcomes;
- the final status of the identity proofing.

The result is used exclusively within Entaksi's qualified trust services.

For physical certificates, the private key and certificate are delivered on a physical cryptographic token shipped via priority mail.

For remote certificates, the certificate is issued within a certified remote qualified signature/seal creation device in accordance with eIDAS and ETSI TS 119 431-1.

All identity proofing records are retained in accordance with legal and contractual obligations.

5. Facility, management, and operational controls

For all matters relating to facility security controls, organizational and managerial controls, operational procedures, and the overall security framework adopted by Entaksi, reference shall be made to the document "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN".

That document describes, in full detail, the physical, procedural, administrative, and technical controls applied by Entaksi as a Qualified Trust Service Provider, including those indirectly supporting the Identity Proofing Service.

6. Technical security controls

For all technical security controls — including system security, cryptographic controls, trusted hardware requirements, network security, and protection of sensitive data — reference shall be made to "MAN eIDAS 20230426 Certificate Policy and Certification Practice Statement EN", which defines the complete set of technical and procedural measures adopted by Entaksi in accordance with ETSI EN 319 401 and other applicable standards.

6.1. Subcontracted Identity Proofing Service Provider

Entaksi adopts Onfido as a subcontracted Identity Proofing Service Provider (IPSP) for the execution of automated components of remote identity verification. Onfido operates exclusively within the scope defined by Entaksi and does not independently perform identity proofing, issue identity proofing results, or make determinations regarding eligibility for certificate issuance.

All activities executed by Onfido form part of the identity proofing workflow governed by this IPSPS and remain under the responsibility and oversight of Entaksi.

6.1.1. Scope of activities performed by Onfido

Onfido provides automated mechanisms supporting the following technical steps within the identity proofing process, applicable to remote unattended identity proofing use case:

- automated capture of identity documents using mobile or web interfaces;
- automated document verification;
- automated biometric checks;
- extraction and normalization of identity attributes for subsequent validation by Entaksi;
- secure transfer of evidence and verification data to Entaksi's systems.

Onfido provides automated tools for document capture, document authenticity analysis, biometric face capture, and automated biometric comparisons. These outputs constitute preliminary evidence, which is always subject to manual validation by an Entaksi Registration Authority Officer (RAO).
The RAO is ultimately responsible for confirming the accuracy, integrity, and suitability of all evidence produced by the automated system and for validating the final binding between the applicant and the identity attributes.

Onfido's operations are performed through secure APIs and controlled integrations, with all evidence collected and processed according to instructions defined contractually by Entaksi. The processing of identity data is carried out in accordance with GDPR requirements, under a data processing agreement that establishes Onfido as a Processor and Entaksi as the Data Controller for the personal data processed during the identity proofing activities.

6.1.2. Oversight, monitoring, and quality controls

Entaksi conducts periodic reviews of Onfido's performance to ensure that the automated systems operate within the expected levels of reliability and accuracy. Quality controls include verification of false acceptance/false rejection rates, document-type coverage, biometric performance metrics, and compliance with the regulatory framework.

Onfido is subject to contractual obligations requiring compliance with relevant trust service standards, security controls, and confidentiality provisions. All activities performed by Onfido must remain fully traceable and auditable, ensuring that Entaksi retains evidence.

7. Compliance audit and other assessments

The applicable legal system is declared in References.

The configuration of the Entaksi's Integrated Management System is regularly checked by the management to avoid any change which violate Entaksi's security policies.
The system is checked by at least yearly by an accredited certification body, recognized by Accredia, the Italian Accreditation Body.

Audit working papers and inspection documents are classified as confidential.

The conformity certificates and their updates are published in accordance with the assessment results on the Entaksi's website at the following link: https://www.entaksi.eu/en/certifications.html

7.1. Frequency or circumstances of assessment

Assessments are conducted yearly.

7.2. Identity/qualifications of assessor

The conformity checks (audits) on Entaksi are conducted by an assessment body accredited in accordance with Regulation (EC) no. 765/2008, through qualified and competent personnel on the subject of conformity assessments, according to the ETSI EN 319 403-1 standard, of Trust Service Providers and related trust services provided pursuant to the eIDAS Regulation.

7.3. Assessor's relationship to assessed entity

The assessment bodies that conduct audits on Entaksi have no relationship with Entaksi.

The internal auditor does not belong to the structure that deals with Entaksi activities.

7.4. Topics covered by assessment

Assessment activities cover all topics required under the eIDAS framework, including the correct operation of the identity proofing service. In particular, assessments verify:

- the correct identification and authentication of subjects requesting certificates;
- the appropriate management and retention of registration and identity-proofing documentation;
- the proper issuance of certificates in accordance with applicable procedures and requirements;
- the correct management of cryptographic keys;
- the proper handling of certificate revocation requests;
- the timely and accurate update of Certificate Revocation Lists (CRLs).

In addition, physical, technical and operational security measures are examined to ensure full compliance with this Identity Proofing Service Policy and Practice Statement, the applicable Certificate Policy and Certification Practice Statement, and all other relevant regulatory and standard requirements.

7.5. Actions taken as a result of deficiency

The actions resulting from any issue found during the audits, (e.g., failure to meet the requirements defined in the applicable regulations, standards, procedures) depend on the nature and severity of the issue.

Entaksi commits to produce a remediation plan to address deviations from relevant standards and regulations.

7.6. Communication of results

The assessment body report is communicated to the Entaksi Management.

8. Other business and legal matters

The Identity Proofing Service provided by Entaksi is not offered as an autonomous commercial service, but exclusively as a component of the qualified trust services delivered by the Trust Service Provider (TSP).
Accordingly, identity proofing activities performed by Entaksi are carried out solely for the purpose of enabling:

- **the issuance of qualified certificates for electronic signatures**;
- **the issuance of qualified certificates for electronic seals**;
- **the qualified service for the management of remote qualified electronic signature creation devices**;
- **the qualified service for the management of remote qualified electronic seal creation devices**.

For any business or legal matters relating to these qualified trust services, including contractual rights and obligations, subscribers shall refer to the applicable service-specific Terms and Conditions issued by the TSP.

Any aspects not expressly covered in this IPSPS shall be governed by the general Terms and Conditions of the qualified trust services (“Condizioni Generali del Servizio”), which define the guarantees, responsibilities, and liabilities of each party.

8.1. Confidentiality of business information

As stated in the terms and conditions and in the privacy policy, all the following information are considered confidential:

- personal data and information provided by applicants, subscribers, and subjects, excluding data required to appear in certificates or otherwise legally non-confidential;
- identity proofing requests and related communications received from applicants or subscribers;
- operational and technical communications exchanged among PKI / Trust Service participants;
- technical and operational information generated or managed by Entaksi (e.g., secure credentials, activation data for remote signature/seal devices, identity proofing materials);
- system logs and audit logs produced during identity proofing operations;
- contractual documentation and information exchanged with Registration Authorities or contractual partners involved in identity proofing activities.

8.1.1. Scope of confidential information

As data controller, Entaksi processes personal data in full compliance with General Data Protection Regulation (EU) 2016/679, using such data exclusively for:

- the execution of identity proofing activities,
- the fulfilment of legal and regulatory obligations related to qualified trust services,
- the fulfilment of contractual obligations toward the TSP and subscribers.

8.1.2. Information not within the scope of confidential information

Information not deemed confidential includes:

- certificates and the identity information contained therein;
- certificate status information made available through CRLs or OCSP;
- any information that must be published by law or by applicable certification and trust service standards (e.g., RFC 5280);
- information explicitly requested by the certificate holder or subscriber to be public.

8.1.3. Responsibility to protect confidential information

Entaksi processes all confidential information in compliance with applicable data protection and privacy laws, ensuring it is physically and/or logically protected from unauthorized access (even if read-only) and the risk of loss due to disasters.

8.2. Privacy of personal information

Any personal information relating to applicants, subscribers or subjects, obtained during identity proofing operations, is processed as confidential and non-public.
This includes all personal data collected, validated or produced during the identity proofing lifecycle.

Information specifically intended for public use, such as the public key, information contained in the certificate (if requested by the Subject), in the certificate revocation, and suspension dates, may be exceptions to this confidentiality rule.

As part of the processing of personal data related to the performance of the activities provided for qualified trust services, Entaksi acts as a Processor, by virtue of by specific legal delegation conferred by the Customer.

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

The complete set of provisions relating to the processing of personal data performed by Entaksi is reported at the following link: https://www.entaksi.eu/en/privacy.html.

8.3. Intellectual property rights

Entaksi retains ownership of all intellectual and industrial property rights, along with any other rights associated with its Trust Services (including trademarks, patents, designs, know-how, etc.), unless expressly indicated otherwise by third-party ownership. Utilization rights for the Services and their related technological solutions are exclusively reserved for Entaksi.

The subscriber is granted permission to use the service(s) within the specified limits and conditions outlined in this document.

8.4. Compliance with applicable law

The main applicable framework is:

EU Regulation No. 910/2014 of the European Parliament and of the Council - eIDAS

EU Regulation 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

EU Regulation No. 1183/2024 – eIDAS 2

Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

General Data Protection Regulation (EU) 2016/679

Regulation (EU) 2016/679 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, and repealing Directive 95/46/EC (General Data Protection Regulation)

Decreto Legislativo 10 agosto 2018, n. 101

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

8.5. Accessibility

Entaksi provides its documentation, contract forms, and web-based interfaces for Trust Services management through channels designed to be accessible to persons with disabilities and users with accessibility needs, in accordance with the requirements of ETSI EN 301 549 and applicable national legislation.

Where a subscriber or relying party cannot reasonably use the standard online channels due to an accessibility need or disability, Entaksi will provide alternative accessible means (like assisted support via email or telephone) to guarantee access to identical information and services without discrimination.

Entaksi takes into account feedbacks that involve accessibility issues from users and is committed to continually improving the accessibility of its services.

8.5.1. User interface accessibility

Entaksi delivers its Qualified Trust Services through a web-based interface (Entaksi's Console).
Entaksi develops the user interface using Angular, an open-source, TypeScript-based framework and platform developed by Google. While accessibility is not automatic, Angular provides a structured, component-based architecture that supports the correct implementation of accessibility features; in particular, it facilitates the use of semantic HTML, consistent form-handling

patterns, keyboard event management, and reusable interface components, providing a stable technical basis for meeting the ETSI EN 301 549 clause 9 (*WCAG 2.1 Level AA*) requirements.
The user interface currently supports:

- text alternatives for non-text elements;
- structured and semantic HTML with programmatic headings and landmarks;
- keyboard operability for core functions;
- programmatically associated labels for buttons and input fields;
- compatibility with assistive technologies such as screen readers;
- responsive layouts supporting zoom, viewport resizing, and text scaling.

Periodic accessibility reviews are carried out as part of Entaksi's quality and maintenance processes. These reviews include both automated evaluations—using recognized accessibility testing tools—and manual checks such as keyboard navigation testing, screen-reader verification, and visual inspection of contrast and layout behaviour. The objective of these activities is to identify potential accessibility barriers and ensure continuing alignment with the requirements of ETSI EN 301 549.

Entaksi monitors and evaluates all accessibility-related requests, feedback, and defect reports received from users, customers, or internal teams. Once the issue has been verified, it is addressed in the maintenance improvement cycle to further enhance the accessibility features.

8.5.2. Documentation accessibility

All service documentation is provided in accessible electronic PDF format. These PDFs are produced with accessibility considerations in accordance with the requirements of ETSI EN 301 549 clause 10 for non-web documents. In particular, documentation includes:

- alternative text for images and non-text elements;
- a tagged and logical reading order;
- semantic and properly structured headings and lists;
- accessible tables with correctly defined headers;
- visual elements with adequate colour contrast.

All these measures support the readability and usability of the documentation for persons with disabilities and users with accessibility needs.

Upon request documentation can be provided in the HTML alternative accessible format, where reasonably practicable.

8.5.3. Support for accessibility

Entaksi's Help Desk, accessible at helpdesk@entaksi.eu, provides information on the accessibility and compatibility features of the service portal and its documentation, and ensures effective communication with persons with disabilities and users with accessibility needs.

Support services can be accessed through the channels described in the service's Terms and Conditions, including:

- accessible email communication channels;
- telephone support;
- alternative communication methods upon request.

Any documentation or information supplied through the support service is provided in accessible formats consistent with Entaksi's documentation accessibility practices.

8.6. Other provisions

Please refer to the general terms and conditions of the qualified CA service ("Condizioni Generali del Servizio") for any other detail about the guarantees and responsibilities incumbent on each party.