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 20230426 PKI Disclosure Statement EN

Entaksi Solutions SpA

Table of contents

Document information

Project	Integrated Management System
Type	Manual
Document ID	MAN eIDAS 20230426 PKI Disclosure Statement EN
Version	1.1.0
Creation Date	26/04/2023
Last Revision	06/12/2023
Author	Alessia Soccio
Status	Released
Classification	Public

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

Revisions and releases

Date	Version	Name	Mansion	Action	Release
26/04/2023	0.0.1	Alessia Soccio	IMSM	Draft creation.	Internal
10/05/2023	1.0.0	Alessia Soccio	IMSM	Review and release.	Public
06/12/2023	1.1.0	Alessia Soccio	IMSM	Usage extention to qualified certificates for electronic signatures and seals.	Public

Document approval

Date	Employee	Role	Signature
06/12/2023	Alessandro Geri	SM	*Digitally signed*

1. Introduction

This is the **PKI Disclosure Statement of the Trust Service Provider (TSP) 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.

This document complies with the requirements of the European standard ETSI EN 319 411-1, and in particular is drawn up following the structure defined in Annex A of the aforementioned standard.

The Certification Authority (CA) run by Entaksi as a TSP follows the 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 (hereinafter "eIDAS Regulation").

This document does not substitute or replace the Terms and Conditions of the CA services, of which is an attachment, nor the Certificate Policy and Certification Practice Statement, which are published on Entaksi's website (see CPS, CP).

1.1. 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.

1.2. 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.

2. TSP contact info

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), Italia

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

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/

2.1. Revocation or suspension request

The revocation or the suspension of a certificate can be requested by sending a specific form at ca@entaksi.eu.
The form is available on Entaksi's website at the following link: https://www.entaksi.eu/en/documentation.html.

3. Certificate types, validation procedures and usage

Entaksi issues qualified certificates for the following usages:

- **Qualified certificates for electronic signatures**;
- **Qualified certificates for electronic seals**;
- **Qualified certificates for Time-stamping Units issuing qualified Time-stamps**.

The certificates respond to the following European standards:

- **ETSI EN 319 401 V2.3.1 (2021-05)**;
- **ETSI EN 319 411-1 V1.4.1 (2023-10)**;
- **ETSI EN 319 411-2 V2.5.1 (2023-10)**;
- **ETSI EN 319 412-1 V1.5.1 (2023-09)**;
- **ETSI EN 319 412-2 V2.3.1 (2023-09)**;
- **ETSI EN 319 412-3 V1.3.1 (2023-09)**;
- **ETSI EN 319 412-5 V2.4.1 (2023-09)**;
- **ETSI EN 319 421 V1.2.1 (2023-05)**
- *ETSI EN 319 422 V1.1.1 (2016-03).

The algorithm used for signing certificates can be one of the following:

- `sha256WithRSAEncryption` (OID 1.2.840.113549.1.1.11);
- `sha384WithRSAEncryption` (OID 1.2.840.113549.1.1.12);
- `sha512WithRSAEncryption` (OID 1.2.840.113549.1.1.13);
- `ecdsa-with-SHA256` (OID 1.2.840.10045.4.3.2);
- `ecdsa-with-SHA384` (OID 1.2.840.10045.4.3.3);
- `ecdsa-with-SHA512` (OID 1.2.840.10045.4.3.4);

Entaksi implements the following certificate policies.

Table 1. Certificate policies

Policy	OID	Description
`QCP-n-qscd`	`0.4.0.194112.1.2`	Certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD
`QCP-l-qscd`	`0.4.0.194112.1.3`	Certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD

The Entaksi CA also issues certificates for the Entaksi TSA Time-stamping Unit (TSU). Certificate type issued by the CA for the TSU contains the QcStatements field (OID 1.3.6.1.5.5.7.1.3) specifying `esi4-qtstStatement-1` as defined in clause 9.1 of ETSI EN 319 422.

4. Reliance limits

Entaksi does not set reliance limits for certificates issued by the Certification Authority, however reliance limits may be set by applicable law in the EU country where the service is used or by customer agreement.

5. Obligations of subscribers

Key pair shall be used in accordance with the limitation notified to the subscriber.
Unauthorized use of the private key is prohibited.

Use of the private key for cryptographic functions shall occur within the secure cryptographic device.

The subscriber is responsible for:

- providing the TSP accurate and complete information during the registration;
- using the key pair only in accordance with any limitations notified in the Certificate Policy and Certification Practice Statement;
- preventing any unauthorized use of the private key;
- maintaining the sole control of the private key;
- not attempting to use private key for cryptographic functions outside the secure cryptographic device;
- performing subject's keys generation within the secure cryptographic device in every procedure where the key generation is under control of the subscriber (for instance during certificate renewal);
- notifying Entaksi without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
  - private key has been lost, stolen, potentially compromised;
  - control over the private key has been lost due to compromise of activation data or other reasons;
  - inaccuracy or changes to the certificate content;
- immediately and permanently discontinuing the use of a compromised key, except for key decipherment;
- in the case of being informed that the certificate has been revoked by Entaksi, or that the issuing CA has been compromised, ensuring that the private key is no longer used.

6. Certificate status checking obligations of relying parties

Before placing any reliance on a digital signature that uses a certificate issued by the Certification Authority, including Time-stamps, relying parties must verify that the signature is correct and that the private key used to sign the document has not been revoked verifying the status of the public key certificate.

The relying party should take into account any limitation on usage indicated in the Certificate Practice Statement and any other reasonable precautions.

The public key certificate status can be verified using the Certificate Revocation List (CRL) reported in the TSU certificate `CRLDistributionPoints` extension (OID 2.5.29.31) or querying the Online Certificate Status Protocol responder reported in the `AuthorityInformationAccess` (OID 1.3.6.1.5.5.7.1.1) of the same certificate.

Revocation status of the certificate can be verified after the expiration of the certificate according to the `QcRetentionPeriod` statement (OID 0.4.0.1862.1.3) specified in the `QcStatements` field of the certificate (OID 1.3.6.1.5.5.7.1.3).

7. Limited warranty and disclaimer/Limitation of liability

Warranty and liability limitations are specified in the Terms and Conditions of the Qualified Certification Authority service.

The Certification Authority service Terms and Conditions are available in the Entaksi web site at the following link: https://www.entaksi.eu/en/documentation.html.

8. Applicable agreements, CPS, CP

Applicable agreements are composed by the following documents:

- General Terms and Conditions;
- This PKI Disclosure Statement;
- The PKI Certificate Policy and Certification Practice Statement (CPS);
- Any additional document within the aforementioned.

All the TSP documents are available at the following link: https://www.entaksi.eu/en/documentation.html.

9. Privacy policy

Entaksi PKI complies with applicable regulation and legal requirements (including GDPR and eIDAS Regulation) as well as the requirements of the Entaksi Privacy Policy (see https://www.entaksi.eu/en/privacy.html).

The complete set of provisions relating to the processing of personal data and information security is reported on the Entaksi website (see https://www.entaksi.eu/en/ispd.html).

Entaksi Management operates to guarantee that appropriate technical and organizational measures will be constantly taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

10. Refund policy

The primary reference for Entaksi refund policy is the general Terms and Condition of the Qualified CA service. This document form is publicly available on Entaksi's website at the following link: https://www.entaksi.eu/en/documentation.html.

Entaksi does not refund fees for Certification Authority services that have already been paid.

11. Applicable law, complaints and dispute resolution

Certificates issued to clients located in Ireland are provided in accordance with Irish laws. Certificate issued outside Ireland are provided in accordance with Italian laws.

Entaksi looks for a peaceful and negotiated settlement of any disputes that may arise from its operation of the Certification Authority.

For any controversy the exclusive competent court will be Pistoia (Italy), except for subscribers located in Ireland that can submit the controversy to the competent court of Ireland.

12. TSP and repository licenses, trust marks, and audit

Entaksi has several certifications, whose full and updated list of is available at https://www.entaksi.eu/en/certifications.html.

Entaksi is a **Trust Service Provider** for

- **Issuing of qualified certificates for electronic signatures and seals,**
- **Creation of electronic time stamps,**
- **Long-term preservation of electronic signatures and seals,**

according to EU Regulation no. 910/2014 - eIDAS.

Entaksi TSP is enlisted in the Irish List of Trust Service Providers published by Department of the Environment, Climate and Communications of the Government of Ireland.

Entaksi TSP services are subject to conformity assessment every year by an accredited certification body, according to ETSI Standards as required by the eIDAS Regulation.

Audit working papers and inspection documents are classified as confidential, but the conformity certificates and their updates are published on the previously mentioned website page.

The trusted list of TSP can be checked at the following link: https://eidas.ec.europa.eu/efda/tl-browser/.