TECHNICAL ANNEX
Time Stamp

Contents

***

1. External references

Documentation	Detailed links
Practice Statement	https://qtsp.infocert.it/pdf/ICERT_INDI_TSA_ENG.pdf https://qtsp.infocert.it/pdf/ICERT_INDI_TDS-ENG.pdf
User Manual	N/A
Web Attachment	https://developers.infocert.digital/timestamps/
Support links (FAQs, videos, guides)	https://knowledgecenter.infocert.digital/

2. Service description – Introduction

Tinexta Infocert S.p.A. (hereinafter "Infocert"), for the purposes of this document, acts as a qualified trust service provider (hereinafter "QTSP") and, in particular, as a provider of qualified and non-qualified electronic time-stamping services (hereinafter also "TSA" – Time Stamping Authority), for the provision of the time-stamping service (hereinafter the "Service"), in accordance with the provisions of the ICERT-INDI-TSA Operational Manual (hereinafter also "Operational Manual").
For this Service, Infocert has obtained a conformity assessment carried out by the Conformity Assessment Body CSQA Certificazioni S.r.l., in accordance with Regulation (EU) No 910/2014, as amended and supplemented (hereinafter the "eIDAS Regulation"), as well as the applicable implementing regulations and ETSI standards, including ETSI EN 319 401, ETSI EN 319 421 and ETSI EN 319 422, in accordance with the eIDAS assessment scheme defined by ACCREDIA pursuant to the standards ETSI EN 319 403 and UNI CEI ISO/IEC 17065:2012.
The Service involves the issuance of qualified electronic time stamps, consisting of the association of a certain date and time with electronic data, in order to certify that such data existed at a specific point in time and have not been subsequently altered without such alteration being detectable.
Qualified electronic time stamping is presumed to be accurate in terms of the date and time it indicates and the integrity of the data to which this information is linked, in accordance with the eIDAS Regulation.

The Service is provided in compliance with the eIDAS Regulation, the applicable ETSI standards and the policies and practices set out in the Operating Manual, and is delivered in accordance with a specific time-stamping policy identified by an Object Identifier (OID), as described in the Operating Manual.
The Service may be purchased by the Customer in the form of predefined packages or quantities of Time Stamps, which are subsequently requested and used in accordance with the procedures set out in this document.
This Technical Annex forms an integral and essential part of the service purchase agreement (hereinafter the "Agreement") entered into with the Customer.
The General Terms and Conditions of Activation (hereinafter the "GTC"), of which this Technical Annex forms an integral part, apply to any party that activates, uses or relies on the Service; it being understood that, in dealings with the Customer, the provisions of the Agreement also apply.

2.1 Definition of the Parties

Customer
A natural or legal person, body or organisation with whom the contract for the provision of the Service (Agreement) has been formalised. The Customer may be the same as the Applicant.

Applicant
A natural or legal person, body or organisation that requests the issuance of Time Stamps and uses the Service, even if they are not the same as the Customer.

User
A party that verifies a Time Stamp in order to ascertain the validity of the date and time associated with it and the integrity of the data to which the Time Stamp relates.

3. Technical and Regulatory Specifications

3.1 Description and operation of the Service

3.1.1 Time Stamp and Time Stamping Certificate

A time stamp is an electronic record that certifies the link between a set of data and a specific point in time, in order to demonstrate that such data existed at a specific moment and that any subsequent changes can be detected.
The Time Stamp is electronically signed by Infocert, in its capacity as a Time Stamping Authority (TSA), using a private key associated with a time-stamping certificate, which allows its origin and integrity to be verified.

3.1.2 Issuance of the Time Stamp

The Time Stamp is generated following a request from the Applicant, who transmits to the Service the hash of the data to be time-stamped, obtained using a cryptographic hash function.
Upon receiving the request, the TSA system automatically:

- associate a time reference with the hash, based on a source synchronised with Coordinated Universal Time (UTC);
- generate the Time Stamp;
- apply the TSA's electronic signature;
- return the Time Stamp to the Applicant.

The issuance process is carried out automatically within secure infrastructures managed by Infocert.

3.1.3 Use and verification of the Time Stamp

The Time Stamp is used to certify the existence of electronic data or documents at a specific point in time and is employed in IT processes that require proof of the data's temporal precedence and integrity.
In particular, the Time Stamp may be used:

- in conjunction with electronic documents, to certify their existence at a specific date and time;
- in combination with electronic signatures, to support the verification of the validity of signatures over time, even after the expiry of certificates;
- as part of digital preservation processes, to certify the date of creation or processing of documents;
- within applications or information systems that require a time stamp for operations or transactions.

The Time Stamp is used by linking it to the original data to which it refers, ensuring that the fingerprint contained in the Time Stamp corresponds to the data being stamped.
Verification of the Time Stamp consists of the following checks:

- verification of the electronic signature affixed by the TSA;
- verification of the validity of the time-stamping certificate and the associated certificate chain;
- verification of the certificate's status using the available validation services;
- recalculation of the data's digital fingerprint and comparison with that contained in the Time Stamp;
- verification of the consistency of the time reference.

These verifications may be carried out by the Applicant or by a User (relying party) and enable the authenticity of the Time Stamp, the integrity of the data and the correct association between the data and the time reference to be ascertained.

3.1.4 Validity and effectiveness over time

The time reference associated with the Time Stamp is generated on the basis of a source synchronised with Coordinated Universal Time (UTC), in accordance with mechanisms that guarantee its accuracy.
The Time Stamp takes effect with reference to the moment of its issuance and serves to certify the existence of the data at that moment.
The validity over time of the Time Stamp is contingent upon the ability to verify its constituent elements, including the TSA's signature, the time-stamping certificate, the relevant certificate chain and information on the status of the certificates used.

3.1.5 Revocation or suspension of the TSA's certificate

Time Stamps are signed by Infocert in its capacity as the Time Stamping Authority (TSA) using a certificate employed for the provision of the Service. This certificate is managed by Infocert throughout its lifecycle and may be suspended or revoked in the circumstances set out in the Operating Manual.
The suspension or revocation of the certificate results in the immediate cessation of its use for the issuance of new Time Stamps and its replacement within the Service with a valid certificate.
Following revocation or suspension, the status of the certificate is made available via Certificate Revocation Lists (CRLs) and other verification services provided, in order to enable the event to be detected as part of verification activities.
Time Stamps already issued remain verifiable on the basis of the elements they contain and the information available at the time of verification. Any Time Stamps generated after the revocation or suspension event are to be considered invalid.

.

3.1.6 Traceability and retention of Service data

Infocert records and retains information relating to the provision of the Service for twenty years, including operation logs and events relevant to the security, traceability and management of the Service.

The Service is designed to process exclusively the hash of the data transmitted by the Applicant for the purpose of generating the Time Stamp. Infocert neither acquires nor retains the original data to which the hash refers, nor the content of any associated documents.
The information processed and retained is limited to that necessary for the generation of Time Stamps and the operational management of the Service, in accordance with the Operating Manual and applicable legislation.

3.2 Products and Services

3.2.1 Qualified Time-Stamping Service

The qualified time-stamping service is provided by Infocert in its capacity as a QTSP in accordance with the policies identified by OIDs as described in the Operating Manual, and is presumed to be accurate in terms of the date and time it indicates and the integrity of the data to which such information is associated. Qualified time stamps certify the association between electronic data and a qualified time reference.

3.2.2 Non-qualified time-stamping service

Infocert may also provide non-qualified time-stamping services, based on technical mechanisms similar to those of the qualified service.
These services do not fall within the scope of qualified trust services under the eIDAS Regulation and do not benefit from the relevant legal presumptions.

3.2.3 Technical characteristics of the Service

The Service is based on the Time-Stamp Protocol (TSP), which complies with the IETF specifications RFC 3161 and RFC 5816.
Time-stamping requests consist of the data fingerprint and are processed by the TSA system, which returns a response containing the time stamp.
The Service is compatible with the main electronic signature formats that require the use or inclusion of time stamps, including XAdES, CAdES, PAdES, JAdES and ASiC, as well as with the relevant baseline levels, where supported.
For up-to-date details of the supported formats, integration methods, APIs, cryptographic capabilities and further technical specifications of the Service, please refer to the Operating Manual and/or the Web Annex.

3.2.4 Methods of provision and use of the Service

The Service is made available via application interfaces that enable authorised parties to submit time-stamping requests and receive the corresponding Time Stamps.
Access to the Service is granted via application credentials issued by Infocert to the Customer and/or to parties authorised by the Customer.
The Service may be used:

- by using applications made available by Infocert;
- by integrating the application into the Customer's systems.

In the case of integration, the Customer uses the credentials issued to access the Service and to submit requests within their own systems and processes, as specified in the Web Annex.
Where applicable, a test environment may be made available for verifying integrations prior to live use.
The Customer may make the Service available to third parties within the scope of its own applications or services; when making time-stamping requests, such third parties act as Requesters within the meaning of this Technical Annex.

3.3 Obligations and Responsibilities

3.3.1 Obligations and Responsibilities of the Requester

The Requester is required to use the Service in accordance with the General Terms and Conditions of Activation (GTC), this Technical Annex, the Operating Manual and applicable legislation.
The Applicant is responsible for the accuracy, completeness and lawfulness of the information provided in connection with the activation and use of the Service, as well as for the accuracy of the hash transmitted for the purpose of generating the Time Stamp and its correspondence with the original data.
The Applicant is also required to:

- to verify the validity of the Time Stamps received;
- to retain the Time Stamps together with the data to which they refer in a manner suitable for verifying them over time and ensuring their integrity;
- to adopt appropriate technical and organisational measures to ensure the security of their systems and the credentials used to access the Service;
- to safeguard the confidentiality of the credentials used to request Time Stamps, preventing their communication or disclosure to unauthorised parties;
- to bring its hardware and software systems into line with the security measures required by the applicable legislation.

The Applicant is also required to make the General Terms and Conditions (GTC), this Technical Annex and any further relevant information relating to the Service available to those who use or verify the Time Stamps.
The provision and use of the internet connection, as well as the hardware and software required to access and use the Service, remain the responsibility of the Applicant.
Use of the Service via the credentials issued is attributed to the Applicant, who remains liable even in cases where the Service is used by third parties operating via the Applicant's systems or credentials.
The Applicant is obliged to indemnify Infocert against any liability arising from use of the Service that does not comply with applicable legislation or the contractual terms and conditions.

3.3.2 User Obligations and Responsibilities

Any User who uses or relies on a Time Stamp is required to verify its validity in accordance with the procedures set out in this Technical Annex and the Operating Manual.
The User is responsible for the checks carried out and for any assessments or decisions made on the basis of the Time Stamps used.

3.3.3 Obligations and Responsibilities of Infocert

Infocert guarantees that the Service is provided in accordance with the requirements for security, reliability and continuity as set out in the eIDAS Regulation, the Implementing Regulations and the applicable ETSI standards, the Operational Manual and the contractual terms and conditions.
As part of the Service, Infocert is responsible for the correct generation of Time Stamps, ensuring the association between the received data fingerprint and a reliable time reference, as well as for the management of the certificate used to issue the Service and the availability of the information necessary for verification.
The Service is designed in such a way that Infocert does not have access to the original data to which the Time Stamp refers, but only to the relevant digital fingerprint; consequently, Infocert does not verify the content, accuracy or lawfulness of the data being time-stamped.
Infocert therefore accepts no liability for activities relating to the generation of the digital fingerprint, the association of the Time Stamp with the data, or the storage and use of Time Stamps by the Applicant or third parties.
Except in cases of wilful misconduct or negligence, Infocert shall not be liable for any malfunctions or unavailability attributable to systems or infrastructure beyond its control, nor for any use of the Service that does not comply with the contractual terms or applicable legislation.

4. SLA and KPIs

In terms of service delivery, the monthly service availability figures are set out in detail in the relevant Operations Manual.