



TECHNICAL ANNEX QSVS Signature and Seal Validation Service

1. EXTERNAL REFERENCES	1
2. Service Description	1
3. Technical and Regulatory Specifications.....	2
4. SLA and KPIs.....	7

1. EXTERNAL REFERENCES

Documentation	Detailed links
Practice Statement	https://qtsp.infocert.it/pdf/ICERT_INDI_QSVS-ENG.pdf
User Manual	N/A
Web attachment	https://developers.infocert.digital/signature-validation/
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 services (hereinafter also “QSVSP” or “SVSP”) for the verification and validation of electronic signatures, electronic seals, time stamps and signature certificates, marking certificates and certificates issued by the Certification Authority (the “Service”), in accordance with the provisions of the ICERT-INDI-QSVS Operational Manual (hereinafter also referred to as the “Operational Manual”) and the “Signature Validation” Web Annex referred to in Article 1.

For this Service, Tinexta Infocert S.p.A. 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 and subsequent amendments and additions (hereinafter the “eIDAS Regulation”), as well as Implementing Decision (EU) 2015/1506 and the applicable ETSI standards, including ETSI EN 319 401, ETSI TS 119 441, ETSI EN 319 102-1, ETSI TS 119 102-2 and ETSI TS 119 172-4, 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.

This Technical Annex forms an integral and essential part of the service purchase contract (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.

Tinexta Infocert S.p.A.

Piazzale Flaminio 1/B, 00196 – Rome (RM), Italy A company subject to the management and coordination of Tinexta S.p.A.

T +39 06 836691 F +39 06 833669634, VAT No. 07945211006 REA No. 1064345

info@infocert.it Subscribed and paid-up share capital €21,099,232.00

infocert.it infocert.digital



2.1 Definition of the Parties

Customer

A natural or legal person, body or organisation that purchases the Service and with whom the Agreement is formalised. The Customer may be the same as the Applicant.

Applicant

A natural person or legal person, body or organisation responsible for implementing the Service within the context of the application systems used.

The General Terms and Conditions of Activation (GTC), this Technical Annex and the applicable provisions of the Agreement as communicated by the Customer apply to the Applicant.

User

A person or application component that uses the Service, either directly or via the Applicant's systems, for the purpose of verifying and validating electronic signatures, electronic seals, certificates or related records.

Verifier / Relying Party

A party that uses the results, reports or evidence generated by the Service as part of its own verification, assessment or decision-making processes

3. TECHNICAL AND REGULATORY SPECIFICATIONS

3.1 Characteristics of the Signature Validation Service

3.1.1 Purpose and nature of the Service

The Signature Validation Service (SVS) and the Qualified Signature Validation Service (QSVS) are trust services designed to verify and validate electronic signatures, electronic seals, time stamps and digital certificates.

The Service enables the technical, cryptographic and regulatory validity of the elements submitted for validation to be verified in accordance with the applicable ETSI standards.

The Service is provided:

- in non-qualified mode (SVS), in accordance with the requirements set out in ETSI TS 119 441;
- in a qualified mode (QSVS), in accordance with the requirements of ETSI TS 119 441, with specific reference to the requirements set out in Annex B 'Qualified Validation Service for QES as defined by Article 33 of Regulation (EU) No 910/2014';

The qualified service (QSVS) and the non-qualified service (SVS) are identified by specific Object Identifiers (OIDs), as described in the Operating Manual.

Validation operations are carried out exclusively in accordance with a specific signature validation policy, identified by an OID and described in the Operating Manual. This signature validation policy is used for the validation of electronic signatures, electronic seals, time stamps and digital certificates in accordance with

Tinexta Infocert S.p.A.

Piazzale Flaminio 1/B, 00196 – Rome (RM), Italy A company subject to the management and coordination of Tinexta S.p.A.

T +39 06 836691 F +39 06 833669634, VAT No. 07945211006 REA No. 1064345

info@infocert.it Subscribed and paid-up share capital €21,099,232.00

infocert.it infocert.digital



the applicable ETSI standards. The Applicant is not permitted to define or modify the signature validation policy applied by the Service.

The Service does not modify the documents or items submitted for validation, but returns only the results and evidence of the validation process.

The data and documents transmitted to the Service are processed solely for the time necessary to process requests and generate the relevant responses, except as provided for technical service logs and any applicable regulatory obligations. The evidence is returned by the Service in real time. The Service does not retain the evidence and, therefore, it cannot be retrieved at a later date via the Service itself.

Tinexta Infocert maintains technical logs of operations carried out for the purposes of security, traceability, verification and auditing. These logs are retained for a period of 7 (seven) years, in accordance with applicable legislation.

The Service is deemed to be activated following the Applicant's acceptance of the General Terms and Conditions and this Technical Annex, upon provision of the means of access to the Service.

The duration and conditions of use of the Service are governed by the Customer Agreement.

3.1.2 Validation Process

The validation process is carried out by the Service in accordance with the algorithm defined by the ETSI EN 319 102-1 standard and on the basis of the applicable signature validation policy, as described in the Operating Manual.

As part of the validation process, the Service carries out the necessary checks on the elements under review, including, where applicable:

- the format of the signature or seal;
- cryptographic validity;
- the identification of the certificates used;
- the validity and status of the certificates;
- the certificate chain;
- the validity of any time stamps.

In order to carry out these checks, the Service may obtain information from external sources, including Certification Authorities, OCSP/CRL services and applicable Trusted Lists.

The Applicant may not define or modify the validation policy applied by the Service, but may specify, where applicable, the required validation level from amongst those supported by the Service.

The validation results are returned in accordance with the classifications set out in the applicable ETSI standards: TOTAL-PASSED, TOTAL-FAILED and INDETERMINATE.

If it is not possible to obtain or verify all the information necessary to complete the validation process, the Service returns a result consistent with the information available at the time of processing.

Tinexta Infocert S.p.A.

Piazzale Flaminio 1/B, 00196 – Rome (RM), Italy A company subject to the management and coordination of Tinexta S.p.A.

T +39 06 836691 F +39 06 833669634, VAT No. 07945211006 REA No. 1064345

info@infocert.it Subscribed and paid-up share capital €21,099,232.00

infocert.it infocert.digital



3.1.3 Validation report and validation evidence

The Service returns the validation results via a validation report containing the key evidence of the validation process carried out.

The validation report includes, where applicable:

- the identification of the validation policy used;
- the results of the checks carried out;
- information relating to certificates and any verified time stamps;
- the overall outcome of the validation.

For the purposes of time-stamping the signature and determining the corresponding Proof of Existence (PoE), the Service primarily uses the time stamps associated with the signature or the document. In the absence of time stamps, the PoE is identified in accordance with the Service's policy.

In the case of the QSVS qualified service, the validation report is sealed using a qualified electronic seal from Tinexta Infocert and accompanied by a time stamp, in order to guarantee its origin and integrity.

3.1.4 Supported formats

The Service supports the validation of electronic signatures, electronic seals, time stamps and digital certificates in the main formats specified by the applicable ETSI standards.

In particular, the Service supports the CAdES, XAdES, PAdES and JAdES formats, including the relevant signature structures (enveloped, enveloping and detached) and the baseline levels set out in the relevant ETSI standards.

The Applicant may specify, within the scope of the methods supported by the Service and described in the 'Signature Validation' Web Annex, the level or type of validation required.

The available validation methods, supported levels, accepted formats, applicable technical constraints and the relevant API invocation specifications are described in the Operating Manual and in the 'Signature Validation' Web Annex.

3.2 How to use the Service

The Service is made available via APIs exposed by Tinexta Infocert in accordance with the procedures described in the Operating Manual and in the 'Signature Validation' Web Annex.

Access to the Service's APIs is via the TLS protocol with OAuth2 authentication of the caller.

The Service exposes the following APIs:

- QSVS API for the qualified validation of signed or time-stamped documents, returning a validation report sealed with a qualified electronic seal from Tinexta Infocert;
- SVS API for the non-qualified validation of signed or time-stamped documents;

Tinexta Infocert S.p.A.

Piazzale Flaminio 1/B, 00196 – Rome (RM), Italy A company subject to the management and coordination of Tinexta S.p.A.

T +39 06 836691 F +39 06 833669634, VAT No. 07945211006 REA No. 1064345

info@infocert.it Subscribed and paid-up share capital €21,099,232.00

infocert.it infocert.digital



- SVS API for the validation of X.509 digital certificates.

For specific methods of using the non-qualified Service, Tinexta Infocert may also make a web interface available for the direct use of the validation functions.

When submitting requests for the validation of signed or time-stamped documents, the Applicant must provide:

- the signed or time-stamped document, or the detached signatures supported by the Service;
- the level or type of validation requested from among those supported by the Service;
- any additional technical parameters required by the applicable APIs.

In the context of requests for the validation of digital certificates, the Applicant must submit the X.509 certificate to be validated in accordance with the formats supported by the Service.

Requests are processed in accordance with the signature validation policy applied by the Service and described in the Operating Manual.

The Service's APIs operate in synchronous mode.

The procedures for invoking the APIs, the structure of requests and responses, and the relevant technical specifications are described in the Operating Manual and in the Web Annex 'Signature Validation'.

3.3 Obligations and responsibilities

3.3.1 Obligations and responsibilities of the Applicant

The Applicant is required to use the Service in accordance with the GTC, this Technical Annex, the "Signature Validation" Web Annex, applicable legislation and the provisions of the Agreement that are applicable and communicated by the Client.

The Applicant is responsible for integrating the Service into its own application systems and is responsible for the correct configuration of the APIs, the management of credentials and authentication mechanisms, as well as the methods by which Users operating via its systems access and use the Service.

The Applicant is also responsible for the accuracy, integrity, completeness and lawfulness of the data, documents, signatures, certificates and other elements submitted for validation via the Service.

The validation results and validation reports returned by the Service must be used taking into account the information and evidence contained therein, the validation policy applied and the inherent limitations of the validation process.

In the case of the QSVS qualified service, the Applicant is required to verify the qualified electronic seal on the validation report in order to verify its origin and integrity.

The Applicant undertakes to use the Service exclusively for the purposes and in the manner set out in the applicable technical documentation and not to use the Service:

- for unlawful purposes or in breach of applicable legislation;
- in a manner that does not comply with the Service's technical specifications;

Tinexta Infocert S.p.A.

Piazzale Flaminio 1/B, 00196 – Rome (RM), Italy A company subject to the management and coordination of Tinexta S.p.A.

T +39 06 836691 F +39 06 833669634, VAT No. 07945211006 REA No. 1064345

info@infocert.it Subscribed and paid-up share capital €21,099,232.00

infocert.it infocert.digital



- by transmitting data, documents or content likely to compromise the security, integrity, availability or proper functioning of the Service.

The Applicant is required to make the GTC, this Technical Annex and any further relevant information relating to the use of the Service available to Users.

3.3.2 Obligations and responsibilities of the User and Relying Parties

Users shall use the Service via the Applicant's systems and in accordance with this document, the instructions and the terms of use defined therein.

Users are responsible for their use of the Service, for the validation requests they make and for the use of the results and validation reports returned by the Service, within the limits of the activities attributable to them.

In the case of the QSVS qualified service, Users are required to verify the qualified electronic seal on the validation report in order to verify its origin and integrity.

Relying Parties use the validation results and validation reports as part of their own verification, assessment or decision-making processes and are responsible for the assessments and decisions made on the basis thereof.

In the case of the QSVS qualified service, Relying Parties are required to verify the qualified electronic seal on the validation report before relying on it

3.3.3 Obligations and responsibilities of Tinexta Infocert

Tinexta Infocert provides the Service in compliance with applicable legislation, the General Terms and Conditions (GTC), this Technical Annex, the Operating Manual and the applicable technical documentation.

Tinexta Infocert carries out validation operations in accordance with the technical procedures and validation policies applied by the Service, ensuring that the validation process is carried out in accordance with the applicable validation policies and ETSI standards.

Without prejudice to the provisions of applicable legislation, Tinexta Infocert shall not be liable:

- the accuracy, authenticity, integrity or lawfulness of the data provided, documents, signatures, certificates or other elements submitted for validation;
- for the use of the validation results or validation reports by the Applicant, Users or Relying Parties;
- for any use of the Service that does not comply with the General Terms and Conditions, this Technical Annex, the applicable technical documentation or current legislation;
- for malfunctions, unavailability or errors in the systems, infrastructure or applications used by the Applicant or third parties;
- delays, unavailability, errors or incompleteness of information originating from Certification Authorities, OCSP/CRL services, Trusted Lists or other third-party services and infrastructure used as part of the validation process

Tinexta Infocert S.p.A.

Piazzale Flaminio 1/B, 00196 – Rome (RM), Italy A company subject to the management and coordination of Tinexta S.p.A.

T +39 06 836691 F +39 06 833669634, VAT No. 07945211006 REA No. 1064345

info@infocert.it Subscribed and paid-up share capital €21,099,232.00

infocert.it infocert.digital



4. SLA AND KPIS

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

Tinexta Infocert S.p.A.

Piazzale Flaminio 1/B, 00196 – Rome (RM), Italy A company subject to the management and coordination of Tinexta S.p.A.

T +39 06 836691 F +39 06 833669634, VAT No. 07945211006 REA No. 1064345

info@infocert.it Subscribed and paid-up share capital €21,099,232.00

infocert.it infocert.digital