ALLEGATO TECNICO
Servizio di Convalida di firme e sigilli QSVS

***

1. RIFERIMENTI ESTERNI

Documentazione	Link di dettaglio
Manuale Operativo	https://qtsp.infocert.it/pdf/ICERT_INDI_QSVS.pdf
Manuale Utente	N.D.
Allegato Web	https://developers.infocert.digital/signature-validation/
Link di supporto (FAQ, Video, Guide)	https://knowledgecenter.infocert.digital/

2. DESCRIZIONE DEL SERVIZIO – INTRODUZIONE

Tinexta Infocert S.p.A. (di seguito "Infocert"), nel contesto del presente documento, opera in qualità di prestatore di servizi fiduciari qualificati (di seguito "QTSP") e, in particolare, quale prestatore del servizio qualificato e non qualificato(di seguito anche "QSVSP" o "SVSP") di verifica e convalida delle firme elettroniche, sigilli elettronici, marche temporali e certificati di firma, di marcatura e della Certification Authority emittente (il "Servizio"), secondo quanto previsto dal Manuale Operativo ICERT-INDI-QSVS (di seguito anche "Manuale Operativo") e dall'Allegato Web "Signature Validation" di cui all'articolo 1.
Per tale Servizio, Tinexta Infocert S.p.A. ha ottenuto una valutazione di conformità effettuata dal Conformity Assessment Body CSQA Certificazioni S.r.l., ai sensi del Regolamento (UE) n. 910/2014 e successive modifiche e integrazioni (di seguito, il "Regolamento eIDAS"), nonché della Implementing Decision (UE) 2015/1506 e delle norme ETSI applicabili, tra cui ETSI EN 319 401, ETSI TS 119 441, ETSI EN 319 102-1, ETSI TS 119 102-2 e ETSI TS 119 172-4, secondo lo schema di valutazione eIDAS definito da ACCREDIA ai sensi delle norme ETSI EN 319 403 e UNI CEI ISO/IEC 17065:2012.

Il presente Allegato Tecnico costituisce parte integrante e sostanziale del contratto di acquisto dei servizi (di seguito, l'"Accordo"), stipulato con il Cliente.
Ai soggetti che attivano, utilizzano o fanno affidamento sul Servizio si applicano le Condizioni Generali di Attivazione (di seguito, "CGA"), di cui il presente Allegato Tecnico costituisce parte integrante, fermo restando che, nei rapporti con il Cliente, trovano applicazione anche le disposizioni dell'Accordo.

2.1 Definizione Delle Parti

Cliente
Persona fisica o giuridica, ente o organizzazione che acquista il Servizio e con cui è formalizzato l'Accordo. Il Cliente può coincidere con il Richiedente.

Richiedente
Persona fisica oppure persona giuridica, ente o organizzazione che cura l'implementazione del Servizio nell'ambito dei sistemi applicativi utilizzati.
Al Richiedente si applicano le Condizioni Generali di Attivazione (CGA), il presente Allegato Tecnico e le disposizioni dell'Accordo applicabili e comunicate dal Cliente.

Utente
Soggetto o componente applicativa che utilizza il Servizio, direttamente o tramite i sistemi del Richiedente, al fine di ottenere la verifica e la convalida di firme elettroniche, sigilli elettronici, certificati o evidenze correlate.

Verifier / Relying Party
Soggetto che utilizza gli esiti, i report o le evidenze generate dal Servizio nell'ambito dei propri processi di verifica, valutazione o decisione

3. SPECIFICHE TECNICO-NORMATIVE

3.1 Caratteristiche del Servizio di Signature Validation

3.1.1 Oggetto e natura del Servizio

Il Signature Validation Service (SVS) e il Qualified Signature Validation Service (QSVS) sono servizi fiduciari finalizzati alla verifica e convalida di firme elettroniche, sigilli elettronici, marche temporali e certificati digitali.
Il Servizio consente di verificare la validità tecnica, crittografica e normativa degli elementi sottoposti a validazione secondo gli standard ETSI applicabili.
Il Servizio è erogato:

- in modalità non qualificata (SVS), conforme ai requisiti previsti dalla ETSI TS 119 441;
- in modalità qualificata (QSVS), conforme ai requisiti della ETSI TS 119 441 con specifico riferimento ai requisiti previsti all'Annex B "Qualified Validation Service for QES as defined by Article 33 of the Regulation (EU) No 910/2014";

Il Servizio qualificato QSVS e il Servizio non qualificato SVS sono identificati mediante specifici Object Identifier (OID), descritti nel Manuale Operativo.

Le operazioni di validazione sono eseguite esclusivamente secondo una specifica signature validation policy, identificata mediante OID e descritta nel Manuale Operativo. Tale signature validation policy è utilizzata per la validazione di firme elettroniche, sigilli elettronici, marche temporali e certificati digitali secondo gli standard ETSI applicabili. Non è consentito al Richiedente definire o modificare la signature validation policy applicata dal Servizio.
Il Servizio non modifica i documenti o gli oggetti sottoposti a validazione, ma restituisce esclusivamente gli esiti e le evidenze del processo di validazione.
I dati e i documenti trasmessi al Servizio sono trattati esclusivamente per il tempo necessario all'elaborazione delle richieste e alla generazione delle relative risposte, salvo quanto previsto per le registrazioni tecniche di servizio (log) e per eventuali obblighi normativi applicabili. Le evidenze sono

restituite dal Servizio in modalità sincrona. Il Servizio non conserva le evidenze e, pertanto, le stesse non sono più recuperabili in un momento successivo tramite il Servizio stesso.
Tinexta Infocert mantiene registrazioni tecniche delle operazioni effettuate ai fini di sicurezza, tracciabilità, verifica e audit. Tali registrazioni sono conservate per un periodo pari a 7 (sette) anni, in conformità alla normativa applicabile.
Il Servizio si considera attivato a seguito dell'accettazione delle CGA e del presente Allegato Tecnico da parte del Richiedente, con la messa a disposizione delle modalità di accesso al Servizio.
La durata e le condizioni di utilizzo del Servizio sono disciplinate dall'Accordo con il Cliente.

3.1.2 Processo di Validazione

Il processo di validazione è eseguito dal Servizio secondo l'algoritmo definito dalla norma ETSI EN 319 102-1 e sulla base della signature validation policy applicabile, descritta nel Manuale Operativo.
Nell'ambito della validazione, il Servizio effettua le verifiche necessarie sugli elementi sottoposti a controllo, tra cui, ove applicabili:

- il formato della firma o del sigillo;
- la validità crittografica;
- l'identificazione dei certificati utilizzati;
- la validità e lo stato dei certificati;
- la catena di certificazione;
- la validità delle eventuali marche temporali.

Per l'esecuzione delle verifiche, il Servizio può acquisire informazioni da fonti esterne, incluse Certification Authority, servizi OCSP/CRL e Trusted List applicabili.
Il Richiedente non può definire o modificare la validation policy applicata dal Servizio, ma può indicare, ove previsto, il livello di validazione richiesto tra quelli supportati dal Servizio.
Gli esiti della validazione sono restituiti secondo le classificazioni previste dagli standard ETSI applicabili: TOTAL-PASSED, TOTAL-FAILED e INDETERMINATE.
Qualora non sia possibile acquisire o verificare tutte le informazioni necessarie al completamento del processo di validazione, il Servizio restituisce un esito coerente con le informazioni disponibili al momento dell'elaborazione.

3.1.3 Validation report ed evidenze di validazione

Il Servizio restituisce gli esiti della validazione mediante un validation report contenente le principali evidenze del processo di validazione effettuato.
Il validation report include, ove applicabili:

- l'identificazione della validation policy utilizzata;
- gli esiti delle verifiche effettuate;

- le informazioni relative ai certificati e alle eventuali marche temporali verificate;
- l'esito complessivo della validazione.

Ai fini della validazione temporale della firma e della determinazione della relativa Proof of Existence (PoE), il Servizio utilizza prioritariamente le marche temporali associate alla firma o al documento. In assenza di marche temporali, la PoE viene identificata secondo quanto previsto dalla policy del Servizio.
Nel caso del Servizio qualificato QSVS, il validation report è sigillato mediante sigillo elettronico qualificato di Tinexta Infocert e corredato di marca temporale, al fine di garantirne origine e integrità.

3.1.4 Formati supportati

Il Servizio supporta la validazione di firme elettroniche, sigilli elettronici, marche temporali e certificati digitali nei principali formati previsti dagli standard ETSI applicabili.

In particolare, il Servizio supporta i formati CAdES, XAdES, PAdES e JAdES, incluse le relative strutture di firma (enveloped, enveloping e detached) e i baseline level previsti dagli standard ETSI di riferimento.

Il Richiedente può specificare, nell'ambito delle modalità supportate dal Servizio e descritte nell'Allegato Web "Signature Validation", il livello o la tipologia di validazione richiesta.

Le modalità di validazione disponibili, i livelli supportati, i formati accettati, i vincoli tecnici applicabili e le relative specifiche di invocazione delle API sono descritti nel Manuale Operativo e nell'Allegato Web "Signature Validation".

3.2 Modalità d'uso del Servizio

Il Servizio è reso disponibile mediante API esposte da Tinexta Infocert secondo le modalità descritte nel Manuale Operativo e nell'Allegato Web "Signature Validation".
L'accesso alle API del Servizio avviene tramite protocollo TLS con autenticazione OAuth2 del chiamante.
Il Servizio espone le seguenti API:

- API QSVS per la validazione qualificata di documenti firmati o marcati temporalmente, con restituzione di un validation report sigillato mediante sigillo elettronico qualificato di Tinexta Infocert;
- API SVS per la validazione non qualificata di documenti firmati o marcati temporalmente;
- API SVS per la validazione di certificati digitali X.509.

Per specifiche modalità di fruizione del Servizio non qualificato, Tinexta Infocert può inoltre rendere disponibile un'interfaccia web per l'utilizzo diretto delle funzionalità di validazione.

Nell'ambito delle richieste di validazione di documenti firmati o marcati temporalmente, il Richiedente trasmette:

- il documento firmato o marcato temporalmente, oppure le firme detached supportate dal Servizio;

- il livello o la tipologia di validazione richiesta tra quelli supportati dal Servizio;
- gli eventuali ulteriori parametri tecnici previsti dalle API applicabili.

Nell'ambito delle richieste di validazione di certificati digitali, il Richiedente trasmette il certificato X.509 da sottoporre a validazione secondo i formati supportati dal Servizio.
Le richieste sono elaborate secondo la signature validation policy applicata dal Servizio e descritta nel Manuale Operativo.
Le API del Servizio operano in modalità sincrona.
Le modalità di invocazione delle API, la struttura delle richieste e delle risposte e le relative specifiche tecniche sono descritte nel Manuale Operativo e nell'Allegato Web "Signature Validation.

3.3 Obblighi e responsabilità

3.3.1 Obblighi e responsabilità del Richiedente

Il Richiedente è tenuto a utilizzare il Servizio nel rispetto delle CGA, del presente Allegato Tecnico, dell'Allegato Web "Signature Validation", della normativa applicabile e delle disposizioni dell'Accordo applicabili e comunicate dal Cliente.
Il Richiedente è responsabile dell'integrazione del Servizio nei propri sistemi applicativi utilizzati ed è responsabile della corretta configurazione delle API, della gestione delle credenziali e dei meccanismi di autenticazione, nonché delle modalità di accesso e utilizzo del Servizio da parte degli Utenti operanti tramite i propri sistemi.
Il Richiedente è altresì responsabile della correttezza, integrità, completezza e liceità dei dati, dei documenti, delle firme, dei certificati e degli ulteriori elementi sottoposti a validazione tramite il Servizio.
Gli esiti della validazione e i validation report restituiti dal Servizio devono essere utilizzati tenendo conto delle informazioni e delle evidenze in essi contenute, della validation policy applicata e dei limiti propri del processo di validazione.
Nel caso del Servizio qualificato QSVS, il Richiedente è tenuto a verificare il sigillo elettronico qualificato sul validation report al fine di verificarne origine e integrità.
Il Richiedente si impegna a utilizzare il Servizio esclusivamente per le finalità e secondo le modalità previste dalla documentazione tecnica applicabile e a non utilizzare il Servizio:

- per finalità illecite o in violazione della normativa applicabile;
- in modo non conforme alle specifiche tecniche del Servizio;
- mediante trasmissione di dati, documenti o contenuti idonei a compromettere la sicurezza, l'integrità, la disponibilità o il corretto funzionamento del Servizio.

Il Richiedente è tenuto a rendere disponibili agli Utenti le CGA, il presente Allegato Tecnico e le ulteriori informazioni rilevanti relative all'utilizzo del Servizio.

3.3.2 Obblighi e responsabilità dell'Utente e delle Relying Party

Gli Utenti utilizzano il Servizio tramite i sistemi del Richiedente e nel rispetto del presente documento, delle istruzioni e delle modalità di utilizzo da questo definite.

Gli Utenti sono responsabili dell'utilizzo del Servizio, delle richieste di validazione effettuate e dell'utilizzo degli esiti e dei validation report restituiti dal Servizio, nei limiti delle attività agli stessi riconducibili.
Nel caso del Servizio qualificato QSVS, gli Utenti sono tenuti a verificare il sigillo elettronico qualificato sul validation report al fine di verificarne origine e integrità.
Le Relying Party utilizzano gli esiti della validazione e i validation report nell'ambito dei propri processi di verifica, valutazione o decisione e sono responsabili delle valutazioni e decisioni assunte sulla base degli stessi.
Nel caso del Servizio qualificato QSVS, le Relying Party sono tenute a verificare il sigillo elettronico qualificato sul validation report prima di farvi affidamento

3.3.3 Obblighi e responsabilità di Tinexta Infocert

Tinexta Infocert eroga il Servizio nel rispetto della normativa applicabile, delle CGA, del presente Allegato Tecnico, del Manuale Operativo e della documentazione tecnica applicabile.

Tinexta Infocert esegue le operazioni di validazione secondo le modalità tecniche e le validation policy applicate dal Servizio, garantendo che il processo di validazione sia eseguito conformemente alle validation policy applicate e agli standard ETSI.

Fermo restando quanto previsto dalla normativa applicabile, Tinexta Infocert non è responsabile:

- della correttezza, autenticità, integrità o liceità dei dati forniti, documenti, firme, certificati o ulteriori elementi sottoposti a validazione;
- dell'utilizzo degli esiti della validazione o dei validation report da parte del Richiedente, degli Utenti o delle Relying Party;
- di utilizzi del Servizio non conformi alle CGA, al presente Allegato Tecnico, alla documentazione tecnica applicabile o alla normativa vigente;
- di malfunzionamenti, indisponibilità o errori dei sistemi, delle infrastrutture o delle applicazioni utilizzate dal Richiedente o da soggetti terzi;
- di ritardi, indisponibilità, errori o incompletezze delle informazioni provenienti da Certification Authority, servizi OCSP/CRL, Trusted List o altri servizi e infrastrutture di terzi utilizzati nell'ambito del processo di validazione

4. SLA E KPI

In termini di erogazione, i valori di disponibilità mensile dei servizi sono rappresentati dettagliatamente nel Manuale Operativo