



ALLEGATO TECNICO Marca Temporale

Sommario

1. Riferimenti esterni.....	1
2. Descrizione del servizio – Introduzione.....	1
3. Specifiche Tecnico Normative	2
4. SLA e KPI.....	6

1. Riferimenti esterni

Documentazione	Link di dettaglio
Manuale Operativo	https://qtsp.infocert.it/pdf/ICERT_INDI_TSA.pdf
	https://qtsp.infocert.it/pdf/ICERT_INDI_TDS.pdf
Manuale Utente	N.D.
Allegato Web	https://developers.infocert.digital/timestamps/
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 validazione temporale elettronica (di seguito anche “TSA” – Time Stamping Authority), per l’erogazione del servizio di marcatura temporale (di seguito, il “Servizio”), secondo quanto previsto dal Manuale Operativo ICERT-INDI-TSA (di seguito anche “Manuale Operativo”).

Per tale Servizio, Infocert 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 dei Regolamenti di esecuzione e degli standard ETSI applicabili, tra cui ETSI EN 319 401, ETSI EN 319 421 e ETSI EN 319 422 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 Servizio ha ad oggetto l’emissione di marche temporali elettroniche qualificate, consistenti nell’associazione di una data e di un’ora certe a dati elettronici, al fine di attestare che tali dati esistevano



in un determinato momento e non sono stati modificati successivamente senza che tale modifica sia rilevabile.

La validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e dell'integrità dei dati ai quali tali informazioni sono associate, ai sensi del Regolamento eIDAS. Il Servizio è reso nel rispetto del Regolamento eIDAS, delle norme ETSI applicabili e delle policy e pratiche definite nel Manuale Operativo, ed è erogato secondo una specifica policy di marcatura temporale identificata mediante Object Identifier (OID), descritta nel Manuale operativo.

Il Servizio può essere acquistato dal Cliente in forma di pacchetti o quantitativi predefiniti di Marche Temporal, che vengono successivamente richieste e utilizzate secondo le modalità previste nel presente documento.

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 con cui è stato formalizzato il contratto di fornitura del Servizio (Accordo). Il Cliente può coincidere con il Richiedente.

Richiedente

Persona fisica o giuridica, ente o organizzazione che richiede l'emissione delle Marche Temporal e utilizza il Servizio, anche qualora non coincida con il Cliente.

Utente

Soggetto che verifica una Marca Temporale, al fine di accertare la validità della data e dell'ora ad essa associate e l'integrità dei dati ai quali la Marca Temporale è riferita.

3. Specifiche Tecnico Normative

3.1 Descrizione e funzionamento del Servizio

3.1.1 Marca Temporale e certificato di marcatura temporale

La Marca Temporale è un'evidenza elettronica che attesta l'associazione tra un insieme di dati e un riferimento temporale determinato, al fine di dimostrare che tali dati esistevano a uno specifico istante e che eventuali modifiche successive risultano rilevabili.

La Marca Temporale è firmata elettronicamente da Infocert, in qualità di Time Stamping Authority (TSA), mediante una chiave privata associata a un certificato di marcatura temporale, che consente di verificarne l'origine e l'integrità.

3.1.2 Rilascio della Marca Temporale

La Marca Temporale è generata a seguito di una richiesta del Richiedente, che trasmette al Servizio l'impronta dei dati da marcare, ottenuta mediante una funzione di hash crittografico.

Il sistema della TSA, ricevuta la richiesta, provvede automaticamente a:

- associare all'impronta un riferimento temporale basato su una sorgente sincronizzata con il Tempo Universale Coordinato (UTC);
- generare la Marca Temporale;



- apporre la firma elettronica della TSA;
- restituire la Marca Temporale al Richiedente.

Il processo di emissione è eseguito in modalità automatizzata all'interno di infrastrutture sicure gestite da Infocert.

3.1.3 Utilizzo e verifica della Marca Temporale

La Marca Temporale è utilizzata per attestare l'esistenza di dati o documenti informatici a un determinato istante ed è impiegata nell'ambito di processi informatici che richiedono la prova dell'anteriorità temporale e dell'integrità dei dati.

In particolare, la Marca Temporale può essere utilizzata:

- in associazione a documenti informatici, al fine di attestare la loro esistenza a una determinata data e ora;
- in combinazione con firme elettroniche, per supportare le attività di verifica della validità delle firme nel tempo, anche oltre la scadenza dei certificati;
- nell'ambito di processi di conservazione digitale, per attestare la data di formazione o di trattamento dei documenti;
- all'interno di applicazioni o sistemi informativi che richiedono l'evidenza temporale di operazioni o transazioni.

L'utilizzo della Marca Temporale avviene mediante associazione della stessa ai dati originari cui si riferisce, mantenendo la corrispondenza tra l'impronta contenuta nella Marca e i dati oggetto di marcatura.

La verifica della Marca Temporale consiste nelle seguenti verifiche:

- verifica della firma elettronica apposta dalla TSA;
- verifica della validità del certificato di marcatura temporale e della relativa catena di certificazione;
- verifica dello stato del certificato mediante i servizi di validazione disponibili;
- ricalcolo dell'impronta dei dati e confronto con quella contenuta nella Marca Temporale;
- verifica della coerenza del riferimento temporale.

Tali verifiche possono essere effettuate dal Richiedente o da un Utente (relying party) e consentono di accertare l'autenticità della Marca Temporale, l'integrità dei dati e la corretta associazione tra i dati e il riferimento temporale.

3.1.4 Validità ed efficacia nel tempo

Il riferimento temporale associato alla Marca Temporale è generato sulla base di una sorgente sincronizzata con il Tempo Universale Coordinato (UTC), secondo meccanismi che ne garantiscono l'accuratezza.

La Marca Temporale produce i propri effetti con riferimento al momento della sua emissione e consente di attestare l'esistenza dei dati a tale istante.

L'efficacia nel tempo della Marca Temporale è subordinata alla possibilità di verificarne gli elementi costitutivi, inclusi la firma della TSA, il certificato di marcatura temporale, la relativa catena di certificazione e le informazioni sullo stato dei certificati utilizzati.

3.1.5 Revoca o sospensione del certificato della TSA

Le Marche Temporalie sono firmate da Infocert in qualità di Time Stamping Authority (TSA) mediante un certificato utilizzato per l'emissione del Servizio. Tale certificato è gestito da Infocert nell'ambito del proprio ciclo di vita e può essere sospeso o revocato nei casi previsti dal Manuale Operativo.

La sospensione o la revoca del certificato comporta l'immediata cessazione del suo utilizzo per l'emissione di nuove Marche Temporalie e la sua sostituzione nell'ambito del Servizio con un certificato valido.



A seguito della revoca o sospensione, lo stato del certificato è reso disponibile tramite le liste di revoca (CRL) e gli altri servizi di verifica previsti, al fine di consentire la rilevazione dell'evento nell'ambito delle attività di verifica.

Le Marche Temporalì già emesse restano verificabili sulla base degli elementi in esse contenuti e delle informazioni disponibili al momento della verifica. Le eventuali Marche Temporalì generate successivamente all'evento di revoca o sospensione sono da considerarsi non valide.

3.1.6 Tracciabilità e conservazione dei dati del Servizio

Infocert registra e conserva per venti anni le informazioni relative all'erogazione del Servizio, inclusi i log delle operazioni e gli eventi rilevanti ai fini della sicurezza, della tracciabilità e della gestione del Servizio. Il Servizio è progettato per trattare esclusivamente l'impronta (hash) dei dati trasmessi dal Richiedente ai fini della generazione della Marca Temporale. Infocert non acquisisce né conserva i dati originari cui l'impronta si riferisce, né il contenuto dei documenti eventualmente associati.

Le informazioni trattate e conservate sono limitate a quelle necessarie alla generazione delle Marche Temporalì e alla gestione operativa del Servizio, in conformità al Manuale Operativo e alla normativa applicabile.

3.2 Prodotti e Servizi

3.2.1 Servizio di marcatura temporale qualificata

Il servizio di marcatura temporale qualificata è erogato da Infocert in qualità di QTSP secondo le policy identificate mediante OID descritte nel Manuale Operativo e gode della presunzione di accuratezza della data e dell'ora che indica e dell'integrità dei dati ai quali tali informazioni sono associate.

Le Marche Temporalì qualificate attestano l'associazione tra dati elettronici e un riferimento temporale qualificato.

3.2.2 Servizio di marcatura temporale non qualificata

Infocert può inoltre erogare servizi di marcatura temporale non qualificata, basati su meccanismi tecnici analoghi a quelli del servizio qualificato.

Tali servizi non rientrano nel perimetro dei servizi fiduciari qualificati ai sensi del Regolamento eIDAS e non beneficiano delle relative presunzioni giuridiche.

3.2.3 Caratteristiche tecniche del Servizio

Il Servizio è basato sul protocollo Time-Stamp Protocol (TSP), conforme alle specifiche IETF RFC 3161 e RFC 5816.

Le richieste di marcatura temporale sono costituite dall'impronta dei dati e sono elaborate dal sistema della TSA, che restituisce una risposta contenente la Marca Temporale.

Il Servizio è compatibile con i principali formati di firma elettronica che prevedono l'utilizzo o l'inclusione di Marche Temporalì, tra cui XAdES, CAdES, PAdES, JAdES e ASiC, nonché con i relativi baseline levels, ove supportati.

Per il dettaglio aggiornato dei formati supportati, delle modalità di integrazione, delle API, delle capacità crittografiche e delle ulteriori specifiche tecniche del Servizio, si rinvia al Manuale Operativo e/o all'Allegato Web.

3.2.4 Modalità di erogazione e fruizione del Servizio

Il Servizio è reso disponibile mediante interfacce applicative che consentono ai soggetti abilitati di inviare richieste di marcatura temporale e ricevere le relative Marche Temporalì.

L'accesso al Servizio avviene mediante credenziali applicative rilasciate da Infocert al Cliente e/o a soggetti da questi autorizzati.

Il Servizio può essere fruito:



- mediante utilizzo di applicativi messi a disposizione da Infocert;
- mediante integrazione applicativa nei sistemi del Cliente.

Nel caso di integrazione, il Cliente utilizza le credenziali rilasciate per l'accesso al Servizio e per l'invio delle richieste nell'ambito dei propri sistemi e processi secondo quanto precisato nell'Allegato Web.

Può essere reso disponibile, ove previsto, un ambiente di test per la verifica delle integrazioni prima dell'utilizzo in esercizio.

Il Cliente può rendere disponibile il Servizio a soggetti terzi nell'ambito delle proprie applicazioni o servizi; tali soggetti, nel momento in cui effettuano richieste di marcatura temporale, operano in qualità di Richiedenti ai sensi del presente Allegato Tecnico.

3.3 Obblighi e Responsabilità

3.3.1 Obblighi e Responsabilità del Richiedente

Il Richiedente è tenuto a utilizzare il Servizio nel rispetto delle Condizioni Generali di Attivazione (CGA), del presente Allegato Tecnico, del Manuale Operativo e della normativa applicabile.

Il Richiedente è responsabile della correttezza, completezza e liceità delle informazioni fornite nell'ambito dell'attivazione e dell'utilizzo del Servizio, nonché della correttezza dell'impronta (hash) trasmessa ai fini della generazione della Marca Temporale e della relativa corrispondenza con i dati originari.

Il Richiedente è inoltre tenuto:

- a verificare la validità delle Marche Temporalì ricevute;
- a conservare le Marche Temporalì unitamente ai dati cui si riferiscono con modalità idonee a consentirne la verifica nel tempo e a garantire integrità;
- ad adottare le misure tecniche e organizzative adeguate a garantire la sicurezza dei propri sistemi e delle credenziali di accesso al Servizio;
- a tutelare la segretezza delle credenziali utilizzate per la richiesta delle Marche Temporalì, evitando comunicazione o divulgazione a soggetti non autorizzati;
- ad adeguare i propri sistemi hardware e software alle misure di sicurezza previste dalla normativa applicabile.

Il Richiedente è altresì tenuto a rendere disponibili ai soggetti che utilizzano o verificano le Marche Temporalì le CGA, il presente Allegato Tecnico e le ulteriori informazioni rilevanti relative al Servizio.

La fornitura e l'utilizzo della connessione Internet, nonché degli strumenti hardware e software necessari per l'accesso e l'utilizzo del Servizio, restano a carico del Richiedente.

L'utilizzo del Servizio mediante le credenziali rilasciate è imputato al Richiedente, che ne risponde anche nei casi di utilizzo da parte di soggetti terzi operanti tramite i propri sistemi o credenziali.

Il Richiedente è tenuto a manlevare Infocert da ogni responsabilità derivante da utilizzi del Servizio non conformi alla normativa applicabile o alle condizioni contrattuali.

3.3.2 Obblighi e Responsabilità dell'Utente

L'Utente che utilizza o fa affidamento su una Marca Temporale è tenuto a verificarne la validità secondo le modalità previste dal presente Allegato Tecnico e dal Manuale Operativo.

L'Utente è responsabile delle verifiche effettuate e delle valutazioni o decisioni assunte sulla base delle Marche Temporalì utilizzate.

3.3.3 Obblighi e responsabilità di Infocert

Infocert garantisce che il Servizio sia erogato conformemente ai requisiti di sicurezza, affidabilità e continuità ai sensi del Regolamento eIDAS, dei Regolamenti esecutivi e delle norme ETSI applicabili, del Manuale Operativo e delle condizioni contrattuali.

Nell'ambito del Servizio, Infocert è responsabile della corretta generazione delle Marche Temporalì, assicurando l'associazione tra l'impronta dei dati ricevuta e un riferimento temporale certo, nonché della



gestione del certificato utilizzato per l'emissione del Servizio e della disponibilità delle informazioni necessarie alla verifica.

Il Servizio è progettato in modo tale che Infocert non abbia accesso ai dati originari cui si riferisce la Marca Temporale, ma esclusivamente alla relativa impronta; conseguentemente, Infocert non verifica né il contenuto, né la correttezza, né la liceità dei dati oggetto di marcatura.

Restano pertanto escluse dalla responsabilità di Infocert le attività relative alla generazione dell'impronta, all'associazione della Marca Temporale ai dati, nonché alla conservazione e all'utilizzo delle Marche Temporal da parte del Richiedente o di terzi.

Fatto salvo il caso di dolo o colpa Infocert non è responsabile per malfunzionamenti o indisponibilità imputabili a sistemi o infrastrutture esterni al proprio controllo, né per utilizzi del Servizio non conformi alle condizioni contrattuali o alla normativa applicabile.

4. SLA e KPI

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