# TIME-STAMP AUTHORITY

## Trust Service Practice Statement

**Codice documento: REGIT-TSA-TSPS**
**Versione: 1.0**
**Redatto da**: Serena Giugni
**Approvato da**: Claudio Corbetta
**Data approvazione**: 01/05/2019

## Sommario

# 1. Introduzione

Register SpA – (P.IVA./Codice fiscale 04628270482), iscritta dal 26.04.1995 al Registro delle Imprese di Firenze.

Register SpA (nel seguito anche "Register") è leader storico in Italia nella fornitura di servizi di registrazione di domini, hosting, protezione del brand e pubblicità in rete.

Si qualifica inoltre come "Gestore di Posta Elettronica Certificata" (PEC), regolarmente iscritto all'elenco pubblico dei gestori PEC coordinato dall'Agenzia per l'Italia Digitale e come Identity Provider accreditato sempre da AgID.

Questo documento descrive il servizio di Marcatura temporale di Register che verrà utilizzato solo ad uso interno.

## 1.1 Riferimenti normativi

I seguenti servizi fiduciari qualificati soddisfano i requisiti eIDAS (Regolamento (EU) N°910/2014) e sono conformi ai seguenti standard:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates.
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles.
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- ETSI EN 319 122 - CAdES digital signatures
- IETF (RFC3161) https://www.ietf.org/rfc/rfc3161.txt
- IETF (RFC3628) https://www.ietf.org/rfc/rfc3628.txt

## 1.2 Versione e storia del documento

| **Versione del documento e storia delle modifiche** | | | |
|---|---|---|---|
| **Versione** | **Data** | **Paragrafo** | **Note sui cambiamenti** |
| **1.0** | 01 Maggio 2019 | *Tutti* | *Prima versione del documento* |

## 2. Definizioni e abbreviazioni

Il presente paragrafo è finalizzato ad agevolare l'interpretazione dei termini e degli acronimi utilizzati nel seguito del documento.

Le principali fonti normative alle quali si è fatto riferimento sono indicate nel paragrafo relativo ai Riferimenti normativi.

| Acronimi | Definizione |
|---|---|
| **CA** | Certification Authority |
| **CAO** | Certificate Authority Officer |
| **TSPP** | TSP Policy |
| **TSPPS** | TSP Practice Statement |
| **CRL** | Certificate Revocation List |
| **ETSI** | European Telecommunications Standards Institute |
| **HSM** | Hardware Security Module |
| **QTSA** | Qualified Time-Stamping Authority |
| **PKI** | Public Key Infrastructure – componente per l'emissione dei certificati. |
| **RAO** | Registration Authority Officer |
| **RFC** | Request For Comments |
| **TIN** | Tax Identification Number |
| **TSA** | Time-Stamping Authority |
| **TSU** | Time Stamping Unit |
| **TLS** | Transport Layer Security |
| **TSP** | Trust Service Provider |

# 3. Concetti generali

## 3.1 Requisiti generali

La policy del servizio di marcatura temporale di Register si basa sull'uso della crittografia a chiave pubblica, sull'uso di certificati digitali e di un riferimento temporale affidabile.

Il servizio viene erogato dal TSP Register, attenendosi alle norme e ai requisiti descritti nella specifica ETSI EN 319 401, comuni a tutti i servizi erogati da qualunque Trust Service Provider.

Le policy e le pratiche specifiche del servizio di marcatura temporale sono dettagliate più avanti in questo documento.

## 3.2 Servizio di marcatura temporale

Il servizio di marcatura temporale (time-stamping) consiste nell'emissione di una evidenza temporale, sotto forma di un Time Stamp Token (i.e. un oggetto digitale conforme alle specifiche IETF RFC 3161).

La marca temporale che viene così emessa ha lo scopo di associare in maniera certa e opponibile a terzi un riferimento temporale UTC a un insieme di dati elettronici, fornendo in tal modo evidenza che questi dati esistevano nell'istante temporale riportato all'interno della marca temporale e garantendo al tempo stesso che tali dati non siano stati successivamente manomessi o modificati.

## 3.3 Time-Stamping Authority (TSA)

Il Trust Service Provider Register ricopre il ruolo di Time-Stamping Authority (TSA) nel processo di emissione di marche temporali (time-stamp), in accordo con la definizione fornita nel paragrafo precedente.

Per l'erogazione del servizio di marcatura temporale, la TSA si avvale dell'uso di una o più Time-Stamping Unit (TSU), costituita dall'insieme degli strumenti hardware e software che concorrono all'emissione della marca temporale.

Ogni TSU gestita da Register utilizza una differente chiave privata per la firma digitale delle marche temporali emesse per conto della TSA.

## 3.4 Utilizzo del servizio

L'utilizzo del servizio di marcatura temporale è soggetto alle condizioni generali di utilizzo dei servizi di Register e comporta l'accettazione delle policy e delle procedure descritte nel presente documento, che regolano e limitano l'emissione delle marche temporali.

Sono considerati utenti del servizio di marcatura temporale di Register tutti gli individui o le organizzazioni autorizzate ad accedere al servizio stesso e a richiedere l'emissione di una marca

temporale, utilizzando adeguati strumenti tecnologici che aderiscano alle specifiche descritte in IETF RFC 3161.

### 3.5 Policy e Practice Statement

Nel presente documento Register, in qualità di TSA, specifica la policy che definisce le condizioni sotto le quali viene erogato il servizio di marcatura temporale, in accordo con quanto previsto dalle specifiche ETSI EN 319 401 e ETSI EN 319 421.

Nei capitoli successivi di questo stesso documento vengono inoltre riportate, sotto forma di un Practice Statement conforme alle specifiche ETSI EN 319 401 e ETSI EN 319 421, le pratiche e le procedure messe in atto da Register per soddisfare i requisiti generali descritti nella policy del servizio di marcatura temporale.

## 4. Time-Stamp Policy

La TSA di Register eroga il servizio di marcatura temporale in conformità con la Best practices Time-Stamp Policy (BTSP) definita nella specifica ETSI EN 319 421.

Pertanto, le marche temporali emesse da Register ammettono come identificativo della policy solamente il seguente OID:

0.4.0.2023.1.1

L'OID è definito insieme alla BTSP ed è così strutturato:

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy(1)

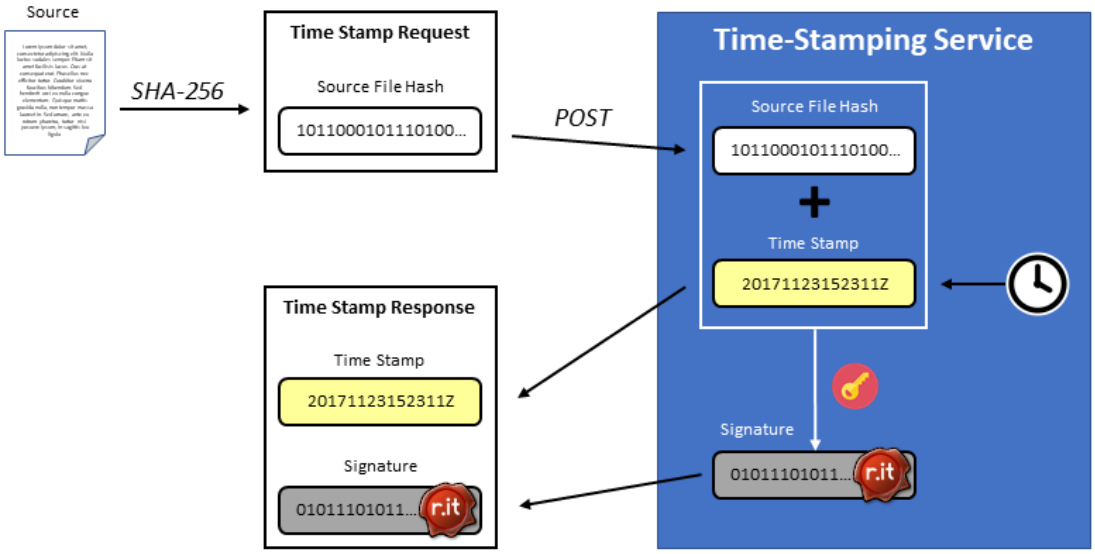
L'inclusione di questo identificativo in tutte le marche temporali emesse da Register ne attesta la conformità con la BTSP.

# 5. Operatività della TSA

## 5.1 Erogazione delle marche temporali

Il servizio di marcatura temporale di Register è accessibile per mezzo di un'interfaccia HTTP su canale sicuro SSL ed è conforme alle specifiche IETF RFC 3161 e ETSI EN 319 422.

Accetta in ingresso una Time-Stamp Request ed emette in risposta una Time-Stamp Response, come schematizzato nella seguente figura:




### 5.1.1 Time-Stamp Request

L'applicazione accetta richieste in HTTP POST, il cui header Content-Type sia uguale a:

application/timestamp-query

Il body della richiesta deve essere un oggetto di tipo Time-Stamp Request (come definito in IETF RFC 3161, par. 2.4.1) opportunamente codificato. Come da specifiche ETSI EN 319 422, i campi *reqPolicy*, *nonce* e *certReq* sono supportati.

La richiesta deve necessariamente contenere l'hash dei dati originali sui quali si vuole apporre la marcatura temporale. L'unico algoritmo accettato per la generazione di tale hash è SHA-256.

### 5.1.2 Time-Stamp Response

A seguito della ricezione di una Time-Stamp Request valida, l'applicazione fornisce come risposta sempre una Time-Stamp Response (in accordo con la definizione data in IETF RFC 3161, par. 2.4.2), opportunamente codificata all'interno di una risposta HTTP con Content-Type uguale a:

application/timestamp-reply

In particolare, in accordo con ETSI EN 319 422, i campi *accuracy* e *nonce* sono supportati e vengono utilizzati nei casi previsti dalle specifiche.

Nei casi in cui la marca temporale non possa essere emessa, viene prodotta una Time-Stamp Response contenente un codice di errore specifico che identifica la natura del problema, in tutti gli altri casi, la risposta contiene un Time-Stamp Token, che è la rappresentazione formale della marca temporale.

La firma apposta sulla marca temporale dalla TSA di Register utilizza l'algoritmo RSA a chiavi asimmetriche, con una chiave di lunghezza non inferiore ai 2048 bit.

### 5.2 Certificato della TSU

Per l'emissione delle marche temporali, la TSA Register utilizza una o più unità denominate TSU (Time-Stamping Unit), che erogano effettivamente il servizio di marcatura temporale per conto della TSA.

La TSU appone una firma digitale sulle marche che emette, utilizzando l'algoritmo RSA con una coppia di chiavi asimmetriche, specifica e diversa per ogni unità.

Il certificato associato alle chiavi della TSU è conforme alle specifiche ETSI EN 319 412-3 e ETSI EN 319 422: in particolare sono opportunamente valorizzati gli attributi *countryName*, *organizationName*, *organizationIdentifier* e *commonName*. Quest'ultimo, in particolare, identifica in modo univoco una specifica TSU appartenente alla TSA di Register.

Inoltre, come specificato in IETF RFC 3161, nel certificato è specificato come *Extended Key Usage* l'OID corrispondente all'emissione di marche temporali (1.3.6.1.5.5.7.3.8).

La lunghezza della chiave associata al certificato è pari almeno a 2048 bit.

Il certificato ha una durata di 90 giorni.

### 5.3 Accuratezza del riferimento temporale

L'accuratezza del riferimento temporale utilizzato dalla TSA di Register per l'apposizione delle marche temporali è *'better than'* 1 secondo, in accordo con la Best practices Time-Stamp Policy (BTSP) definita nella specifica ETSI EN 319 421.

Per garantire che questo vincolo venga rispettato, viene utilizzato un sistema basato sul protocollo NTP: su ogni macchina TSU è installato un NTP client che ha il compito di mantenere sincronizzato l'orologio di sistema con il riferimento temporale dei time server interni di Register che, a loro volta, regolano il proprio orologio con gli orologi dei time server di riferimento per il segnale UTC. Questa piattaforma è compliant con il Network Time Protocol descritto nelle specifiche IETF RFC 5905.

I time server interni di Register realizzano un sistema di sincronizzazione continua con i server di riferimento configurati, scegliendo quello con la distanza temporale minore, in maniera dinamica.

Per ognuno dei time server interni di Register sono configurati diversi server di riferimento *stratum 1* (ossia time server che sincronizzano il proprio orologio interno con un orologio atomico), scelti per

essere raggiungibili su percorsi di rete differenti, in modo da minimizzare la possibilità che un problema di rete geografico dei carrier impedisca la sincronizzazione continua della piattaforma interna.

Avendo degli *stratum 1* come server di riferimento, i time server interni di Register sono degli *stratum 2*, ognuno dei quali è configurato come peer degli altri, formando così un'isola che anche in assenza totale di connessione verso l'esterno deriva meno velocemente di quello che può derivare un singolo server.

I time server interni sono sottoposti a revisione periodica, in modo da verificare costantemente che i time server di riferimento siano raggiungibili e che continuino ad essere degli *stratum 1*. Il rapporto con i server di riferimento viene aggiornato in maniera dinamica: qualora uno dei server di riferimento configurati diventasse migliore (ossia con un delay inferiore) o quello scelto precedentemente iniziasse a derivare (jitter in costante aumento), il time server farebbe riferimento al nuovo *stratum 1*.

I vari server TSU, tramite il loro client NTP, si sincronizzano con i time server interni di Register, diventando quindi degli *stratum 3* e implementando lo stesso processo di sincronizzazione continua e di scelta dinamica del riferimento illustrata per i time server interni, scartando e sostituendo a priori un time server interno che andasse fuori sincrono.

Qualora il sistema di monitoraggio dovesse rilevare che l'orologio di riferimento di una delle TSU avesse uno scostamento maggiore di 1 secondo rispetto all'orario UTC, la macchina corrispondente verrebbe automaticamente rimossa dal cluster e pertanto non sarebbe più utilizzata per l'emissione delle marche temporali, fino a che il suo orologio interno non risulti nuovamente sincronizzato e la macchina venga quindi ripristinata per l'erogazione del servizio.

### 5.4 Log

Il sistema della TSA di Register produce una serie di log di natura diversa, ognuno dei quali viene registrato e successivamente conservato per il periodo di tempo richiesto dalla normativa vigente.

In particolare vengono prodotti:

- *Log di accesso fisico*: tutti gli accessi fisici ai locali, alle macchine e ai dispositivi che compongono il sistema di marcatura temporale vengono registrati in un apposito log
- *Log di sincronizzazione*: le operazioni di sincronizzazione dell'orologio di sistema effettuate in accordo con il protocollo NTP vengono registrate in un log specifico
- *Log di sicurezza*: le operazioni di generazione, installazione e revoca dei certificati utilizzati dalla TSU sono soggette a registrazione in appositi log
- *Log di traffico*: le interazioni con il servizio di marcatura temporale da parte di client producono dei log di traffico HTTP, che vengono opportunamente trattati

- *Log applicativi*: l'applicazione che gestisce il funzionamento della TSU produce dei log applicativi che registrano l'emissione delle marche temporali

### 5.5 Verifica della marca temporale

La verifica delle marche temporali emesse dalla TSA di Register può essere effettuata con i seguenti passi:

a. Generazione dell'hash in SHA-256 a partire dai dati originari
b. Combinazione dell'hash con il timestamp riportato all'interno della marca temporale
c. Verifica della firma presente nella marca temporale utilizzando la chiave pubblica della TSU
d. Verifica formale del certificato della TSU e della sua validità

Qualsiasi software che soddisfi le specifiche dell'IETF RFC 3161 può portare a termine il processo appena descritto in modo automatico.

# 6. Gestione e manutenzione della TSA

## 6.1 Misure di sicurezza (fisica, procedure, personale)

Le misure di sicurezza logica e fisica seguono quanto definito e descritto all'interno del piano della sicurezza e le procedure in esso richiamate.

## 6.2 Gestione dei controlli crittografici

### 6.2.1 Generazione e installazione delle chiavi della TSU

Ogni 90 giorni la chiave di firma della TSU viene generata direttamente sugli HSM tramite la apposita appliance di gestione e lo stesso è per la relativa CSR.

Una volta firmato, il certificato viene importato sempre negli HSM e accoppiato alla chiave di firma.

### 6.2.2 Protezione della chiave privata

La chiave privata è contenuta all'interno degli HSM Thales  e non è esportabile. Gli HSM presenti nella piattaforma sono due, acceduti tramite un sistema di bilanciamento e due appliance sempre di Thales, in modo da assicurare la continuità di funzionamento.

### 6.2.3 Certificato pubblico della TSU

I certificati pubblici della TSU saranno reperibili direttamente su internet senza bisogno di autenticazioni tramite un web server dedicato con connessione sicura (https) che fornisce solo questo servizio.

## 6.3 Manutenzione del software

### 6.3.1 Aggiornamento delle applicazioni proprietarie

Il core applicativo della TSU è costituito da un software proprietario, sviluppato in linguaggio Java. Ogni modifica a tale software è soggetta alle procedure interne di change management del TSP Register e prevede, in aggiunta, l'esecuzione di un'apposita suite di test, che copre i principali requisiti tecnici specificati in IEFT RFC 3161 e in ETSI EN 319 422, al fine di verificare che una eventuale modifica non vada a compromettere l'erogazione delle funzionalità di base del sistema.

La piattaforma di monitoraggio, inoltre, verifica costantemente a intervalli regolari che il servizio di marcatura temporale venga erogato correttamente e che le marche che vengono prodotte siano valide e conformi alle specifiche.

### 6.3.2 Aggiornamento dei software di terze parti

Sistemi operativi e appliance crittografica sono sistematicamente aggiornati per security bug tramite i canali ufficiali dei vendor. I dettagli di procedura sono descritti nelle procedure interne richiamate nel piano della sicurezza.

## 6.4 Piano di cessazione della TSA

Nel caso la TSA di Register dovesse cessare la propria attività, verrà messa in atto la procedura descritta di seguito:

a. Viene comunicata l'intenzione di terminare il servizio ad AgID e agli utenti, con un anticipo di almeno 60 giorni rispetto alla data prevista di cessazione

b. Register si impegna a mantenere accessibili i certificati e le chiavi pubbliche per la verifica delle marche temporali già emesse per un periodo di tempo ragionevole dopo la cessazione o in alternativa a trasmetterle a un soggetto sostituivo che li renderà disponibili per il medesimo periodo

c. Al momento della cessazione del servizio, tutte le chiavi private delle TSU verranno distrutte in modo irreversibile e si procederà alla revoca dei certificati corrispondenti

## 6.5 Gestione degli incidenti e Risk Assessment

La gestione degli incidenti e l'analisi del rischio è riportata all'interno del Piano della Sicurezza del servizio di Marcatura Temporale.