Manuale Operativo
per il Servizio di Validazione Temporale Elettronica Qualificata

Notartel S.p.A – S.B.

Versione: 1.1

Data: 30/07/2024

SOMMARIO

VERSIONI DOCUMENTO

VERSIONE	DESCRIZIONE MODIFICA	DATA EMISSIONE
1.0	Prima emissione	1 marzo 2022
1.1	• Aggiornamento dei riferimenti normativi e dei dati identificativi di Notartel; • Revisione del capitolo 6 “Tariffe”.	30 luglio 2024

DEFINIZIONI AI FINI DEL PRESENTE MANUALE OPERATIVO

DEFINIZIONE	DESCRIZIONE
AgID	Agenzia per l'Italia Digitale. Ente Nazionale per la digitalizzazione della Pubblica Amministrazione. Sostituisce il CNIPA e DigitPA.
Certificato	Documento informatico in formato ITU X.509 v.3 o successivo contenente informazioni relative al Titolare e alla sua chiave pubblica di firma, firmato da un prestatore di servizi fiduciari, con la propria chiave privata di certificazione.
Certificato qualificato	Documento informatico, che attesta, con una firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto (persona fisica), rilasciato da prestatori di servizi fiduciari qualificati, che risponde ai requisiti del Regolamento UE 910/2014 nonché avente le caratteristiche fissate dal DPCM 22 febbraio 2013 e dalla Determinazione AgID n. 147/2019.
Certificatore	Certification Authority (CA) è l'ente pubblico o privato abilitato a rilasciare certificati tramite la procedura di certificazione che segue standard internazionali ed è conforme alla normativa interna e comunitaria in materia.
Certificazione	Il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto Titolare cui essa appartiene.
Chiave privata	Elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto Titolare, mediante il quale si appone la firma digitale sul documento informatico.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione. Sostituito da AgID
Coppia di chiavi	Coppia di chiavi asimmetriche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di firma digitale di documenti informatici.
CRL (Certificate Revocation List)	Lista firmata digitalmente, tenuta ed aggiornata dai prestatori di servizi fiduciari qualificati, contenente i certificati emessi dagli stessi stesso e successivamente sospesi o revocati.
Destinatario	Destinatario di un documento informatico firmato digitalmente.
DigitPA	Ente Nazionale per la digitalizzazione della Pubblica Amministrazione. Sostituito da AgID.
Dispositivo di firma	Un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali.

DEFINIZIONE	DESCRIZIONE
Dispositivo sicuro per la creazione di una firma	L'apparato strumentale, usato per la creazione di una firma elettronica, rispondente ai requisiti del DPCM 22 febbraio 2013.
Distinguished Name (Dname)	Identificativo univoco del Titolare presso il Prestatore di Servizi fiduciari qualificati.
Documento Informatico	La rappresentanza informatica di atti, fatti o dati giuridicamente rilevanti che non contiene macroistruzioni o codici eseguibili tali da attivare funzioni che possono modificare gli atti, i fatti o i dati nello stesso rappresentati.
Firma Qualificata	Firma basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Firma remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
Giornale di controllo	Insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche di base.
Local Registration Authority (LRA)	È la persona fisica o giuridica delegata dal Certificatore allo svolgimento delle operazioni di emissione dei Certificati, secondo le modalità individuate e descritte nel presente Manuale. L'ente deve aver preventivamente stipulato accordi di servizio con il Certificatore. L'LRA può avvalersi di RAO per le operazioni identificazione, registrazione ed emissione
Manuale operativo	Documento pubblico depositato presso il AgID che definisce le procedure applicate dal prestatore di servizi fiduciari qualificati che rilascia certificati qualificati nello svolgimento della propria attività.
Marca temporale	Il riferimento temporale che consente la validazione temporale.
Notartel S.p.A. – S.B.	Società informatica del Consiglio Nazionale del Notariato (CNN), ente pubblico non economico, istituito con legge 3 agosto 1949, n. 577, qui in veste di CA
OTP	One Time Password – password valida per una singola sessione di accesso o di firma costituita da codici numerici
PIN (Personal Identification Number)	Numero di identificazione personale.
PKCS (Public Key Cryptographic Standard)	Standard tecnici per applicazioni crittografiche, realizzati dalla RSA Laboratories della EMC2 Corporation.
PKI (Public Key Infrastructure)	Infrastruttura a Chiave pubblica.
Prestatore di Servizi Fiduciari	Trusted Service Provider, ad esempio, Certificatore accreditato, Conservatore accreditato, etc., ai sensi del Regolamento UE 910/2014.

DEFINIZIONE	DESCRIZIONE
PUK (Personal Unlock Key)	Chiave personale di sblocco del PIN.
QSCD	Qualified Signature Creation Device, il dispositivo di firma certificato.
QTSP	Un prestatore di servizi fiduciari qualificato fornisce servizi fiduciari che soddisfano i requisiti stabiliti dal Regolamento eIDAS e ne fornisce le relative garanzie in termini di sicurezza e qualità.
Registration Authority (RA)	Soggetto che esegue l'identificazione dei Richiedenti dei certificati qualificati applicando le procedure definite dal Certificatore.
Registration Authority Operator (RAO)	Soggetto espressamente delegato allo svolgimento, per conto della CA, delle operazioni di identificazione e registrazione del Titolare, nonché l'emissione dei Certificati.
Registrazione	Attività d'acquisizione, verifica e archiviazione dei dati dei richiedenti.
Registro dei certificati	Registro contenente i certificati emessi dal prestatore di servizi fiduciari qualificati, la lista dei certificati revocati e la lista dei certificati sospesi, accessibile anche telematicamente.
Revoca del certificato	Operazione con cui il prestatore di servizi fiduciari qualificati annulla la validità del certificato da un dato momento in poi.
Richiedenti	I richiedenti sono tutti coloro che lavorano in ambito notarile.
Riferimento temporale	Informazione contenente la data e l'ora che viene associata ad uno o più documenti informatici.
Sospensione del certificato	Operazione con cui il Prestatore di Servizi fiduciari qualificati sospende la validità del certificato da un dato momento e per un determinato periodo di tempo.
SSL (Secure Socket Layer)	Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica
Titolare	Cittadino a favore del quale è stato emesso un certificato firma qualificato da Notartel S.p.A. – S.B.
TSA CA	Certification Authority dedicata al servizio di marcatura temporale che ha la principale funzione di emettere i certificati con i quali vengono rilasciate le marche temporale.
TSP	Trusted Service Provider, prestatore di servizi fiduciari (es. Prestatore di Servizi Fiduciari accreditato, Conservatore accreditato, etc.) ai sensi del Regolamento 910/2014
TSS / TSU	Time Stamping Server, o Time Stamping Unit, è un componente che emette e firma le marche temporali che gli utenti inoltrano alla Time Stamping Authority utilizzando i certificati emessi dalla TSA CA.
Validazione temporale	Risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, un riferimento temporale opponibili ai terzi.

1 INTRODUZIONE

1.1 Scopo del documento

Questo documento definisce le procedure seguite da **Notartel S.p.A. – S.B.** nello svolgimento dell'attività di prestatore di servizi fiduciari che eroga un servizio di validazione temporale elettronica qualificata ai sensi del Regolamento 910/2014 – eIDAS (nel seguito "regolamento").
Esso si riferisce al servizio di:

- Generazione di marche temporali qualificate.

Il manuale operativo vincola il prestatore di servizi fiduciari e tutti i soggetti che entrano in relazione con esso.
Il presente documento definisce inoltre gli obblighi e le responsabilità del prestatore di servizi fiduciari, degli utenti e di quanti accedono ai servizi per la verifica della marca temporale qualificata.
Il servizio è configurato secondo la normativa vigente e recepisce eventuali obblighi aggiuntivi ascrivibili direttamente o indirettamente per l'applicazione delle marche temporali.

1.2 Riferimenti normativi

Il Manuale Operativo è conforme a quanto previsto dalla comunitaria e interna e, in particolare a:

- Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
- Decisione di esecuzione (UE) 2015/1505 della Commissione, dell'8 settembre 2015, che stabilisce le specifiche tecniche e i formati relativi agli elenchi di fiducia di cui all'articolo 22, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
- Decisione di esecuzione (UE) 2016/650 della Commissione, del 25 aprile 2016, che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
- Decisione di esecuzione (UE) 2015/1506 della Commissione, dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

- Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale (CAD) e successive modifiche ed integrazioni.
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
- Art. 15, comma 2, Legge 15 marzo 1997 n. 59.
- Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.
- Determinazione n. 185/2017 - Modalità per la domanda di qualificazione per i servizi eIDAS - sostituisce la Circolare n. 48/2005.
- Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate (Determinazione AgID n. 147/2019 rettifica per errore materiale la Determinazione AgID n.121/2019).
- CNIPA, Deliberazione n. 45, del 21 maggio 2009 e successive modificazioni - La presente deliberazione ha abrogato: Deliberazione CNIPA 17 febbraio 2005 n. 4, Deliberazione CNIPA 18 maggio 2006 n. 34 Regole per il riconoscimento e la verifica del documento informatico.
- DigitPA - Determinazione Commissariale n. 69/2010 - Modifica della Deliberazione CNIPA 21 maggio 2009, n. 45, "Regole per il riconoscimento e la verifica del documento informatico",
- CNIPA Limiti d'uso nei CQ - Limiti d'uso garantiti agli utenti ai sensi dell'articolo 12, comma 6, lettera c) della Deliberazione CNIPA 21 maggio 2009, n. 45.

Si precisa che i riferimenti normativi indicati in precedenza e nel prosieguo del presente manuale dovranno intendersi anche relativi alle norme in corso di emanazione in materia, modificative o sostitutive di quelle attualmente vigenti.

Vai al sommario

2 DATI IDENTIFICATIVI DEL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI

I dati identificativi relativi alla Notartel S.p.A. – S.B. sono i seguenti:

Denominazione e Ragione sociale:	Notartel S.p.A. – S.B.
Sede legale:	Via Giovanni Vincenzo Gravina 4, 00196 Roma
Rappresentante legale:	Gian Mario Braido
Telefono: +39- 0636769300	Fax: +39 0632650077
Sedi operative: Via Flaminia 160, 00196 Roma Via Giovanni Vincenzo Gravina 4, 00196 Roma Via Flaminia 133-135, 00196 Roma	Indirizzo E-mail: notartel.amministrazione@postacertificata.notariato.it esercizio@postacertificata.notariato.it
Indirizzi Internet: https://ca.notartel.it https://www.notartel.it	Customer Care: customercare@notartel.it

Vai al sommario

3 MANUALE OPERATIVO

3.1 Dati identificativi del Manuale operativo

Il presente Manuale operativo pubblicato da Notartel S.p.A. – S.B. e depositato presso il AgID, è identificato col nome "MO_NTL_TSA_v1.1_20240730" ed è consultabile per via telematica all'indirizzo Internet:

https://ca.notartel.it

Il presente documento è identificato con il numero di versione 1.1
Il presente Manuale Operativo è, inoltre, referenziato dai seguenti OID (Object Identifier Number):
1.3.6.1.4.1. 41870.1.2.5 Servizio di marcatura temporale qualificata
In aggiunta, si definisce in questo stesso manuale una policy per il rilascio delle marche temporali che sarà referenziato attraverso il seguente OID.
0.4.0.2023.1.1 Policy di marcatura temporale ETSI (in conformità allo standard ETSI EN 319 421 v1.2.1)

Tali OID identificano:

Notartel S.p.A. – S.B.	1.3.6.1.4.1.41870
Certification Service Provider	1.3.6.1.4.1.41870.1
Certificate Policy	1.3.6.1.4.1.41870.1.1
Policy di marcatura temporale	1.3.6.1.4.1.41870.1.2
Servizio marcatura temporale qualificata (ambito europeo)	1.3.6.1.4.1.41870.1.2.1
Policy di marcatura temporale qualificata ETSI	0.4.0.2023.1.1

Il Prestatore di Servizi fiduciari qualificati si riserva la possibilità di pubblicare ulteriori CP qualora avesse necessità di rilasciare certificati caratterizzati da certificate policy differenti, in conformità agli standard dichiarati nel presente manuale operativo.

3.2 Responsabile del Manuale operativo

La responsabilità del presente Manuale Operativo è del Certificatore, nella figura del Responsabile del Servizio.

3.3 Tipologia delle utenze

La Notartel S.p.A. – S.B. rilascia esclusivamente marche temporali utilizzate dagli utenti.
Ai fini del presente documento, i termini marca temporale e marca temporale qualificata sono sinonimi e sono riferiti alla validità della stessa in ambito europeo ai sensi del regolamento UE 910/2014; eventuali eccezioni saranno espressamente riportate.

Vai al sommario

4 TERMINI E CONDIZIONI

4.1 Obblighi del prestatore di servizi fiduciari

Il servizio erogato dal prestatore di servizi fiduciari è stato valutato, e periodicamente viene rivalutato, in conformità alle direttive del Regolamento eIDAS e degli standard ETSI vigenti e ai requisiti contenuti nel presente manuale operativo.
Inoltre, nello svolgimento della sua attività, il prestatore di servizi fiduciari:

1. adotta tutte le misure organizzative e tecniche idonee ad evitare danno a terzi;
2. emette e gestisce le marche temporali qualificate in modo conforme alla normativa europea, con le procedure descritte nel presente manuale operativo;
3. identifica con certezza il richiedente;
4. si attiene alle regole tecniche emanate in seguito a regolamento UE 910/2014;
5. si attiene alle misure minime di sicurezza per il trattamento dei dati personali al Regolamento UE 679/2016;
6. genera le marche temporali mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'accuratezza del riferimento temporale con precisione inferiore al secondo (accuracy < 1s);
7. conserva i riferimenti delle marche temporali per un periodo di tempo almeno pari al minimo di quello indicato dalla normativa in vigore;
8. comunica per iscritto a AgID ogni variazione dei requisiti per l'iscrizione all'Elenco pubblico dei prestatori di servizi fiduciari ai sensi del regolamento, e, in ogni caso, periodicamente conferma la permanenza dei requisiti per l'esercizio dell'attività di validazione temporale;
9. comunica tempestivamente a AgID, ogni variazione significativa delle soluzioni tecnico-organizzative adottate;
10. comunica tempestivamente a AgID e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso;
11. comunica ad AgID ed agli utenti, con un preavviso di almeno sei mesi, la cessazione dell'attività, specificando che tutti i certificati dei componenti TSS / TSU, non scaduti al momento della cessazione, devono essere revocati.

4.2 Obblighi dell'utente

L'utente è tenuto ad assicurare la custodia delle credenziali di accesso al servizio e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente le marche temporali richieste.
L'utente deve, inoltre:

1. fornire tutte le informazioni richieste dal prestatore di servizi fiduciari, garantendone, sotto la propria responsabilità, l'attendibilità;

2. conservare con la massima diligenza e riservatezza le informazioni di abilitazione all'uso del servizio di marcatura temporale;
3. attivare e mantenere costantemente aggiornati strumenti che si oppongano all'inserimento di codice malevolo (malware) nel sistema utilizzato per apporre le marche temporali e che, ove esso sia presente, siano in grado di individuarlo, nel qual caso l'utente è tenuto a curarne l'eliminazione;
4. redigere per iscritto la richiesta di disattivazione del servizio, specificando la sua decorrenza.

È vietata la cessione delle credenziali di accesso al servizio a terzi.

4.3 Obblighi dei destinatari

I destinatari delle marche temporali devono verificare:

1. la validità del certificato di TSS / TSU che ha firmato la marca temporale;
2. l'assenza del certificato di TSS / TSU dalle Liste di Revoca dei certificati (CRL) del prestatore di servizi fiduciari;

e in caso di marca temporale qualificata:

3. che il certificato di CA della TSA sia presente nella lista dei servizi fiduciari qualificati pubblicata da Agid (https://eidas.agid.gov.it/TL/TSL-IT.xml)

e opzionalmente:

4. che la precisione del riferimento temporale sia inferiore al secondo;
5. che la marca temporale contenga l'estensione esi4-qtstStatement-1;
6. che la marca temporale contenga l'OID 0.4.0.2023.1.1.

4.4 Reclami

Il Titolare ha facoltà di inviare un reclamo in merito al servizio di erogazione dei certificati qualificati ai contatti di seguito riportati.

- Telefono: +39 - 0636769306
- Fax: + 39 - 0632650077
- E-mail: customercare@notartel.it

4.5 Legge Applicabile – Foro Competente

Per quanto ivi non esplicitamente previsto nel presente Manuale si applicano le norme del Codice. Ogni controversia che dovesse sorgere tra le parti in relazione all'esecuzione del servizio di erogazione dei certificati qualificati, regolato dal presente Manuale, sarà devoluta alla competenza esclusiva del Foro di Roma.

Vai al sommario

5 RESPONSABILITÀ E LIMITI D'USO

5.1 Responsabilità del prestatore di servizi fiduciari

Il prestatore di servizi fiduciari è responsabile verso gli utenti, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal Regolamento (UE) 910/2014, dal Regolamento UE 679/2016, dal D. Lgs. n. 82/05, dalla deliberazione 185/2017, dalla Determinazione AgID n. 147/2019, dal D. Lgs. 159/2006, dal D.P.C.M. 22 febbraio 2013.
La Notartel S.p.A. – S.B. è responsabile nei confronti di qualunque soggetto faccia ragionevole affidamento sulle marche temporali emesse dallo stesso, nei limiti di cui all'art. 30 del D.Lgs. n. 82/2005. L'esistenza e la validità del certificato di TSA non dispensano però l'utente dall'eseguire ogni altra verifica che appaia opportuna secondo criteri di oculata prudenza, anche in relazione al rilievo, economico o d'altra natura, degli interessi coinvolti. La responsabilità della Notartel S.p.A. – S.B. è comunque rigorosamente circoscritta a:

- l'esattezza delle informazioni contenute nella marca temporale alla data e ora di rilascio, ivi compresa la precisione del riferimento temporale, e la loro completezza rispetto ai requisiti fissati per le marche temporali;
- la garanzia che, al momento del rilascio della marca temporale, l'utente detenesse i privilegi per la richiesta.

È esclusa qualunque responsabilità della Notartel S.p.A. – S.B., anche di natura sussidiaria, in relazione a fatti diversi da quelli sopra enunciati, ed in particolare per fatti riconducibili alla sfera operativa del titolare, ivi compresi, a titolo esemplificativo, il mancato rispetto delle procedure, vizi formali o sostanziali relativi al documento marcato ed al suo contenuto, lo smarrimento o la sottrazione o l'incauto affidamento ad altro soggetto delle credenziali di accesso al servizio, l'erronea identificazione del documento sottoposto alla procedura di firma.
È altresì esclusa qualsivoglia responsabilità della Notartel S.p.A. – S.B. laddove i terzi non si attengano alle prescrizioni stabilite dal presente documento ed in particolare non rispettino le procedure stabilite per la verifica delle marche temporali o facciano affidamento su di esse al di fuori dei casi e dei limiti previsti dal relativo certificato.
Ogni responsabilità è comunque esclusa laddove la Notartel S.p.A. – S.B. provi d'aver agito senza colpa, ed in ogni caso in cui la responsabilità è esclusa dall'art. 30 del D. Lgs. n. 82/2005.

Vai al sommario

6 TARIFFE

L'emissione di una marca temporale può comportare l'addebito al richiedente di un importo in euro. In caso di richiesta di più marche temporali contestuali l'addebito sarà effettuato per ciascuna marca temporale richiesta.

Le tariffe per l'emissione di una marca temporale sono pubblicate sul portale dei servizi della Notartel S.p.A. – S.B. all'indirizzo https://ca.notartel.it/ all'interno della sezione "Condizioni di Servizio".

Vai al sommario

7 IDENTIFICAZIONE E REGISTRAZIONE

7.1 Registrazione e identificazione

La registrazione ed identificazione degli utenti è svolta dal prestatore di servizi fiduciari che provvede ad acquisire tutti i dati necessari all'abilitazione del servizio di validazione temporale elettronica qualificata secondo quanto indicato nel Manuale Operativo della Certification Authority della Notartel S.p.A. – S.B.
Tali dati sono inseriti nell'archivio di registrazione della Notartel S.p.A. – S.B. ai fini dell'emissione delle marche temporali.

7.2 Comunicazioni tra il prestatore di servizi fiduciari e gli utenti

Il prestatore di servizi fiduciari utilizza la casella di posta elettronica presente nei propri archivi per inviare comunicazioni all'utente.
L'eventuale variazione dell'indirizzo di posta elettronica dovrà essere comunicata alla Notartel S.p.A. – S.B. con messaggio sottoscritto dall'utente.

Vai al sommario

8 SERVIZIO DI VALIDAZIONE TEMPORALE E RIFERIMENTO TEMPORALE DEL PRESTATORE DI SERVIZI FIDUCIARI

La Notartel S.p.A. – S.B. fornisce un servizio di validazione temporale elettronica qualificata di documenti informatici, siano essi firmati digitalmente o non firmati, ai sensi del Regolamento UE 910/2014.
Il servizio di marcatura temporale permette di associare un riferimento temporale ai documenti elettronici in modo da garantire inequivocabilmente l'esistenza del documento informatico in un determinato istante temporale.
La marca temporale è una struttura dati firmata digitalmente che lega in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo (data e ora), provandone l'esistenza a quella data e ora.
La marca temporale viene firmata ed emessa da una specifica autorità denominata Time Stamping Authority (TSA) che emette e firma le marche temporali mediante uno o più sistemi dedicati (Time Stamping Server, TSS o TSU) al quale gli utenti indirizzano le loro richieste.
Una Certification Authority (TSA CA), dedicata ed inclusa nella lista dei servizi fiduciari qualificati pubblicata da Agid, emette i certificati con i quali i TSS firmano le marche temporali, ed è gestita in conformità a quanto indicato nel manuale operativo della Certification Authority della Notartel S.p.A. – S.B.
La verifica di una marca temporale comporta la verifica della catena di certificazione TSS - TSA CA.

8.1 Generazioni chiavi

La generazione della coppia di chiavi è effettuata mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata.
Il sistema di generazione delle chiavi assicura:

- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- l'equiprobabilità di generazione di tutte le coppie possibili.

La generazione delle chiavi avviene all'interno di un dispositivo sicuro.

8.2 Lunghezza delle chiavi di marcatura temporale

La lunghezza delle chiavi di marcatura temporale è di almeno 2048 bit.

8.3 Algoritmi

Per la generazione e la verifica delle marche temporali è usato il seguente algoritmo:

- RSA (Rivest-Shamir-Adleman algorithm).

La funzione di hash utilizzata per la generazione dell'impronta è:

- SHA-256 (Dedicated Hash Function 4).

8.4 Chiavi di marcatura temporale

8.4.1 Generazione delle chiavi di marcatura temporale

La generazione delle chiavi di marcatura temporale qualificata avviene con le stesse modalità previste per la generazione delle chiavi di certificazione.

8.4.2 Certificazione delle chiavi di marcatura temporale

Per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale sono utilizzate chiavi di certificazione diverse da quelle utilizzate per i certificati relativi alle chiavi di sottoscrizione.

8.4.3 Scadenza delle chiavi di marcatura temporale

Le chiavi di marcatura temporale hanno durata massima coincidente con la scadenza della CA che le certifica e sono sostituite dopo periodo congruo con la sicurezza e l'affidabilità degli algoritmi scelti e della lunghezza delle chiavi, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato, in conformità agli standard ETSI.

8.5 Richiesta di emissione o di verifica di marca temporale qualificata

La richiesta di emissione di marca temporale qualificata può essere effettuata utilizzando il software di firma fornito dalla Notartel S.p.A. – S.B., che consente di apporre la marca temporale a documenti informatici, anche firmati digitalmente, e di eseguire le operazioni di verifica.
La verifica deve essere effettuata tramite il software di firma oppure tramite il verificatore online, forniti dalla Notartel S.p.A. – S.B. o da altro prestatore di servizi fiduciari accreditato nell'elenco dei servizi fiduciari tenuto dall'AgID.
La richiesta è inoltrata al server TSS che la elabora, genera la marca temporale e la rinvia al client, che restituisce all'utente l'esito della richiesta.
Per la richiesta di emissione di marca temporale, l'utente seleziona il documento informatico da marcare e il formato della marca temporale; l'opportuna procedura software ne calcola l'hash, che invia poi al TSS per la marcatura; l'utente riceve in risposta un unico file nel formato prescelto contenente la marca temporale.
I formati possibili sono:

- Time stamp response, previsto dalla normativa vigente, contiene la sola marca temporale;
- Timestamped Data, previsto dalla normativa vigente, contiene la marca temporale e il documento a cui è associata.

Per la richiesta di verifica di marca temporale, l'utente deve fornire, come dati in ingresso al software di verifica, il file contenente la marca temporale e, opzionalmente a seconda del formato utilizzato, il documento informatico a cui la marca è associata.
Il software di verifica della marca temporale svolge i seguenti controlli:

a) verifica la firma del TSS, validando la catena di certificazione, usando la chiave pubblica corrispondente alla chiave privata utilizzata per la generazione della marca temporale e la

chiave pubblica della CA corrispondente alla chiave privata che ha firmato il certificato del TSS;

b) verifica che il valore dell'impronta contenuto nella marca temporale corrisponda allo stesso valore dell'impronta che è stato inviato al TSS in fase di richiesta.

   Il software di verifica visualizza le seguenti informazioni:

   - data e ora di creazione della marca temporale;
   - numero seriale, identificativo della marca temporale;
   - identificativo dell'ente emittente la marca temporale;
   - conformità alla normativa vigente;
   - verifica dello stato del certificato del TSS;
   - gli algoritmi utilizzati per l'impronta e per la firma;

c) verifica se la marca temporale è una marca temporale qualificata.

   Il software di verifica controlla inoltre le seguenti informazioni:

   - presenza dell'OID relativo alla time-stamp policy ETSI;
   - valore dell'accuracy inferiore al secondo;
   - presenza dell'estensione esi4-qtstStatement-1.

   Durante la richiesta di emissione o verifica di marcatura temporale il software può segnalare all'utente eventuali anomalie.

8.6 Emissione di una marca temporale

L'emissione della marca temporale viene effettuata dal server TSS, gestito dal prestatore di servizi fiduciari, che è in grado di calcolare con precisione la data e l'ora di generazione della marca temporale con riferimento al Tempo Universale Coordinato (UTC), generare la struttura di dati contenente le informazioni necessarie.
La struttura dati della marca temporale contiene, tra le varie informazioni, l'impronta generata dall'utente e la data/ora corrente ottenuta da una fonte esatta.
Il server TSS appone la firma alla struttura dati generata, ottenendo la marca temporale.
Terminata la procedura di generazione della marca temporale, quest'ultima viene inviata all'utente.

8.7 Validità della marca temporale

La marca temporale è valida per l'intero periodo di conservazione a cura della Notartel S.p.A. – S.B. La Notartel S.p.A. – S.B. conserva le marche temporali qualificate per un periodo di tempo almeno pari a quello indicato dalla normativa in vigore.

8.8 Marca Temporale

8.8.1 Formato e contenuto della marca temporale

Il formato delle marche temporali ed il protocollo di colloquio con la TSA rispettano le specifiche tecniche riportate in RFC 3161 “Internet X.509 Public Key InfrastructureTime Stamp Protocol (TSP)” - PKIX Working Group IETF – Agosto 2001.
Ogni marca temporale qualificata emessa contiene tutte le informazioni richieste dalla normativa europea, ovvero:

- identificativo della Notartel S.p.A. – S.B.;
- numero di serie della marca temporale;
- algoritmo di sottoscrizione della marca temporale;
- identificativo del certificato del TSS relativo alla chiave di verifica della marca temporale;
- data ed ora di generazione, con riferimento al Tempo Universale Coordinato (UTC);
- algoritmo di hash utilizzato per generare l’impronta;
- valore dell’impronta del documento sottoposto a validazione temporale;
- la precisione del riferimento temporale;
- l’OID della policy di time-stamp richiesto dallo standard ETSI;
- l’estensione esi4-qtstStatement-1.

8.8.2 Accuratezza del riferimento temporale

In fase di generazione di una marca temporale, il server TSS ricava la data/ora dal clock del sistema, mantenuto allineato con l’ora esatta UTC (Tempo Universale Coordinato) grazie al segnale di sincronia ottenuto da un ricevitore esterno del segnale emesso dalla rete dei satelliti GPS.
Il segnale orario così ottenuto rispetta i margini di precisione richiesti dalla normativa ed è inferiore al secondo.
In caso di perdita della sincronizzazione del segnale orario il prestatore di servizi fiduciari non rilascia marche temporali fino al ripristino delle normali condizioni di funzionamento.

8.8.3 Verifica della marca temporale

Il sistema di verifica della marcata temporale deve:

- visualizzare le informazioni presenti contenute nella marca;
- verificare lo stato dei certificati di firma della marca temporale.

Per la verifica della marca temporale la Notartel S.p.A. - S.B. mette a disposizione un’applicazione di verifica raggiungibile dal sito: https://ca.notartel.it.
Mediante tale sistema è possibile verificare una marca apposta a documenti informatici secondo i formati definiti da AgID.

8.9 Tempi di emissione della marca temporale

La generazione delle marche temporali garantisce che il tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, a meno di impedimenti nell'emissione della marca stessa, non sarà superiore ai tempi previsti dalla normativa in vigore.

8.10 Registrazione delle marche generate

Tutte le marche temporali emesse, assieme alle relative richieste sono conservate in un apposito archivio digitale non modificabile per il periodo indicato dal prestatore di servizi fiduciari.
L'accesso ai dati, contenuti nei diversi archivi, è consentito solo agli operatori opportunamente abilitati.
L'utente può ottenere una copia della marca temporale facendone richiesta fornendo i seguenti dati:

- data di erogazione (*);
- ora di erogazione (*);
- numero seriale della marca;
- valore dell'impronta.

I dati contrassegnati con (*) sono OBBLIGATORI.

8.11 Sicurezza del sistema di validazione temporale

Il sistema per il servizio di marcatura temporale qualificata può essere attivato solo da operatori autorizzati.
Un eventuale arresto del sistema può essere risolto solamente dagli operatori autorizzati.
I dettagli operativi sono riportati nel Piano per la sicurezza del prestatore di servizi fiduciari.

8.12 Revoca di certificati relativi a chiavi di marcatura temporale

8.12.1 Circostanze di revoca

La revoca del certificato relativo ad una coppia di chiavi di marcatura temporale qualificata effettuata su iniziativa del prestatore di servizi fiduciari è consentita esclusivamente nei seguenti casi:

- compromissione della chiave privata;
- guasto del dispositivo di firma delle marche.

8.12.2 Procedura di revoca dei certificati relativi a chiavi di marcatura temporale

Il certificato revocato deve essere inserito in una lista di revoca aggiornata immediatamente e pubblicata, le stesse informazioni sono disponibili tramite servizio OCSP.
Della pubblicazione della CRL è fatta annotazione nel giornale di controllo.

8.12.3 Sostituzione delle chiavi di marcatura temporale

Conformemente a quanto stabilito dal presente manuale operativo, le chiavi di marcatura temporale sono sostituite dopo non più di tre mesi di utilizzo, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato.

Vai al sommario

9 PROTEZIONE DELLA RISERVATEZZA

9.1 Modalità di protezione della riservatezza

Tutti i dati che risiedono su database sono protetti da prodotti che implementano politiche di autorizzazione per l'accesso ai dati legati a meccanismi di autenticazione degli utenti.
Le misure di protezione adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali emanate con il Regolamento UE 679/2016.

Vai al sommario

10 GESTIONE DELLE COPIE DI SICUREZZA

Il prestatore di servizi fiduciari effettua periodicamente, e secondo politiche ben definite, copie di sicurezza del sistema di validazione temporale qualificata.
Tali copie sono mantenute in armadi di sicurezza siti in locali diversi e ugualmente protetti. In tal modo viene garantita l'integrità dei dati e la continuità del servizio di validazione temporale.
Le procedure per la gestione delle copie di sicurezza sono descritte nel Piano per la sicurezza.

Vai al sommario

11 DISPONIBILITÀ DEL SERVIZIO

Nell'ambito della strategia di *disaster recovery* adottata, è prevista l'esistenza, oltre ai due siti primari, di un sito di disaster recovery che garantisce, l'espletamento dei servizi di validazione temporale entro i tempi di ripristino previsti, a partire dalla dichiarazione di disastro.
Sono oggetto di disaster recovery i seguenti servizi:

- verifica Marche temporali: servizio di verifica della validità dei certificati con i quali sono state firmate le marche temporali.

Una opportuna architettura e delle apposite procedure permettono il ripristino dei servizi nei tempi dichiarati.
Il Prestatore di servizi fiduciari eroga i servizi sopra descritti nell'arco delle 24 h per 7 giorni a settimana, con una disponibilità pari al 99% su base annua.

Vai al sommario

12 GESTIONE DEGLI EVENTI CATASTROFICI

Il Prestatore di servizi fiduciari qualificati garantisce la continuità del servizio di verifica delle marche temporali, in caso di disastro, attraverso la predisposizione di opportune procedure che consentono il ripristino.
Le procedure per la gestione degli eventi catastrofici sono dettagliatamente descritte nel Piano per la sicurezza e nella Procedura di Disaster Recovery.

Vai al sommario

13 GIORNALE DI CONTROLLO

Tutte le richieste di validazione temporale sono annotate nel Giornale di controllo.

13.1 Dati da archiviare

Nel giornale di controllo sono annotati i seguenti eventi per il servizio di validazione temporale, cui è associata la data e l'ora dell'effettuazione:

1. la generazione dei certificati di TSS / TSU;
2. la revoca dei certificati di TSS / TSU emessi;
3. l'entrata e l'uscita dai locali protetti del sistema di generazione delle marche;
4. gli eventi di sincronizzazione temporale;
5. le richieste di marca temporale qualificata.

13.2 Conservazione dei dati e log

Le registrazioni sono effettuate indipendentemente su supporti distinti e di tipo differente. Esse riportano la data e l'ora in cui sono state effettuate e sono conservate per un periodo di tempo almeno pari al minimo di quello indicato dalla normativa in vigore.
La data e l'ora utilizzate provengono da NTP server la cui precisione è conforme alla normativa in vigore, e cioè discosta al massimo di 1 secondo dal tempo UTC (IEN).

13.3 Protezione dell'archivio

Il Giornale di controllo è tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza.

13.4 Gestione del Giornale di controllo

Vengono effettuate operazioni di back-up, controlli e report periodici.

13.5 Verifiche

L'integrità del Giornale di controllo è verificata con frequenza mensile.

Vai al sommario

14 CESSAZIONE DELL'ATTIVITÀ DEL PRESTATORE DI SERVIZI FIDUCIARI

In caso di cessazione dell'attività, il prestatore di servizi fiduciari comunica ad AgID la data di cessazione con un anticipo di sei mesi, indicando eventualmente il prestatore di servizi fiduciari sostitutivo e garantendo la conservazione delle informazioni fino alla scadenza dei certificati di TSA. Entro lo stesso periodo il prestatore di servizi fiduciari informa gli utenti del servizio, specificando che tutte le marche temporali qualificate emesse precedentemente al momento della cessazione sono valide e che tutti i certificati dei componenti TSS / TSU, non scaduti al momento della cessazione, devono essere revocati. Sono da ritenere non valide le marche eventualmente richieste in seguito alla revoca dei certificati di TSS / TSU.
AgID rende nota nell'elenco pubblico dei servizi fiduciari la data di cessazione.

Vai al sommario

Il presente manuale operativo è stato approvato dal Responsabile Servizio TSA.

Roma, 30/07/2024

Firmato digitalmente da
Pasquale Starace
C: IT