Manuale Operativo
per il servizio di certificazione
delle chiavi pubbliche

Notartel S.p.A - S.B.

Versione: 2.1

Data: 16/07/2024

SOMMARIO

VERSIONI DOCUMENTO

VERSIONE	DESCRIZIONE MODIFICA	DATA EMISSIONE
1.0	Prima emissione	1 marzo 2022
2.0	Introduzione firma one-shot	13 febbraio 2024
2.1	• Revisione capitolo 6 “Tariffe” • Revisione capitolo 7.2 “identificazione in VdC” • Inserimento capitolo 10.4 “Limiti d’uso certificati One-Shot”	16 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.
Certificato OneShot	Si intende certificato di firma elettronica qualificata per procedura remota disciplinato nel presente Manuale Operativo le cui chiavi, una volta generate, sono disponibili solo nell'ambito di un dominio informatico ed esclusivamente per la transazione di firma per le quali sono state emesse.
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 rappresentazione 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.
PUK (Personal Unlock Key)	Chiave personale di sblocco del PIN.

DEFINIZIONE	DESCRIZIONE
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 opponibile ai terzi.

1 INTRODUZIONE

1.1 Scopo del documento

Il presente documento rappresenta il Manuale Operativo del servizio di certificazione digitale erogato da Notartel S.p.A – S.B. (CP e CPS per il regolamento eIDAS) e ha come scopo la descrizione delle regole e delle procedure operative adottate dalla stessa Notartel per tutte le attività inerenti l'emissione e la gestione dei certificati di sottoscrizione qualificati, come previsto dal regolamento eIDAS (electronic IDentification Authentication and Signature) UE n° 910/2014 sull'identità digitale.

Ai fini del presente documento il contesto della gestione dei certificati riguarda due ambiti specifici:

1. il primo per l'emissione di certificati di sottoscrizione qualificati di durata triennale validi a tutti gli effetti di legge nell'ambito delle norme europee eIDAS;

2. il secondo si riferisce al rilascio certificati di firma denominati "OneShot", destinati all'uso esclusivo all'interno della Piattaforma del Notariato Italiano. Questi certificati hanno lo scopo specifico di abilitare i richiedenti a firmare digitalmente un atto notarile digitale o una procura e qualsiasi documento associato (come allegati, ecc.).

Il presente documento definisce, inoltre, gli obblighi e le responsabilità della Notartel S.p.A. – S.B., degli operatori in qualità di Registration Authority – RA e dei titolari dei certificati di sottoscrizione.

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.
- Circolare CNIPA 6 settembre 2005 - Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
- 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
Sede operativa: 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

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_CA_v2.1_20240716" ed è consultabile per via telematica all'indirizzo Internet: https://ca.notartel.it.
Il presente documento è identificato con il numero di versione 2.1.
Il presente Manuale Operativo è, inoltre, referenziato dai seguenti OID (Object Identifier Number):

Notartel S.p.A. – S.B.	1.3.6.1.4.1.41870
Certification Service Provider	1.3.6.1.4.1.41870.1
Policy CA Firma Qualificata	1.3.6.1.4.1.41870.1.1
Policy CA Timestamp	1.3.6.1.4.1.41870.1.2
Certificate-Policy per certificati emessi in conformità alla policy ETSI QCP-n-qscd (QSCD)	0.4.0.194112.1.2
Certificate-Policy per certificato qualificato emesso a persona fisica per firma remota su dispositivo qualificato.	1.3.6.1.4.1.41870.1.1.8
Certificate-Policy per certificato OneShot emesso a persona física per firma remota su dispositivo qualificato.	1.3.6.1.4.1.41870.1.1.9

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. certifica esclusivamente le chiavi pubbliche emesse nei confronti dei richiedenti e rilascia esclusivamente a tal fine certificati qualificati per supportare firme digitali generate mediante un dispositivo sicuro.
Pertanto, ai fini del presente documento, i termini certificato e certificato qualificato coincidono; eventuali eccezioni saranno espressamente riportate.

Vai al sommario

4 TERMINI E CONDIZIONI

4.1 Obblighi del Certificatore

Il servizio erogato da Notartel S.p.A. – S.B. 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, Notartel S.p.A. – S.B.:

1. adotta tutte le misure organizzative e tecniche idonee ad evitare danno a terzi;
2. emette e gestisce i certificati in modo conforme alla normativa italiana ed europea, con le procedure descritte nel presente Manuale Operativo;
3. rilascia e rende pubblico il certificato;
4. si accerta dell'autenticità della richiesta di emissione di un certificato;
5. richiede la prova del possesso della chiave privata e verifica il corretto funzionamento della coppia di chiavi, eventualmente richiedendo la sottoscrizione di uno o più documenti di prova;
6. si attiene alle misure minime di sicurezza per il trattamento dei dati personali di cui al Regolamento UE 679/2016;
7. genera le coppie di chiavi 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;
8. procede tempestivamente alla revoca od alla sospensione del certificato in tutti i casi previsti dal presente Manuale Operativo;
9. comunica le richieste di revoca o sospensione al Titolare;
10. fornisce o indica al Titolare i dispositivi sicuri di firma utilizzati nell'ambito del processo di rilascio del certificato qualificato per la generazione delle chiavi, la conservazione della chiave privata e le operazioni di firma, idonei a proteggere la chiave privata ed i dati per la creazione della firma del Titolare con criteri di sicurezza adeguati alla normativa vigente e alle conoscenze scientifiche e tecnologiche più recenti;
11. dà tempestiva pubblicazione della revoca e della sospensione del certificato;
12. conserva le richieste scritte di registrazione e le richieste di certificazione per un periodo di almeno 20 anni dalla data di scadenza del certificato;
13. comunica per iscritto ad AgID ogni variazione dei requisiti per l'iscrizione all'Elenco pubblico dei Certificatori accreditati ai sensi del D.P.C.M. 22 febbraio 2013 e all'art. 29 del Decreto Legislativo 7 marzo 2005 n.82, e, in ogni caso, periodicamente conferma la permanenza dei requisiti per l'esercizio dell'attività di certificazione;
14. comunica tempestivamente ad AgID, ogni variazione significativa delle soluzioni tecnico-organizzative adottate;
15. comunica immediatamente ad AgID e agli soggetti coinvolti eventuali malfunzionamenti che determinino disservizi, sospensioni o interruzioni del servizio stesso;

16. comunica ad AgID ed agli altri soggetti coinvolti, con un preavviso di almeno sei mesi, della cessazione dell'attività, della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento, specificando che tutti i certificati non scaduti al momento della cessazione devono essere revocati;
17. garantisce le condizioni del servizio descritto nel presente manuale per tutta la durata dello stesso, salvo modifiche rese necessarie da requisiti aggiuntivi o modifiche della normativa vigente;
18. in caso di modifica alle condizioni del presente manuale operativo fornisce informativa agli altri soggetti coinvolti titolari ed ai destinatari mediante pubblicazione del manuale aggiornato sul sito della CA;
19. si attiene alle indicazioni di AgID in caso di compromissione degli algoritmi utilizzati;
20. assicura la precisa determinazione della data e dell'ora di rilascio, scadenza, revoca e sospensione dei certificati qualificati;
21. registra sul giornale di controllo, l'emissione dei certificati qualificati, con la specificazione della data e dell'ora di generazione; il momento di generazione del certificato è attestato tramite riferimento temporale;
22. fornisce almeno un sistema che consenta ai soggetti coinvolti di effettuare la verifica della firma qualificata.

4.2 Obblighi dell'operatore in qualità di Registration Authority

L'operatore RA, (Registration Authority Officer - RAO), ha l'obbligo di:

1. identificare con certezza il soggetto richiedente;
2. informare espressamente, in modo compiuto e chiaro, il Titolare (richiedente) riguardo agli obblighi in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi di firma, nonché sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
3. consegnare quanto è necessario per l'utilizzo del dispositivo di firma;
4. revocare i certificati tutte le volte in cui ciò si renda necessario;
5. riattivare i certificati sospesi;
6. richiedere la sostituzione delle chiavi di firma dei titolari in accordo con i relativi paragrafi del presente manuale;
7. informare il Titolare delle misure di sicurezza adottate per il trattamento dei dati personali, ai sensi della normativa vigente;
8. comunicare alla Notartel S.p.A. – S.B. tutti i dati e documenti acquisiti durante l'identificazione del Titolare e previsti dalle procedure del Certificatore al fine di attivare tempestivamente la procedura di emissione del certificato;
9. verificare ed inoltrare alla Notartel S.p.A. – S.B. le richieste di revoca/sospensione richieste dal Titolare;

10. assicurarsi che il Titolare abbia preso visione delle Condizioni Generali di contratto;
11. consegnare al Titolare copia della documentazione di richiesta di emissione del Certificato dallo stesso sottoscritta.

4.3 Obblighi del Titolare

Il Titolare è tenuto ad assicurare la custodia dei codici personali per l'apposizione della firma e a adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente le chiavi di firma.

Il Titolare deve, inoltre:

1. prendere visione del presente documento prima di richiedere il Certificato qualificato e rispettarne le prescrizioni per quanto di propria competenza;
2. fornire tutte le informazioni richieste dalla RA, garantendone, sotto la propria responsabilità, l'attendibilità;
3. conservare con la massima diligenza i codici personali al fine di garantire l'integrità e la conservazione delle informazioni di abilitazione all'uso della chiave privata;
4. mantenere in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma;
5. accertare che il documento da sottoporre alla firma non contenga macroistruzioni o codici eseguibili, tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati nello stesso rappresentati;
6. attivare e mantenere costantemente aggiornati strumenti che si oppongano all'inserimento di codice malevolo (malware) nel sistema utilizzato per apporre le firme digitali e che, ove esso sia presente, siano in grado di individuarlo, nel qual caso il Titolare è tenuto a curarne l'eliminazione;
7. richiedere immediatamente la revoca dei certificati relativi alle chiavi di firma inutilizzabili, di cui abbia perduto il possesso o il controllo esclusivo o qualora abbia il ragionevole dubbio che esse possano essere usate da altri;
8. redigere per iscritto la richiesta di revoca, specificando la sua decorrenza;
9. sporgere denuncia, in caso di smarrimento o sottrazione delle chiavi di firma, alle autorità competenti;
10. dismettere l'utilizzo della firma in seguito alla avvenuta pubblicazione della revoca.

In ogni caso è vietata la duplicazione della chiave privata.

4.4 Obblighi dei destinatari

I destinatari dei documenti informatici firmati digitalmente dal Titolare devono verificare:

1. la validità del certificato;
2. l'assenza del certificato dalle Liste di Revoca dei certificati (CRL);

3. l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare.

4.5 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

4.6 Legge Applicabile – Foro Competente

Per quanto al riguardo non esplicitamente previsto nel presente Manuale, si applicano le previsioni di cui alle norme generali in materia.
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

5.1 Responsabilità di Notartel S.p.A. – S.B.

Notartel è responsabile verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal Regolamento EIDAS 910/2014, dal Regolamento UE 679/2016, dal D. Lgs. n. 82/05 e ss.mm.ii., dalla Determinazione AgID n. 147/2019, 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 sui certificati emessi dalla stessa, nei limiti di cui all'art. 30 del D.Lgs. n. 82/2005. L'esistenza e la validità del certificato 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 nel certificato alla data di rilascio e la loro completezza rispetto ai requisiti fissati per i certificati;
- la garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare;
- l'esecuzione della procedura di revoca o sospensione nei termini e con le modalità previste dal presente manuale operativo.

È esclusa qualunque responsabilità della Notartel S.p.A.- S.B., anche di natura sussidiaria, in relazione a fatti diversi da quelli sopra enunciati.
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 firme e 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

Le tariffe per l'emissione di un certificato qualificato 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

Ai fini dell'identificazione del richiedente sono ammesse sei diverse modalità di identificazione, alcune delle quali limitate alla sola emissione dei certificati OneShot.

- Modalità 1: Identificazione in presenza;
- Modalità 2: identificazione tramite sistema di videoconferenza;
- Modalità 3: identificazione tramite firma digitale;
- Modalità 4: identificazione tramite CIE, Passaporto Elettronico, SPID (almeno di livello 2);
- Modalità 5: identificazione tramite un precedente certificato one-shot (solo OneShot);
- Modalità 6: identificazione tramite Intermediario notaio (solo OneShot).

7.1 Identificazione in presenza

L'identificazione del richiedente avviene attraverso l'esibizione all'operatore RA tramite il riscontro con un documento, valido e non scaduto, secondo quanto previsto dall'art. 35, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445:

✓ Cittadini residenti in Italia:
- carta d'identità;
- carta d'identità elettronica (CIE);
- passaporto;
- patente di guida.

✓ Cittadini residenti in stato membro UE:
- carta d'identità elettronica (CIE);
- passaporto.

✓ Cittadini residenti in stato extra UE:
- Passaporto.

7.2 Identificazione in VDC

Il sistema di identificazione di persona fisica attraverso l'uso di videoconferenza è un processo dettagliato e regolamentato, attuato dall'operatore RA che ha ricevuto una formazione specifica per gestire tali procedure. La videoconferenza è eseguita da un apposito sistema messo a disposizione del certificatore e che garantisce la riservatezza della comunicazione mediante l'adozione di meccanismi standard.
Questo metodo di identificazione si svolge come segue:

1. **Inizializzazione della videochiamata**: il richiedente inizia una videochiamata con l'operatore RA e dichiara le proprie generalità dichiarando di volersi dotare di una firma qualificata;

2. Verifica dell'identità: l'operatore RA procede alla verifica dell'identità del richiedente, richiedendo di inquadrare, fronte e retro, il documento di riconoscimento utilizzato dal soggetto, assicurandosi che sia possibile visualizzare chiaramente la fotografia e leggere tutte le informazioni contenute nello stesso.
Il documento deve rispettare i criteri stabiliti dall'articolo 35 del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, che definisce le modalità di riconoscimento dell'identità personale.
Durante la sessione, l'operatore RA richiede al soggetto di compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta.
L'operatore RA che effettua l'identificazione può escludere in qualunque momento l'ammissibilità della sessione audio/video per qualunque ragione, inclusa l'eventuale inadeguatezza del documento presentato dal richiedente o la cattiva qualità del video.
I dati di registrazione, costituiti da file audio-video, immagini e metadati strutturati in formato elettronico vengono conservati nel giornale di controllo.

7.3 Identificazione tramite firma digitale

Il titolare che è già in possesso di un dispositivo di firma con un associato certificato qualificato ancora in corso di validità, inoltra alla CA NTL la richiesta di emissione del Certificato. In tal caso compila e firma digitalmente la richiesta.

7.4 Identificazione tramite documento elettronico o SPID

Il titolare, già in possesso di un dispositivo sicuro con un certificato CiE o di identità SPID ancora in corso di validità, si autentica al portale del certificatore ed inoltra la richiesta di emissione del certificato.

7.5 Identificazione tramite precedente firma OneShot

Modalità valida solo per il rilascio di una firma OneShot.
Se un richiedente ha già ottenuto, entro l'anno dall'ultima richiesta, un precedente certificato di firma one-shot dal certificatore Notartel, la richiesta sarà sottoscritta sfruttando il riconoscimento già effettuato.

7.6 Identificazione tramite intermediazione notaio

Modalità valida solo per il rilascio di una firma OneShot.
Questa modalità è prevista solo in caso di rilascio in presenza, quando il richiedente è sprovvisto di qualsiasi sistema tecnologico per l'identificazione. In tal caso il notaio, come descritto in premessa, procede all'inoltro della richiesta di certificato per il richiedente da lui autenticata nella veste di pubblico ufficiale (intermediario) utilizzando le funzionalità messe a disposizione dal certificatore Notartel in PNI.
La richiesta digitale è conservata dal certificatore, analogamente a quanto descritto nelle modalità precedenti e una copia stampata e firmata dal soggetto richiedente resta al notaio agli atti di studio a sua tutela.

Vai al sommario

8 REGISTRAZIONE

La registrazione è svolta dall'operatore RA che provvede ad acquisire tutti i dati necessari all'emissione dei certificati, una volta accerta, tramite documento di riconoscimento, l'identità del richiedente.
Nei casi di identificazione senza operatore, è lo stesso titolare, attraverso apposita applicazione messa a disposizione dalla Notartel S.p.A. – S.B., a fornire i dati necessari all'emissione dei certificati. Tali dati saranno inseriti nell'archivio di registrazione della Notartel S.p.A. – S.B. ai fini dell'emissione dei certificati.

8.1 Contenuto della richiesta del certificato

La richiesta di certificazione include obbligatoriamente tutti i seguenti dati del richiedente/Titolare:

- nome e cognome;
- codice fiscale;
- luogo e data di nascita;
- indirizzo di posta elettronica;
- numero di cellulare.

8.2 Comunicazioni tra Notartel S.p.A. e i Titolari

Il Titolare deve disporre di una casella di posta elettronica e un numero di cellulare, che potrà essere utilizzata da Notartel S.p.A. – S.B. per inviare comunicazioni.
Lo scambio di informazioni tra la Notartel S.p.A. – S.B. e il Titolare durante la procedura di emissione e pubblicazione dei certificati avviene su un canale sicuro.

8.3 Emissione di certificati successiva ad una revoca

Un certificato revocato non è mai riattivabile. La richiesta di un nuovo certificato comporta la ripetizione dell'intera procedura di rilascio.

Vai al sommario

9 GENERAZIONE DELLE CHIAVI

9.1 Sistemi di generazione

La generazione delle coppie di chiavi è effettuata mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza delle coppie generate, nonché la segretezza delle chiavi private.
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;
- l'identificazione del soggetto che attiva la procedura di generazione.

La generazione delle chiavi avviene in modo sicuro all'interno dei dispositivi crittografici (HSM) custoditi presso la Notartel S.p.A. – S.B. garantendo integrità e segretezza della chiave.

9.2 Lunghezza delle chiavi

La lunghezza delle chiavi di certificazione è di almeno 4096 bit.
La lunghezza delle chiavi di sottoscrizione è di almeno 2048 bit.

9.3 Algoritmi

Gli algoritmi utilizzati rispettano le indicazioni di AgID e sono conformi a ETSI 119 312.
Per la generazione e la verifica delle firme digitali 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)

9.4 Chiavi di certificazione

Il Prestatore di Servizi fiduciari qualificati si avvale delle seguenti chiavi di certificazione:

- chiavi di certificazione per firmare i certificati relativi alle chiavi di sottoscrizione, le liste di revoca (CRL) e il certificato OCSP;

Il certificato corrispondente alle chiavi di certificazione della Notartel S.p.A. – S.B., valido dal 7 dicembre 2021, è un certificato di root, che non prevede CA subordinate, ed è così identificato:

CN = Notartel Qualified Electronic Signature CA 2021,
OU = Qualified Trust Service Provider,
organizationIdentifier = VATIT-05364151000,
O = Notartel S.p.A.,
C = IT
Numero seriale 03:47:56:a9:ca:b2:ba:6b:a6:ef
Identificatore chiave del soggetto
33:E1:9E:EA:DF:26:3F:23:DB:4E:66:A1:9C:1A:85:C9:F4:E2:24:5E

9.5 Generazione delle chiavi di certificazione

La generazione delle chiavi di certificazione è effettuata esclusivamente dal Responsabile del servizio che le utilizzerà. Essa avviene all'interno dei dispositivi crittografici certificati secondo quanto previsto dalla normativa vigente e utilizzando procedure sicure.

9.6 Chiavi di sottoscrizione

Le chiavi di sottoscrizione, ovvero di firma, consentono 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.
Alla firma qualificata è allegato il certificato corrispondente alla chiave pubblica da utilizzare per la verifica.
Il Titolare deve avvalersi del dispositivo OTP o di analogo software ricevuto dalla Notartel S.p.A. – S.B. per qualunque operazione di firma.
In caso di firma OneShot, il codice OTP viene trasmesso al Titolare tramite SMS al numero di cellulare dichiarato al momento della richiesta di emissione.

9.7 Generazione delle chiavi di sottoscrizione

A seguito della registrazione della richiesta, il certificato viene generato in modo sicuro e reso disponibile al richiedente.

9.8 Requisiti del dispositivo di firma remota

I dispositivi crittografici (HSM) devono essere in grado di memorizzare le chiavi private e di generare le firme qualificate, senza mai comunicare la chiave stessa all'esterno.
L'utilizzo delle chiavi private da parte del Titolare è subordinato alla sua autenticazione mediante un PIN che deve essere digitato dal medesimo ogni volta che egli intende usare il dispositivo. L'utilizzo delle chiavi di firma remota è subordinato all'autenticazione del Titolare mediante PIN in abbinamento al codice OTP.

10 EMISSIONE DEI CERTIFICATI

10.1 Informazioni contenute nel certificato

Il certificato contiene le informazioni previste dalla Determinazione AgID n. 147/2019. In particolare:

- numero di serie del certificato;
- denominazione della Notartel S.p.A. in qualità di Prestatore di Servizi fiduciari qualificati;
- codice identificativo del Titolare presso Notartel S.p.A. (nel campo Subject come specificato nella Determinazione AgID n. 147/2019);
- nome, cognome e codice fiscale del Titolare;
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità del certificato;
- algoritmo di sottoscrizione del certificato;
- l'indicazione che il certificato è qualificato;
- policy di emissione del certificato qualificato;
- le informazioni per il recepimento dello stato del certificato (CRL e OCSP);
- riferimento al presente manuale operativo;
- tipologia delle chiavi.

10.2 Profilo del certificato

Il certificato è un documento informatico, firmato digitalmente dalla Notartel S.p.A. – S.B. in qualità di Prestatore di Servizi fiduciari qualificati, che deve essere generato e pubblicato, a cura dello stesso. I certificati sono conformi alla norma ISO/IEC 9594-8:2005 e successive modificazioni o integrazioni e alle specifiche RFC 3280, ETSI TS 102 280 ed ETSI TS 101 862, come previsto dalla Determinazione AgID n. 147/2019.
Le informazioni contenute nel certificato seguono le regole previste dalla Determinazione AgID n. 147/2019.
È inoltre presente il campo "IssuerAlternativeName" riportante l'indirizzo di posta elettronica della Notartel S.p.A.
In conformità allo standard ETSI 319 412 – 5 il certificato del Titolare contiene l'estensione qCStatement, ed in particolare:

- contiene il campo identificato come esi4-qcStatement-1 (id-etsi-qcs-QcCompliance OID: 0.4.0.1862.1.1) che indica che il certificato è qualificato e conforme al regolamento UE 910/2014.
- non contiene l'estensione esi4-qcStatement-2 (id-etsi-qcs-QcLimitValue OID: 0.4.0.1862.1.2), assente in quanto non sono applicabili limiti nelle negoziazioni;

- contiene il campo esi4-qcStatement-3 (id-etsi-qcs-QcRetentionPeriod OID: 0.4.0. 1862.1.3), che definisce il periodo di conservazione da parte della CA, il valore indicato è pari a 20 anni, ma è ovviamente esteso a tutto il tempo di conservazione da parte della Notartel S.p.A. in qualità di Prestatore di Servizi Fiduciari;
- contiene il campo esi4-qcStatement-4 (id-etsi-qcs-QcSSCD OID: 0.4.0. 1862.1.4), che indica la memorizzazione della chiave privata internamente ad un dispositivo sicuro.
- contiene il campo esi4-qcStatement-5 che contiene la URL al Disclosure Statement.
- non contiene il campo esi4-qcStatement-6 relativo al tipo di certificato in base alle Annex del regolamento.

In conformità allo standard ETSI 319 411 -2, il certificato del Titolare riporta come Certificate Policy l'identificativo QCP-n-qscd (id-etsi-qcp OID: 0.4.0.194112.1.2) e la policy di emissione (vedi capitolo 3.1).
Limitatamente al certificato OneShot, oltre all'identificativo della policy (OID: 1.3.6.1.4.1.41870.1.9), nel certificato è riportato anche l'identificativo della transazione di firma per cui il certificato è stato emesso.

10.3 Emissione del certificato

Il certificato è generato con un sistema utilizzato esclusivamente per tale funzione, situato in locali protetti come descritto nel Piano per la sicurezza.
L'accesso al sistema di generazione dei certificati avviene attraverso un'operazione di riconoscimento mediante l'uso di un dispositivo di autenticazione forte.
I certificati relativi alle chiavi pubbliche dei titolari sono conservati, a cura della Notartel S.p.A. – S.B. per venti anni dalla data di scadenza del certificato.

10.4 Limiti d'uso certificati One-Shot

I certificati rilasciati con la modalità OneShot sono destinati unicamente alla firma dei documenti legati a una specifica operazione di firma. Per questo motivo, il codice identificativo dell'operazione viene incluso all'interno del certificato di firma (come illustrato nel capitolo 10.2) e viene revocato in automatico alla conclusione o in caso di annullamento dell'operazione (come descritto nel capitolo 11.2).
È vietato l'uso di tali certificati per firmare documenti non correlati o per ottenere forme di identità secondarie.

Vai al sommario

11 REVOCA E SOSPENSIONE DEI CERTIFICATI

La Notartel S.p.A. – S.B. pubblica la revoca e la sospensione dei certificati mediante la Lista dei certificati revocati (CRL) ogni 24 ore e mediante servizio OCSP (Online Certificate Status Protocol).
la Notartel S.p.A. – S.B. provvede a rimuovere da tale Lista i certificati che non sono più sospesi, mantenendo traccia nei propri sistemi del periodo di sospensione.
I certificati revocati o sospesi permangono nella CRL, anche dopo la loro naturale scadenza, fino alla scadenza del relativo certificato di CA.
La lista è consultabile telematicamente, secondo le modalità descritte nel presente Manuale operativo.

11.1 Motivi per la revoca o sospensione del certificato

Il mantenimento del certificato qualificato è sempre a cura della Notartel S.p.A. – S.B. che deve:

- revocarlo in caso di cessazione dell'attività della stessa Notartel S.p.A. – S.B. in qualità di Prestatore di Servizi Fiduciari;
- revocarlo in caso sia terminato il rapporto tra Titolare e la Notartel S.p.A. – S.B.;
- revocarlo in caso di certificato Oneshot al termine o all'annullamento della transazione di firma per la quale è stato emesso;
- revocarlo o sospenderlo in esecuzione di un provvedimento dell'autorità giudiziaria;
- revocarlo a seguito di richiesta del Titolare, nei casi in cui:
    - sia stato smarrito o danneggiato il token OTP;
    - sia venuta meno la segretezza della chiave privata o delle credenziali di accesso al dispositivo di generazione della firma;
    - si sia verificato un qualunque evento che abbia compromesso l'affidabilità della chiave;
    - siano mutati i dati di riferimento del Titolare indicati nel certificato o si siano accertati abusi o falsificazioni.

Il Titolare ha facoltà di richiedere la revoca del certificato per un qualunque motivo dallo stesso ritenuto valido ed in qualsiasi momento.

11.2 Modalità per la revoca o sospensione del certificato

La revoca o la sospensione di un certificato avviene attraverso l'invio di una richiesta tramite apposito portale di gestione messo a disposizione della Notartel S.p.A. – S.B. che provvederà a eseguire la revoca nei tempi previsti nel presente manuale. A tal scopo, il titolare utilizza codici ricevuti dalla Notartel S.p.A. – S.B. per richiedere la revoca del proprio certificato.
In caso di indisponibilità di tali codici, il titolare può richiedere agli operatori RA della Notartel S.p.A. la revoca tramite richiesta sottoscritta.
Il titolare deve indicare nella richiesta:

- nome e cognome;
- dati identificativi del certificato;
- motivazione e decorrenza della revoca;

La Notartel S.p.A. – S.B. garantisce, la disponibilità del servizio di revoca sul portale 24 ore su 24, mentre il servizio di revoca tramite operatore è previsto negli stessi orari della assistenza.
In caso di revoca del certificato OneShot, la richiesta è inviata dalle applicazioni di firma integrate con il portale di gestione e processata automaticamente.
Il certificato revocato viene inserito nella CRL entro 1 ora dalla richiesta di revoca e comunque in nessuna circostanza oltre le 24 ore successive all'operazione.

Vai al sommario

12 SOSTITUZIONE DELLE CHIAVI DI CERTIFICAZIONE

La Notartel S.p.A. – S.B., tre anni prima della scadenza del certificato relativo ad una chiave di certificazione, avvia la procedura di sostituzione, generando una nuova coppia di chiavi.
I certificati così generati sono forniti ad AgID che provvede all'aggiornamento della lista dei certificati delle chiavi di certificazione contenuta nell'elenco pubblico dei Certificatori ed al suo inoltro ai Certificatori per la pubblicazione.
In tale occasione, Notartel S.p.A. – S.B. esegue la procedura di creazione delle coppie delle chiavi di certificazione da utilizzare in caso di disastro.

Vai al sommario

13 REGISTRO DEI CERTIFICATI

13.1 Informazioni contenute nel Registro dei certificati

La Notartel S.p.A. – S.B. pubblica nel Registro dei certificati la lista dei certificati revocati e sospesi (CRL).
Le liste dei certificati revocati e sospesi sono conformi alla specifica RFC 5280, capitolo 5, esclusi i paragrafi 5.2.4 e 5.2.6 come previsto dalla Determinazione AgID n. 147/2019.

13.2 Procedura di gestione del Registro dei certificati

Il Registro dei certificati è consultabile da qualsiasi soggetto 24 ore al giorno, 7 giorni su 7, esclusi i tempi dedicati alla manutenzione programmata ed alla soluzione di eventuali problemi tecnici non prevedibili.
Il Registro dei certificati è gestito dalla directory di sistema ITU-T X.500.
la Notartel S.p.A. – S.B. mantiene una copia di riferimento del Registro dei certificati, inaccessibile dall'esterno, allocata su un sistema sicuro installato in locali protetti; sistematicamente, verifica la conformità tra la copia operativa e la copia di riferimento del Registro, annotando ogni discordanza nel Registro operativo.
Le modificazioni al contenuto del Registro dei certificati sono effettuate esclusivamente da personale autorizzato. Tali operazioni sono sistematicamente registrate sul Giornale di controllo.

13.3 Modalità di accesso al Registro dei certificati

La copia operativa del registro dei certificati è un server http. Il registro dei certificati è accessibile a qualsiasi soggetto tramite l'indirizzo Internet del Registro dei Certificati.
Nel campo CRLDistributionPoint, presente in ogni certificato, è riportato l'indirizzo da cui è possibile accedere alla Lista di revoca (CRL) nella quale ne saranno riportati gli estremi, in caso di sua revoca.

Vai al sommario

14 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 con riferimento al Regolamento UE 679/2016.

Vai al sommario

15 GESTIONE DELLE COPIE DI SICUREZZA

La Notartel S.p.A. – S.B. effettua periodicamente, e secondo politiche ben definite, copie di sicurezza del sistema di certificazione.
Tali copie sono mantenute su sistemi e/o 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 certificazione.
Le procedure per la gestione delle copie di sicurezza sono descritte nel Piano per la sicurezza.

Vai al sommario

16 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 seguenti servizi, a partire dalla dichiarazione di disastro:

- Verifica certificati: servizio di verifica della validità dei certificati qualificati;
- Revoca/sospensione: i servizi di revoca/sospensione dei certificati qualificati.

La Notartel S.p.A. – S.B. 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

17 GESTIONE DEGLI EVENTI CATASTROFICI

La Notartel S.p.A. – S.B. garantisce la continuità del servizio, 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

18 GIORNALE DI CONTROLLO

Tutte le registrazioni effettuate automaticamente dai dispositivi installati presso La Notartel S.p.A. – S.B. sono archiviate ed annotate nel Giornale di controllo.

18.1 Dati da archiviare

I dati da annotare e da archiviare, cui è associata la data e l'ora dell'effettuazione, sono i seguenti:

1. ogni sessione di lavoro relativa alla generazione della coppia di chiavi;
2. la personalizzazione del dispositivo di firma;
3. la generazione dei certificati qualificati
4. la revoca dei certificati emessi;
5. la sospensione dei certificati emessi;
6. l'entrata e l'uscita dai locali protetti del sistema di generazione dei certificati;
7. le richieste di revoca e sospensione

La data e l'ora utilizzate provengono da NTP server la cui precisione è conforme alla normativa in materia e cioè si discosta al massimo di 1 secondo dal tempo UTC (IEN).

18.2 Conservazione dei dati

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 20 anni.

18.3 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.

18.4 Gestione del Giornale di controllo

Al Responsabile del Servizio è demandato il compito di gestire il Giornale di controllo, attraverso l'effettuazione di operazioni di back-up, controlli e report periodici.

18.5 Verifiche

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

Vai al sommario

19 CESSAZIONE DELL'ATTIVITÀ

Notartel S.p.A. – S.B., in qualità di Prestatore di Servizi fiduciari qualificati, qualora intendesse cessare l'attività, comunicherà ad AgID la data di cessazione con un anticipo di sei mesi, indicando il Prestatore di Servizi Fiduciari sostitutivo ovvero il depositario del Registro dei certificati e della relativa documentazione.
Entro lo stesso periodo, la Notartel S.p.A. – S.B. informerà i possessori dei certificati da essa emessi, specificando che tutti i certificati non scaduti al momento della cessazione debbono essere revocati.
AgID rende nota nell'elenco pubblico la data di cessazione con l'indicazione del Prestatore di Servizi Fiduciari sostitutivo ovvero del depositario del Registro dei certificati e della relativa documentazione.

Vai al sommario

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

Roma, 16/07/2024

Firmato digitalmente da
Pasquale Starace
C: IT