CONSIGLIO NAZIONALE DEL NOTARIATO

Consiglio Nazionale del Notariato

Manuale operativo del
Consiglio Nazionale del Notariato
per il servizio di certificazione
delle chiavi pubbliche

versione 6.0

SOMMARIO

VERSIONI DOCUMENTO

VERSIONE	DESCRIZIONE MODIFICA	DATA emissione
1.0	Prima emissione	20 maggio 2002
1.0.1	1. par. 6 inserite tariffe per l'emissione dei certificati e delle marche temporali; 2. par. 9.6: precisata decorrenza periodo di conservazione del certificato scaduto; 3. par. 7.1: correzione indicazione autorità emittente il documento unico di riconoscimento del notaio.	8 agosto 2002
2.0	1. par. 3.1: modificati i dati identificativi del manuale operativo; 2. par. 7.7.1: modificata procedura di generazione e certificazione remota delle chiavi pubbliche; 3. par. 7.7.2: modificata procedura di generazione e certificazione centralizzata delle chiavi pubbliche;.	05/02/04
3.0	1. Adeguamento normativo 2. Modifica procedure	5/5/2006
3.5	1. Adeguamento normativo 2. Semplificazione delle procedure, ed, in particolare, eliminazione dell'emissione centralizzata dei certificati 3. Allineamento delle procedure operative ai requisiti tecnici indicati nel DPCM 13/01/2004, ed, in particolare: a. Eliminazione dell' emissione immediata della CRL (la CRL viene emessa solo ogni ore) b. Eliminazione della pubblicazione dei certificati dei titolari sul	1/7/2008

	registro pubblico dei certificati c. Eliminazione dell' emissione di marca temporale all'atto della pubblicazione della CRL	
4.0	1. Adeguamento normativo DPCM 30 marzo 2009 2. Allineamento delle procedure operative ai requisiti tecnici previsti dalla Deliberazione 45 del 21 Maggio 2009 ed in particolare modifica degli algoritmi di hash; 3. Modifica del tempo di emissione delle CRL. (la CRL viene emessa solo ogni 8 ore)Aggiornamento dei riferimenti normativi 4.	29/01/2013
4.1	1. Modifiche per l'introduzione del servizio di Timestamping in house 2. Revoca per provvedimenti disciplinari 3. Verifica SLA 4. Aggiornamento riferimenti normativi DPCM 22 febbraio 2013 5. Istruzioni per staticizzare documenti	02/12/2013
5.0	1. Aggiornamento riferimenti normativi 2. Rimozione servizio validazione temporale	01/06/2017
6.0	1. Emissione di certificati di firma remota 2. Eliminazione funzione di sospensione da parte dei presidenti	26/10/2018

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.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione. Sostituito da AgID
DigitPA	Ente Nazionale per la digitalizzazione della Pubblica Amministrazione. Sostituito da AgID.
Autenticazione del documento informatico	La validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione.
Certificato	Documento informatico in formato ITU X.509 v.3 o successive contenente informazioni relative al Titolare e alla sua chiave pubblica di firma, firmato dal Prestatore di Servizi Fiduciari con la propria chiave privata di certificazione.
Certificato qualificato	Ai sensi del Regolamento UE 910/2014 rilasciato da Prestatori di servizi fiduciari qualificati che rispondono ai requisiti del regolamento ed avente anche le caratteristiche fissate dal DPCM 22 febbraio 2013, nonché dalla Deliberazione CNIPA 45/2009.
Prestatore di Servizi Fiduciari	Trusted Service Provider, prestatore di servizi fiduciari (es. Certificatore accreditato, Conservatore accreditato, etc) ai sensi del Regolamento 910/2014
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.
CNN	Consiglio Nazionale del Notariato (CNN), ente pubblico non economico, istituito con legge 3 agosto 1949, n. 577.
CND	Consiglio Notarile Distrettuale ai sensi della legge notarile.
Codice riservato (CRN e CRP)	Sequenza di caratteri alfanumerici che deve essere fornita dal Titolare o dal Presidente del Consiglio Notarile Distrettuale al Prestatore di Servizi fiduciari qualificati per effettuare una revoca o sospensione immediata di un certificato.
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)	Vedi Liste di revoca dei certificati.
Destinatario	Destinatario di un documento informatico firmato digitalmente.
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.
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 macro istruzioni o codici eseguibili tali da attivare funzioni che possono modificare gli atti, i fatti o i dati nello stesso rappresentati.
Firma Digitale	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 fi rma 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.
Lista di revoca dei certificati (CRL)	Lista firmata digitalmente, tenuta ed aggiornata dal Prestatore di Servizi fiduciari qualificati contenente i certificati emessi dallo stesso e successivamente sospesi o revocati.
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.
Notaio	Il notaio in esercizio, nonché il coadiutore non notaio. Una volta certificato dal CNN, tale soggetto viene anche definito Titolare.
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.
PUK (Personal Unlock Key)	Chiave personale di sblocco del PIN.
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.
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.
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.
QSCD	Qualified Signature Creation Device, il dispositivo di firma certificato.
SSL (Secure Socket Layer)	Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica
Presidente del Consiglio Notarile Distrettuale	Tale ai sensi della legge notarile.
Titolare	Notaio a favore del quale è stato emesso un Certificato dal CNN.
Validazione temporale	Risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, un riferimento temporale opponibili ai terzi.
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
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.
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.

1. INTRODUZIONE

1.1 Scopo del documento

Questo documento definisce le procedure seguite dal CNN nello svolgimento dell'attività di Prestatore di Servizi Fiduciari accreditato, ai sensi dell'art. 29 del Decreto Legislativo n.82/2005, e di Trusted Service Provider (TSP) ai sensi del Regolamento UE 910/2014 per la generazione dei certificati di firma qualificata. Esso si riferisce al servizio di:

- Certificazione delle chiavi pubbliche dei notai

Il Manuale Operativo vincola il Prestatore di Servizi fiduciari qualificati e tutti i soggetti che entrano in relazione con il Prestatore di Servizi Fiduciari.

Il presente documento definisce inoltre gli obblighi e le responsabilità del Prestatore di Servizi fiduciari qualificati, del Titolare e di quanti accedono per la verifica della firma e della marca temporale.

1.2 Riferimenti normativi

Il Manuale Operativo è conforme a quanto previsto dalla normativa italiana e comunitaria e in particolare:

- Legge 16 febbraio 1913 n. 89 (legge notarile)
- Art. 15, comma 2, Legge 15 marzo 1997 n. 59
- 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
- Decreto Legislativo 7 marzo 2005 n. 82
- Decreto Legislativo 4 aprile 2006 n.159
- Circolare CNIPA 6 settembre 2005, n.48
- Decreto legislativo 30 dicembre 2010 n. 235
- DPCM 30 marzo 2009
- Deliberazione CNIPA n. 45 del 21 maggio 2009
- DPCM 22 febbraio 2013
- 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

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 delle precedenti.

2. DATI IDENTIFICATIVI DEL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI

I dati identificativi relativi al CNN sono i seguenti:

Denominazione e Ragione sociale:	Consiglio Nazionale del Notariato
Sede legale:	via Flaminia 160, 00196 Roma
Rappresentante legale:	Presidente pro tempore del CNN
Telefono: +39-06362091	**Fax:** +39-063221594
Sede operativa: via Flaminia 160, 00196 Roma via Giovanni Vincenzo Gravina 4 00196 Roma	**Indirizzo E-mail:** segreteria.cnn@postacertificata.notariato.it esercizio@postacertificata.notariato.it
Indirizzi Internet: http://ca.notariato.it http://www.notariato.it	**Help Desk:** helpdesk@notariato.it

3. MANUALE OPERATIVO

3.1 Dati identificativi del Manuale operativo

Il presente Manuale operativo, conservato presso i locali del Prestatore di Servizi fiduciari qualificati e depositato presso il AgID, è identificato col nome "MOConsiglioNazionaleNotariato" ed è consultabile per via telematica all'indirizzo Internet:

http://ca.notariato.it/documentazione/MOCNN.pdf

Il presente documento è identificato con il numero di versione 6.

Il presente Manuale Operativo è, inoltre, referenziato dai seguenti OID (Object Identifier Number):

1.3.6.1.4.1.8526.1.1.6 Certificazione Chiavi.

In aggiunta, si definisce in questo stesso manuale una policy per il rilascio delle marche temporali non qualificate che sarà referenziato attraverso il seguente OID.

1.3.6.1.4.1.8526.1.2.4 Servizio di marcatura temporale non qualificato

Tali OID identificano:

Consiglio Nazionale del Notariato	1.3.6.1.4.1.8526
Certification Service Provider	1.3.6.1.4.1.8526.1
Certificate-Policy per certificati emessi in conformità alla policy ETSI QCP-n-qscd (QSCD)	0.4.0.194112.1.2
Policy per certificati di firma su dispositivo (QSCD)	1.3.6.1.4.1.8526.1.1.5
Timestamp policy	1.3.6.1.4.1.8526.1.2
Policy marcatura temporale	1.3.6.1.4.1.8526.1.2.4
Policy per certificati di firma remota	1.3.6.1.4.1.8526.1.1.6

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

Il Responsabile del Manuale operativo è il presidente pro-tempore del Consiglio Nazionale del Notariato.

Telefono: +39-06362091

E-mail: segreteriapresidenza.cnn@notariato.it

3.3 Tipologia delle utenze

Il CNN certifica esclusivamente le chiavi pubbliche utilizzate dai notai nell'esercizio delle loro funzioni in tutti i casi in cui sia previsto l'intervento del notaio ai sensi di legge.

Il CNN rilascia esclusivamente a tal fine certificati qualificati per supportare firme digitali generate mediante un dispositivo sicuro per la creazione di una firma.

Pertanto, ai fini del presente documento, i termini certificato e certificato qualificato coincidono; eventuali eccezioni saranno espressamente riportate.

L'eventuale utilizzo per scopi diversi è ammesso solo se autorizzato espressamente dal CNN.

4. TERMINI E CONDIZIONI

4.1 Obblighi del Prestatore di Servizi fiduciari qualificati

Il servizio erogato dal prestatore di servizi fiduciari qualificati 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.

Il servizio di CA è conforme alla versione corrente del documento Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates pubblicato presso http://www.cabforum.org. In caso di contrasto tra il manuale operativo e tali requisiti, i Requisiti hanno la precedenza su questo documento.

Inoltre, nello svolgimento della sua attività, il Prestatore di Servizi fiduciari qualificati:

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. identifica con certezza il notaio richiedente ed il fatto che sia regolarmente in esercizio ai sensi della legge notarile;
4. informa espressamente, in modo compiuto e chiaro, il Titolare 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;
5. rilascia e rende pubblico il certificato;
6. si attiene alle regole tecniche emanate con D.P.C.M. 22 febbraio 2013;
7. si accerta dell'autenticità della richiesta di certificazione;
8. 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;
9. si attiene alle misure minime di sicurezza per il trattamento dei dati personali di cui al Regolamento UE 679/2016;
10. 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;
11. procede tempestivamente alla revoca od alla sospensione del certificato in tutti i casi previsti dal presente Manuale Operativo;
12. comunica le richieste di revoca o sospensione al Titolare;
13. dà tempestiva pubblicazione della revoca e della sospensione del certificato;
14. conserva le richieste scritte di registrazione e le richieste di certificazione per un periodo di almeno 30 anni dalla data di scadenza del certificato;
15. comunica per iscritto a 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;
16. comunica tempestivamente a AgID, ogni variazione significativa delle soluzioni tecnico-organizzative adottate;
17. comunica immediatamente a AgID e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso;
18. comunica al AgID ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività, della conseguente rilevazione della documentazione da parte di altro Prestatore di Servizi Fiduciari o del suo annullamento, specificando che tutti i certificati non scaduti al momento della cessazione devono essere revocati.

19. 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.
20. in caso di modifica alle condizioni del presente manuale operativo fornisce informativa ai titolari ed ai destinatari mediante pubblicazione del manuale aggiornato sul sito della CA.
21. si attiene alle indicazioni di Agid in caso di compromissione degli algoritmi utilizzati.

4.2 Obblighi del Titolare

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

Il Titolare delle chiavi deve, inoltre:

1. fornire tutte le informazioni richieste dal Prestatore di Servizi fiduciari qualificati, garantendone, sotto la propria responsabilità, l'attendibilità;
2. conservare con la massima diligenza i codici personali, e il dispositivo fisico di firma (smartcard) e l'eventuale generatore di PINI (OTP)al fine di garantire l'integrità e la conservazione delle informazioni di abilitazione all'uso della chiave privata;
3. mantenere in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma;
4. accertare che il documento da sottoporre alla firma non contenga macro istruzioni o codici eseguibili, tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati nello stesso rappresentati;
5. 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;
6. 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;
7. redigere per iscritto la richiesta di revoca, specificando la sua decorrenza;
8. redigere la richiesta di sospensione secondo le modalità previste nel presente Manuale Operativo, specificandone il periodo durante il quale la validità del certificato deve essere sospesa;
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.

4.3 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.

4.4 Obblighi del Presidente del CND

Il Presidente del CND ha l'obbligo di:

1. verificare l'identificazione e la registrazione;
2. accertarsi che i codici di attivazione siano consegnati integri al destinatario
3. consegnare quanto e necessario per l'utilizzo del dispositivo di firma;
4. sottoscrivere la richiesta di emissione dei certificati;
5. accertarsi che soltanto i notai in esercizio effettivo nel distretto siano dotati del relativo certificato e provvedere alla revoca nel caso in cui il notaio titolare cessi dall'esercizio in quel distretto;
6. sospendere e revocare i certificati tutte le volte in cui ciò si renda necessario;
7. riattivare i certificati sospesi;
8. richiedere la sostituzione delle chiavi di firma dei titolari in accordo con i relativi paragrafi del presente manuale.

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: 06.36209306
- Fax: 06.32650077
- E-mail: helpdesk@notariato.it

4.6 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.

5. RESPONSABILITÀ

5.1 Responsabilità del Prestatore di Servizi fiduciari qualificati

Il Prestatore di Servizi fiduciari qualificati è responsabile verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dalla Regolamento EIDAS 910/2014, Regolamento UE 679/2016, dal D. Lgs. n. 82/05 e s.m.i., dalla Determinazione Agid n. 185/2017, , dalla Deliberazione CNIPA n. 45/09, dal D.P.C.M. 22 febbraio 2013.

Il CNN è responsabile nei confronti di qualunque soggetto faccia ragionevole affidamento sui certificati emessi dallo stesso, 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 del CNN 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, al momento del rilascio del certificato, il notaio detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
- la garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il Prestatore di Servizi fiduciari qualificati generi entrambi;
- l'esecuzione della procedura di revoca o sospensione nei termini e con le modalità previste dal presente manuale operativo.

E' esclusa qualunque responsabilità del CNN, anche di natura sussidiaria, in relazione a fatti diversi da quelli sopra enunciati, ed in particolare per fatti riconducibili alla sfera operativa del notaio, ivi compresi, a titolo esemplificativo, il mancato rispetto delle procedure, vizi formali o sostanziali relativi al documento firmato ed al suo contenuto, lo smarrimento o la sottrazione o l'incauto affidamento ad altro soggetto delle chiavi di firma, l'erronea identificazione del documento sottoposto alla procedura di firma.

E' altresì esclusa qualsivoglia responsabilità del CNN 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 il CNN 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.

6. TARIFFE

L'emissione del certificato può comportare l'addebito al richiedente di un importo in euro pubblicato sul portale dei servizi del notariato.

Le tariffe sono pubblicate sul portale dei servizi del notariato.

7. IDENTIFICAZIONE E REGISTRAZIONE

7.1 Identificazione

L'identificazione del notaio richiedente avviene attraverso l'esibizione di uno dei seguenti documenti di riconoscimento:

- carta d'identità;
- passaporto;
- documento unico di riconoscimento dei notai rilasciato dal Consiglio Notarile Distrettuale.

I suddetti documenti devono essere validi e presentati in originale.

7.2 Registrazione

La registrazione dei Notai è svolta dal Prestatore di Servizi Fiduciari che provvede ad acquisire dai CND, per mezzo dei presidenti, tutti i dati necessari all'emissione dei certificati.

Tali dati saranno inseriti nell'archivio di registrazione del CNN ai fini dell'emissione dei certificati.

Il presidente CND autorizza l'emissione dei certificati qualificati per il notaio.

Spetta al notaio la scelta di attivar solo la smartcard oppure dotarsi anche di firma remota

Il Presidente del CND richiede al CNN l'emissione delle chiavi di firma contestualmente ad ogni richiesta di registrazione di decreto di nomina o trasferimento di notaio.

7.3 Contenuto della richiesta del certificato

La richiesta di certificazione include i seguenti dati:

- nome e cognome del notaio;
- codice fiscale;
- luogo e data di nascita;
- distretto notarile;
- sede di esercizio e/o indirizzo dello studio;
- indirizzo di posta elettronica;

il tutto sulla base del decreto registrato di nomina del notaio e, per quanto in esso non contenuto, sulla base di dichiarazione sottoscritta dell'interessato.

7.4 Obblighi di Identificazione

Il Prestatore di Servizi fiduciari qualificati, per il tramite dei Presidenti dei CND, effettua l'identificazione e la registrazione, secondo le modalità previste nel presente Manuale Operativo.

Il Presidente del CND è responsabile per l'eventuale difformità dei dati comunicati nella richiesta rispetto a quelli risultanti da documenti ufficialmente acquisiti dallo stesso CND a norma di legge.

7.5 Comunicazioni tra il Prestatore di Servizi fiduciari qualificati e i Titolari

Il titolare deve disporre di una casella di posta elettronica, che potrà essere utilizzata dal Prestatore di Servizi Fiduciari qualificati per inviare comunicazioni.

Lo scambio di informazioni tra il CNN e il CND durante la procedura di emissione e pubblicazione dei certificati avviene su un canale sicuro.

7.6 Codici riservati

1.1.1. Codice riservato per il notaio (CRN)

Il Prestatore di Servizi fiduciari qualificati fornisce al notaio un codice riservato che permetterà allo stesso di attivare le chiavi di firma e, in casi di emergenza, di richiedere telefonicamente la revoca o la sospensione immediata del certificato.

1.1.2. Codice riservato per il Presidente (CRP)

Al Presidente del Consiglio Notarile Distrettuale sono affidati, in singole buste sigillate, i codici riservati necessari alla gestione delle revoche e sospensioni mediante richiesta telefonica, in numero che sarà concordato con il Prestatore di Servizi fiduciari qualificati in relazione al numero dei notai del Distretto. Ciascun codice è utilizzabile una sola volta per revocare uno qualunque dei certificati dei notai del Distretto.

7.7 Procedure per la generazione e la certificazione delle chiavi pubbliche di firma

Per la generazione e certificazione delle chiavi pubbliche di firma si utilizza la seguente procedura.

CND	Notaio	CA-CNN
Il Presidente, nella funzione di RA, invia al CNN richiesta di rilascio di uno o più chiavi di firma. La richiesta contiene i dati anagrafici del notaio e l'indirizzo al quale spedire il dispositivo di firma e/o l'eventuale dispositivo OTP.	Il Notaio sulla applicazione WebRA può inoltre fare richiesta di una firma remota. In questo caso viene avviato un flusso di registrazione che inoltra agli operatori di CA la richiesta di invio di nuova scartchcard ed eventualmente del dispositivo OTP	
		Per ogni chiave di firma richiesta: • associa ad ogni notaio un codice identificativo ed un codice riservato; • inizializza e/o personalizza per il notaio ogni dispositivo di firma (es. serigrafia, inizializzazione elettrica); • trasmette all'indirizzo indicato nella richiesta del CND un plico intestato al notaio contenente il dispositivo di firma e/o il dispositivo OTP e spedisce al CND altro plico contenente i codici identificativi con gli associati codici riservati ed ogni altro codice (es. PIN, PUK) necessario alla generazione delle chiavi.
Il Presidente del CND, contestualmente o successivamente all'iscrizione a ruolo nel distretto di competenza, consegna i codici al notaio.		
	Il notaio, al ritiro dei codici, dopo averne verificato l'integrità, firma un'apposita dichiarazione attestante lo stato di integrità dei codici stessi e, ove esse risultino integri, l'uso esclusivo della firma nell'espletamento delle funzioni di notaio.	

	Generazione di chiavi di firma su smart card Successivamente esegue la generazione delle chiavi internamente al dispositivo di firma effettuando le seguenti operazioni: • accede ad un apposito software identificandosi con il codice identificativo e il codice riservato allegato al dispositivo di firma; • verifica che i propri dati anagrafici presentati dal software siano corretti. In caso di errore, il titolare interrompe la procedura e comunica la discrepanza al CND di appartenenza; • avvia la procedura di generazione della coppia di chiavi internamente al dispositivo di firma; • firma la richiesta di certificazione della chiave pubblica in formato PKCS#10 e la trasmette al CNN su canale sicuro Generazione di chiavi di firma remota • in seguito alla ricezione della scratchcard il notaio procede con l'attivazione della firma remota, che avviene mediante i codici di enroll presenti sulla scratchcard e il codice OTP generato al momento dell'attivazione	
		Il Prestatore di Servizi Fiduciari genera il certificato digitale sulla base della richiesta pervenuta.
	In caso di firma con smart card: Il titolare, tramite apposito applicativo software, memorizza il certificato digitale all'interno del dispositivo di firma. In caso di firma remota: Il titolare, tramite apposito applicativo software, memorizza il certificato sui dispositivi	

	crittografici (HSM) custoditi presso il Prestatore di Servizi Fiduciari	

Tutte le fasi del processo seguono criteri di verifica della corretta formulazione dei formati e dei dati contenuti.

Tutte le richieste che presentano anomalie vengono scartate e tale evento viene comunicato al titolare mediante messaggio di posta elettronica.

7.8 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.

8. GENERAZIONE DELLE CHIAVI

8.1 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 del dispositivo di firma certificato SSCD, oppure all'interno dei dispositivi crittografici (HSM) custoditi presso il Prestatore di Servizi fiduciari qualificati garantendo integrità e segretezza della chiave.

8.2 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.

8.3 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)

8.4 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;
- chiavi di certificazione per firmare i certificati relativi alle chiavi di marcatura temporale, e il relativo certificato OCSP.

Il certificato corrispondente alle chiavi di certificazione del CNN, valido dal 6 aprile 2017, è un certificato di root, che non prevede CA subordinate, ed è così identificato:

organizationIdentifier=VATIT-80052590587

CN=Consiglio Nazionale del Notariato Qualified Certification Authority

OU=Servizio Firma Digitale

O=Consiglio Nazionale del Notariato

C=IT

Numero seriale 01a8

Identificatore chiave del soggetto 06:59:5D:86:F9:10:3F:2B:D8:8F:04:8D:6C:17:C1:E2:15:B9:43:30

Il certificato corrispondente alle chiavi di certificazione del CNN, valido dal 15 luglio 2008, è un certificato di root, che non prevede CA subordinate, ed è così identificato:

CN = Consiglio Nazionale del Notariato Qualified Certification Authority

OU = Servizio Firma Digitale

O = Consiglio Nazionale del Notariato

C = IT

Serial Number = 80052590587

Numero seriale 01a8

Identificatore chiave del soggetto d4 ce 59 d7 98 fc cf ca 5a ce 91 2f aa 54 41 6a 2e 63 40 78

8.4.1 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 del dispositivi crittografici certificati secondo quanto previsto dalla normativa vigente e utilizzando procedure sicure.

8.5 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 digitale è allegato il certificato corrispondente alla chiave pubblica da utilizzare per la verifica.

Il Titolare deve avvalersi del dispositivo di firma e/o del dispositivo OTP consegnati dal CNN, per qualunque operazione di firma.

8.6 Dispositivo di firma

Il dispositivo di firma utilizzato per la generazione delle firme è conforme a requisiti di sicurezza non inferiori a quelli previsti dal livello di valutazione E3 con robustezza dei meccanismi HIGH dell'ITSEC o dal livello EAL 4+ della norma ISO/IEC 15408 o superiori.

Le chiavi private devono essere conservate e custodite all'interno del dispositivo di firma.

Ciascuna coppia di chiavi è attribuita ad un solo Titolare. La duplicazione della chiave privata o dei dispositivi che la contengono è vietata.

I dispositivi crittografici (HSM) utilizzati per la firma remota sono custoditi dal Prestatore di Servizi fiduciari qualificati e sono certificati ai sensi della normativa vigente

8.7 Requisiti del dispositivo di firma

Il dispositivo di firma e i dispositivi crittografici (HSM) devono essere in grado di memorizzare le chiavi private e di generare le firme digitali, senza mai comunicare la chiave stessa all'esterno.

L'utilizzo delle chiavi private da parte del notaio è subordinato alla sua autenticazione mediante un PIN che deve essere digitato dal titolare ogni volta che egli intende usare il dispositivo. L'utilizzo delle chiavi di firma remota è subordinata all'autenticazione del notaio mediante PIN in abbinamento al codice OTP.

9. EMISSIONE DEI CERTIFICATI

9.1 Informazioni contenute nel certificato

Il certificato contiene le informazioni previste dalla deliberazione CNIPA 45 del 21 maggio 2009. In particolare:

- numero di serie del certificato;
- denominazione e sede legale del Prestatore di Servizi fiduciari qualificati;
- codice identificativo del Titolare presso il Prestatore di Servizi Fiduciari (nel campo Subject come specificato nella Deliberazione CNIPA 45/2009);
- nome, cognome e codice fiscale del Titolare;
- l'indicazione che il titolare è notaio;
- distretto notarile di esercizio;
- 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 dell'uso esclusivo della chiave privata per l'esercizio della funzione notarile;
- l'indicazione che il certificato è qualificato;
- le informazioni per il recepimento dello stato del certificato (CRL e OCSP);

- riferimento al presente manuale operativo;
- tipologia delle chiavi.

9.2 Profilo del certificato

Il certificato è un documento informatico, firmato digitalmente dal 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 Del. CNIPA 45/2009.

Le informazioni contenute nel certificato seguono le regole previste dalla deliberazione CNIPA n.45/2009 e successive modificazioni e integrazioni.

In aggiunta a quanto previsto dalla deliberazione CNIPA n.45/2009, all'interno del campo "Subject" è presente un sottocampo O (Organization) riportante il distretto notarile di esercizio.

Sono inoltre presenti i campi "SubjectAlternativeName" "IssuerAlternativeName" riportanti rispettivamente l'indirizzo di posta elettronica del titolare e del Prestatore di Servizi fiduciari qualificati.

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 30 anni, ma è ovviamente esteso a tutto il tempo di conservazione da parte del 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.

9.3 Emissione e pubblicazione 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 notai sono conservati, a cura del Prestatore di Servizi fiduciari qualificati per trenta anni dalla data di scadenza del certificato.

Su richiesta del titolare il certificato è pubblicato nel registro dei certificati.

9.3.1 Emissione del certificato sul dispositivo di firma

Il titolare si autentica ai servizi o alle applicazioni messe a disposizione dalla RA.

La coppia di chiavi crittografiche viene generata dalla RA direttamente sul dispositivo di firma; la RA invia quindi alla Certification Authority la richiesta di certificazione della chiave pubblica in formato PKCS#10, che è firmata digitalmente con le chiavi generate.

La Certification Authority, procede alla generazione del certificato qualificato, che viene memorizzato sul dispositivo di firma.

9.3.2 Emissione del certificato di firma remota

Il titolare si autentica ai servizi o alle applicazioni messe a disposizione dalla RA.

La coppia di chiavi crittografiche viene generata dalla RA direttamente sull'HSM; la RA invia quindi alla Certification Authority la richiesta di certificazione della chiave pubblica in formato PKCS#10, che è firmata digitalmente con le chiavi generate.

La Certification Authority, procede alla generazione del certificato qualificato, che viene memorizzato sul HSM.

10. DOCUMENTI INFORMATICI E LORO UTILIZZO

I documenti da sottoporre alla firma sono esclusivamente i documenti informatici così come definiti nel paragrafo "DEFINIZIONI AI FINI DEL PRESENTE MANUALE OPERATIVO

Essi non devono contenere, pertanto, macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati ai sensi del comma 3 dell'art.4 del DPCM 22 febbraio 2013.

Alcuni formati di documenti permettono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che questo ne alteri la struttura binaria e tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati rappresentati nel documento medesimo. I file firmati digitalmente che contengono tali strutture non producono gli effetti di cui all'articolo 21, comma 2 del CAD. E' obbligo del Titolare assicurarsi, tramite le funzionalità tipiche di ciascun prodotto, dell'assenza di tale codice eseguibile.

Nell'Appendice A si riportano alcune modalità operative finalizzate alla staticizzazione dei documenti.

10.1 Formati

I documenti informatici sottoposti alla firma devono essere statici non modificabili.

Sono ammessi esclusivamente i seguenti formati documentali: PDF/A, RTF, TXT, TIFF, JPEG, GIF, XML, ODT.

Il CNN si riserva di accettare eventuali ulteriori formati.

Per i formati elencati vanno, in particolare, rispettate le seguenti avvertenze:

1. I documenti in formato PDF devono essere convertiti in PDF/A; qualora siano presenti elementi che per le loro caratteristiche intrinseche rendano impossibile tale conversione il documento deve essere rigenerato a partire dal formato di origine scegliendo la modalità di conversione che produce un documento in formato PDF/A.
2. Il formato XML deve essere associato, laddove possibile, a un preciso XML Stylesheet, preferibilmente disponibile su un sito internet reso affidabile mediante protocolli sicuri (quale SSL/TLS) e reso sicuro mediante meccanismi quali la firma digitale o la pubblicazione del loro *digest* e dell'algoritmo con cui calcolarlo.

Nota: altri formati, diversi da quelli indicati, dovrebbero essere evitati in quanto, anche se il Notaio all'atto della firma sia certo dell'assenza di codice nascosto quale quello a cui fa riferimento l'art. 4, comma 3, del DPCM 22/02/2013, i documenti prodotti in tale formato possono essere rifiutati da chi verifica le firme digitali apposte a tali documenti.

10.2 Modalità di generazione della firma digitale

Il titolare è tenuto a generare la firma digitale su una propria postazione di lavoro dotata di sistemi di sicurezza atti a garantire la non compromissione della postazione stessa.

La generazione della firma deve avvenire all'interno del dispositivo di firma oppure sui dispositivi crittografici (HSM) del Prestatore di Servizi fiduciari qualificati e deve essere attivata a seguito di riconoscimento del titolare tramite codice identificativo (PIN) o tramite abbinamento ad un codice OTP. Non è consentita in nessun caso l'apposizione del codice identificativo con ricorso a strumenti automatici.

Il titolare è tenuto a mantenere segreto il PIN, a non comunicarlo ad alcuno e a sostituirlo a intervalli regolari di tempo.

Per la generazione della firma il CNN mette a disposizione del titolare un'applicazione di firma e verifica, scaricabile dal portale della Registration Authority (WebRA) nell'area riservata per l'utente. Il portale è raggiungibile dal sito: http://ca.notariato.it.

Mediante tale software è possibile:

- firmare digitalmente documenti con i dispositivi di firma rilasciato al notaio;
- verificare una firma apposta a documenti firmati digitalmente secondo i formati definiti dallAGID

Le istruzioni per l'utilizzo del prodotto, per la firma e la verifica, sono incluse in un apposito manuale utente disponibile sul portale WebRA, ed è considerato parte integrante del presente Manuale Operativo.

10.3 Verifica delle firme

Il sistema di verifica delle firme digitali deve:

- presentare lo stato di aggiornamento delle informazioni di validità dei certificati di certificazione;
- visualizzare le informazioni presenti nel certificato qualificato;
- in caso di firme multiple, visualizzare l'eventuale dipendenza tra queste;
- visualizzare lo stato dei certificati qualificati;
- evidenziare l'eventuale modifica del documento informatico dopo la sottoscrizione dello stesso.

Le istruzioni per l'utilizzo del prodotto per la verifica sono incluse in un apposito manuale utente disponibile sul portale WebRA, ed è considerato parte integrante del presente Manuale Operativo.

11. REVOCA E SOSPENSIONE DEI CERTIFICATI

11.1 Premessa

Il Prestatore di Servizi fiduciari qualificati pubblica la revoca e la sospensione dei certificati mediante la Lista dei certificati revocati (CRL) ogni 8 ore.

Il Prestatore di Servizi Fiduciari 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.

11.2 Revoca e sospensione dei certificati

La revoca di un certificato determina la cessazione anticipata della sua validità.

La sospensione di un certificato comporta l'interruzione temporanea della sua validità.

La revoca e la sospensione sono registrate nel Giornale di controllo e sono efficaci a partire dal momento della pubblicazione della lista che le contiene.

Il Prestatore di Servizi fiduciari qualificati procede tempestivamente alla pubblicazione dell'aggiornamento della lista, qualora la richiesta di revoca riguardi un sospetto di compromissione della chiave.

Il certificato è revocato o sospeso su:

- richiesta del notaio titolare;
- richiesta del Presidente del CND;
- iniziativa del Prestatore di Servizi fiduciari qualificati;
- ordine dell'autorità giudiziaria.

Il titolare di un certificato e il Presidente del CND di appartenenza vengono informati di ogni evento concernente la revoca o sospensione del certificato stesso.

11.2.1 Revoca di certificati

Su richiesta del notaio:

Il notaio deve richiedere tempestivamente al Prestatore di Servizi fiduciari qualificati la revoca del proprio certificato nei seguenti casi:

- perdita del possesso delle chiavi di firma (smarrimento, distruzione, sottrazione, furto);
- guasto o cattivo funzionamento delle chiavi di firma;
- sospetti abusi o falsificazioni;
- compromissione della segretezza della chiave privata.

In caso di perdita del possesso del dispositivo di firma e/o del dispositivo OTP, il notaio titolare deve anche sporgere denuncia alle Autorità competenti.

Il notaio può richiedere in ogni tempo la revoca del proprio certificato per iscritto, specificandone la decorrenza.

Il Presidente del CND richiede tempestivamente la revoca di tutti i certificati del notaio per:

- decadenza dalla nomina;
- cessazione dall'esercizio notarile per dispensa, rimozione, destituzione;
- trasferimento ad altro distretto;
- altre ipotesi di cessazione definitiva dalle funzioni;
- esecuzione di provvedimenti dell'autorità giudiziaria comportanti la cessazione anche temporanea dalle funzioni notarili.

Il Prestatore di Servizi fiduciari qualificati deve procedere tempestivamente alla revoca oltre che nei casi di richiesta da parte dei soggetti a ciò abilitati, nei casi di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi e falsificazioni e negli altri casi previsti dal presente manuale salvo i casi di urgenza, la revoca del certificato è preventivamente comunicata dal Prestatore di Servizi Fiduciari al notaio titolare, con specificazione della data e dell'ora a partire dalla quale il certificato non sarà più valido.

11.3 Sospensione di certificati

I certificati sono sospesi per un periodo di tempo stabilito, comunque non superiore a 1 anno.

Decorso tale termine senza che siano pervenute indicazioni da parte del soggetto che ha richiesto la sospensione, il certificato viene riattivato dal Prestatore di Servizi fiduciari qualificati con decorrenza dalla data di fine del periodo di sospensione.

Sospensione su richiesta del notaio

Il notaio può richiedere in ogni tempo la sospensione dei suoi certificati solo in caso di concessione del permesso di assenza per il periodo relativo.

Sospensione su richiesta del Prestatore di Servizi fiduciari qualificati

Il Prestatore di Servizi fiduciari qualificati deve procedere tempestivamente alla sospensione, oltre che nei casi di richiesta da parte dei soggetti a ciò abilitati, anche quando, ricevuta una richiesta di revoca, non ha la possibilità di accertare in tempo utile l'autenticità della richiesta stessa; in tal caso il certificato rimane sospeso fino alla verifica della richiesta di revoca.

11.4 Revoca dei certificati relativi a chiavi di certificazione

11.4.1 Circostanze di revoca

Il Prestatore di Servizi fiduciari qualificati procede alla revoca del certificato relativo ad una coppia di chiavi di certificazione esclusivamente nei seguenti casi (D.P.C.M. 22 febbraio 2013):

- compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza della chiave privata;
- guasto del dispositivo di firma;
- cessazione dell'attività.

11.4.2 Obbligo di notifica

La revoca è comunicata al AgID, a tutti i possessori di certificati sottoscritti con la chiave privata appartenente alla coppia revocata e a tutti gli altri certificatori (TSP), entro le 24 ore.

La comunicazione contiene i riferimenti alle informazioni compromesse.

11.4.3 Obbligo di revoca

I certificati per i quali risulti compromessa la chiave di certificazione con cui sono stati sottoscritti vengono revocati d'ufficio.

11.4.4 Procedura di revoca dei certificati relativi a chiavi di certificazione

Il Prestatore di Servizi Fiduciari procede alla revoca dei certificati relativi a chiavi di certificazione, inserendoli nella Lista di revoca (CRL) che rende pubblica.

Successivamente, notifica entro 24 ore, la revoca al AgID ed ai Titolari dei certificati sottoscritti con la chiave privata della coppia di chiavi revocata.

Della revoca è fatta annotazione nel giornale di controllo.

11.5 Modalità di revoca o sospensione dei certificati di sottoscrizione

Le richieste di revoca devono essere inoltrate per iscritto specificandone la motivazione e la decorrenza.

Le richieste di sospensione devono essere inoltrate per iscritto, salvo il caso di richieste di sospensione in emergenza dettagliate più oltre, specificandone la motivazione ed indicando il periodo durante il quale la validità del certificato deve essere sospesa.

Salvo i casi di maggiore urgenza da evidenziarsi all'atto della richiesta, ovvero di emergenza, le richieste di revoca e sospensione vanno presentate con almeno due giorni feriali di anticipo rispetto alla data di entrata in vigore.

In casi di emergenza, la richiesta di revoca o sospensione potrà essere inoltrata telefonicamente utilizzando il codice riservato ed il codice identificativo secondo la modalità prevista dal presente manuale. Parallelamente il richiedente deve attivare la procedura ordinaria per iscritto. Fino al completamento della procedura ordinaria o alla richiesta di riattivazione, il certificato sarà sospeso.

Una volta effettuata la revoca, la sospensione o la riattivazione di un certificato, il Prestatore di Servizi fiduciari qualificati informa il titolare e la terza parte degli estremi della revoca, sospensione o riattivazione, mediante messaggi di posta elettronica.

11.6 Procedure di revoca e sospensione dei certificati su richiesta del Titolare

Il notaio Titolare può inoltrare la richiesta di revoca o sospensione dei suoi certificati attraverso le seguenti modalità:

- Modalità 1: richiesta scritta con firma autografa presso il Presidente del Consiglio Notarile Distrettuale. Questi provvede all'inoltro della richiesta al Prestatore di Servizi Fiduciari mediante una delle modalità descritte nel presente paragrafo;
- Modalità 2: richiesta di revoca o sospensione del certificato sottoscritta con firma digitale;

- Modalità 3: richiesta telefonica in caso di emergenza utilizzando il codice di sospensione riservato del notaio ed il codice identificativo delle chiave di firma al Prestatore di Servizi Fiduciari; questa procedura va successivamente integrata con la richiesta scritta con la Modalità 1.

Modalità 1: richiesta scritta con firma autografa presso il Presidente del Consiglio Notarile Distrettuale.

Il Titolare deve compilare la richiesta indicando:

- nome e cognome;
- sede e distretto di appartenenza;
- dati identificativi del certificato (numero seriale);
- motivazione e decorrenza della revoca o sospensione;
- eventuali altri elementi rilevanti a determinare i casi di maggiore urgenza ovvero di emergenza.

Il Prestatore di Servizi fiduciari qualificati, ricevuta la richiesta, provvede alla revoca o sospensione del certificato, al suo inserimento nell'apposita Lista dei certificati revocati o sospesi (CRL) ed alla pubblicazione della Lista nel Registro dei certificati.

Il Prestatore di Servizi fiduciari qualificati comunica al notaio Titolare ed al Presidente del Consiglio Notarile Distrettuale l'avvenuta revoca o sospensione.

Modalità 2: richiesta di revoca o sospensione del certificato sottoscritta con firma digitale.

La domanda deve essere inoltrata dal notaio Titolare al Prestatore di Servizi Fiduciari, per via telematica, mediante il portale della Registration Authority (http://webra.ca.notariato.org), attraverso una richiesta sottoscritta con firma digitale sull'apposito modulo, con la stessa chiave oggetto di revoca, se ancora disponibile, nei tempi previsti nel presente manuale.

Il Titolare deve indicare nella richiesta:

- nome e cognome;
- sede e distretto di appartenenza;
- dati identificativi del certificato (numero seriale);
- motivazione e decorrenza della revoca o sospensione;
- eventuali altri elementi rilevanti a determinare i casi di maggiore urgenza ovvero di emergenza.

La richiesta firmata digitalmente è verificata dal Prestatore di Servizi fiduciari qualificati che provvede alla revoca o sospensione del certificato, al suo inserimento nell'apposita Lista dei certificati revocati e sospesi (CRL) ed alla pubblicazione della Lista nel Registro dei certificati.

Il Prestatore di Servizi fiduciari qualificati notifica al notaio Titolare ed al Presidente del Consiglio Notarile Distrettuale l'avvenuta revoca o sospensione

Modalità 3: richiesta telefonica in caso di emergenza utilizzando il codice riservato ed il codice identificativo del dispositivo di firma al Prestatore di Servizi Fiduciari.

Il Titolare provvede personalmente ad inoltrare al Prestatore di Servizi fiduciari qualificati (al numero telefonico indicato sul sito http://ca.notariato.it) la richiesta, facendosi identificare attraverso la comunicazione del proprio Codice Riservato e del codice identificativo.

Il Titolare deve fornire successivamente per iscritto i seguenti dati:

- nome e cognome;
- sede e distretto di appartenenza;

- motivazione e decorrenza della revoca o sospensione;
- gli elementi rilevanti a determinare i casi di emergenza.

Il Titolare deve provvedere ad inoltrare la medesima richiesta o a chiedere la riattivazione secondo una delle modalità precedentemente definite nei dieci giorni feriali successivi.

Il Prestatore di Servizi fiduciari qualificati provvede alla sospensione del certificato, al suo inserimento nella Lista dei certificati revocati e sospesi (CRL) ed alla pubblicazione della lista nel Registro dei certificati.

Il Prestatore di Servizi Fiduciari attende il completamento della procedura ordinaria e procede in conformità alla revoca, sospensione o alla riattivazione del certificato.

Il Prestatore di Servizi Fiduciari comunica al Titolare ed al Presidente del Consiglio Notarile Distrettuale l'avvenuta revoca, sospensione o riattivazione. La comunicazione viene effettuata con documento informatico firmato digitalmente, o con lettera raccomandata.

11.7 Procedure di revoca o sospensione dei certificati su richiesta del Presidente del Consiglio Notarile Distrettuale

Il Presidente del Consiglio Notarile Distrettuale può inoltrare la richiesta di revoca o sospensione dei certificati al Prestatore di Servizi fiduciari qualificati attraverso la seguente modalità:

- Modalità 1: richiesta scritta con firma autografa;
- Modalità 2: richiesta di revoca o sospensione del certificato sottoscritta con firma digitale;
- Modalità 3: richiesta telefonica in caso di emergenza utilizzando un codice riservato CRP del Presidente a disposizione del Presidente, come previsto al par. "Codici riservati ed il codice identificativo del notaio".

Modalità 1: richiesta scritta con firma autografa.

La richiesta scritta e sottoscritta dal Presidente del Consiglio Notarile Distrettuale è inoltrata al Prestatore di Servizi fiduciari qualificati nei tempi e con le modalità previste dal presente paragrafo.

La richiesta deve indicare:

- nome e cognome del Titolare;
- sede e distretto di appartenenza;
- dati identificativi del certificato (numero seriale);
- motivazione e decorrenza della revoca o sospensione;
- eventuali altri elementi rilevanti a determinare i casi di maggiore urgenza ovvero di emergenza.

Il Presidente comunica la richiesta al Prestatore di Servizi Fiduciari.

Il Prestatore di Servizi Fiduciari, ricevuta la richiesta, provvede alla revoca o sospensione del certificato, al suo inserimento nella apposita Lista dei certificati revocati o sospesi (CRL) ed alla pubblicazione della lista nel Registro dei certificati.

Il Prestatore di Servizi Fiduciari notifica al Titolare ed al Presidente del Consiglio Notarile Distrettuale l'avvenuta revoca o sospensione.

Modalità 2: richiesta di revoca o sospensione del certificato sottoscritta con firma digitale.

La domanda va inoltrata dal Presidente del Consiglio Notarile Distrettuale al Prestatore di Servizi fiduciari qualificati, per via telematica attraverso una richiesta sottoscritta con firma digitale sull'apposito modulo, nei tempi previsti nel presente manuale.

Il Presidente deve indicare nella richiesta:

- nome e cognome del Titolare;
- sede e distretto di appartenenza;
- dati identificativi del certificato (numero seriale);
- motivazione e decorrenza della revoca o sospensione;
- eventuali altri elementi rilevanti a determinare i casi di maggiore urgenza ovvero di emergenza.

La richiesta firmata digitalmente è verificata dal Prestatore di Servizi Fiduciari che provvede alla revoca o sospensione del certificato, al suo inserimento nella apposita Lista dei certificati revocati o sospesi (CRL) ed alla pubblicazione della lista nel Registro dei certificati.

Il Prestatore di Servizi Fiduciari comunica al Titolare ed al Presidente del Consiglio Notarile Distrettuale l'avvenuta revoca o sospensione.

Modalità 3: richiesta telefonica in caso di emergenza utilizzando un codice riservato per il Presidente al Prestatore di Servizi fiduciari qualificati.

Il Presidente del Consiglio Notarile Distrettuale provvede personalmente ad inoltrare al Prestatore di Servizi Fiduciari, al centro telefonico dallo stesso predisposto, la richiesta, facendosi identificare attraverso la comunicazione del codice riservato per il Presidente.

Il Presidente deve fornire al proprio interlocutore i seguenti dati:

- proprie generalità;
- nome e cognome del Titolare;
- sede e distretto di appartenenza;
- motivazione e decorrenza della revoca o sospensione;
- gli elementi rilevanti a determinare i casi di emergenza.

Il Presidente deve provvedere altresì ad inoltrare la medesima richiesta o a chiedere la riattivazione secondo una delle modalità precedentemente definite nei dieci giorni feriali successivi.

Il Prestatore di Servizi Fiduciari provvede alla sospensione del certificato, al suo inserimento nell'apposita Lista dei certificati revocati e sospesi (CRL) ed alla pubblicazione della lista nel Registro dei certificati.

Il Prestatore di Servizi Fiduciari attende il completamento della procedura ordinaria e procede alla revoca, sospensione o alla riattivazione del certificato.

Il Prestatore di Servizi Fiduciari comunica al Titolare ed al Presidente del Consiglio Notarile Distrettuale l'avvenuta revoca, sospensione o riattivazione. La comunicazione viene effettuata con documento informatico firmato digitalmente, o con lettera raccomandata.

11.8 Procedure di revoca o sospensione dei certificati su iniziativa del Prestatore di Servizi fiduciari qualificati

Il Prestatore di Servizi fiduciari qualificati può revocare o sospendere un certificato, comunicandone la motivazione e la data ed ora a partire dalla quale il certificato non sarà più valido o il periodo in cui risulterà sospeso.

Nei casi di motivata urgenza, il Prestatore di Servizi Fiduciari procede alla revoca senza fornire alcun preavviso al Titolare.

Il Prestatore di Servizi Fiduciari comunica al Titolare ed al Presidente del Consiglio Notarile Distrettuale l'avvenuta revoca, sospensione o riattivazione.

Disponibilità dei servizi di revoca o sospensione

Il Prestatore di Servizi fiduciari qualificati garantisce, per ogni modalità di inoltro delle richieste di revoca o sospensione, una diversa disponibilità del servizio ad essa connessa:

- per le richieste di revoca o sospensione inoltrate tramite modulo firmato digitalmente e trasmesso telematicamente il servizio è attivo 24 ore su 24;
- in caso di richiesta di revoca o sospensione sottoscritta in modo autografo, il servizio è disponibile dal Lunedì al Venerdì, dalle ore 09.00 alle ore 18.00;
- per le richieste di sospensione immediata inoltrate telefonicamente da parte del Presidente del distretto, il servizio sarà disponibile dal Lunedì al Venerdì, dalle ore 08.30 alle ore 20.00;
- per le richieste di sospensione immediata inoltrate telefonicamente da parte del titolare il servizio è attivo 24 su 24.

11.9 Aggiornamento delle Liste dei Certificati revocati e sospesi (CRL)

Le liste dei certificati revocati e sospesi sono aggiornate e pubblicate nel Registro dei certificati ogni 8 (otto) ore.

12. RIATTIVAZIONE DI UN CERTIFICATO SOSPESO

Il certificato sospeso, inserito nella Lista dei certificati sospesi e pubblicato nel Registro dei certificati, acquista nuovamente validità:

- automaticamente alla scadenza del periodo di sospensione;
- a seguito di una richiesta scritta di riattivazione del Presidente del CND con le stesse modalità previste per la richiesta di revoca o di sospensione.
- a seguito di richiesta tramite modulo firmato digitalmente da parte del Presidente di distretto e trasmessa telematicamente.

Alla cessazione dello stato di sospensione del certificato, esso sarà considerato come mai sospeso.

12.1 Procedura di riattivazione del certificato sospeso

Alla scadenza del periodo di sospensione, oppure su richiesta scritta di riattivazione, presentata con le modalità di cui in precedenza, il Prestatore di Servizi fiduciari qualificati procede alla riattivazione del certificato attraverso la cancellazione dello stesso dalla Lista dei certificati revocati e sospesi (CRL). Dell'avvenuta riattivazione è data comunicazione al Titolare ed al Presidente del CND, mediante documento informatico firmato digitalmente o con lettera raccomandata.

12.1.1 Procedura di riattivazione automatica del certificato sospeso

Il Prestatore di Servizi fiduciari qualificati attiva la procedura di riattivazione del certificato che prevede la:

- cancellazione del Certificato da riattivare dalla lista dei certificati revocati e sospesi (CRL);
- pubblicazione della lista CRL;
- registrazione dell'avvenuta Riattivazione nel Giornale di controllo;
- invio di un messaggio al Notaio e al Presidente del CND relativo all'avvenuta riattivazione.

13. REVOCA DEI CERTIFICATI RELATIVI ALLE CHIAVI DIAGID

13.1 Procedura di revoca e sostituzione dei certificati relativi alle chiavi dell'Autorità

AgID in caso di compromissione della propria chiave segreta ovvero a seguito della sostituzione dei soggetti designati alla sottoscrizione dell'elenco pubblico dei certificatori richiede a ciascun Prestatore di Servizi Fiduciari la revoca tempestiva del certificato ad essa rilasciato.

AgID procede alla sostituzione della chiave revocata. I Certificatori provvedono quindi, alla certificazione della nuova coppia di chiavi generata da AgID.

14. RINNOVO DEI CERTIFICATI DI FIRMA

14.1 Rinnovo dei Certificati del Titolare

I certificati di firma hanno una validità di tre anni. Tale validità vincola e limita l'utilizzo dei certificati, e delle relative chiavi, da parte del Titolare che, almeno novanta giorni prima della scadenza, dovrà chiedere la sostituzione delle chiavi di firma al Presidente del CND. Il Presidente richiede un nuovo certificato secondo la procedura riportata al par 7.7.

La procedura in oggetto si applica nei casi di rinnovo o di revoca fermo restando il mantenimento delle condizioni di rilascio del dispositivo di firma.

14.2 Sostituzione delle chiavi di certificazione

Il Prestatore di Servizi fiduciari qualificati, 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 adAgID 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, il Prestatore di Servizi Fiduciari esegue la procedura di creazione delle copie delle chiavi di certificazione da utilizzare in caso di disastro.

15. REGISTRO DEI CERTIFICATI

15.1 Informazioni contenute nel Registro dei certificati

Il Prestatore di Servizi fiduciari qualificati pubblica le seguenti informazioni nel Registro dei certificati:

- il certificato, relativo alla chiave di certificazione, sottoscritto con la chiave privata della coppia cui il certificato si riferisce
- il certificato rilasciato ad AgID;
- 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 Deliberazione CNIPA 45/2009.

15.2 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.

Il Prestatore di Servizi Fiduciari 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.

15.3 Procedura di aggiornamento del Registro dei certificati

Il Prestatore di Servizi fiduciari qualificati provvede all'aggiornamento del Registro dei certificati quando:

- emette nuovi certificati per AgID;
- pubblica Liste dei certificati revocati e sospesi in seguito alla revoca o alla sospensione di un certificato ogni 8 (otto) ore.

Il Prestatore di Servizi Fiduciari cura l'allineamento tra copia di riferimento copia operativa e copia di sicurezza del Registro dei certificati secondo la seguente procedura:

- Il Responsabile del Registro dei certificati controlla l'applicazione che pubblica ed aggiorna la Lista dei certificati emessi indicati al paragrafo 15.1 sulla copia di riferimento. L'inserimento/cancellazione di un certificato nella copia di riferimento viene registrato nel Giornale di controllo;
- Il Responsabile del Registro dei certificati controlla l'applicazione che pubblica ed aggiorna le Liste dei certificati revocati e sospesi sulla copia di riferimento. L'inserimento/cancellazione di un certificato nella CRL viene registrato nel Giornale di controllo;
- Il Responsabile del Registro dei certificati cura l'allineamento tra la copia di riferimento e la copia operativa.

15.4 Modalità di accesso al Registro dei certificati

La copia operativa del registro dei certificati è un Internet Directory Server e server LDAP compatibile con le specifiche X.500 e che supporta il protocollo LDAP v.3. 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.

16. PROTEZIONE DELLA RISERVATEZZA

16.1 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 con riferimento al Regolamento UE 679/2016.

17. GESTIONE DELLE COPIE DI SICUREZZA

Il Prestatore di Servizi fiduciari qualificati 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.

18. 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, 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.

18.1 Disponibilità dei servizi

Il Prestatore di servizi fiduciari garantisce i servizi descritti nel precedente paragrafo al 99% di disponibilità su base annua.

18.2 Gestione degli eventi catastrofici

Il Prestatore di servizi fiduciari qualificati garantisce la continuità del servizio, in caso di disastro, attraverso la predisposizione di opportune procedure che consentono il ripristino, in tempi brevi, di quei servizi del sistema di certificazione che devono essere mantenuti sempre disponibili.

I rischi che minacciano l'integrità di un servizio sono classificabili in tre tipologie:

- naturali;
- umani;
- tecnici.

Nello schema che segue sono descritti i principali eventi catastrofici gestiti dal Prestatore di servizi fiduciari ed i tempi di ripristino per i soli servizi ad alta priorità.

Tipo di disastro	Tempi di ripristino servizi
Calamità naturali	48 ore
Incendio (esterno)	48 ore

Incendio (interno)	48 ore
Dolo	48 ore
Indisponibilità prolungata del sistema	48 ore
Esplosioni (est./Int.)	48 ore

Nota: i tempi di ripristino riportati in tabella sono al netto del tempo necessario a dichiarare lo stato di disastro.

18.3 Procedure di gestione degli eventi catastrofici

Le procedure per la gestione degli eventi catastrofici sono dettagliatamente descritte nel Piano per la sicurezza e nella Procedura di Disaster Recovery.

19. GIORNALE DI CONTROLLO

Tutte le registrazioni effettuate automaticamente dai dispositivi installati presso il Prestatore di Servizi Fiduciari sono archiviate ed annotate nel Giornale di controllo.

19.1 Dati da archiviare

Secondo quanto stabilito dal D.P.C.M. in vigore, 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

19.2 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 30 anni.

La data e l'ora utilizzate provengono da NTP server la cui precisione è conforme con il DPCM in vigore, e cioè discosta al massimo di 1 minuto dal tempo UTC(IEN). L'allineamento dei sistemi dedicati alla CA avviene ogni ora.

19.3 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.

19.4 Gestione del Giornale di controllo

Alla funzione della Sicurezza Dati è demandato il compito di gestire il Giornale di controllo, attraverso l'effettuazione di operazioni di back-up, controlli e report periodici.

19.5 Verifiche

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

20. CESSAZIONE DELL'ATTIVITÀ DEL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI

Il Prestatore di Servizi fiduciari qualificati se intende cessare l'attività comunica 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 il Prestatore di Servizi Fiduciari informa i possessori dei certificati da esso 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.

21. APPENDICE A - MODALITÀ OPERATIVE PER STATICIZZARE I DOCUMENTI

A.1 Macro e codici automatici

Le macro e i codici automatici (come ad es. i campi automatici, indici e riferimenti) sono delle procedure automatizzate che permettono di fare diverse operazioni automatiche nei documenti alterandone il contenuto.
Esse possono essere eseguite all'atto dell'apertura di un documento e possono accedere a tutte le funzioni del sistema operativo.

Tutti i software di videoscrittura o di composizione documenti possono contenere delle macro e pertanto è necessario, prima di procedere alla firma, staticizzare il documento preferibilmente nel formato pdf/A.

A.2 Precauzioni per il formato TIFF

Per quanto riguarda il formato TIFF va adottata la seguente cautela: modificare l'estensione del file da .TIF a .HTM e verificare che, aprendolo, non compaia nulla che abbia senso compiuto, nel qual caso il file in questione non deve essere utilizzato.

Il formato TIFF può infatti nascondere tracce di script che ne alterano il contenuto.

A.3 Produzione di un PDF/A

Il formato pdf/A è normato dallo standard ISO 19005-1:2005 e consente di staticizzare i documenti in quanto non consente l'inserimento di contenuti audio/video e javascript, include i font utilizzati, e altro ancora. E' possibile generare un documento in formato staticizzato pdf/A:

- con Adobe Acrobat
- con altri software open source come PDFCreator, OpenOffice.
- da qualsiasi software di produzione documentale scegliendo Stampa, quindi Adobe PDF come stampante (se disponibile Adobe Acrobat).

Di seguito a titolo di esempio si riportano alcune istruzioni per Adobe Acrobat.

Innanzitutto è possibile verificare se il pdf che si sta elaborando è compatibile con pdf/A selezionando l'opzione "Verifica preliminare" dal menu "Avanzate".

1. Se l'icona PDF/X o PDF/A nella parte inferiore sinistra della finestra di dialogo Verifica preliminare indica che il PDF non è compatibile con PDF/X o PDF/A, eseguire una delle operazioni seguenti:

Fare clic sull'icona accanto al testo "Non è un file PDF/A".

Scegliere Converti PDF corrente in PDF/A dal menu Opzioni.

2. Selezionare uno standard PDF/A.
3. Specificare le opzioni di conversione, quindi fare clic su OK.
4. In base ai risultati della conversione, scegliere una delle seguenti procedure:

a) Se la conversione viene eseguita correttamente, salvare il file PDF. Nella finestra di dialogo Verifica preliminare viene visualizzato un segno di spunta di colore verde.
b) Se la conversione non riesce, visualizzare i risultati nell'elenco Risultati oppure fare clic su Rapporto per visualizzarli. Nella finestra di dialogo Verifica preliminare viene visualizzata un segno X di colore rosso. Quando richiesto, fare clic su OK per visualizzare i risultati della Verifica preliminare.

Si può generare un file pdf/A da altro software di produzione documentale (es. Word, OpenOffice), scegliendo Stampa, quindi Adobe PDF come stampante. Poi cliccando sul pulsante Proprietà, e sulla scheda Preferenze Adobe PDF, occorre scegliere dal primo menu a tendina "Opzioni predefinite" la voce "PDF/A-1b(RGB)". E procedere poi con il salvataggio del file.

Il presente manuale operativo è stato approvato dal responsabile, presidente pro-tempore del Consiglio Nazionale del Notariato.

Roma, 26/10/2018.

Il presidente del CNN