CONSIGLIO NAZIONALE DEL NOTARIATO

Consiglio Nazionale del Notariato

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

versione 4.1

SOMMARIO

VERSIONI DOCUMENTO

VERSIONE	DESCRIZIONE MODIFICA	DATA emissione
1.0.0	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 maggio 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	i. luglio 2008

	registro pubblico dei certificati c. Eliminazione dell' emissione di marca temporale all'atto della pubblicazione della CRL	
4	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

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 Certificatore con la propria chiave privata di certificazione.
Certificato qualificato	Ai sensi dell'articolo 1, comma 1, lett. f del decreto legislativo 7 marzo 2005 n. 82, è il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciato da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva ed avente le caratteristiche fissate dal DPCM 30 marzo 2009, nonché dalla Deliberazione CNIPA 45/2009.
Certificatore	Ente che svolge le attività di generazione, emissione, conservazione, revoca e sospensione dei certificati.
Certificatore accreditato	Certificatore iscritto nell'albo tenuto dal DigitPA/AgID, ai sensi degli artt. 3 e 4 della direttiva n. 1999/93/CE, come previsto dall'art. 29 del Dlgs 82/2005
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 Certificatore 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 30 marzo 2009.
Distinguished Name	Identificativo univoco del Titolare presso il Certificatore.

(Dname)	
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.
Lista di revoca dei certificati (CRL)	Lista firmata digitalmente, tenuta ed aggiornata dal Certificatore contenente i certificati emessi dallo stesso e successivamente sospesi o revocati.
Manuale operativo	Documento pubblico depositato presso il DigitPA/AgID che definisce le procedure applicate dal Certificatore 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.
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 Certificatore, la lista dei certificati revocati e la lista dei certificati sospesi, accessibile anche telematicamente.
Revoca del certificato	Operazione con cui il Certificatore 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 Certificatore 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
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.
TSS	Time Stamping Server 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 certificatore accreditato, ai sensi dell'art. 29 del Decreto Legislativo n.82/2005. Esso si riferisce ai servizi di:

- Certificazione delle chiavi pubbliche dei notai
- Generazione di marche temporali

Il Manuale Operativo vincola il Certificatore e tutti i soggetti che entrano in relazione con il Certificatore.

Il presente documento definisce inoltre gli obblighi e le responsabilità del Certificatore, 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)
- Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche
- Art. 15, comma 2, Legge 15 marzo 1997 n. 59
- Decreto Legislativo 30 giugno 2003 n. 196
- 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

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 CERTIFICATORE

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	Indirizzo E-mail: certificazione@notariato.it
Indirizzo Internet: http://ca.notariato.it	Call Center: 06-36209306

3. MANUALE OPERATIVO

3.1 Dati identificativi del Manuale operativo

Il presente Manuale operativo, conservato presso i locali del Certificatore e depositato presso il DigitPA/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 4.1.

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

1.3.6.1.4.1.8526.1.1.4 Certificazione Chiavi.

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

1.3.6.1.4.1.8526.1.2.4 Servizio di marcatura temporale

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	1.3.6.1.4.1.8526.1.1
Manuale Operativo ver 4	1.3.6.1.4.1.8526.1.1.4
Timestamp policy	1.3.6.1.4.1.8526.1.2
Policy marcatura temporale	1.3.6.1.4.1.8526.1.2.4

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. OBBLIGHI DEL CERTIFICATORE, DEL TITOLARE E DI QUANTI ACCEDONO PER LA VERIFICA DELLE FIRME

4.1 Obblighi del Certificatore

Nello svolgimento della sua attività, il Certificatore:

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. 30 marzo 2009;
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 Decreto Legislativo 30 giugno 2003 n. 196;
10. non si rende depositario di chiavi private dei Titolari;

11. 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;
12. procede tempestivamente alla revoca od alla sospensione del certificato in tutti i casi previsti dal presente Manuale Operativo;
13. comunica le richieste di revoca o sospensione al Titolare;
14. dà tempestiva pubblicazione della revoca e della sospensione del certificato;
15. conserva le richieste scritte di registrazione e le richieste di certificazione per un periodo di almeno 30 anni dalla data di scadenza del certificato;
16. comunica per iscritto a DigitPA/AgID ogni variazione dei requisiti per l'iscrizione all'Elenco pubblico dei Certificatori accreditatidi cui all'art. 39 del D.P.C.M. 30 marzo 2009 e all'art. 29 del Decreto Legislativo 7 marzo 2005 n.82, e, in ogni caso, annualmente conferma la permanenza dei requisiti per l'esercizio dell'attività di certificazione;
17. comunica tempestivamente a DigitPA/AgID, ogni variazione significativa delle soluzioni tecnico-organizzative adottate;
18. comunica immediatamente a DigitPA/AgID e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso;
19. comunica al DigitPA/AgID ed agli utenti, 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.

4.2 Obblighi del Titolare

Il Titolare è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

Il Titolare della chiave deve, inoltre:

1. fornire tutte le informazioni richieste dal Certificatore, garantendone, sotto la propria responsabilità, l'attendibilità;
2. conservare le chiavi private all'interno del dispositivo di firma;
3. conservare con la massima diligenza la chiave privata e il dispositivo che la contiene al fine di garantirne l'integrità e conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave;
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 macro istruzioni 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 contenute in dispositivi di firma inutilizzabili, di cui abbia perduto il possesso o o il controllo esclusivo o qualora abbia il ragionevole dubbio che essi possano essere usati da altri;

8. redigere per iscritto la richiesta di revoca, specificando la sua decorrenza;
9. 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;
10. sporgere denuncia, in caso di smarrimento o sottrazione del dispositivo di firma, alle Autorità competenti.

E' vietata la duplicazione della chiave privata e dei dispositivi che la contengono.

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 le buste oscurate siano consegnate integre al destinatario e consegnare quanto eventualmente necessario per l'utilizzo del dispositivo di firma;
3. sottoscrivere la richiesta di emissione dei certificati;
4. 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;
5. sospendere e revocare i certificati tutte le volte in cui ciò si renda necessario;
6. riattivare i certificati sospesi;
7. richiedere la sostituzione dei dispositivi di firma dei titolari in accordo con i relativi paragrafi del presente manuale.

5. RESPONSABILITÀ

5.1 Responsabilità del certificatore

Il Certificatore è responsabile verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dalla Direttiva Europea 13 dicembre 1999 n. 1999/93/CE, dal D. Lgs n.196/2003, dal D. Lgs. n. 82/05, dalla Circolare CNIPA 6 settembre 2005, n.48, dalla Deliberazione CNIPA n. 45/09, dal D. Lgs. 159/2006, dal D.P.C.M. 30 marzo 2009.

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 certificatore 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 del dispositivo 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 sito ca.notariato.it.

L'emissione di una marca temporale può comporta l'addebito al richiedente di un importo in euro pubblicato sul sito ca.notariato.it

In caso di richiesta di più marche temporali contestuali l'addebito sarà effettuato per ciascuna marca temporale richiesta.

Le tariffe sono pubblicate sul sito ca.notariato.it..

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 Certificatore 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 del CND richiede al CNN l'emissione di una coppia di chiavi 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 Certificatore, 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 Certificatore e i Titolari

Il titolare deve disporre di una casella di posta elettronica, che potrà essere utilizzata dal Certificatore per inviare comunicazioni.

L'eventuale variazione dell'indirizzo di posta elettronica dovrà essere comunicata al CNN con messaggio sottoscritto dal Titolare.

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 Certificatore fornisce al notaio un codice riservato che permetterà allo stesso, 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 Certificatore 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 dispositivi di firma. La richiesta contiene i dati anagrafici del notaio e l'indirizzo al quale spedire il dispositivo di firma e quanto relativo.		
		Per ogni dispositivo di firma richiesto: • associa ad ogni notaio un codice identificativo ed un codice riservato contenuto in una busta oscurata; • 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 spedisce al CND altro plico contenente le buste oscurate con il codice identificativo con l'associato codice riservato ed ogni altro codice (es. PIN, PUK) necessario alla generazione delle chiavi internamente al dispositivo di firma.
Il Presidente del CND, contestualmente o successivamente all'iscrizione a ruolo nel distretto di competenza, consegna le buste oscurate al notaio.		

	Il notaio, al ritiro delle buste, dopo averne verificato l'integrità, firma un'apposita dichiarazione attestante lo stato di integrità o di manomissione delle buste stesse e, ove esse risultino integre, l'uso esclusivo della firma nell'espletamento delle funzioni di notaio.	
	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.	
		Il Certificatore genera il certificato digitale sulla base della richiesta pervenuta.
	Il titolare, tramite apposito applicativo software, memorizza il certificato digitale all'interno del dispositivo di firma.	

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

Il sistema di generazione delle chiavi assicura:

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

La generazione delle chiavi avviene all'interno del dispositivo di firma.

8.2 Lunghezza delle chiavi

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

La lunghezza delle chiavi di sottoscrizione è di almeno 1024 bit.

8.3 Algoritmi

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 Certificatore si avvale delle seguenti chiavi di certificazione:

- chiavi di certificazione per firmare i certificati relativi alle chiavi di sottoscrizione e le liste di revoca (CRL);
- chiavi di certificazione per firmare i certificati relativi alle chiavi di marcatura temporale.

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 dispositivo di firma personalizzato dalla postazione predisposta a tale funzione dal Certificatore.

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 consegnato dal CND, 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.

8.7 Requisiti del dispositivo di firma

Il dispositivo di firma deve essere in grado di memorizzare la chiave privata e di generare la firma digitale, senza mai comunicare la chiave stessa all'esterno.

L'utilizzo della chiave privata 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 ovvero, potrà essere subordinato al positivo riconoscimento biometrico.

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 Certificatore;
- codice identificativo del Titolare presso il Certificatore (nel campo Subject come specificato nella Deliberazione CNIPA 45/2009);
- nome, cognome ecodice 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 Certificatore, 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 certificatore.

Sempre in conformità alla Deliberazione DigitPA n. 45/2009 il certificato del titolare contiene l'estensione qCStatement, ed in particolare:

- contiene il campo identificato come id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1) che indica che il certificato è qualificato.
- non contiene l'estensione id-etsi-qcs-QcLimitValue (OID: 0.4.0.1862.1.2), assente in quanto non sono applicabili limiti nelle negoziazioni;
- contiene il campo 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 Certificatore;
- contiene il campo id-etsi-qcs-QcSSCD (OID: 0.4.0. 1862.1.4), che indica la memorizzazione della chiave privata internamente ad un dispositivo sicuro.

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 Certificatore per trenta anni dalla data di scadenza del certificato.

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 e deve essere attivata a seguito di riconoscimento del titolare tramite codice identificativo (PIN) o tramite un eventuale sistema di riconoscimento biometrico. 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 il dispositivi di firma rilasciato al notaio;verificare una firma apposta a documenti firmati digitalmente secondo il formato definito dallaDeliberazione CNIPA 45/2009

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 Certificatore pubblica la revoca e la sospensione dei certificati mediante la Lista dei certificati revocati (CRL) ogni 8 ore.

Il Certificatore 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 Certificatore 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 Certificatore;
- 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 certificatore la revoca del proprio certificato nei seguenti casi:

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

In caso di perdita del possesso del dispositivo di firma, 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.

Su richiesta del Presidente del CND:

Il Presidente del CND richiede tempestivamente la revoca dei certificati per:

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

Su iniziativa del certificatore:

1. Il Certificatore 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.
2. Salvo i casi di urgenza, la revoca del certificato è preventivamente comunicata dal Certificatore 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 certificatore con decorrenza dalla data di fine del periodo di sospensione.

Su richiesta del notaio:

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

Su richiesta del Presidente del CND:

Il Presidente CND richiede la sospensione dei certificati in tutti i casi di cessazione temporanea dall'esercizio notarile non derivanti dall'esecuzione di provvedimenti dell'autorità giudiziaria.Il Presidente del CND può richiedere la sospensione dei certificati per concessione di permesso di assenza al notaio titolare.

Su iniziativa del certificatore:

Il Certificatore 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 Certificatore procede alla revoca del certificato relativo ad una coppia di chiavi di certificazione esclusivamente nei seguenti casi (art. 27 del D.P.C.M. 30 marzo 2009):

- 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 DigitPA/AgID, ed a tutti i possessori di certificati sottoscritti con la chiave privata appartenente alla coppia revocata, entro le 24 ore.

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 Certificatore 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 DigitPA/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 certificatore 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 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 Certificatore 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 del dispositivo di firma al Certificatore; 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 Certificatore, 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 Certificatore 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 Certificatore, 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 Certificatore 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 Certificatore 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 Certificatore.

Il Titolare provvede personalmente ad inoltrare al Certificatore (al numero telefonico indicato sul sito http://ca.notariato.it) la richiesta, facendosi identificare attraverso la comunicazione del proprio Codice riservato (CRN) 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 Certificatore 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 Certificatore attende il completamento della procedura ordinaria e procede in conformità alla revoca, sospensione o alla riattivazione del certificato.

Il Certificatore 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 Certificatore 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 Certificatore 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 Certificatore.

Il Certificatore, 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 Certificatore 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 Certificatore, 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 Certificatore 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 Certificatore 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 Certificatore.

Il Presidente del Consiglio Notarile Distrettuale provvede personalmente ad inoltrare al Certificatore, 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 Certificatore 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 Certificatore attende il completamento della procedura ordinaria e procede alla revoca, sospensione o alla riattivazione del certificato.

Il Certificatore 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 Certificatore

Il certificatore 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 certificatore procede alla revoca senza fornire alcun preavviso al Titolare.

Il Certificatore comunica al Titolare ed al Presidente del Consiglio Notarile Distrettuale l'avvenuta revoca, sospensione o riattivazione.

Disponibilità dei servizi di revoca o sospensione

Il Certificatore 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 (quattro) 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 Certificatore 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 Certificatore 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. SERVIZIO DI MARCATURA TEMPORALE E RIFERIMENTO TEMPORALE DEL CERTIFICATORE

Il CNN fornisce un servizio di validazione temporale di documenti informatici, siano essi firmati digitalmente o non firmati.

Il servizio di marcatura temporale permette di associare un riferimento temporale ai documenti elettronici in modo da garantire inequivocabilmente l'esistenza del documento informatico in un determinato istante temporale.

La marca temporale è una struttura dati firmata digitalmente che lega in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo (data e ora).

La marca temporale viene firmata ed emessa da una specifica autorità denominata Time Stamping Authority (TSA) che emette e firma le marche temporali mediante uno o più sistemi dedicati (Time Stamping Server (TSS)) al quale gli utenti indirizzano le loro richieste.

Una Certification Authority (TSA CA) dedicata emette i certificati con i quali i TSS firmano le marche temporali.

La verifica di una marca temporale comporta la verifica della catena di certificazione TSS - TSA CA.

13.1 Generazione chiavi

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

Il sistema di generazione delle chiavi assicura:

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

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

13.2 Lunghezza delle chiavi di marcatura temporale

La lunghezza delle chiavi di marcatura temporale è di almeno 1024 bit.

13.3 Algoritmi

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

- RSA (Rivest-Shamir-Adleman algorithm).

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

- SHA-256 (Dedicated Hash Function 4)

13.4 Chiavi di marcatura temporale

13.4.1 Generazione delle chiavi di marcatura temporale

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

13.4.2 Certificazione delle chiavi di marcatura temporale

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

13.4.3 Scadenza delle chiavi di marcatura temporale

Le chiavi di marcatura temporale hanno durata massima coincidente con la scadenza della CA che le certifica e sono sostituite dopo non più di 3 mesi di utilizzo, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato.

13.5 Richiesta di emissione o di verifica di marca temporale

La richiesta di emissione di marca temporale può essere effettuata utilizzando il software di firma fornito dal CNN, che consente di apporre la marca temporale a documenti informatici, anche firmati digitalmente, e di eseguire le operazioni di verifica.

La verifica deve essere effettuata tramite il software di firma oppure tramite il verificatore online, forniti dal CNN o da altro certificatore accreditato presso l'albo dell' AID.

La richiesta è inoltrata al server TSS che la elabora, genera la marca temporale e la rinvia al client, che restituisce all'utente l'esito della richiesta.

Per la richiesta di emissione di marca temporale, l'utente seleziona il documento informatico da marcare e il formato della marca temporale; l'opportuna procedura software ne calcola l'hash, che invia poi al TSS per la marcatura; l'utente riceve in risposta un unico file nel formato prescelto contenente la marca temporale.

I formati possibili sono:

- Time stamp response, previsto dalla normativa vigente, contiene la sola marca temporale.
- Timestamped Data, previsto dalla normativa vigente, contiene la marca temporale e il documento a cui è associata.
- M7M, formato proprietario di InfoCamere, utilizzato per alcuni adempimenti verso le camere di commercio.

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

Il software di verifica della marca temporale svolge i seguenti controlli:

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

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

Il sistema di verifica visualizza le seguenti informazioni:

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

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

13.6 Emissione di una marca temporale

L'emissione della marca temporale viene effettuata dal server TSS, gestito dal Certificatore, che è in grado di calcolare con precisione la data e l'ora di generazione della marca temporale con riferimento al Tempo Universale Coordinato (UTC), generare la struttura di dati contenente le informazioni necessarie.

La struttura dati della marca temporale contiene, tra le varie informazioni, l'impronta generata dall'utente e la data/ora corrente ottenuta da una fonte esatta.

Il server TSS appone la firma alla struttura dati generata, ottenendo la marca temporale.

Terminata la procedura di generazione della marca temporale, quest'ultima viene inviata all'utente.

13.7 Validità della marca temporale

La marca temporale e' valida per l'intero periodo di conservazione a cura del Certificatore CNN.

Il CNN conserva le marche temporali per un periodo di tempo almeno pari al minimo di quello indicato dalla normativa in vigore.

13.8 Marca Temporale

13.8.1 Formato e contenuto della marca temporale

Il formato delle marche temporali ed il protocollo di colloquio con la TSA rispettano le specifiche tecniche riportate in RFC 3161 "Internet X.509 Public Key InfrastructureTime Stamp Protocol (TSP)" - PKIX Working Group IETF – Agosto 2001.

Ogni marca temporale emessa contiene tutte le informazioni richieste dalla normativa, ovvero:

- identificativo del C.N.N.;
- numero di serie della marca temporale;
- algoritmo di sottoscrizione della marca temporale;
- identificativo del certificato del TSS relativo alla chiave di verifica della marca temporale;
- data ed ora di generazione, con riferimento al Tempo Universale Coordinato (UTC);
- algoritmo di hash utilizzato per generare l'impronta;
- valore dell'impronta del documento sottoposto a validazione temporale;

13.8.2 Precisione del riferimento temporale

In fase di generazione di una marca temporale, il server TSS ricava la data/ora dal clock del sistema, mantenuto allineato con l'ora esatta UTC (Tempo Universale Coordinato) grazie al segnale di sincronia ottenuto da un ricevitore esterno del segnale emesso dalla rete dei satelliti GPS.

Il segnale orario così ottenuto rispetta i margini di precisione richiesti dalla normativa vigente.

13.9 Tempi di emissione della marca temporale

La generazione delle marche temporali garantisce che il tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, a meno di impedimenti nell'emissione della marca stessa, non sarà superiore al minuto primo.

13.10 Registrazione delle marche generate

Tutte le marche temporali emesse, assieme alle relative richieste sono conservate in un apposito archivio digitale non modificabile per il periodo indicato dalla normativa vigente.

L'accesso ai dati, contenuti nei diversi archivi, è consentito solo agli operatori opportunamente abilitati.

L'utente può ottenere una copia della marca temporale facendone richiesta fornendo i seguenti dati:

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

I dati contrassegnati con (*) sono OBBLIGATORI.

13.11 Sicurezza del sistema di validazione temporale

Il sistema per il servizio di marcatura temporale può essere attivato solo da operatori autorizzati.

Un eventuale arresto del sistema può essere risolto solamente dagli operatori autorizzati.

I dettagli operativi sono riportati nel Piano per la sicurezza del certificatore.

13.12 Revoca di certificati relativi a chiavi di marcatura temporale

13.12.1 Circostanze di revoca

La revoca del certificato relativo ad una coppia di chiavi di marcatura temporale effettuata su iniziativa del certificatore ed è consentita esclusivamente nei seguenti casi:

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

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

Il certificato revocato deve essere inserito in una lista di revoca aggiornata immediatamente e pubblicata.

Della pubblicazione della CRL è fatta annotazione nel giornale di controllo.

13.13 Sostituzione delle chiavi di marcatura temporale

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

14. REVOCA DEI CERTIFICATI RELATIVI ALLE CHIAVI DEL DIGITPA/AGID

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

Il DigitPA/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 Certificatore la revoca tempestiva del certificato ad essa rilasciato.

Il DigitPA/AgID procede alla sostituzione della chiave revocata. I Certificatori provvedono quindi, alla certificazione della nuova coppia di chiavi generata dal DigitPA/AgID.

15. MODALITÀ DI SOSTITUZIONE DEI DISPOSITIVI DI FIRMA

15.1 Sostituzione delle chiavi 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 del dispositivo di firma al Presidente del CND. Il Presidente rilascia un nuovo dispositivo secondo la procedura riportata al par 7.7.

15.2 Sostituzione delle chiavi di certificazione

Il Certificatore, novanta giorni prima della scadenza del certificato relativo ad una chiave di certificazione, avvia la procedura di sostituzione, generando una nuova coppia di chiavi.

In aggiunta al certificato relativo alla nuova coppia di chiavi di certificazione di cui sopra, il Certificatore genera:

- un certificato, relativo alla nuova chiave pubblica sottoscritto con la chiave privata della vecchia coppia;
- un certificato relativo alla vecchia chiave pubblica sottoscritto con la nuova chiave privata.

I certificati così generati sono forniti al DigitPA/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, il Certificatore esegue la procedura di creazione delle copie delle chiavi di certificazione da utilizzare in caso di disastro.

16. REGISTRO DEI CERTIFICATI

16.1 Informazioni contenute nel Registro dei certificati

Il Certificatore 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 al DigitPA/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.

16.2 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 Certificatore 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.

16.3 Procedura di aggiornamento del Registro dei certificati

Il Certificatore provvede all'aggiornamento del Registro dei certificati quando:

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

Il Certificatore 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 16.1 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.

16.4 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.

17. PROTEZIONE DELLA RISERVATEZZA

17.1 Modalità di protezione della riservatezza

Tutti i dati che risiedono su database sono protetti da prodotti che implementano politiche di autorizzazione per l'accesso ai dati legati a meccanismi di autenticazione degli utenti.

Le misure di protezione adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali emanate con il Decreto Legislativo 196/2003 nell'esecuzione delle seguenti attività:

- individuazione degli incaricati;
- assegnazione di codici identificativi;
- protezione degli elaboratori;
- modalità di designazione degli incaricati del trattamento.

18. GESTIONE DELLE COPIE DI SICUREZZA

Il Certificatore effettua periodicamente, e secondo politiche ben definite, copie di sicurezza del sistema di certificazione.

Tali copie sono mantenute in armadi di sicurezza siti in locali diversi e ugualmente protetti. In tal modo viene garantita l'integrità dei dati e la continuità del servizio di certificazione.

Le procedure per la gestione delle copie di sicurezza sono descritte nel Piano per la sicurezza.

19. DISPONIBILITÀ DEL SERVIZIO

19.1 Classificazione dei servizi

Nell'ambito della politica di disaster recovery i servizi forniti dal sistema sono stati classificati secondo tre livelli di priorità:

- PRIORITÀ 1: A questa classe appartengono tutti i servizi per i quali, in caso di disastro, sono richiesti tempi di ripristino minimi;
- PRIORITÀ 2: A questa classe appartengono tutti i servizi per i quali, in caso di disastro, non sono richiesti tempi di ripristino del servizio minimi.
- PRIORITÀ 3: A questa classe appartengono i servizi per i quali non è previsto il ripristino del servizio sul sito di disaster recovery ma solo il ripristino presso il sito principale

Nell'ambito della strategia di *disaster recovery* adottata, è prevista l'esistenza di un sito di "backup" che garantisce, in primo luogo l'espletamento dei servizi cui è assegnato un livello di priorità 1 ed in un secondo momento anche l'espletamento dei servizi con priorità più bassa. Per i servizi afferenti alla priorità 3 è previsto il ripristino del servizio solo presso il sito primario con una politica di di intervento basata sul "best effort".

Alle classi di priorità definite in precedenza vengono associati i seguenti servizi: PRIORITÀ 1 – "mission critical"

- Verifica certificati: servizio di verifica della validità dei certificati, che si poggia sul funzionamento, 24 ore al giorno e 7 giorni su 7, delle macchine sulle quali sono in esecuzione i Directory Service. Revoca/sospensione: i servizi di revoca/sospensione dei certificati e di aggiornamento o archiviazione del Giornale di controllo che si poggiano sul funzionamento del Certification Authority server e del rispettivo database.
- Verifica Marche temporali: servizio di verifica della validità dei certificati con i quali sono state firmate le marche temporali. Tale servizio si poggia sul funzionamento 24 ore al giorno e 7 giorni su 7 delle macchine sulle quali sono in esecuzione il Directory Service sia presso il sito primario che presso il sito secondario.

I servizi a priorità più bassa sono :

PRIORITÀ 2

- Registrazione-Generazione: in caso di disastro, l'interruzione temporanea - nell'ordine di qualche giorno - del servizio di registrazione e generazione dei certificati relativi a chiavi di sottoscrizione può essere tollerata. E' stata prevista a tal scopo un'opportuna architettura ed appropriate procedure, idonee a ripristinare il servizio in tempi brevi.

PRIORITÀ 3

- Generazione Marche temporali: in caso di indisponibilità il servizio viene ripristinato con una politica di "best effort" presso il sito principale. A tal fine una opportuna architettura e delle appropriate procedure permettono il ripristino in tempi brevi.

19.2 Disponibilità dei servizi

Il Certificatore garantisce i servizi classificati nel precedente paragrafo secondo le seguenti percentuali di disponibilità del servizio:

Tipo di Servizio	Disponibilità del Servizio
Servizi in Priorità 1	99% di disponibilità su base annua
Servizi in Priorità 2	99% di disponibilità su base annua
Servizi in Priorità 3	98% di disponibilità su base annua

19.3 Gestione degli eventi catastrofici

Il Certificatore 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 Certificatore.

Tipo di disastro	Tempi di ripristino servizi priorità 1	Tempi di ripristino servizi priorità 2	Tempi di ripristino servizi priorità 2
Calamità naturali	48 ore	72 ore	120 ore
Incendio (esterno)	48 ore	72 ore	120 ore
Incendio (interno)	48 ore	72 ore	120 ore
Dolo	48 ore	72 ore	120 ore
Indisponibilità prolungata del sistema	48 ore	72 ore	120 ore
Esplosioni (est./Int.)	48 ore	72 ore	120 ore

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

19.4 Procedure di gestione degli eventi catastrofici

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

20. GIORNALE DI CONTROLLO

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

20.1 Dati da archiviare

Secondo quanto stabilito dal D.P.C.M. 30 marzo 2009, 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 al di fuori del dispositivo di firma;
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

20.2 Conservazione dei dati

Le registrazioni sono effettuate indipendentemente su supporti distinti e di tipo. 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.

20.3 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.

20.4 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.

20.5 Verifiche

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

21. CESSAZIONE DELL'ATTIVITÀ DEL CERTIFICATORE

Il Certificatore se intende cessare l'attività comunica al DigitPA/AgID la data di cessazione con un anticipo di sei mesi, indicando il Certificatore sostitutivo ovvero il depositario del Registro dei certificati e della relativa documentazione.

Entro lo stesso periodo il Certificatore informa i possessori dei certificati da esso emessi, specificando che tutti i certificati non scaduti al momento della cessazione debbono essere revocati.

Il DigitPA/AgID rende nota nell'elenco pubblico la data di cessazione con l'indicazione del Certificatore sostitutivo ovvero del depositario del Registro dei certificati e della relativa documentazione.

22. 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 documentialterandone 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 contentere 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 ancota. 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, 10 dicembre 2013.

Il presidente del CNN