Consiglio Nazionale del Notariato

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

Pagina intenzionalmente lasciata in bianco

SOMMARIO

Pagina intenzionalmente lasciata in bianco

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

Pagina intenzionalmente lasciata in bianco

DEFINIZIONI

DEFINIZIONE	DESCRIZIONE
AIPA	Autorità per l'Informatica nella Pubblica Amministrazione.
Certificato	Documento informatico in formato ITU X.509 v.3 o successive contenente informazioni relative al Titolare e la sua chiave pubblica di firma, firmato dal Certificatore con la propria chiave privata di certificazione.
Certificatore	Ente che svolge le attività di generazione, emissione, conservazione, revoca e sospensione dei certificati.
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, destinato ad essere utilizzato soltanto dal Titolare. Essa è utilizzata per firmare digitalmente.
Chiave pubblica	Elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico. Essa è utilizzata per la verifica della firma.
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.
CSL (Certificate Suspension List)	Vedi Liste di sospensione 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 per la creazione di una firma sicura	L'apparato strumentale, usato per la creazione di una firma elettronica, rispondente ai requisiti di cui all'articolo 10 del D.Lgs. 23 gennaio 2002 n. 10.
Distinguished Name (Dname)	Identificativo univoco del Titolare presso il Certificatore.

DEFINIZIONE	DESCRIZIONE
Firma Digitale	Il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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, contrassegnata da una marca temporale, contenente i certificati emessi dallo stesso e successivamente revocati.
Lista di sospensione dei certificati (CSL)	Lista firmata digitalmente, tenuta ed aggiornata dal Certificatore, contrassegnata da una marca temporale, contenente i certificati emessi dallo stesso e successivamente sospesi.
Manuale operativo	Documento pubblico depositato presso l'AIPA che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività.
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.
PINGEN (PIN Generation Number)	Codice per attivare le procedure di generazione della coppia di chiavi all'interno del dispositivo di firma
PUK (Personal Unlock Key)	Chiave personale di sblocco del PIN.
PKCS (Public Key Cryptographic Standard)	Standard tecnici per applicazioni crittografiche, realizzati dalla RSA Data Security Inc.
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.
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 una evidenza informatica, una data ed un orario opponibili ai terzi.

Pagina intenzionalmente lasciata in bianco

1. INTRODUZIONE

1.1. Scopo del documento

Questo documento definisce le procedure seguite dal CNN nello svolgimento dell'attività di certificatore, ai sensi dell'art. 29 comma 3 del d.p.r. n. 445/2000. Esso si riferisce ai servizi di:

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

Il Manuale Operativo è rivolto a 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 dalle Direttive dell'UE e in particolare:

- Legge 16 febbraio 1913 n. 89 (legge notarile)
- Direttiva 13 dicembre 1999 n. 1999/93/CE
- Decreto Legislativo 23 gennaio 2002 n. 10
- Art. 15, comma 2, Legge 15 marzo 1997 n. 59
- D.P.R. 28 dicembre 2000 n. 445
- D.P.C.M. 8 febbraio 1999
- D.P.C.M. 7 dicembre 2000
- Circolare AIPA 19 giugno 2000 n. AIPA/CR/24
- Circolare AIPA 16 febbraio 2001 n. AIPA/CR/27
- Legge 31 dicembre 1996 n. 675
- D.P.R. 28 luglio 1999 n. 318

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: 06362091	**Fax**: 063221594
Sede operativa: via Flaminia, 160 00196 Roma	**Indirizzo E-mail:** certificazione@notariato.it
Indirizzo Internet: http://ca.notariato.it	**Call Center**:

3. MANUALE OPERATIVO

3.1. Dati identificativi del Manuale operativo

Il presente Manuale operativo, conservato presso i locali del Certificatore e depositato presso la AIPA, è identificato col nome "**MOConsiglioNazionaleNotariato**" ed è consultabile per via telematica all'indirizzo Internet:

http://www.notariato.it/firmadigitale/manualeoperativo

Il presente documento è identificato con il numero di versione 1.0.1.

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

1.3.6.1.4.1.8526.1.1.1 Certificazione Chiavi.

Tale OID identifica:

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-firma digitale	1.3.6.1.4.1.8526.1.1.1

3.2. Responsabile del Manuale operativo

Il Responsabile del Manuale operativo è:

Nome: Gian Mario
Cognome: Braido
Telefono: 39-06-362091
E-mail: **gbraido@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 firme digitali o altri tipi di firme elettroniche avanzate, basate su di un certificato e generate mediante un dispositivo per la creazione di una firma.

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 ad altri;

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) informa espressamente il Titolare in ordine agli eventuali accordi di certificazione stipulati con altri Certificatori;

6) rilascia e rende pubblico il certificato avente le caratteristiche fissate dagli artt.11 e 12 del D.P.C.M. 8 febbraio 1999;

7) si attiene alle regole tecniche emanate con D.P.C.M. 8 febbraio 1999;

8) si accerta dell'autenticità della richiesta di certificazione;

9) verifica che la chiave pubblica di cui si richiede la certificazione non sia stata già certificata da uno dei Certificatori iscritti nell'elenco pubblico, compatibilmente con quanto consentito dallo stato della tecnologia e di interoperabilità con gli altri certificatori;

10) richiede, prima di pubblicare il certificato, 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;

11) si attiene alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996 n. 675 e successive modificazioni e integrazioni;

12) non si rende depositario di chiavi private dei Titolari;

13) genera le coppie di chiavi dei Titolari, all'interno del dispositivo di firma nell'ipotesi di cui al par. *Procedura centralizzata di generazione e certificazione delle chiavi pubbliche di firma*;

14) genera la coppia 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;

15) procede tempestivamente alla revoca od alla sospensione del certificato in tutti i casi previsti dal presente Manuale Operativo;

16) comunica le richieste di revoca o sospensione al Titolare;

17) dà tempestiva pubblicazione della revoca e della sospensione della coppia di chiavi asimmetriche;

18) conserva le richieste scritte di registrazione e le richieste di certificazione per un periodo di almeno 30 anni dalla data di scadenza del certificato;

19) comunica per iscritto all'AIPA ogni variazione dei requisiti per l'iscrizione all'Elenco pubblico dei Certificatori di cui all'art. 16 del D.P.C.M. 8 febbraio 1999 e, non appena istituito, all'elenco dei Certificatori accreditati di cui all'art. 10 del D.Lgs. 23 gennaio 2002 n. 10, e, in ogni caso, annualmente conferma la permanenza dei requisiti per l'esercizio dell'attività di certificazione;

20) comunica tempestivamente all'AIPA, ogni variazione significativa delle soluzioni tecnico-organizzative adottate;

21) comunica all'AIPA 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 adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri. 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) richiedere tempestivamente la revoca dei certificati relativi alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi;

5) redigere per iscritto la richiesta di revoca, specificando la motivazione e la sua decorrenza;

6) redigere per iscritto la richiesta di sospensione, specificandone la motivazione ed il periodo durante il quale la validità del certificato deve essere sospesa;

7) 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 (CRL) e dalle Liste di Sospensione (CSL) dei certificati;

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 partecipare alle fasi di

1) identificazione e registrazione;

2) generazione delle chiavi e consegna dei dispositivi di firma;

3) richiesta ed emissione dei certificati;

4) sospensione e revoca dei certificati;

5) riattivazione dei certificati sospesi;

6) sostituzione delle chiavi 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 13 dicembre 1999 n. 1999/93/CE, dal D.P.R. 445/2000, dal D.P.C.M. 8/2/99, dalla Circolare AIPA 16 febbraio 2001 n° AIPA/CR/27 e dalla Legge 675/1996.

Il CNN è responsabile nei confronti di qualunque soggetto faccia ragionevole affidamento sui certificati emessi dallo stesso, nei limiti di cui all'art. 28 bis del D.P.R. 445/2000, come introdotto dal D.Lgs. 23 gennaio 2002 n. 10. 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 CNN provi d'aver agito senza colpa, ed in ogni caso in cui la responsabilità è esclusa dall'art. 28 bis del D.P.R. 445/2000, come introdotto dall'art. 7 del D.Lgs. 10/2002

6. TARIFFE

L'emissione del certificato comporta l'addebito al richiedente di un importo in euro che sarà stabilito al momento dell'attivazione del servizio e comunque non superiore a € 15,00.

L'emissione di una marca temporale comporta l'addebito al richiedente di un importo in euro che sarà stabilito al momento dell'attivazione del servizio e comunque non superiore a € 1,00.

In caso di richiesta di più marche temporali contestuali l'addebito sarà stabilito al momento dell'attivazione del servizio e comunque non superiore a € 1,00 per ciascuna marca temporale richiesta.

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.

In via transitoria, per i notai già in esercizio al momento dell'entrata in funzione del sistema, il Presidente di ciascun CND provvede ad inoltrare la richiesta (anche in via cumulativa) per tutti i notai in esercizio nel distretto.

7.3. Contenuto della richiesta del certificato

La richiesta di certificazione include i seguenti dati:

- nome e cognome del notaio;
- luogo e data di nascita;
- distretto notarile
- sede di esercizio;
- indirizzo dello studio;
- telefono e fax, se disponibili, dello studio;
- indirizzo di posta elettronica ed eventuale URL;

il tutto sulla base del decreto registrato 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 forniti nella richiesta rispetto ai 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

7.6.1. 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.

7.6.2. Codice riservato per il Presidente (CRP)

al Presidente del Consiglio Notarile Distrettuale sono affidate 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 è possibile utilizzare una delle due seguenti procedure, identificate come "Procedura remota" e "Procedura centralizzata".

7.7.1. Procedura remota

CND	NOTAIO	CA-CNN
Richiede uno o più dispositivi di firma: Invia al Certificatore un elenco contenente i nominativi ed i dati anagrafici dei Notai da certificare		

CND	NOTAIO	CA-CNN
		Per ogni dispositivo di firma richiesto: Invia al CND il dispositivo con un PINGEN per la sua successiva personalizzazione Invia con un corriere differente una busta contenente il PIN ed il relativo PUK per utilizzare il dispositivo di firma
		Il dispositivo inviato contiene: Sistema Operativo. Certificato del CNN Record per la registrazione delle chiavi File di servizio
Convoca il Notaio che ha richiesto il certificato e in sua presenza avvia la procedura di generazione delle chiavi di sottoscrizione che prevede: generazione della coppia di chiavi di sottoscrizione mediante il codice PINGEN Generazione della richiesta del certificato in formato PKCS#10 (a seguito della esportazione dal dispositivo di firma della chiave pubblica relativa alla coppia di chiavi di sottoscrizione) Firma della richiesta di certificazione prodotta (PKCS#7) Apertura di una sessione di comunicazione su canale sicuro con il CNN Invio del plico così prodotto al CNN per la certificazione della chiave Archiviazione del PINGEN per una successiva operazione di rinnovo		

CND	NOTAIO	CA-CNN
		Verifica la firma del CND Estrae il PKCS#10 dal PKCS#7 Verifica che il nome del Notaio appartenga all'elenco precedentemente ricevuto Verifica l'unicità della chiave pubblica di sottoscrizione Emette il certificato relativo alla coppia di chiavi Invia al CND il certificato generato Archivia il PKCS#7 Invia al Notaio il codice riservato da usare in caso di richiesta telefonica di revoca o sospensione del certificato (in busta chiusa o nella sua casella di posta elettronica)
Inserisce il certificato nel dispositivo di firma Consegna al titolare la busta sigillata contenente il PIN ed il PUK relativo al dispositivo di firma Esegue la personalizzazione del dispositivo		
Prova il funzionamento del dispositivo in presenza del Notaio provando le chiavi di sottoscrizione firmando una ricevuta elettronica di avvenuta emissione	Attiva la procedura di identificazione	

CND	NOTAIO	CA-CNN
Se la prova del dispositivo fallisce, lo ritira ed attiva le procedure di revoca del certificato Se la prova ha esito positivo consegna al notaio una ricevuta cartacea da firmare ed invia al CNN la richiesta di pubblicazione del certificato Archivia la ricevuta cartacea e ne trasmette duplo al CA-CNN per la successiva archiviazione. Consegna al Notaio il dispositivo personalizzato Consegna al Notaio un kit hw\sw (applicativo Client) con le istruzioni per l'installazione ed il Manuale Operativo		
		Pubblica i certificati ed emette una marca temporale relativa alla loro pubblicazione Aggiorna il giornale di controllo Invia al CND la marca temporale relativa alla pubblicazione
Archivia la marca temporale e ne consegna una copia al notaio		
	Firma la copia cartacea della ricevuta di emissione del certificato Sottoscrive un documento attestante l'uso esclusivo della firma nell'espletamento delle sole funzioni di Notaio	

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

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

7.7.2. Procedura centralizzata

CND	NOTAIO	CA-CNN

CND	NOTAIO	CA-CNN
Richiede una o più dispositivi di firma: Invia al Certificatore un elenco contenente i nominativi ed i dati anagrafici dei Notai da certificare		
		Per ogni nominativo presente nella lista, deve pre-personalizzare i dispositivi di firma con i dati dei notai da certificare generare le coppie di chiavi emettere i certificati effettuare la registrazione nel dispositivo di firma del certificato emesso attivare i sistemi di distribuzione per la consegna del dispositivo di firma e dei codici PIN e PUK relativi, utilizzando due corrieri differenti
Convoca il Notaio che ha richiesto il certificato		
prova il funzionamento del dispositivo di firma in presenza del Notaio, provando le chiavi di sottoscrizione	Attiva la procedura di identificazione	
Se la prova del dispositivo fallisce, lo ritira ed avvia le procedure di revoca Se la prova ha esito positivo invia al Certificatore la richiesta di emissione del certificato (per la pubblicazione)		

CND	NOTAIO	CA-CNN
		dopo aver ricevuto la richiesta firmata: Pubblica i certificati ed emette una marca temporale relativa alla loro pubblicazione Aggiorna il giornale di controllo Invia al CND i certificati e la marca temporale relativa alla pubblicazione Invia al Notaio il codice riservato da usare in caso di richiesta telefonica di revoca del certificato
Archivia la marca temporale e ne consegna una copia al notaio Consegna al Notaio: il dispositivo personalizzato una busta contenente il PIN ed il relativo PUK per attivare la funzione di firma una ricevuta cartacea da firmare un kit hw\sw (applicativo Client) con le istruzioni per l'installazione ed il Manuale Operativo.		
	Firma una ricevuta di avvenuta emissione Firma una ricevuta di emissione e sottoscrive un documento attestante l'uso esclusivo della firma nell'espletamento delle sole funzioni di Notaio	

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

Tutte le richieste che presentano anomalie vengono scartate e tali eventi vengono tempestivamente comunicati ai rispettivi Titolari.

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 2048 bit.

La lunghezza delle chiavi di sottoscrizione è di 1024 bit.

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

8.3. Algoritmi

Per la generazione e 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-1 (Dedicated Hash Function 3)

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, liste di revoca e liste di sospensione (CRL-CSL);
- 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 marcatura temporale

8.5.1. 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.

Ogni coppia di chiavi utilizzata per la validazione temporale è univocamente associata ad un sistema di validazione temporale.

8.5.2. Certificazione delle chiavi di marcatura temporale

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

8.5.3. Scadenza delle chiavi di marcatura temporale

Le chiavi di marcatura temporale sono soggette agli stessi termini di scadenza delle chiavi di certificazione. Tuttavia, le chiavi di marcatura temporale saranno sostituite dopo non più di un mese di utilizzo, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato, seguendo le procedure descritte nel par. *Scadenza e rinnovo delle marche temporali*

8.6. Chiavi di sottoscrizione

Le chiavi di sottoscrizione, ovvero di firma, consentono al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

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

8.6.1. Generazione delle chiavi di sottoscrizione

La generazione delle chiavi di sottoscrizione avviene all'interno del dispositivo di firma presso il CND in presenza del notaio richiedente, nel caso di procedura di generazione remota, oppure presso il Certificatore, sempre nel dispositivo di firma, nel caso di procedura centralizzata, come descritto nel

presente manuale nei par. *Procedura remota di generazione e certificazione delle chiavi pubbliche di firma* e *Procedura centralizzata di generazione e certificazione delle chiavi pubbliche di firma*

Il Titolare deve avvalersi del dispositivo di firma consegnato dal CND, per qualunque operazione di firma.

8.7. Dispositivo di firma

Il dispositivo di firma utilizzato per la generazione delle firme è conforme ai requisiti di sicurezza imposti dai criteri previsti dal livello di valutazione E3 e robustezza dei meccanismi HIGH dell'ITSEC 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.

8.8. Procedura di personalizzazione del dispositivo di firma

Il CND personalizza il dispositivo di firma provvedendo alla registrazione, nel dispositivo stesso, dei certificati relativi alle chiavi di certificazione del Certificatore ed all'inserimento dei dati del titolare,

8.9. 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'accesso alla chiave privata da parte del notaio è protetto con un PIN che deve essere digitato dal titolare ogni volta che egli intende usare il dispositivo.

L'accesso alla chiave privata da parte del notaio potrà inoltre essere subordinato al positivo riconoscimento biometrico.

8.10. Consegna del dispositivo di firma

La consegna al notaio avviene contestualmente alla iscrizione a ruolo del notaio o in un momento successivo, ove quanto necessario non sia ancora pervenuto.

Il dispositivo di firma è spedito in busta sigillata al CND richiedente; con separato plico sigillato sono trasmessi il PIN iniziale ed il relativo PUK, inoltre viene spedito direttamente al Notaio, in busta chiusa o nella sua casella di posta elettronica, il codice riservato per la richiesta di revoca o di sospensione.

Ricevuto il plico, il Presidente del CND convoca il notaio, verifica l'integrità dei sigilli, apre la busta in presenza del notaio stesso, di cui accerta l'identità, e gli consegna personalmente:

- il dispositivo di firma;
- un *kit hardware/software* per l'apposizione e la verifica delle firme, comprendente un lettore, l'eventuale sistema di riconoscimento biometrico, le istruzioni per l'installazione e l'uso;
- una copia del manuale operativo.

Il dispositivo di firma ed il kit h*ardware/software* sono subito provati al momento della consegna.

Ove le prove anzidette non abbiano buon esito, è inibito al Presidente consegnare il dispositivo di firma al notaio, egli inoltre attiverà le procedure di revoca del certificato anche se non è stato ancora pubblicato.

Il notaio provvede alla variazione del PIN iniziale, creandone uno personalizzato e firma, con la chiave privata appena ottenuta, la ricevuta di avvenuta emissione.

Le operazioni di consegna e la richiesta di emissione del certificato sono comunicate dal presidente del CND al CNN, in via telematica con un canale sicuro, e successivamente confermate mediante spedizione raccomandata entro tre giorni lavorativi della dichiarazione sottoscritta su carta dal notaio, il tutto anche ai fini della registrazione nel giornale di controllo.

9. EMISSIONE DEI CERTIFICATI

9.1. Informazioni contenute nel certificato

Il certificato contiene:

- numero di serie del certificato;
- denominazione del Certificatore e stato di stabilimento;
- codice identificativo del Titolare presso il Certificatore (nel campo Subject come specificato nella Circolare AIPA\24);
- nome, cognome, codice fiscale, luogo e data di nascita 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;
- indicazione dell'uso esclusivo della chiave privata per l'esercizio della funzione notarile;
- 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 9594-8:1995 con le estensioni definite nella Variante 1, ovvero alla specifica pubblica PKCS#6 e PKCS#9 e successive modificazioni o integrazioni.

9.3. Unicità della chiave pubblica

Il Certificatore prima di procedere all'emissione di un certificato verifica che la chiave pubblica non sia già stata certificata da uno dei Certificatori iscritti nell'elenco pubblico, compatibilmente con quanto consentito dallo stato della tecnologia e di interoperabilità con gli altri certificatori.

9.4. 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 del dispositivo di firma.

Il Certificatore, verificato il completamento delle operazioni di consegna ed il ricevimento della richiesta di emissione procede alla pubblicazione del certificato contenente la chiave pubblica, con l'apposizione di una marca temporale.

Successivamente invia al CND, mediante canale sicuro, un messaggio contenente il certificato generato, nonché la marca temporale attestante il momento dell'avvenuta pubblicazione.

I certificati relativi alle chiavi pubbliche dei notai sono conservati, a cura del Certificatore, nel Registro dei certificati per trenta anni dalla data di scadenza del certificato.

Tale registro è consultabile telematicamente.

9.5. Procedura di generazione del certificato relativo alle chiavi di sottoscrizione secondo la modalità remota

Il CND inoltra la richiesta di certificazione presso il Certificatore a seguito della generazione della coppia di chiavi di sottoscrizione: la generazione e la richiesta di certificazione delle relative chiavi pubbliche delle coppie generate, avvengono nella stessa sessione operativa.

Il Certificatore, quindi, procede alla generazione del certificato contenente la chiave pubblica di sottoscrizione e lo invia al CND.

Solo dopo aver avuto conferma del corretto funzionamento del dispositivo ed aver ricevuto per prova una ricevuta di emissione firmata digitalmente dal Notaio, lo pubblica nel Registro dei certificati, asseverando il momento con l'apposizione di una marca temporale.

Successivamente invia al CND, le marche temporali attestanti il momento dell'avvenuta pubblicazione.

I certificati relativi alle chiavi pubbliche del Titolare sono conservati, a cura del Certificatore, nel Registro dei certificati per trenta anni.

Tale Registro è consultabile telematicamente, secondo le modalità descritte nel Manuale operativo.

9.6. Procedura di generazione del certificato relativo alle chiavi di sottoscrizione secondo la modalità centralizzata

Il CND, ricevute e controllate le informazioni di registrazione dei richiedenti, le invia al Certificatore.

Il Certificatore, provvede ad inserirle nel database di registrazione e ad attivare il sistema di generazione dei certificati.

Il sistema realizza una procedura che associa dei dispositivi di firma parzialmente personalizzati agli utenti da certificare ed automatizza la procedura manuale di generazione delle chiavi.

Il processo di generazione, emissione dei certificati e i controlli e registrazioni effettuate sono i medesimi del paragrafo precedente.

Una volta emessi, i certificati di firma vengono importati nel dispositivo di firma completandone la personalizzazione.

Solo dopo la prova del corretto funzionamento del dispositivo di firma da parte del Notaio, il Certificato viene pubblicato ed il momento viene asseverato con l'emissione di una marca temporale.

I dispositivi di firma e i PIN e PUK relativi vengono consegnati attraverso canali di distribuzione differenti ai Presidenti di CND. Sarà cura dei Presidenti far pervenire al Titolare il relativo dispositivo di firma e la busta contenente PIN e PUK.

Il dispositivo di firma, una volta effettuata l'installazione del software sulla postazione del Titolare è pronto all'uso.

Il certificato relativo alla chiave pubblica di firma del Titolare è conservato, a cura del Certificatore, nel Registro dei certificati per trenta anni dalla data di scadenza dello stesso ed è consultabile telematicamente, secondo le modalità descritte nel Manuale operativo.

9.7. Procedura di generazione dei certificati relativi alle chiavi di certificazione di altri Certificatori (Accordi di certificazione)

Il Certificatore può stipulare accordi di certificazione con altri Certificatori come previsto dall'art. 21, del D.P.C.M. 08/02/99.

Con l'accordo di certificazione, un Certificatore emette a favore di un altro Certificatore un certificato relativo a ciascuna chiave di certificazione che viene riconosciuta nel proprio ambito. I certificati così emessi debbono definire la corrispondenza tra le clausole dei rispettivi Manuali operativi considerate equivalenti.

Il Certificatore informerà espressamente i richiedenti la certificazione ed i Titolari di certificati di firma, in ordine ad accordi di certificazione stipulati (art. 24, comma 2, D.P.C.M. 08/02/99).

10. REVOCA E SOSPENSIONE DEI CERTIFICATI

10.1. Premessa

Il Certificatore utilizza per la revoca e per la sospensione la Lista dei certificati revocati (CRL) e la Lista dei Certificati sospesi (CSL).

Il certificatore provvede a rimuovere dalla Lista dei certificati sospesi i certificati che non sono più sospesi, mantenendo traccia del periodo di sospensione.

La lista è consultabile telematicamente, secondo le modalità descritte nel Manuale operativo.

10.2. 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 momento di pubblicazione della lista è provato mediante l'apposizione di una marca temporale.

Il Certificatore procede immediatamente 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.

10.2.1. 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 i motivi e 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 dalle funzioni notarili.

Su iniziativa del certificatore

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.

Salvo i casi di urgenza, la revoca del certificato è preventivamente comunicata dal Certificatore al notaio titolare, con specificazione dei motivi, nonché della data e dell'ora a partire dalla quale il certificato non sarà più valido.

10.2.2. Sospensione di certificati

I certificati sono sospesi per un periodo di tempo stabilito.

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 del CND richiede la sospensione dei certificati per:

- sospensione temporanea del notaio;
- cessazione temporanea dall'esercizio notarile;
- interdizione temporanea ed inabilitazione all'ufficio notarile;

- esecuzione di provvedimenti dell'autorità giudiziaria comportanti la cessazione temporanea dalle funzioni notarili.

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.

10.3. Revoca dei certificati relativi a chiavi di certificazione

10.3.1. Circostanze di revoca

Il Certificatore procede alla revoca del certificato relativo ad una coppia di chiavi di certificazione esclusivamente nei seguenti casi (art. 38, comma 1, D.P.C.M. 08/02/99):

- compromissione della chiave privata;
- guasto del dispositivo di firma;
- cessazione dell'attività.

10.3.2. Obbligo di notifica

La revoca è comunicata all'AIPA, ed a tutti i possessori di certificati sottoscritti con la chiave privata appartenente alla coppia revocata, entro le 24 ore.

10.3.3. Obbligo di revoca

I certificati per i quali risultino compromesse o la chiave di certificazione con cui sono stati sottoscritti, o quella utilizzata per la generazione della marca temporale di cui al comma 4 dell'articolo 28, D.P.C.M. 08/02/99, vengono revocati d'ufficio.

10.3.4. 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 dopo avervi apposto una marca temporale.

Successivamente, notifica entro 24 ore, la revoca all'AIPA ed ai Titolari dei certificate sottoscritti con la chiave privata della coppia di chiavi revocata.

10.4. Revoca di certificati relativi a chiavi di marcatura temporale

10.4.1. Circostanze di revoca

La revoca del certificato relativo ad una coppia di chiavi di marcatura temporale è consentita esclusivamente nei seguenti casi:

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

10.4.2. 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, con la relativa apposizione di una marca temporale, generata con una nuova coppia di chiavi di marcatura temporale.

La revoca deve essere comunicata a tutti i notai titolari di un valido certificato emesso dal CNN.

Della revoca è fatta annotazione nel giornale di controllo.

10.5. Modalità di revoca o sospensione

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

Le richieste di sospensione devono essere inoltrate per iscritto, 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 (Contenuto nel campo Subject,AIPA\24) 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.

10.5.1. 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 riservato CRN del notaio ed il codice identificativo (Contenuto nel campo Subject,AIPA\24) al Certificatore .

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

La richiesta scritta è consegnata dal notaio titolare al presidente del consiglio notarile distrettuale il quale inoltra al Certificatore la richiesta nei tempi e con le modalità previste dal presente paragrafo.

Il Titolare deve compilare la richiesta indicando:

- nome e cognome;
- sede e distretto di appartenenza;
- codice identificativo (Contenuto nel campo Subject,AIPA\24);
- 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 dei certificati sospesi (CRL-CSL) 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. La comunicazione viene effettuata con documento informatico firmato digitalmente, o con lettera raccomandata.

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

La domanda va inoltrata dal notaio Titolare al Certificatore, per via telematica 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;
- codice identificativo (Contenuto nel campo Subject,AIPA\24);
- 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 o dei certificati sospesi (CRL-CSL) 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. La comunicazione viene effettuata con documento informatico firmato digitalmente, o con lettera raccomandata.

Modalità 3: richiesta telefonica in caso di emergenza utilizzando il codice riservato ed il codice identificativo (Contenuto nel campo Subject,AIPA\24) al Certificatore .

Il Titolare provvede personalmente ad inoltrare al Certificatore, al centro telefonico dallo stesso predisposto, la richiesta, facendosi identificare attraverso la comunicazione del proprio Codice riservato (CRN) e del codice identificativo.

Il Titolare deve fornire 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 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 sospesi (CSL) 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.

10.5.2. 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 (Contenuto nel campo Subject, AIPA\24)

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;

- codice identificativo (Contenuto nel campo Subject, AIPA\24);
- 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, che ne rilascia ricevuta.
- Il Certificatore, ricevuta la richiesta, provvede alla revoca o sospensione del certificato, al suo inserimento nella apposita Lista dei certificati revocati o sospesi (CRL-CSL) 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. La comunicazione viene effettuata con documento informatico firmato digitalmente o con lettera raccomandata.

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;
- codice identificativo (Contenuto nel campo Subject,AIPA\24);
- 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-CSL) 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. La comunicazione viene effettuata con documento informatico firmato digitalmente o con lettera raccomandata.

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 sospesi (CSL) 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.

10.5.3. 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.

10.6. 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 Sabato, dalle ore 08.30 alle ore 20.00.
- per le richieste di sospensione immediata inoltrate telefonicamente il servizio sarà disponibile dal Lunedì al Sabato, dalle ore 08.30 alle ore 20.00.

10.7. Aggiornamento delle Liste dei Certificati revocati e sospesi (CRL-CSL)

Le liste di revoca e sospensione dei certificati sono aggiornate in seguito ad ogni richiesta di revoca o sospensione e ad esse è apposta una marca temporale.

La pubblicazione nel Registro dei certificati avviene ogni 4 (quattro) ore.

In caso di richiesta di revoca del certificato per certa o sospetta compromissione, manomissione o perdita del possesso della chiave privata, il Certificatore procede all'inserimento del certificato nella Lista di revoca e alla pubblicazione immediata della stessa nel Registro dei certificati.

11. RIATTIVAZIONE DI UN CERTIFICATO SOSPESO

11.1. 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, che può essere presentata dal Titolare o dal Presidente del CND con le stesse modalità previste per la richiesta di revoca o di sospensione.

11.2. 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 sospesi (CSL). Dell'avvenuta riattivazione è data comunicazione al Titolare ed al Presidente del CND, mediante documento informatico firmato digitalmente o con lettera raccomandata.

11.2.1. Procedura di riattivazione automatica del certificato sospeso:

Il Certificatore attiva la procedura di riattivazione del certificato e procede alla:

- cancellazione del Certificato da riattivare dalla lista di Sospensione (CSL);
- pubblicazione della lista CSL;
- apposizione di una marca temporale alla lista così aggiornata;
- registrazione dell'avvenuta Riattivazione nel Giornale di controllo;
- invio di un messaggio al Notaio e al Presidente del CND relativo all'avvenuta riattivazione.

12. EMISSIONE DI MARCHE TEMPORALI

12.1. Servizio di validazione temporale

Il C.N.N. svolge un servizio di validazione temporale per i documenti informatici a richiesta esclusiva da parte di notai in esercizio titolari di un certificato di chiave pubblica emesso dallo stesso C.N.N.

Possono essere oggetto di marcatura temporale i documenti informatici di qualunque specie, prodotti ed eventualmente sottoscritti, da un notaio o da altri soggetti.

La validazione temporale è, inoltre, applicata alla pubblicazione ed alla revoca e sospensione dei certificati, come previsto dal presente manuale operativo.

12.2. Invio della richiesta di validazione temporale

La richiesta di validazione temporale è inviata telematicamente al C.N.N., via *World Wide Web* utilizzando il protocollo *http* o mediante *software client* distribuito dal C.N.N. che supporta tale protocollo o mediante posta elettronica o altro metodo coerente con i dettami dello standard rfc3161.

La richiesta deve includere l'impronta del documento oggetto della validazione temporale e deve essere firmata digitalmente dal notaio richiedente utilizzando la chiave privata corrispondente alla chiave pubblica certificata dal C.N.N. L'impronta del documento è generata con lo stesso algoritmo previsto per la firma digitale (SHA-1) e imbustata secondo il formato *standard* PKCS#7.

12.2.1. Procedura di Richiesta (ed identificazione) di una marca temporale:

Titolare abilitato	Certificatore
• Il Titolare abilitato, secondo le modalità descritte nel presente paragrafo, redige la richiesta e la trasmette al server di accettazione	
	Il server di accettazione delle richieste: • verifica la validità della firma; • estrae dalla richiesta stessa il certificato digitale associato; • verifica la validità del certificato; • verifica che il titolare sia abilitato ad accedere al servizio di marcatura temporale

12.3. Generazione della marca temporale

La procedura di generazione della marca temporale è subordinata alla verifica della firma digitale del richiedente.

Il sistema informatico mantiene la data e l'ora, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN), di cui al Decreto del Ministro dell'Industria, del Commercio e dell'Artigianato 30 novembre 1993, n. 591, al momento della sua generazione.

La marca temporale viene generata, conformemente alla richiesta, nel più breve tempo possibile e comunque entro un minuto dalla completa ricezione della richiesta come sopra formulata. Tale termine decorre dalla attivazione dell'istanza di marcatura al sottosistema specificamente ed unicamente preposto alla validazione temporale, escludendo il tempo necessario per la ricezione e verifica della richiesta e la sua trasmissione al sottosistema preposto.

La marca temporale generata entro i suddetti termini è trasmessa telematicamente al richiedente con comunicazione dell'avvenuta ricezione. L'eventuale esito negativo della richiesta è parimenti comunicato al richiedente con l'indicazione della motivazione.

L'algoritmo di firma utilizzato è lo stesso previsto per la generazione della firma digitale.

12.3.1. Procedure di Generazione della Marca Temporale:

Titolare abilitato	Certificatore
	• Il server di accettazione, a seguito delle verifiche effettuate, richiede l'emissione della marca temporale al server dedicato. • Il server di Marcatura Temporale provvede a restituire la Marca emessa al server di accettazione delle richieste.
	• Il server di accettazione, ricevuta la marca temporale, provvede alla sua trasmissione, unitamente all'impronta del documento, al titolare abilitato che ne ha fatto richiesta. • Viene aggiornato il database contenente il numero di richieste fatte dall'utente, registrando data ed ora. • Viene archiviata la marca temporale generata, unitamente all'impronta cui si riferisce
• Il titolare riceve la marca temporale richiesta e l'impronta del documento. • Il titolare invia conferma della ricezione.	

12.4. Contenuto della marca temporale

Una marca temporale contiene:

- identificativo del C.N.N.;
- numero di serie della marca temporale;
- algoritmo di sottoscrizione della marca temporale;
- identificativo del certificato relativo alla chiave di verifica della marca temporale;
- data ed ora di generazione, con riferimento al Tempo Universale Coordinato (UTC);
- algoritmo di *hash* utilizzato;

- impronta del documento sottoposto a validazione temporale;
- eventuale identificatore del documento sottoposto a validazione temporale;
- sottoscrizione digitale del C.N.N.

12.5. Sicurezza dei sistemi di validazione temporale

Ogni sistema di validazione temporale deve automaticamente registrare in un apposito giornale di controllo su un supporto non riscrivibile tutte le richiesta di marcatura temporale con l'identificazione dell'utente e la data e l'ora della richiesta.

Qualsiasi anomalia o tentativo di manomissione che possa modificare il funzionamento dell'apparato in modo da renderlo incompatibile con i requisiti di sicurezza prescritti dal presente manuale operativo e dalle regole tecniche emanate con d.p.c.m. 8/2/1999, ed in particolare con il requisito della precisione temporale, deve essere annotato sul detto giornale di controllo e causare il blocco del sistema. Il blocco del sistema di validazione temporale può essere rimosso esclusivamente con l'intervento di personale espressamente autorizzato.

12.6. Scadenza e rinnovo delle marche temporali

Prima della scadenza della marca temporale, il periodo di validità può essere ulteriormente esteso associando una nuova marca all'evidenza informatica costituita dal documento iniziale, dalla eventuale relativa firma e dalle marche temporali già ad esso associate.

Tutte le marche temporali generate dal C.N.N sono conservate in un apposito archivio gestito dallo stesso C.N.N., fino alla scadenza della chiave utilizzata per la loro generazione.

13. REVOCA DEI CERTIFICATI RELATIVI ALLE CHIAVI DELL'AIPA

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

L'AIPA in caso di compromissione della propria chiave segreta ovvero di guasto del dispositivo di firma richiede a ciascun Certificatore la revoca immediata del certificato ad essa rilasciato.

L'AIPA procede alla sostituzione della chiave revocata. I Certificatori provvedono quindi, alla certificazione della nuova coppia di chiavi generata dall'AIPA

14. MODALITÀ DI SOSTITUZIONE DELLE CHIAVI

14.1. 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 sessanta giorni prima della scadenza, dovrà chiederne la sostituzione al Certificatore. La sostituzione di un certificato consiste nella generazione:

- di una nuova coppia di chiavi;
- del certificato relativo alla chiave pubblica della nuova coppia generata.

La prima sostituzione può essere effettuata per via telematica direttamente dal Titolare. Il processo di rinnovo dei certificati relativi alle chiavi pubbliche del titolare è il seguente:

1. La procedura di rinnovo deve essere attivata prima della scadenza del certificato; l'utente viene avvertito via posta elettronica sessanta giorni prima e poi quindici giorni prima della scadenza.
2. Il Presidente del CND comunica al Certificatore la persistenza in capo al Titolare delle funzioni notarili ed eventualmente la loro prevista cessazione nel successivo triennio.
3. Il Titolare, con gli strumenti messi a sua disposizione dal Certificatore, genera la nuova coppia di chiavi di firma e la richiesta di certificazione, in formato PKCS#10.
4. Il pacchetto contenente la richiesta di certificazione viene firmato con la vecchia chiave di sottoscrizione, ancora valida.
5. Viene attivata la connessione con il sistema remoto di ricezione delle richieste e trasmesso il pacchetto precedentemente firmato.
6. A seguito dell'autorizzazione viene trasmessa la richiesta alla CA affinché provveda alla generazione del nuovo certificato.

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

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

Qualora siano trascorsi tre anni dalla prima sostituzione, il Titolare, che intende continuare ad avvalersi del servizio di certificazione, dovrà presentarsi invece personalmente dal Presidente del Consiglio Notarile Distrettuale e ripetere nuovamente la procedura d'identificazione e registrazione.

Laddove si utilizzi una procedura centralizzata di generazione ed emissioni certificati, si deve ripetere la procedura descritta nel par. *Emissione di certificati successiva ad una revoca* che implica anche la sostituzione del dispositivo di firma.

14.2. Sostituzione delle chiavi di certificazione

Il Certificatore, 90 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:

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

I certificati così generati sono forniti all'AIPA 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.

Alla scadenza delle chiavi di certificazione, il Certificatore ripete la procedura di generazione delle chiavi di certificazione da utilizzare in caso di disastro.

14.3. Sostituzione delle chiavi di marcatura temporale

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

15. REGISTRO DEI CERTIFICATI

15.1. Informazioni contenute nel Registro dei certificati

Il Certificatore pubblica le seguenti informazioni nel Registro dei certificati:

- elenco di tutti i certificati emessi;
- lista dei certificati revocati (CRL);
- lista dei certificati sospesi (CSL).

Le liste dei certificati revocati e sospesi sono conformi allo standard ITU X.509.

15.2. Procedura di gestione del Registro dei certificati

Il Registro dei certificati è consultabile da qualsiasi soggetto 24 ore al giorno, 7/7 giorni, esclusi i tempi dedicati alla manutenzione programmata.

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.

Modificazioni al contenuto del Registro dei certificati sono effettuate esclusivamente da personale autorizzato. Tali operazioni sono sistematicamente registrate sul Giornale di controllo inoltre sono annotate la data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il Registro dei certificati non risulta accessibile dall'esterno, nonché quelle relative a ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile.

Una copia di sicurezza della copia operativa e di quella di riferimento del Registro dei certificati sono conservate in armadi di sicurezza distinti, situati in locali diversi.

15.3. Procedura di aggiornamento del Registro dei certificati

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

- emette nuovi certificati;
- pubblica Liste di revoca in seguito alla revoca di un certificato;
- pubblica Liste di sospensione in seguito alla sospensione di un certificato.

Ogni aggiornamento viene asseverato mediante apposizione di marca temporale.

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 sulla copia di riferimento. L'inserimento/cancellazione di un certificato nella copia di riferimento viene registrato nel Giornale di controllo e asseverato mediante apposizione di marca temporale
- Il Responsabile del Registro dei certificati controlla l'applicazione che pubblica ed aggiorna le Liste di revoca e di sospensione sulla copia di riferimento. L'inserimento/cancellazione di un certificato nella CRL/CSL viene registrato nel Giornale di controllo e asseverato mediante apposizione di marca temporale.
- 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

Il registro dei certificati è un Internet Directory Server e server LDAP compatibile con le specifiche X.500 1993 e che supporta il protocollo LDAP v. 3. Il registro dei certificati è accessibile a qualsiasi soggetto secondo le seguenti modalità:

- Indirizzi elettronici di accesso al registro:

  l'indirizzo Internet del Registro dei Certificati è " ldap://ldap.ca.notariato.it ". riportato sul sito Web del Certificatore (e nell'Elenco pubblico dei Certificatori tenuto dall'AIPA)

- Indirizzi telefonici di accesso al registro:

  è disponibile un accesso dalla rete telefonica pubblica, con autenticazione utilizzando il codice riservato ed il codice identificativo (Contenuto nel campo Subject, AIPA\24), per consentire la raggiungibilità del registro dei certificati anche quando sia impossibile attraverso il normale canale internet. Il numero telefonico da chiamare è nel sito predisposto dal CNN all'URL : http://www.notariato.it/

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 emanate con il D.P.R. 28 luglio 1999, n. 318, ai sensi dell'art. 15, comma 2, della legge 675/96 nell'esecuzione delle seguenti attività:

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

17. 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..

18. EVENTI CATASTROFICI

18.1. Classificazione dei servizi

Nell'ambito della politica di disaster recovery i servizi forniti dal sistema sono stati classificati secondo due 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.

Nell'ambito della strategia di disaster recovery adottata, è prevista l'esistenza di un sito di back-up 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.

I servizi di seguito elencati, non devono subire discontinuità, se non nei termini di qualche ora necessaria alla loro riattivazione, e si definiscono servizi "mission critical".

I servizi a priorità più alta sono:

PRIORITÀ 1

- **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 rispettivamente, il Directory Service Master e Shadow presso il Main Site;

- **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.

- **Marche temporali:** servizio di apposizione delle marche temporali per le operazioni interne all'Infrastruttura di Certificazione. In questo caso occorre che il TimeStamping Server e soprattutto il collegamento con la sorgente di tempo fidata sia sempre disponibile.

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.

18.2. 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
Calamità naturali	8 ore	48 ore
Incendio (esterno)	8 ore	48 ore
Incendio (interno)	8 ore	48 ore
Dolo	8 ore	48 ore
Indisponibilità prolungata del sistema	8 ore	48 ore
Esplosioni (est./Int.)	8 ore	48 ore

18.3. Procedure di gestione degli eventi catastrofici

Le procedure per la gestione degli eventi catastrofici, sono dettagliatamente descritte nel Piano per la sicurezza.

19. GIORNALE DI CONTROLLO

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

19.1. Dati da archiviare

Secondo quanto stabilito dall'allegato tecnico (D.P.C.M. 08/02/99), 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, siano essi relativi a chiavi di sottoscrizione che a chiavi di certificazione o di marcatura temporale;
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. l'inizio e la fine di ciascuna sessione di lavoro inerente alla generazione dei certificati;
8. tutte le operazioni che modificano il contenuto del Registro dei certificati, ossia l'aggiornamento delle liste di revoca/sospensione e la pubblicazione dei certificati generati;
9. la data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il Registro dei certificati non risulta accessibile dall'esterno, nonché quelle relative a ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile.

19.2. 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.

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 CERTIFICATORE

Il Certificatore se intende cessare l'attività comunica all'AIPA 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.

L'AIPA 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.

Il presente manuale operativo è stato approvato dal responsabile Dott. Gian Mario Braido e dal presidente pro tempore del Consiglio Nazionale del Notariato Antonio Mascheroni.

Roma, 8 agosto 2002

Il responsabile

Gian Mario Braido

Il presidente

Antonio Mascheroni

Pagina intenzionalmente lasciata in bianco