

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:



# **Consiglio Nazionale del Notariato**

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

**versione 8.0**

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## SOMMARIO

<b>1. INTRODUZIONE.....</b>	<b>10</b>
1.1. SCOPO DEL DOCUMENTO .....	10
1.2. RIFERIMENTI NORMATIVI .....	10
<b>2. DATI IDENTIFICATIVI DEL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI ...</b>	<b>11</b>
<b>3. MANUALE OPERATIVO.....</b>	<b>12</b>
3.1. DATI IDENTIFICATIVI DEL MANUALE OPERATIVO .....	12
3.2. RESPONSABILE DEL MANUALE OPERATIVO .....	12
3.3. TIPOLOGIA DELLE UTENZE .....	13
<b>4. TERMINI E CONDIZIONI.....</b>	<b>14</b>
4.1. OBBLIGHI DEL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI .....	14
4.2. OBBLIGHI DEL TITOLARE.....	15
4.3. OBBLIGHI DEI DESTINATARI .....	15
4.4. OBBLIGHI DEL PRESIDENTE DEL CND .....	16
4.5. RECLAMI.....	16
4.6. LEGGE APPLICABILE – FORO COMPETENTE.....	16
<b>5. RESPONSABILITÀ.....</b>	<b>17</b>
5.1. RESPONSABILITÀ DEL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI .....	17
<b>6. TARIFFE .....</b>	<b>17</b>
<b>7. IDENTIFICAZIONE E REGISTRAZIONE .....</b>	<b>18</b>
7.1. IDENTIFICAZIONE .....	18
7.2. REGISTRAZIONE.....	18
7.3. CONTENUTO DELLA RICHIESTA DEL CERTIFICATO .....	18
7.4. OBBLIGHI DI IDENTIFICAZIONE.....	18
7.5. COMUNICAZIONI TRA IL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI E I TITOLARI.....	19
7.6. CODICI RISERVATI.....	19
7.7. PROCEDURE PER LA GENERAZIONE E LA CERTIFICAZIONE DELLE CHIAVI PUBBLICHE DI FIRMA .....	19
7.8. EMISSIONE DI CERTIFICATI SUCCESSIVA AD UNA REVOCATA .....	22
<b>8. GENERAZIONE DELLE CHIAVI .....</b>	<b>23</b>
8.1. SISTEMI DI GENERAZIONE .....	23
8.2. LUNGHEZZA DELLE CHIAVI .....	23
8.3. ALGORITMI.....	23
8.4. CHIAVI DI CERTIFICAZIONE .....	23
8.4.1. GENERAZIONE DELLE CHIAVI DI CERTIFICAZIONE .....	24
8.5. CHIAVI DI SOTTOSCRIZIONE.....	25
8.6. DISPOSITIVO DI FIRMA .....	25
8.7. REQUISITI DEL DISPOSITIVO DI FIRMA .....	25
<b>9. EMISSIONE DEI CERTIFICATI.....</b>	<b>26</b>
9.1. INFORMAZIONI CONTENUTE NEL CERTIFICATO.....	26
9.2. PROFILO DEL CERTIFICATO .....	26
9.3. EMISSIONE DEL CERTIFICATO .....	27
9.3.1. EMISSIONE DEL CERTIFICATO SUL DISPOSITIVO DI FIRMA .....	27
9.3.2. EMISSIONE DEL CERTIFICATO DI FIRMA REMOTA.....	27
<b>10. REVOCÀ E SOSPENSIONE DEI CERTIFICATI DI SOTTOSCRIZIONE.....</b>	<b>28</b>
10.1. PREMESSA.....	28

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

10.2. REVOCA DEI CERTIFICATI .....	28
10.2.1. REVOCA DA PARTE DEL TITOLARE .....	29
10.2.2. REVOCA DA PARTE DEL PRESIDENTE DI DISTRETTO.....	30
10.2.3. REVOCA DA PARTE DEL PRESTATORE .....	31
10.3. SOSPENSIONE DI CERTIFICATI .....	32
10.3.1. SOSPENSIONE DA PARTE DEL TITOLARE.....	32
10.3.2. SOSPENSIONE DA PARTE DEL PRESTATORE.....	33
10.4. RIATTIVAZIONE DI CERTIFICATI .....	33
<b>11. REVOCA DEI CERTIFICATI RELATIVI ALLE CHIAVI DI CERTIFICAZIONE .....</b>	<b>34</b>
11.1. CIRCOSTANZE DI REVOCA .....	34
11.2. OBBLIGO DI NOTIFICA .....	34
11.3. OBBLIGO DI REVOCA .....	34
11.4. PROCEDURA DI REVOCA DEI CERTIFICATI RELATIVI A CHIAVI DI CERTIFICAZIONE .....	34
11.5. MODALITÀ DI REVOCA DEI CERTIFICATI DI SOTTOSCRIZIONE.....	34
<b>12. RINNOVO DEI CERTIFICATI DI FIRMA .....</b>	<b>35</b>
12.1. RINNOVO DEI CERTIFICATI DEL TITOLARE .....	35
12.2. SOSTITUZIONE DELLE CHIAVI DI CERTIFICAZIONE .....	35
<b>13. REGISTRO DEI CERTIFICATI.....</b>	<b>36</b>
13.1. INFORMAZIONI CONTENUTE NEL REGISTRO DEI CERTIFICATI.....	36
13.2. PROCEDURA DI GESTIONE DEL REGISTRO DEI CERTIFICATI .....	36
13.3. PROCEDURA DI AGGIORNAMENTO DEL REGISTRO DEI CERTIFICATI.....	36
13.4. MODALITÀ DI ACCESSO AL REGISTRO DEI CERTIFICATI.....	36
<b>14. PROTEZIONE DELLA RISERVAZZA.....</b>	<b>37</b>
<b>15. GESTIONE DELLE COPIE DI SICUREZZA .....</b>	<b>37</b>
<b>16. DISPONIBILITÀ DEL SERVIZIO.....</b>	<b>37</b>
<b>17. GESTIONE DEGLI EVENTI CATASTROFICI .....</b>	<b>37</b>
<b>18. GIORNALE DI CONTROLLO.....</b>	<b>38</b>
18.1. DATI DA ARCHIVIARE .....	38
18.2. CONSERVAZIONE DEI DATI.....	38
18.3. PROTEZIONE DELL'ARCHIVIO .....	38
18.4. GESTIONE DEL GIORNALE DI CONTROLLO .....	38
18.5. VERIFICHE .....	38
<b>19. CESSAZIONE DELL'ATTIVITÀ DEL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI.....</b>	<b>39</b>

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## VERSIONI DOCUMENTO

VERSIONE	DESCRIZIONE MODIFICA	DATA emissione
<b>1.0</b>	Prima emissione	20/05/2002
<b>1.1</b>	<ul style="list-style-type: none"> <li>1. par. 6 inserite tariffe per l'emissione dei certificati e delle marche temporali;</li> <li>2. par. 9.6: precisata decorrenza periodo di conservazione del certificato scaduto;</li> <li>3. par. 7.1: correzione indicazione autorità emittente il documento unico di riconoscimento del notaio.</li> </ul>	08/08/2002
<b>2.0</b>	<ul style="list-style-type: none"> <li>1. par. 3.1: modificati i dati identificativi del manuale operativo;</li> <li>2. par. 7.7.1: modificata procedura di generazione e certificazione remota delle chiavi pubbliche;</li> <li>3. par. 7.7.2: modificata procedura di generazione e certificazione centralizzata delle chiavi pubbliche.</li> </ul>	05/02/2004
<b>3.0</b>	<ul style="list-style-type: none"> <li>1. Adeguamento normativo</li> <li>2. Modifica procedure</li> </ul>	5/5/2006
<b>3.1</b>	<ul style="list-style-type: none"> <li>1. Adeguamento normativo.</li> <li>2. Semplificazione delle procedure, ed, in particolare, eliminazione dell'emissione centralizzata dei certificati.</li> <li>3. Allineamento delle procedure operative ai requisiti tecnici indicati nel DPCM 13/01/2004, ed, in particolare: <ul style="list-style-type: none"> <li>a. Eliminazione dell'emissione immediata della CRL (la CRL viene emessa solo ogni ore).</li> <li>b. Eliminazione della pubblicazione dei certificati dei titolari sul registro pubblico dei certificati.</li> <li>c. Eliminazione dell' emissione di marca temporale all'atto della pubblicazione della CRL.</li> </ul> </li> </ul>	1/7/2008
<b>4.0</b>	<ul style="list-style-type: none"> <li>1. Adeguamento normativo DPCM 30 marzo 2009</li> <li>2. Allineamento delle procedure operative ai requisiti tecnici previsti dalla Deliberazione 45 del 21 maggio 2009 ed in particolare modifica degli algoritmi di hash;</li> <li>3. Modifica del tempo di emissione delle CRL. (la CRL viene emessa solo ogni 8 ore);</li> <li>4. Aggiornamento dei riferimenti normativi.</li> </ul>	29/01/2013

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

VERSIONE	DESCRIZIONE MODIFICA	DATA emissione
<b>4.1</b>	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
<b>5.0</b>	1. Aggiornamento riferimenti normativi 2. Rimozione servizio validazione temporale	01/06/2017
<b>6.0</b>	1. Emissione di certificati di firma remota 2. Eliminazione funzione di sospensione da parte dei presidenti	26/10/2018
<b>7.0</b>	1. Aggiornamento riferimenti certificato di root CA 2. Aggiornamento riferimenti normativi	25/05/2020
<b>8.0</b>	1. Aggiornamento riferimenti certificato di root CA 2. Aggiornamento riferimenti normativi	02/12/2024

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## DEFINIZIONI AI FINI DEL PRESENTE MANUALE OPERATIVO

DEFINIZIONE	DESCRIZIONE
<b>AgID</b>	Agenzia per l'Italia Digitale. Ente Nazionale per la digitalizzazione della Pubblica Amministrazione. Sostituisce il CNIPA e DigitPA.
<b>CNIPA</b>	Centro Nazionale per l'Informatica nella Pubblica Amministrazione. Sostituito da AgID
<b>DigitPA</b>	Ente Nazionale per la digitalizzazione della Pubblica Amministrazione. Sostituito da AgID.
<b>Autenticazione del documento informatico</b>	La validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione.
<b>Certificato</b>	Documento informatico in formato ITU X.509 v.3 o successive contenente informazioni relative al Titolare e alla sua chiave pubblica di firma, firmato dal Prestatore di Servizi Fiduciari con la propria chiave privata di certificazione.
<b>Certificato qualificato</b>	Ai sensi del Regolamento UE 910/2014 rilasciato da Prestatori di servizi fiduciari qualificati che rispondono ai requisiti del regolamento ed avente anche le caratteristiche fissate dal DPCM 22 febbraio 2013, nonché dalla Determinazione AgID n. 147/201.
<b>Prestatore di Servizi Fiduciari</b>	Trusted Service Provider, prestatore di servizi fiduciari (es. Certificatore accreditato, Conservatore accreditato, etc) ai sensi del Regolamento 910/2014
<b>Certificazione</b>	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.
<b>Chiave privata</b>	Elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.
<b>CNN</b>	Consiglio Nazionale del Notariato (CNN), ente pubblico non economico, istituito con legge 3 agosto 1949, n. 577.
<b>CND</b>	Consiglio Notarile Distrettuale ai sensi della legge notarile.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

DEFINIZIONE	DESCRIZIONE
<b>Codice riservato (CRN e CRP)</b>	Sequenza di caratteri alfanumerici che deve essere fornita dal Titolare o dal Presidente del Consiglio Notarile Distrettuale al Prestatore di Servizi fiduciari qualificati per effettuare una revoca o sospensione immediata di un certificato.
<b>Coppia di chiavi</b>	Coppia di chiavi asimmetriche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di firma digitale di documenti informatici.
<b>CRL (Certificate Revocation List)</b>	Vedi Liste di revoca dei certificati.
<b>Destinatario</b>	Destinatario di un documento informatico firmato digitalmente.
<b>Dispositivo di firma</b>	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.
<b>Dispositivo sicuro per la creazione di una firma</b>	L'apparato strumentale, usato per la creazione di una firma elettronica, rispondente ai requisiti del DPCM 22 febbraio 2013.
<b>Distinguished Name (Dname)</b>	Identificativo univoco del Titolare presso il Prestatore di Servizi fiduciari qualificati.
<b>Documento Informatico</b>	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.
<b>Firma Digitale</b>	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.
<b>Firma remota</b>	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
<b>Lista di revoca dei certificati (CRL)</b>	Lista firmata digitalmente, tenuta ed aggiornata dal Prestatore di Servizi fiduciari qualificati contenente i certificati emessi dallo stesso e successivamente sospesi o revocati.
<b>Manuale operativo</b>	Documento pubblico depositato presso il AgID che definisce le procedure applicate dal Prestatore di Servizi fiduciari qualificati che rilascia certificati qualificati nello svolgimento della propria attività.
<b>Marca temporale</b>	Il riferimento temporale che consente la validazione temporale.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

DEFINIZIONE	DESCRIZIONE
<b>Notaio</b>	Il notaio in esercizio, nonché il coadiutore non notaio. Una volta certificato dal CNN, tale soggetto viene anche definito Titolare.
<b>OTP</b>	One Time Password – password valida per una singola sessione di accesso o di firma costituita da codici numerici
<b>PIN (Personal Identification Number)</b>	Numero di identificazione personale.
<b>PUK (Personal Unlock Key)</b>	Chiave personale di sblocco del PIN.
<b>PKCS (Public Key Cryptographic Standard)</b>	Standard tecnici per applicazioni crittografiche, realizzati dalla RSA Laboratories della EMC2 Corporation.
<b>PKI (Public Key Infrastructure)</b>	Infrastruttura a Chiave pubblica.
<b>Registrazione</b>	Attività d'acquisizione, verifica e archiviazione dei dati dei richiedenti.
<b>Registro dei certificati</b>	Registro contenente i certificati emessi dal Prestatore di Servizi fiduciari qualificati, la lista dei certificati revocati e la lista dei certificati sospesi, accessibile anche telematicamente.
<b>Revoca del certificato</b>	Operazione con cui il Prestatore di Servizi fiduciari qualificati annulla la validità del certificato da un dato momento in poi.
<b>Riferimento temporale</b>	Informazione contenente la data e l'ora che viene associata ad uno o più documenti informatici.
<b>Sospensione certificato</b> <b>del</b>	Operazione con cui il Prestatore di Servizi fiduciari qualificati sospende la validità del certificato da un dato momento e per un determinato periodo di tempo.
<b>QSCD</b>	Qualified Signature Creation Device, il dispositivo di firma certificato.
<b>SSL (Secure Socket Layer)</b>	Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica
<b>Presidente del Consiglio Notarile Distrettuale</b>	Tale ai sensi della legge notarile.
<b>Titolare</b>	Notaio a favore del quale è stato emesso un Certificato dal CNN.
<b>Validazione temporale</b>	Risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, un riferimento temporale opponibili ai terzi.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

DEFINIZIONE	DESCRIZIONE
<b>TSA CA</b>	Certification Authority dedicata al servizio di marcatura temporale che ha la principale funzione di emettere i certificati con i quali vengono rilasciate le marche temporali.
<b>TSP</b>	Trusted Service Provider, prestatore di servizi fiduciari (es. Prestatore di Servizi Fiduciari accreditato, Conservatore accreditato, etc) ai sensi del Regolamento 910/2014
<b>QTSP</b>	Un prestatore di servizi fiduciari qualificato fornisce servizi fiduciari che soddisfano i requisiti stabiliti dal Regolamento eIDAS e ne fornisce le relative garanzie in termini di sicurezza e qualità.
<b>TSS / TSU</b>	Time Stamping Server, o Time Stamping Unit, è un componente che emette e firma le marche temporali che gli utenti inoltrano alla Time Stamping Authority utilizzando i certificati emessi dalla TSA CA.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 1. INTRODUZIONE

### 1.1. Scopo del documento

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

- Certificazione delle chiavi pubbliche dei notai.

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

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

### 1.2. Riferimenti normativi

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

- Legge 16 febbraio 1913 n. 89 (legge notarile);
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Decreto Legislativo 7 marzo 2005 n. 82 (Codice dell'amministrazione digitale);
- Determinazione n. 185/2017 (Modalità per la domanda di qualificazione per i servizi eIDAS);
- DPCM 22 febbraio 2013 (regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali);
- REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- Decisione di esecuzione (UE) 2015/1505 della Commissione, dell'8 settembre 2015, che stabilisce le specifiche tecniche e i formati relativi agli elenchi di fiducia di cui all'articolo 22, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno;
- Decisione di esecuzione (UE) 2016/650 della Commissione, del 25 aprile 2016, che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno;
- Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate (Determinazione n. 147/2019 rettifica per errore materiale la Determinazione n.121/2019).

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.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 2. DATI IDENTIFICATIVI DEL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI

I dati identificativi relativi al CNN sono i seguenti:

<b>Denominazione e Ragione sociale:</b>	Consiglio Nazionale del Notariato
<b>Sede legale:</b>	via Flaminia 160, 00196 Roma
<b>Rappresentante legale:</b>	Presidente pro tempore del CNN
<b>Telefono:</b> +39-06362091	<b>Fax:</b> +39-063221594
<b>Sede operativa:</b> via Flaminia 133-135, 00196 Roma via Giovanni Vincenzo Gravina 4 00196 Roma	<b>Indirizzo E-mail:</b> <a href="mailto:segreteria.cnn@postacertificata.notariato.it">segreteria.cnn@postacertificata.notariato.it</a> <a href="mailto:esercizio@postacertificata.notariato.it">esercizio@postacertificata.notariato.it</a>
<b>Indirizzi Internet:</b> <a href="https://ca.notariato.it">https://ca.notariato.it</a> <a href="https://www.notariato.it">https://www.notariato.it</a>	<b>Customer Care:</b> customercare@notariato.it

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

### 3. MANUALE OPERATIVO

#### 3.1. Dati identificativi del Manuale operativo

Il presente Manuale operativo, conservato presso i locali del Prestatore di Servizi fiduciari qualificati e depositato presso il AgID, è identificato col nome "MO\_CNN\_CA\_8" ed è consultabile per via telematica all'indirizzo Internet:

[https://ca.notariato.it/documentazione/MOCNN\\_CA.pdf](https://ca.notariato.it/documentazione/MOCNN_CA.pdf)

Il presente documento è identificato con il numero di versione 8.0.

Tali OID identificano:

Consiglio Nazionale del Notariato	1.3.6.1.4.1.8526
Certification Service Provider	1.3.6.1.4.1.8526.1
Certificate-Policy per certificati emessi in conformità alla policy ETSI QCP-n-qscd (QSCD)	0.4.0.194112.1.2
Policy per certificati di firma su dispositivo (QSCD)	1.3.6.1.4.1.8526.1.1.5
Timestamp policy	1.3.6.1.4.1.8526.1.2
Policy per certificati di firma remota	1.3.6.1.4.1.8526.1.1.6
Policy per certificati di firma su dispositivo (QSCD) conformi al profilo della Determinazione AgID n. 147/2019	1.3.6.1.4.1.8526.1.1.7
Policy per certificati di firma remota conformi al profilo della Determinazione AgID n. 147/2019	1.3.6.1.4.1.8526.1.1.8

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

#### 3.2. Responsabile del Manuale operativo

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

Telefono: +39-06362091

E-mail: [segreteria.cnn@postacertificata.notariato.it](mailto:segreteria.cnn@postacertificata.notariato.it)

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

### 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.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 4. TERMINI E CONDIZIONI

### 4.1. Obblighi del Prestatore di Servizi fiduciari qualificati

Il servizio erogato dal prestatore di servizi fiduciari qualificati è stato valutato, e periodicamente viene rivalutato, in conformità alle direttive del Regolamento eIDAS e degli standard ETSI vigenti e ai requisiti contenuti nel presente manuale operativo.

Il servizio di CA è conforme alla versione corrente del documento Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates pubblicato presso <https://www.cabforum.org>.

In caso di contrasto tra il manuale operativo e tali requisiti, i Requisiti hanno la precedenza su questo documento.

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

1. adotta tutte le misure organizzative e tecniche idonee ad evitare danno a terzi;
2. emette e gestisce i certificati in modo conforme alla normativa italiana ed europea, con le procedure descritte nel presente Manuale Operativo;
3. identifica con certezza il notaio richiedente ed il fatto che sia regolarmente in esercizio ai sensi della legge notarile;
4. informa espressamente, in modo compiuto e chiaro, il Titolare riguardo agli obblighi in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi di firma, nonché sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
5. rilascia e rende pubblico il certificato;
6. si attiene alle regole tecniche emanate da AgID;
7. si accerta dell'autenticità della richiesta di certificazione;
8. richiede la prova del possesso della chiave privata e verifica il corretto funzionamento della coppia di chiavi, eventualmente richiedendo la sottoscrizione di uno o più documenti di prova;
9. si attiene alle misure minime di sicurezza per il trattamento dei dati personali di cui al Regolamento UE 679/2016;
10. genera le coppie di chiavi mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata;
11. procede tempestivamente alla revoca od alla sospensione del certificato in tutti i casi previsti dal presente Manuale Operativo;
12. comunica le richieste di revoca o sospensione al Titolare;
13. dà tempestiva pubblicazione della revoca e della sospensione del certificato;
14. conserva le richieste scritte di registrazione e le richieste di certificazione per un periodo di almeno 30 anni dalla data di scadenza del certificato;
15. comunica per iscritto a AgID ogni variazione dei requisiti per l'iscrizione all'Elenco pubblico dei Certificatori accreditati ai sensi della normativa vigente e, in ogni caso, periodicamente conferma la permanenza dei requisiti per l'esercizio dell'attività di certificazione;
16. comunica tempestivamente a AgID, ogni variazione significativa delle soluzioni tecnico-organizzative adottate;
17. comunica immediatamente a AgID e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso;

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

- 18. comunica a AgID ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività, della conseguente rilevazione della documentazione da parte di altro Prestatore di Servizi Fiduciari o del suo annullamento, specificando che tutti i certificati non scaduti al momento della cessazione devono essere revocati;
- 19. garantisce le condizioni del servizio descritto nel presente manuale per tutta la durata dello stesso, salvo modifiche rese necessarie da requisiti aggiuntivi o modifiche della normativa vigente;
- 20. in caso di modifica alle condizioni del presente manuale operativo fornisce informativa ai titolari ed ai destinatari mediante pubblicazione del manuale aggiornato sul sito della CA;
- 21. si attiene alle indicazioni di Agid in caso di compromissione degli algoritmi utilizzati.

#### **4.2. Obblighi del Titolare**

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

Il Titolare delle chiavi deve, inoltre:

- 1. fornire tutte le informazioni richieste dal Prestatore di Servizi fiduciari qualificati, garantendone, sotto la propria responsabilità, l'attendibilità;
- 2. conservare con la massima diligenza i codici personali, e il dispositivo fisico di firma (smartcard) e l'eventuale generatore di PIN (OTP) al fine di garantire l'integrità e la conservazione delle informazioni di abilitazione all'uso della chiave privata;
- 3. mantenere in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma;
- 4. accertare che il documento da sottoporre alla firma non contenga macroistruzioni o codici eseguibili, tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati nello stesso rappresentati;
- 5. attivare e mantenere costantemente aggiornati strumenti che si oppongano all'inserimento di codice malevolo (malware) nel sistema utilizzato per apporre le firme digitali e che, ove esso sia presente, siano in grado di individuarlo, nel qual caso il titolare è tenuto a curarne l'eliminazione;
- 6. richiedere immediatamente la revoca o la sospensione dei certificati nei casi e con le modalità previste dal presente Manuale Operativo;
- 7. sporgere denuncia, in caso di smarrimento o sottrazione delle chiavi di firma, alle Autorità competenti.
- 8. dismettere l'utilizzo della firma in seguito alla avvenuta pubblicazione della revoca.

In ogni caso è vietata la duplicazione della chiave privata.

#### **4.3. Obblighi dei destinatari**

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

- 1. la validità del certificato;
- 2. l'assenza del certificato dalle Liste di Revoca dei certificati (CRL);
- 3. l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

#### 4.4. Obblighi del Presidente del CND

Il Presidente del CND ha l'obbligo di:

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

#### 4.5. Reclami

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

- Telefono: 06.36769306
- Fax: 06.32650077
- E-mail: [customercare@notariato.it](mailto:customercare@notariato.it)

#### 4.6. Legge Applicabile – Foro Competente

Per quanto ivi non esplicitamente previsto nel presente Manuale si applicano le norme del Codice.

Ogni controversia che dovesse sorgere tra le parti in relazione all'esecuzione del servizio di erogazione dei certificati qualificati, regolato dal presente Manuale sarà devoluta alla competenza esclusiva del Foro di Roma.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 5. RESPONSABILITÀ

### 5.1. Responsabilità del Prestatore di Servizi fiduciari qualificati

Il Prestatore di Servizi fiduciari qualificati è responsabile verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dalla Regolamento EIDAS 910/2014, Regolamento UE 679/2016, dal D. Lgs. n. 82/05 e s.m.i., dalla Determinazione AgID n. 185/2017, dalla Determinazione AgID n. 147/2019, dal D.P.C.M. 22 febbraio 2013.

Il CNN è responsabile nei confronti di qualunque soggetto faccia ragionevole affidamento sui certificati emessi dallo stesso, nei limiti di cui all'art. 30 del D.Lgs. n. 82/2005. L'esistenza e la validità del certificato non dispensano però l'utente dall'eseguire ogni altra verifica che appaia opportuna secondo criteri di oculata prudenza, anche in relazione al rilievo, economico o d'altra natura, degli interessi coinvolti. La responsabilità del CNN è comunque rigorosamente circoscritta a:

- l'esattezza delle informazioni contenute nel certificato alla data di rilascio e la loro completezza rispetto ai requisiti fissati per i certificati;
- la garanzia che, al momento del rilascio del certificato, il notaio detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
- la garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il Prestatore di Servizi fiduciari qualificati generi entrambi;
- l'esecuzione della procedura di revoca o sospensione nei termini e con le modalità previste dal presente manuale operativo.

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

È altresì esclusa qualsivoglia responsabilità del CNN laddove i terzi non si attengano alle prescrizioni stabilite dal presente documento ed in particolare non rispettino le procedure stabilite per la verifica delle firme e delle marche temporali o facciano affidamento su di esse al di fuori dei casi e dei limiti previsti dal relativo certificato.

Ogni responsabilità è comunque esclusa laddove il CNN provi d'aver agito senza colpa, ed in ogni caso in cui la responsabilità è esclusa dall'art. 30 del D. Lgs. n. 82/2005.

## 6. TARiffe

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

Le tariffe sono pubblicate sul portale dei servizi del notariato.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 7. IDENTIFICAZIONE E REGISTRAZIONE

### 7.1. Identificazione

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

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

I suddetti documenti devono essere validi e presentati in originale.

### 7.2. Registrazione

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

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

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

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

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

### 7.3. Contenuto della richiesta del certificato

La richiesta di certificazione include i seguenti dati:

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

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

### 7.4. Obblighi di Identificazione

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

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

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

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

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

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

## 7.6. Codici riservati

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

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

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

CND	Notaio	CA-CNN
Il Presidente, nella funzione di RA, invia al CNN richiesta di rilascio di uno o più chiavi di firma. La richiesta contiene i dati anagrafici del notaio e l'indirizzo al quale spedire il dispositivo di firma e/o l'eventuale dispositivo OTP.	Il Notaio se dispone già di un certificato attivo su smart card può fare richiesta di una firma remota, specificando il tipo di OTP scelto. In questo caso viene avviato un flusso di registrazione automatico che inoltra agli operatori di CA la richiesta di invio di nuovi codici ed eventualmente del dispositivo OTP fisico.	

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

CND	Notaio	CA-CNN
		<p>Per ogni chiave di firma richiesta:</p> <ul style="list-style-type: none"> <li>• associa ad ogni notaio un codice identificativo ed un codice riservato;</li> <li>• inizializza e/o personalizza per il notaio ogni dispositivo di firma (es. serigrafia, inizializzazione elettrica);</li> <li>• trasmette all'indirizzo indicato nella richiesta del CND un plico intestato al notaio contenente il dispositivo di firma e/o il dispositivo OTP e spedisce al CND altro plico contenente i codici identificativi con gli associati codici riservati ed ogni altro codice (es. PIN, PUK) necessario alla generazione delle chiavi.</li> </ul>
Il Presidente del CND, contestualmente o successivamente all'iscrizione a ruolo nel distretto di competenza, consegna i codici riservati al notaio.		
	Il notaio, al ritiro dei codici, dopo averne verificato l'integrità, firma un'apposita dichiarazione attestante lo stato di integrità dei codici stessi e, ove esse risultino integri, l'uso esclusivo della firma nell'espletamento delle funzioni di notaio.	

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

CND	Notaio	CA-CNN
	<p>Generazione di chiavi di firma su smart card.</p> <p>Successivamente esegue la generazione delle chiavi internamente al dispositivo di firma effettuando le seguenti operazioni:</p> <ul style="list-style-type: none"> <li>• accede ad un apposito software identificandosi con il codice identificativo e il codice riservato allegato al dispositivo di firma;</li> <li>• 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;</li> <li>• avvia la procedura di generazione della coppia di chiavi internamente al dispositivo di firma;</li> <li>• firma la richiesta di certificazione della chiave pubblica in formato PKCS#10 e la trasmette al CNN su canale sicuro.</li> </ul> <p>Generazione di chiavi di firma remota:</p> <ul style="list-style-type: none"> <li>• in seguito alla ricezione dei codici il notaio procede con l'attivazione della firma remota, utilizzandoli in combinazione con il codice OTP generato.</li> </ul>	
		Il Prestatore di Servizi Fiduciari genera il certificato digitale sulla base della richiesta pervenuta.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

CND	Notaio	CA-CNN
	<p>In caso di firma con smart card: Il titolare, tramite apposito applicativo software, memorizza il certificato digitale all'interno del dispositivo di firma.</p> <p>In caso di firma remota: Il titolare, tramite apposito applicativo software, memorizza il certificato sui dispositivi crittografici (HSM) custoditi presso il Prestatore di Servizi Fiduciari.</p>	

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.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 8. GENERAZIONE DELLE CHIAVI

### 8.1. Sistemi di generazione

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

Il sistema di generazione delle chiavi assicura:

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

La generazione delle chiavi avviene in modo sicuro all'interno del dispositivo di firma certificato SSCD, oppure all'interno dei dispositivi critografici (HSM) custoditi presso il Prestatore di Servizi fiduciari qualificati garantendo integrità e segretezza della chiave.

### 8.2. Lunghezza delle chiavi

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

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

### 8.3. Algoritmi

Gli algoritmi utilizzati rispettano le indicazioni di AgID e sono conformi a ETSI TS 119 312.

Per la generazione e la verifica delle firme digitali è usato il seguente algoritmo:

- RSA (Rivest-Shamir-Adleman algorithm).

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

- SHA-256 (Dedicated Hash Function 4)

### 8.4. Chiavi di certificazione

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

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

Il certificato corrispondente alle chiavi di certificazione del CNN, valido dal 28 novembre 2024, è un certificato di root, che non prevede CA subordinate, ed è così identificato:

organizationIdentifier=VATIT-80052590587

CN= Consiglio Nazionale del Notariato Qualified Certification Authority 2024

OU= Qualified Trust Service Provider

O=Consiglio Nazionale del Notariato

C=IT

Numeros seriale: 28:41:45:15:3d:f6:2b:c6:09:93:cc:1d:b1:ce:4c:76:33:4a:8e:9e

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

Identificatore chiave del soggetto D9:F7:D1:A7:05:4B:E4:89:D9:35:05:15:48:D9:95:FD:B0:C0:7A:D8

Il certificato corrispondente alle chiavi di certificazione del CNN, valido dal 22 ottobre 2019, è un certificato di root, che non prevede CA subordinate, ed è così identificato:

organizationIdentifier=VATIT-80052590587

CN= Consiglio Nazionale del Notariato Qualified Certification Authority 2019

OU=Servizio Firma Digitale

O=Consiglio Nazionale del Notariato

C=IT

Numero seriale 01

Identificatore chiave del soggetto D7:41:68:C6:CE:84:34:6A:7F:37:4F:67:88:63:E1:57:E7:4A:61:8A

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

organizationIdentifier=VATIT-80052590587

CN=Consiglio Nazionale del Notariato Qualified Certification Authority

OU=Servizio Firma Digitale

O=Consiglio Nazionale del Notariato

C=IT

Numero seriale 01a8

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

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

CN = Consiglio Nazionale del Notariato Qualified Certification Authority

OU = Servizio Firma Digitale

O = Consiglio Nazionale del Notariato

C = IT

Serial Number = 80052590587

Numero seriale 01a8

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

#### **8.4.1.Generazione delle chiavi di certificazione**

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

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 8.5. Chiavi di sottoscrizione

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

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

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

## 8.6. Dispositivo di firma

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

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

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

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

## 8.7. Requisiti del dispositivo di firma

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

L'utilizzo delle chiavi private da parte del notaio è subordinato alla sua autenticazione mediante un PIN che deve essere digitato dal titolare ogni volta che egli intende usare il dispositivo.

L'utilizzo delle chiavi di firma remota è subordinato all'autenticazione del notaio mediante PIN in abbinamento al codice OTP.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 9. EMISSIONE DEI CERTIFICATI

### 9.1. Informazioni contenute nel certificato

Il certificato contiene le informazioni previste dai regolamenti AGID. In particolare:

- numero di serie del certificato;
- denominazione del Prestatore di Servizi fiduciari qualificati;
- codice identificativo del Titolare presso il Prestatore di Servizi;
- nome, cognome e codice fiscale del Titolare;
- l'indicazione che il titolare è notaio;
- distretto notarile di esercizio;
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità del certificato;
- algoritmo di sottoscrizione del certificato;
- l'indicazione dell'uso esclusivo della chiave privata per l'esercizio della funzione notarile;
- l'indicazione che il certificato è qualificato;
- le informazioni per il recepimento dello stato del certificato (CRL e OCSP);
- riferimento al presente manuale operativo;
- tipologia delle chiavi.

### 9.2. Profilo del certificato

Il certificato è un documento informatico, firmato digitalmente dal Prestatore di Servizi fiduciari qualificati, che deve essere generato e pubblicato, a cura dello stesso. I certificati sono conformi alla norma ISO/IEC 9594-8:2005 e successive modificazioni o integrazioni e alle specifiche RFC 3280, ETSI TS 102 280 ed ETSI TS 101 862, come previsto dalla Determinazione AgID n. 147/2019.

Le informazioni contenute nel certificato seguono le regole previste dalla Determinazione AgID n. 147/2019.

In conformità a quanto previsto dalla Determinazione AgID n. 147/2019, all'interno del campo "Subject" è presente un sottocampo O (Organization) riportante il distretto notarile di esercizio. È inoltre presente il campo "IssuerAlternativeName" riportante l'indirizzo di posta elettronica del del Prestatore di Servizi fiduciari qualificati.

In conformità allo standard ETSI 319 412 – 5 il certificato del titolare contiene l'estensione qCStatement, ed in particolare:

- contiene il campo identificato come esi4-qcStatement-1 (id-etsi-qcs-QcCompliance OID: 0.4.0.1862.1.1) che indica che il certificato è qualificato e conforme al regolamento UE 910/2014.
- non contiene l'estensione esi4-qcStatement-2 (id-etsi-qcs-QcLimitValue OID: 0.4.0.1862.1.2), assente in quanto non sono applicabili limiti nelle negoziazioni;
- contiene il campo esi4-qcStatement-3 (id-etsi-qcs-QcRetentionPeriod OID: 0.4.0. 1862.1.3), che definisce il periodo di conservazione da parte della CA, il valore indicato è pari a 30 anni, ma è ovviamente esteso a tutto il tempo di conservazione da parte del Prestatore di Servizi Fiduciari;

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

- contiene il campo esi4-qcStatement-4 (id-etsi-qcs-QcSSCD OID: 0.4.0. 1862.1.4), che indica la memorizzazione della chiave privata internamente ad un dispositivo sicuro.
- contiene il campo esi4-qcStatement-5 che contiene la URL al Disclosure Statement.
- non contiene il campo esi4-qcStatement-6 relativo al tipo di certificato in base alle Annex del regolamento.

### **9.3. Emissione del certificato**

Il certificato è generato con un sistema utilizzato esclusivamente per tale funzione, situato in locali protetti come descritto nel Piano per la sicurezza.

L'accesso al sistema di generazione dei certificati avviene attraverso un'operazione di riconoscimento mediante l'uso di un dispositivo di autenticazione forte.

I certificati relativi alle chiavi pubbliche dei notai sono conservati, a cura del Prestatore di Servizi fiduciari qualificati per trenta anni dalla data di scadenza del certificato.

#### **9.3.1. Emissione del certificato sul dispositivo di firma**

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

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

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

#### **9.3.2. Emissione del certificato di firma remota**

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

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

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

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 10. REVOCA E SOSPENSIONE DEI CERTIFICATI DI SOTTOSCRIZIONE

### 10.1. Premessa

Il Prestatore di Servizi fiduciari qualificati pubblica la revoca e la sospensione dei certificati di sottoscrizione mediante la Lista dei certificati revocati (CRL) ogni 8 ore e mediante servizio OCSP (Online Certificate Status Protocol).

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.

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

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

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

Il Prestatore di Servizi fiduciari qualificati 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 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 titolare il servizio è disponibile dal Lunedì al Venerdì, dalle ore 09.00 alle ore 18.00.

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.

### 10.2. Revoca dei certificati

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

Il certificato è revocato su:

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

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

Il Prestatore di Servizi fiduciari qualificati in tutti i casi provvede alla revoca del certificato, al suo inserimento nell'apposita Lista dei certificati revocati (CRL) ed alla pubblicazione della Lista nel Registro dei certificati e mediante servizio OCSP.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

### 10.2.1. Revoca da parte del titolare

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

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

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

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

- Modalità 1: richiesta scritta con firma autografa presso il Prestatore;
- Modalità 2: richiesta di revoca del certificato sottoscritta con firma digitale.

**Modalità 1:** richiesta scritta di revoca con firma autografa presso il Prestatore di Servizi fiduciari.

Il Titolare deve compilare la richiesta indicando:

- nome e cognome;
- codice fiscale;
- distretto di appartenenza;
- dati identificativi del certificato;
- motivazione e decorrenza della revoca;
- eventuali altri elementi rilevanti a determinare i casi di maggiore urgenza ovvero di emergenza.

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

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

La domanda deve essere inoltrata dal notaio Titolare al Prestatore di Servizi Fiduciari, mediante il portale della Registration Authority, 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;
- codice fiscale;
- distretto di appartenenza;
- dati identificativi del certificato;
- motivazione e decorrenza della revoca o sospensione;
- eventuali altri elementi rilevanti a determinare i casi di maggiore urgenza ovvero di emergenza.

La richiesta firmata digitalmente è verificata dal Prestatore di Servizi fiduciari qualificati che provvede alla revoca del certificato.

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

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 10.2.2. Revoca da parte del presidente di distretto

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

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

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

- Modalità 1: richiesta di revoca scritta con firma autografa;
- Modalità 2: richiesta di revoca del certificato sottoscritta con firma digitale;

Il Prestatore di Servizi fiduciari qualificati in tutti i casi provvede alla revoca del certificato, al suo inserimento nell'apposita Lista dei certificati revocati (CRL) ed alla pubblicazione della Lista nel Registro dei certificati e mediante servizio OCSP.

**Modalità 1:** richiesta scritta con firma autografa.

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

La richiesta deve indicare:

- nome e cognome del Titolare;
- codice fiscale del Titolare;
- distretto di appartenenza;
- dati identificativi del certificato;
- motivazione e decorrenza della revoca;

Il Presidente inoltra la richiesta al Prestatore di Servizi Fiduciari.

Il Prestatore di Servizi Fiduciari, ricevuta la richiesta, provvede alla revoca del certificato.

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

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

La domanda va inoltrata dal Presidente del Consiglio Notarile Distrettuale al Prestatore di Servizi fiduciari qualificati, mediante il portale della Registration Authority, 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;
- codice fiscale del Titolare;
- distretto di appartenenza;
- dati identificativi del certificato;
- motivazione e decorrenza della revoca;

La richiesta firmata digitalmente è verificata dal Prestatore di Servizi Fiduciari che provvede alla revoca del certificato.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

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

### **10.2.3.Revoca da parte del Prestatore**

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

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

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

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

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 10.3. Sospensione di certificati

La durata della sospensione viene scelta dal soggetto richiedente e non può essere superiore al periodo di validità del certificato.

Alla scadenza del periodo di sospensione richiesto, la validità del certificato viene ripristinata tramite la rimozione del certificato dalla lista di revoca e sospensione (CRL).

### 10.3.1. Sospensione da parte del titolare

Il notaio può richiedere in ogni tempo la sospensione dei suoi certificati nei seguenti casi:

- permesso di assenza per il periodo relativo;
- perdita del possesso delle chiavi di firma (smarrimento).

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

- Modalità 1: richiesta di sospensione del certificato sottoscritta con firma digitale;
- Modalità 2: richiesta telefonica in caso di emergenza utilizzando il codice di sospensione riservato del notaio ed il codice identificativo delle chiave di firma al Prestatore di Servizi Fiduciari.

**Modalità 1:** richiesta di sospensione del certificato sottoscritta con firma digitale.

La domanda deve essere inoltrata dal notaio Titolare al Prestatore di Servizi Fiduciari, mediante il portale della Registration Authority, attraverso una richiesta sottoscritta con firma digitale sull'apposito modulo, con la stessa chiave oggetto di sospensione, se ancora disponibile, nei tempi previsti nel presente manuale.

Il Titolare deve indicare nella richiesta:

- nome e cognome;
- codice fiscale;
- distretto di appartenenza;
- dati identificativi del certificato;
- motivazione e decorrenza della sospensione;

La richiesta firmata digitalmente è verificata dal Prestatore di Servizi fiduciari qualificati che provvede alla sospensione del certificato.

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

**Modalità 2:** richiesta telefonica di sospensione in caso di emergenza utilizzando il codice riservato e i dati identificativi del certificato al Prestatore di Servizi Fiduciari.

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

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

### 10.3.2. Sospensione da parte del Prestatore

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

### 10.4. Riattivazione di certificati

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 con firma autografa di riattivazione da parte del Presidente del Consiglio Notarile Distrettuale e inoltrata al Prestatore di Servizi fiduciari qualificati.
- a seguito di richiesta tramite modulo firmato digitalmente da parte del Presidente del Consiglio Notarile Distrettuale e trasmessa telematicamente.

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

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 11. REVOCA DEI CERTIFICATI RELATIVI ALLE CHIAVI DI CERTIFICAZIONE

### 11.1. Circostanze di revoca

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

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

### 11.2. Obbligo di notifica

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

La comunicazione contiene i riferimenti alle informazioni compromesse.

### 11.3. 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. Procedura di revoca dei certificati relativi a chiavi di certificazione

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

Successivamente, notifica entro 24 ore, la revoca ad 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 dei certificati di sottoscrizione

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

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

In casi di emergenza, la richiesta di revoca 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, il Prestatore di Servizi fiduciari qualificati informa il titolare e la terza parte degli estremi della revoca mediante messaggi di posta elettronica.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 12. RINNOVO DEI CERTIFICATI DI FIRMA

### 12.1. Rinnovo dei Certificati del Titolare

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

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

### 12.2. Sostituzione delle chiavi di certificazione

Il Prestatore di Servizi fiduciari qualificati, tre anni prima della scadenza del certificato relativo ad una chiave di certificazione, avvia la procedura di sostituzione, generando una nuova coppia di chiavi.

I certificati così generati sono forniti ad AgID che provvede all'aggiornamento della lista dei certificati delle chiavi di certificazione contenuta nell'elenco pubblico dei Certificatori ed al suo inoltro ai Certificatori per la pubblicazione.

In tale occasione, il Prestatore di Servizi Fiduciari esegue la procedura di creazione delle copie delle chiavi di certificazione da utilizzare in caso di disastro.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 13. REGISTRO DEI CERTIFICATI

### 13.1. Informazioni contenute nel Registro dei certificati

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

- il certificato, relativo alla chiave di certificazione, sottoscritto con la chiave privata della coppia cui il certificato si riferisce;
- lista dei certificati revocati e sospesi (CRL).

Le liste dei certificati revocati e sospesi sono conformi alla specifica RFC 5280, capitolo 5, esclusi i paragrafi 5.2.4 e 5.2.6 come previsto dalla Determinazione AgID n. 147/2019.

### 13.2. Procedura di gestione del Registro dei certificati

Il Registro dei certificati è consultabile da qualsiasi soggetto 24 ore al giorno, 7 giorni su 7, esclusi i tempi dedicati alla manutenzione programmata ed alla soluzione di eventuali problemi tecnici non prevedibili.

Il Registro dei certificati è gestito dalla directory di sistema ITU-T X.500.

Il Prestatore di Servizi Fiduciari mantiene una copia di riferimento del Registro dei certificati, inaccessibile dall'esterno, allocata su un sistema sicuro installato in locali protetti.

Sistematicamente, verifica la conformità tra la copia operativa e la copia di riferimento del Registro, annotando ogni discordanza nel Registro operativo.

Le modificazioni al contenuto del Registro dei certificati sono effettuate esclusivamente da personale autorizzato. Tali operazioni sono sistematicamente registrate sul Giornale di controllo.

### 13.3. Procedura di aggiornamento del Registro dei certificati

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

- pubblica Liste dei certificati revocati e sospesi in seguito alla revoca o alla sospensione di un certificato ogni 8 (otto) ore e aggiorna il servizio OCSP.

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

- Il Responsabile del Registro dei certificati controlla l'applicazione che pubblica ed aggiorna 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.

### 13.4. 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.

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 14. PROTEZIONE DELLA RISERVATEZZA

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

Le misure di protezione adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali con riferimento al Regolamento UE 679/2016.

## 15. GESTIONE DELLE COPIE DI SICUREZZA

Il Prestatore di Servizi fiduciari qualificati effettua periodicamente, e secondo politiche ben definite, copie di sicurezza del sistema di certificazione.

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

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

## 16. DISPONIBILITÀ DEL SERVIZIO

Nell'ambito della strategia di disaster recovery adottata, è prevista l'esistenza, oltre ai due siti primari, di un sito di disaster recovery che garantisce, l'espletamento dei seguenti, a partire dalla dichiarazione di disastro:

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

Il Prestatore di servizi fiduciari eroga i servizi sopra descritti nell'arco delle 24 h per 7 giorni a settimana, con una disponibilità pari al 99% su base annua.

## 17. GESTIONE DEGLI EVENTI CATASTROFICI

Il Prestatore di servizi fiduciari qualificati garantisce la continuità del servizio, in caso di disastro, attraverso la predisposizione di opportune procedure che consentono il ripristino.

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

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## 18. GIORNALE DI CONTROLLO

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

### 18.1. Dati da archiviare

Secondo quanto stabilito dal D.P.C.M. in vigore, i dati da annotare e da archiviare, cui è associata la data e l'ora dell'effettuazione, sono i seguenti:

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

### 18.2. Conservazione dei dati

Le registrazioni sono effettuate indipendentemente su supporti distinti e di tipo differente. Esse riportano la data e l'ora in cui sono state effettuate e sono conservate per un periodo di 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 secondo dal tempo UTC (IEN).

### 18.3. Protezione dell'archivio

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

### 18.4. Gestione del Giornale di controllo

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

### 18.5. Verifiche

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

Emesso da: <b>Consiglio Nazionale del Notariato</b>	Tipo documento: <b>Manuale operativo</b> Codice doc.: MO_CNN_CA_8
Titolo documento: <i>Manuale operativo del Consiglio Nazionale del Notariato per il servizio di certificazione delle chiavi pubbliche</i>	Edizione: 8.0 n.ro allegati:

## **19. CESSAZIONE DELL'ATTIVITÀ DEL PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATI**

Il Prestatore di Servizi fiduciari qualificati, se intende cessare l'attività, comunica ad AgID la data di cessazione con un anticipo di sei mesi, indicando il Prestatore di Servizi Fiduciari sostitutivo ovvero il depositario del Registro dei certificati e della relativa documentazione.

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

AgID rende nota nell'elenco pubblico la data di cessazione con l'indicazione del Prestatore di Servizi Fiduciari sostitutivo ovvero del depositario del Registro dei certificati e della relativa documentazione.

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

Roma, 02/12/2024

Il presidente del CNN