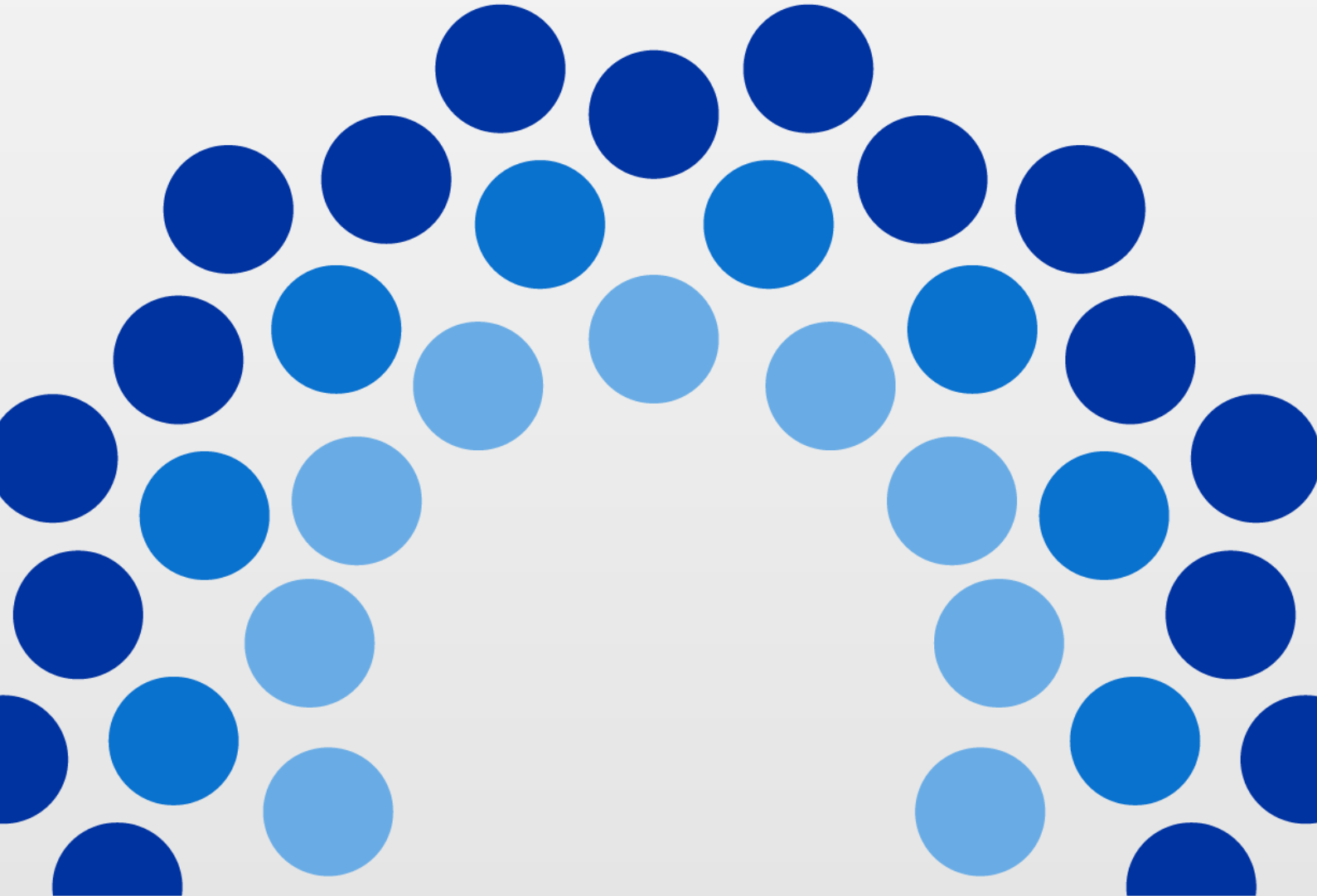
Camera di Commercio Industria Artigianato Agricoltura

Ente Emettitore
Carta Nazionale dei Servizi
Manuale Operativo - CA InfoCamere

Codice documento: IC-MO-CCIAA-CNS

La Camera di Commercio che adotta il presente manuale, lo rende noto nel proprio sito internet.



Indice

1 Introduzione al documento 4
1.1 Novità introdotte rispetto alla precedente emissione 4
1.2 Scopo e campo di applicazione del documento 4
1.3 Riferimenti normativi e tecnici 4
1.4 Riferimenti tecnici 5
1.5 Definizioni 5
1.6 Acronimi e abbreviazioni 7

2 Generalità 8
2.1 Identificazione del documento 8
2.2 Ente Emettitore 9
2.3 Contatto per utenti finali e comunicazioni 9
2.4 Pubblicazione 9
2.4.1 Pubblicazione delle informazioni 9
2.5 Tutela dei dati personali 9
2.6 Tariffe 9
2.6.1 Rilascio e rinnovo del certificato 9
2.6.2 Revoca e sospensione del certificato 10
2.6.3 Accesso al certificato e alle liste di revoca 10

3 Obblighi e Responsabilità 11
3.1 Obblighi dei Titolari 11
3.2 Responsabilità 11
3.2.1 Limitazioni di responsabilità 11

4 Amministrazione del Manuale Operativo 12
4.1 Procedure per l'aggiornamento 12
4.2 Responsabile dell'approvazione 12

5 Identificazione e Autenticazione 13
5.1 Identificazione ai fini del primo rilascio 13
5.1.1 Soggetti abilitati ad effettuare l'identificazione 13
5.1.2 Procedure per l'identificazione 13

6 Operatività 15
6.1 Registrazione 15
6.2 Rilascio del certificato 15
6.2.1 Generazione e protezione delle coppie di chiavi 15
6.3 Emissione del certificato 15
6.3.1 Formato e contenuto dei certificati di autenticazione e sottoscrizione 15
6.3.2 Validità dei certificati 17
6.4 Interdizione di una CNS 17
6.4.1 Motivi per la revoca di un certificato 18
6.4.2 Procedura per la richiesta di revoca 18
6.4.3 Motivi per la Sospensione di un certificato 19
6.4.4 Procedura per la richiesta di sospensione 19

6.4.5 Procedura di richiesta di riattivazione 19
6.4.6 Pubblicazione e frequenza di emissione della CRL 20
6.5 Attivazione della CNS 20
6.6 Rinnovo del Certificato 20

7 Disponibilità del servizio 21

1 Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	3.0	**Data Versione/Release**:	*28/12/2023*
Descrizione modifiche:	inserimento figura Master Registration Authority (MRA) § 1.5: aggiunta definizione MRA, § 5. inserimento MRA tra i soggetti abilitati ad effettuare l'identificazione ed integrazione con procedura riconoscimento da remoto; revisione documento		
Motivazioni:	Aggiornamenti tecnici e procedurali		

Precedenti versioni:

Versione/Release n°:	2.0	**Data Versione/Release**:	*18/12/2020*
Descrizione modifiche:	§§ 5.1, 5.1.2: aggiornati riferimenti documenti di riconoscimento § 5.1.2.2: aggiunto dato obbligatorio nell'anagrafica		
Motivazioni:	Aggiornamenti tecnici e procedurali		

1.2 Scopo e campo di applicazione del documento

Il presente documento contiene le regole e le procedure operative che governano l'emissione della **Carta Nazionale dei Servizi (CNS) e dei relativi certificati** sottoscritti dall'Ente Certificatore InfoCamere; la CNS è emessa dalla Camera di Commercio. Questo manuale indica inoltre le procedure da seguire in caso di smarrimento, furto o timore di compromissione della carta.

Le indicazioni di questo documento hanno validità per le attività relative alla Camera di Commercio in qualità di Ente Emettitore e ad InfoCamere nel ruolo di Master Registration Authority e di Certificatore, per i CDRL/RA, per i soggetti incaricati ad effettuare l'identificazione/registrazione dei Titolari e/o a consegnare/inviare i dispositivi CNS ai medesimi, per gli stessi Titolari e per gli Utenti.

Per la compilazione di questo documento si è fatto riferimento ai seguenti documenti:

- **InfoCamere** Ente Certificatore - Manuale Operativo IC-MO-TSP;
- **InfoCamere** Ente Certificatore - Certificati di Autenticazione per la Carta Nazionale dei Servizi - Certificate Policy-MO-CNS-CCIAA

1.3 Riferimenti normativi e tecnici

Riferimenti normativi

[1] Decreto Legislativo 7 marzo 2005, n.82 – Codice dell'amministrazione digitale e successive modifiche ed integrazioni (nel seguito referenziato come CAD).

[2] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (nel seguito referenziato come TU).

[3] Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali

[4] Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e

ss.mm.iii. e il 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

[5] Decreto del Presidente della Repubblica 2 marzo 2004, n. 117 e successive modificazioni. modificazioni - "Regolamento concernente la diffusione della carta nazionale dei servizi".

[6] Decreto interministeriale 9 dicembre 2004, Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi.

[7] "Linee guida per l'emissione e l'utilizzo della Carta Nazionale dei Servizi", Ufficio Standard e tecnologie d'identificazione, CNIPA, Versione 3.0, 15 maggio 2006.

1.4 Riferimenti tecnici

[8] Deliverable EN 319 401 v.2.2.1 "*General Policy Requirements for Trust Service Providers*" – Aprile 2018

[9] RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (rende obsoleto l'RFC 3280)

[10] RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"

[11] RFC 3647 (Novembre 2003) "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework "

[12] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (2016) | ISO/IEC 9594-8

[13] Ente Certificatore InfoCamere – Manuale Operativo IC-MO-TSP

[14] Ente Certificatore InfoCamere – Certificati di autenticazione per la CNS, Certificate Policy (MO-CNS-CCIAA)

[15] Deliverable EN 319 411-1 v1.3.1 "*Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements" – Maggio 2021*

1.5 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal CAD [1], DPR 445/2000 [2], dal DPCM 22 febbraio 2013 [3] e dal DPR 2 marzo 2004, n. 117 [5] si rimanda alle definizioni stabilite dagli stessi decreti. Dove appropriato viene indicato tra parentesi quadre il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

Accreditamento facoltativo
Il riconoscimento del possesso, da parte del certificatore che lo richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Carta Nazionale dei Servizi
Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni.

Certificato Elettronico, Certificato Digitale, Certificato X.509 *[Digital Certificate]*

Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica.

Nel certificato compaiono altre informazioni tra cui:

- il Certificatore che lo ha emesso;
- il periodo di tempo in cui il certificato può essere utilizzato;
- altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.

Certificatore *[Certification Authority – CA]* – cfr. [1]

Certificatore Accreditato – cfr. [1]

Certificatore Qualificato – cfr. [1]

Chiave Privata e Chiave Pubblica – cfr. [1]

Dati per la creazione di una firma – cfr. [3]

Dispositivo sicuro di firma
Il dispositivo sicuro di firma utilizzato dal Titolare è costituito da un microprocessore generalmente installato su un supporto di plastica (smart card) o all'interno di un lettore con interfaccia USB (token). Rispetta i requisiti di sicurezza richiesti dalla normativa vigente.

Ente Emettitore
Ente responsabile della formazione e del rilascio della CNS.

È la Pubblica Amministrazione che rilascia la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS.

Evidenza Informatica
Sequenza di simboli binari (bit) che può essere oggetto di una procedura informatica.

Firma elettronica – cfr. [1]

Firma elettronica avanzata – cfr. [1] Firma

elettronica qualificata – cfr. [1] Firma

digitale *[digital signature]* – cfr. [1]

Lista dei Certificati Revocati o Sospesi *[Certificate Revocation List – CRL]*
È una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva, sospensione se temporanea.

Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla lista CRL, che viene quindi pubblicata nel registro dei certificati.

Marca temporale *[digital time stamping]*
Il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Manuale Operativo
Il Manuale Operativo definisce le procedure che il Certificatore e l'Ente Emettitore applicano nello svolgimento del servizio di rilascio e gestione della CNS e del relativo Certificato.

Master Registration Authority /MRA

La Società Consortile delle Camere di Commercio italiane incaricata a gestire l'attività relativa al riconoscimento ed alla registrazione dei richiedenti la CNS, alla produzione, personalizzazione e postalizzazione dei dispositivi ed al rilascio sicuro delle componenti per utilizzarli (PIN/PUK) con facoltà di sub-delegare parte delle suddette attività ad autonomi ODR/RAO, sottoposti al coordinamento e vigilanza della stessa.

Pubblico Ufficiale
Soggetto che, nell'ambito delle attività esercitate è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.

Registration Authority/RA
L'Ente Emettitore o altro Ente delegato dall'Ente Emettitore o dalla Master Registration Authority a seguito di apposita convenzione, che svolge le attività necessarie al rilascio, dei certificati digitali, nonché alla consegna/invio della CNS.

Registration Authority Officer /RAO
Soggetto incaricato a verificare l'identità e, se applicabile, ogni specifico attributo di un Titolare, nonché ad attivare la procedura di certificazione per conto del Certificatore.

Registro dei Certificati *[Directory]*
Il Registro dei Certificati è un archivio pubblico che contiene:

- i certificati validi emessi dal Certificatore per i quali i Titolari hanno richiesto la pubblicazione;
- la lista dei certificati revocati e sospesi (CRL).

Revoca o sospensione di un Certificato
È l'operazione con cui il Certificatore annulla la validità del certificato prima della naturale scadenza. Vedi Lista dei Certificati Revocati o Sospesi - CRL.

Richiedente *[Subscriber]*
È il soggetto fisico che richiede all'Ente Emettitore il rilascio della CNS.

Titolare *[Subject]*
È il soggetto in favore del quale è rilasciata la CNS ed identificato nel certificato digitale come il legittimo possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato stesso: al Titolare stesso è attribuita la firma elettronica avanzata generata con la chiave privata della coppia.

Utente *[Relying Party]*
Soggetto che riceve un certificato digitale e che fa affidamento sul certificato medesimo o sulla firma elettronica avanzata basata su quel certificato.

1.6 Acronimi e abbreviazioni

CNS – Carta Nazionale dei Servizi

CRL – Certificate Revocation List
Lista dei certificati revocati o sospesi.

DN – Distinguished Name
Identificativo del Titolare di un certificato di chiave pubblica; tale codice è unico nell'ambito degli utenti del Certificatore.

ERC – Codice utente di emergenza
Codice personalizzato per ciascuna CNS che permette dieffettuare le operazioni di sospensione, riattivazione e revoca dei certificati (in caso di smarrimento o di particolari esigenze) attraverso l'apposita sezione del sito id.infocamere.it

ETSI – European Telecommunications Standards Institute

IETF - Internet Engineering Task Force
IETF è una comunità aperta ed internazionale di progettisti di rete, operatori, venditori e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet.

ISO - International Organization for Standardization
Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione.

ITU - International Telecommunication Union
Organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni.

LDAP – Lightweight Directory Access Protocol
Protocollo utilizzato per accedere al registro dei certificati.

OID – Object Identifier
È costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.

ODR/RAO – Operatore di Registrazione

PIN – Personal Identification Number
Codice associato alla CNS, utilizzato dall'utente per l'accesso alle funzioni.

PUK
Codice personalizzato per ciascuna CNS, utilizzato dal Titolare per riattivare il proprio dispositivo di firma in seguito al blocco dello stesso per errata digitazione del PIN.

2 Generalità

Un certificato digitale è l'associazione tra una chiave pubblica di crittografia ed un insieme di informazioni che identificano il soggetto che possiede la corrispondente chiave privata, chiamato anche Titolare della coppia di chiavi asimmetriche (pubblica e privata). Il certificato è utilizzato da altri soggetti (gli Utenti) per ricavare la chiave pubblica, contenuta e distribuita con il certificato, e verificare, tramite questa, il possesso della corrispondente chiave privata, identificando in tal modo il Titolare della stessa.

Il certificato garantisce la corrispondenza tra la chiave pubblica ed il Titolare. Il grado di affidabilità di questa associazione è legato a diversi fattori, quali, ad esempio, la modalità con cui il Certificatore ha emesso il certificato, le misure di sicurezza adottate e le garanzie offerte dallo stesso, gli obblighi assunti dal Titolare per la protezione della propria chiave privata.

A tale proposito i certificati di Autenticazione CNS emessi dall'Ente Certificatore accreditato InfoCamere, sono emessi su richiesta diretta del Titolare, successivamente all'identificazione fisica o da remoto dello stesso da parte dell'Ente Emettitore, della MRA o di altro soggetto da questi delegato, e rilasciati su dispositivo sicuro di firma (Smart card o Token USB).

Il presente documento contiene le procedure operative che si attuano per l'emissione delle CNS e dei relativi Certificati di Autenticazione (in seguito anche chiamati più brevemente **Certificati**) sottoscritti dal Certificatore. Esso indica inoltre le procedure da seguire in caso di smarrimento, furto o timore di compromissione della CNS.

Informazioni riguardanti in modo più specifico l'Ente Certificatore sono presenti nel documento [14].

In quest'ultimo documento vengono inoltre specificati:

- gli ambiti di utilizzo del certificato CNS;
- il formato del certificato CNS
- gli obblighi e le responsabilità dell'Ente Certificatore, dell'Ente Emettitore, del titolare e dell'utente;
- la policy applicata dall'Ente Certificatore per quanto riguarda:
    - l'identificazione e l'autenticazione dei richiedenti il certificato CNS;
    - la revoca e la sospensione del certificato CNS;
    - il rinnovo del certificato CNS;
    - l'emissione della CRL o di altre modalità di notifica della validità dei certificati;
- la gestione della sicurezza e il livello di servizio dell'Ente Certificatore.

La Certificate Policy [14] è pubblicata a cura dell'Ente Certificatore InfoCamere ed è riferita mediante URL all'interno del certificato di autenticazione CNS stesso. Essa consente sia ai Richiedenti che agli Utenti di valutare le caratteristiche e l'affidabilità del servizio di certificazione.

2.1 Identificazione del documento

Questo documento è denominato "**Carta Nazionale dei Servizi - Manuale Operativo – CA InfoCamere**" ed è caratterizzato dal codice documento: IC-MO-CCIAA-CNS
La versione e la data di emissione sono identificabili in calce ad ogni pagina.

Questo documento è distribuito in formato elettronico presso il sito Web http://id.infocamere.it

2.2 Ente Emettitore

L'Ente Emettitore è, in generale, la Pubblica Amministrazione che rilascia la CNS, nel caso specifico la Camera di Commercio, ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS. I dati completi dell'organizzazione che svolge la funzione di Ente Emettitore sono i seguenti:

Denominazione Sociale	**CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA**
Sede legale	Queste informazioni sono reperibili nel sito web della Camera di Commercio che adotta il presente manuale.
Rappresentante legale	
Direzione Generale	
N° telefono	
N° fax	
N° partita IVA	
Sede Operativa	
Sito web per i servizi di certificazione digitale:	https://id.infocamere.it

2.3 Contatto per utenti finali e comunicazioni

La Camera di Commercio è responsabile di questo documento.

Domande, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo di seguito indicato:

InfoCamere S.C.p.A.

Responsabile del Servizio di Certificazione Digitale

Corso Stati Uniti, 14, 35127 Padova PD

Telefono: 049-8288111

Call Center: https://supporto.infocamere.it/

Web: https://id.infocamere.it

e-mail: qtsp@pec.infocamere.it

2.4 Pubblicazione

2.4.1 Pubblicazione delle informazioni

Il presente Manuale Operativo è reperibile:

- in formato elettronico presso il sito web https://id.infocamere.it;

2.5 Tutela dei dati personali

Le informazioni relative al Titolare di cui l'Ente Emettitore viene in possesso nell'esercizio delle sue attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico (es. chiave pubblica, certificato, date di revoca e di sospensione del certificato).

In particolare, i dati personali vengono trattati dall'Ente Emettitore in conformità con il Decreto Legislativo 30 giugno 2003, n.196 e ss.mm.ii. e da quanto disciplinato nel GDPR [4].

2.6 Tariffe

2.6.1 Rilascio e rinnovo del certificato

Sono previste tariffe riguardanti l'emissione e il rinnovo del Certificato di Autenticazione CNS. Tali tariffe sono funzione delle quantità trattate e delle specifiche normative che le regolamentano.

Le tariffe sono disponibili presso la MRA ed le RA.

2.6.2 Revoca e sospensione del certificato

La revoca e sospensione del Certificato sono gratuite.

2.6.3 Accesso al certificato e alle liste di revoca

L’accesso al registro dei certificati pubblicati e alla lista dei certificati revocati o sospesi è libero e gratuito.

3 Obblighi e Responsabilità

3.1 Obblighi dei Titolari

Il Titolare è tenuto a:

1) garantire la correttezza, la completezza e l'attualità delle informazioni fornite all'Ente Emettitore per la richiesta della CNS;
2) proteggere e conservare le proprie chiavi private con la massima accuratezza al fine di garantirne l'integrità e la riservatezza;
3) proteggere e conservare i codici segreti (PIN/PUK/ERC) della CNS, in maniera sicura e separatamente dal dispositivo stesso;
4) adottare ogni altra misura atta ad impedire la perdita, la compromissione o l'utilizzo improprio della chiave privata e della CNS;
5) utilizzare le chiavi e il certificato con le sole modalità previste nel presente Manuale Operativo;
6) inoltrare all'Ente Emettitore senza ritardo la richiesta di revoca o sospensione dei certificati al verificarsi di quanto previsto nel presente Manuale Operativo;
7) adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.2 Responsabilità

3.2.1 Limitazioni di responsabilità

L'Ente Emettitore e il Certificatore accreditato non saranno tenuti a rispondere di eventi a loro non direttamente imputabili ed in particolare di danni subiti dal Titolare, dal Richiedente, dagli Utenti o da terzi, inclusi i danni che direttamente o indirettamente saranno riconducibili:

- all'inosservanza di questo manuale operativo;
- allo svolgimento di attività illecite;
- a comportamenti del fruitore di servizi di certificazione privi delle richieste misure di diligenza atte ad evitare danni a terzi;

In nessun caso l'Ente Emettitore e il Certificatore accreditato saranno altresì responsabili di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.

4 Amministrazione del Manuale Operativo

4.1 Procedure per l'aggiornamento

L'Ente Emettitore si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute a causa di norme di legge o regolamenti.

Ogni revisione, modifica minore o variazione con impatto significativo eseguite comporta l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste. Ogni modifica tecnica o procedurale a questo manuale operativo verrà comunicata tempestivamente alla MRA ed alle RA.

Il Manuale è pubblicato in conformità a quanto indicato al § 2.4.1 in formato elettronico.

4.2 Responsabile dell'approvazione

Ciascuna Camera di Commercio, adottando il presente Manuale Operativo, ne sancisce l'approvazione.

5 Identificazione e Autenticazione

Questo capitolo descrive le procedure usate per:

- l'identificazione del Richiedente al momento della richiesta di rilascio della CNS e del relativo certificato di Autenticazione CNS;
- l'autenticazione del Titolare, nel caso di rinnovo, revoca e sospensione di certificati di Autenticazione CNS.

5.1 Identificazione ai fini del primo rilascio

L'Ente Emettitore, direttamente o tramite un soggetto delegato, verifica con certezza l'identità del Richiedente prima di procedere al rilascio della CNS e del relativo certificato di Autenticazione CNS richiesto.

La procedura di identificazione comporta che il Richiedente sia riconosciuto personalmente – anche da remoto - da uno dei soggetti di cui al § 5.1.1, che ne verifica l'identità attraverso il controllo del documento di identità (tra quelli indicati al § 5.1.2) e gli ulteriori controlli previsti per la procedura di riconoscimento da remoto.

Ove possibile potranno essere utilizzati, in conformità di quanto previsto nei Manuali Operativi del Certificatore, ulteriori strumenti di riconoscimento che non prevedono un interazione di persona o da remoto tra il Richiedente e un incaricato a eseguire il riconoscimento, e che utilizzino, ad esempio un mezzo di identificazione elettronica preesistente (CNS, CIE, SPID livello 2 o superiori) o un certificato digitale di sottoscrizione, se ancora in corso di validità, per firmare il modulo di richiesta di emissione della CNS.

5.1.1 Soggetti abilitati ad effettuare l'identificazione

L'identità del Richiedente può essere accertata da uno dei soggetti di seguito indicati:

1. L'Ente Emettitore, anche tramite suoi Incaricati;
2. La MRA anche tramite suoi incaricati o delegati esterni
3. La RA, anche tramite suoi Incaricati.

5.1.2 Procedure per l'identificazione

L'identificazione è effettuata da uno dei soggetti indicati al § 5.1.1 in presenza fisica del Richiedente o tramite procedura di riconoscimento da remoto.

Il soggetto che effettua l'identificazione ne verifica l'identità tramite il riscontro con uno dei seguenti documenti, valido e non scaduto, secondo quanto previsto dall'art. 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445:

- Carta d'identità
- Passaporto (emesso anche da autorità estera)
- Patente di guida

Al Richiedente viene fornito, in maniera riservata, un codice utente di emergenza che costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro tra Certificatore e lo stesso Titolare.

5.1.2.1 Richiesta di rilascio della CNS e del certificato

I passi principali a cui il Richiedente deve attenersi per ottenere una CNS con certificato di Autenticazione CNS sono:

a) prendere visione del presente Manuale Operativo e della Certificate Policy [14] e dell'eventuale ulteriore documentazione informativa;
b) seguire le procedure di identificazione adottate dall'Ente Emettitore come descritte nei paragrafi che seguono;
c) fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea

documentazione;

d) validare la richiesta di registrazione e prendere visione, accettandole, delle modalità di utilizzo della CNS.

5.1.2.2 Informazioni che il Richiedente deve fornire

Nella richiesta di registrazione sono contenute le informazioni che devono comparire nel certificato e quelle che consentono di gestire in maniera efficace il rapporto tra l'Ente Emettitore ed il Richiedente/Titolare. Il modulo di richiesta deve essere validato dal Richiedente/Titolare.

Sono considerate obbligatorie le seguenti informazioni:

- Cognome e Nome
- Data e luogo di nascita
- Cittadinanza
- Codice fiscale
- Indirizzo di residenza
- Indirizzo email
- Numero di cellulare
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso

Qualora il Richiedente desideri l'inserimento all'interno del certificato delle informazioni inerenti al ruolo, dovrà produrre la documentazione di supporto che gli verrà richiesta.

6 Operatività

Le operazioni necessarie per compiere le attività di emissione, revoca, sospensione, riattivazione e rinnovo dei Certificati sono descritte nei seguenti paragrafi.

6.1 Registrazione

L'emissione di certificati prevede una fase di registrazione dell'utente, previa identificazione: questa avviene presso l'Ente Emettitore o una sua RA o tramite procedura di riconoscimento da remoto gestita anche per mezzo di soggetti delegati.

Le attività relative alla registrazione dei dati dei Titolari seguono quanto descritto all'interno del Manuale Operativo IC-MO-TSP.

È facoltà di ciascuna Camera di Commercio adottare uno o più metodi di rilascio tra quelli indicati nel suddetto Manuale.

6.2 Rilascio del certificato

6.2.1 Generazione e protezione delle coppie di chiavi

Le attività relative alla generazione delle chiavi seguono quanto descritto all'interno del Manuale Operativo IC-MO-TSP.

Le coppie di chiavi per l'Autenticazione e per la Firma Digitale sono generate attraverso le funzionalità messe a disposizione dalla CNS.

Le chiavi sono generate all'interno del dispositivo.

Un'area protetta della smart card genera e custodisce le chiavi private impedendone l'esportazione. In caso di forzatura il sistema operativo del dispositivo protegge i dati al suo interno rendendo illeggibile la carta. L'utilizzo delle chiavi contenute nella CNS è subordinato all'autenticazione del Titolare via PIN segreto.

Il PIN è generato in modo casuale e conservato all'interno dei sistemi del Certificatore in modo protetto. Viene comunicato in modo sicuro (attraverso procedure di invio automatico di busta virtuale opportunamente cifrata) solamente al Titolare. La CNS così personalizzata con la coppia di chiavi generate è protetta da tale PIN personale.

In alcuni casi il titolare, utilizzando i codici di attivazione ricevuti in maniera riservata e gli appositi software messo a disposizione dalla CA, procede ad attivare il dispositivo scegliendo contestualmente il PIN di firma, la cui custodia e tutela è posta esclusivamente in capo al Soggetto stesso.

6.3 Emissione del certificato

I certificati vengono emessi in maniera automatica attraverso apposite applicazioni informatiche predisposte dal Certificatore le quali:

- verificano la correttezza delle richieste di certificato, assicurandosi che:
  - siano presenti tutte le informazioni necessarie al rilascio, in forma completa e corretta;
  - siano valide e della lunghezza prevista le chiavi pubbliche che si intendono certificare;
  - il titolare sia in possesso delle relative chiavi private e le richieste siano autentiche;
- generano e pubblicano i certificati nel registro;
- memorizzano i certificati nella CNS.

6.3.1 Formato e contenuto dei certificati di autenticazione e sottoscrizione

Vengono di seguito riportati i profili minimi dei certificati di Autenticazione CNS e di sottoscrizione, per l'Autorità di Certificazione, InfoCamere.

6.3.1.1 Certificato di autenticazione CNS CA InfoCamere

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 86 (0x56)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=IT, O=InfoCamere S.C.p.A., OU=Trust Service
Provider/serialNumber=02313821007, CN=InfoCamere Servizi di Certificazione CA CL
        Validity
            Not Before: Feb 13 09:51:07 2020 GMT
            Not After : Feb 13 00:00:00 2023 GMT
        Subject: O=Camera di Commercio, OU=CCIAA Milano, C=IT, SN=VERDI,
CN=VRDMRA80R41C351V/7420117620098433.WHRMQQsZdQBujR7BEwJs7P3+j08=/dnQualifier=AUT0
000000041374, GN=MARIO
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c8:4e:c0:55:39:9a:08:fb:bf:06:8f:57:48:81:
                    8e:3d:ae:ed:e2:de:29:7a:e4:4a:fa:43:c4:ac:cf:
                    c9:8b:df:8b:b7:b3:23:9a:b4:7c:4d:67:9b:af:2b:
                    ee:33:a4:31:0f:70:db:54:87:1d:6e:ee:7b:47:e6:
                    02:4a:ae:e9:bf:9d:5b:de:22:f0:7d:73:dd:cc:d3:
                    5a:1c:b0:fc:85:df:5a:ab:4b:17:69:e6:7f:1e:1f:
                    80:dd:97:14:80:9c:92:78:73:93:08:f5:41:2e:16:
                    06:6c:80:53:19:18:13:42:34:98:b1:46:58:66:4f:
                    3f:a2:ab:2f:72:07:57:c8:d7
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
            Authority Information Access:
                OCSP - URL:http://ocsp.sc.ca.infocamere.it

            X509v3 Certificate Policies:
                Policy: 1.3.76.16.2.1
                  User Notice:
                    Explicit Text: Identifies X.509 authentication certificates
issued for the italian National Service Card (CNS) project in according to the
italian regulation
                  CPS: http://www.cnipa.gov.it
                Policy: 1.3.76.14.1.1.80
                  CPS: https://id.infocamere.it/digital-id/firma-
digitale/manuali.html
                  User Notice:
                    Explicit Text: InfoCamere S.C.p.A. CNS Certificate

            X509v3 Issuer Alternative Name:
                email:contatti@infocamere.it
            X509v3 CRL Distribution Points:

                Full Name:
                  URL:http://crl.ca.infocamere.it/ca/sc/CRL01.crl

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
                email:mario.verdi@infocamere.it
            X509v3 Authority Key Identifier:
                keyid:79:46:4A:26:54:8B:C9:35:46:30:A8:29:66:D7:BF:CF:7D:4B:74:19
```

```
            X509v3 Subject Key Identifier:
                9E:03:25:3E:5D:68:43:6C:D7:7E:36:CD:B8:59:BE:3D:3A:44:F3:05
    Signature Algorithm: sha1WithRSAEncryption
         0d:7b:60:ae:a0:1f:35:30:6f:b4:c1:9c:85:81:c0:25:3e:fd:
         43:04:08:30:fc:aa:80:5e:c5:4a:ea:3f:13:6f:6e:d0:a4:96:
         da:9d:c4:b3:14:28:85:84:6a:68:ee:53:16:64:84:85:46:96:
         79:26:14:ff:aa:48:3e:fd:56:19:49:60:96:29:3a:60:72:ba:
         c6:50:86:22:7e:fc:29:45:ba:09:2d:02:94:ad:df:e7:1e:ae:
         fb:be:ca:fa:85:e8:a9:cc:d4:0e:de:59:5d:52:69:a9:35:7b:
         59:ad:69:d3:20:ed:2e:e9:94:d0:62:83:c9:e3:dd:99:82:81:
         a0:e3:2d:52:26:13:c7:b9:27:64:35:fd:22:f2:62:4f:7b:c2:
         a5:19:5f:8c:8f:e1:6a:ad:33:4c:11:4e:34:98:02:11:25:f9:
         5c:0b:74:a2:1f:26:f2:9a:36:f7:89:b4:0c:3d:cd:01:b4:cf:
         ac:de:38:81:f5:7e:3e:b5:83:6d:10:d6:dc:53:33:da:e2:59:
         17:33:20:c3:84:a2:27:c9:03:0b:80:fd:b5:6c:f1:f2:3b:2f:
         85:e1:6c:61:4c:24:c7:6a:73:05:86:34:3c:15:b3:ba:da:c9:
         89:4e:f0:f5:d3:88:23:11:3f:b9:50:e7:20:00:bc:c0:54:a1:
         43:66:d4:d7:6b:4e:05:c8:77:2e:28:24:da:54:d0:9d:fc:9a:
         81:8c:91:2d:3c:bc:00:54:40:35:94:fb:c7:4e:87:8c:03:b5:
         4e:85:ba:cf:0f:6e:7d:a1:00:5d:de:ec:e1:3d:e8:de:18:a2:
         65:e7:fe:4c:b6:0e:61:0d:d4:e8:70:a2:dc:77:b3:85:35:f6:
         fb:ed:bc:4a:4a:ae:76:6a:c5:ef:0f:88:c5:7d:e0:78:cf:49:
         83:77:73:de:8b:33:ef:fd:11:5c:5c:bb:e3:ad:f0:4f:d5:65:
         be:1a:03:d7:61:db:ae:e3:bd:06:d3:02:49:1d:60:e1:e1:96:
         73:2d:5e:72:61:1d:11:16:e5:64:9e:73:b7:9c:3a:1e:20:36:
         36:86:68:bc:6c:c2:33:ce:99:1b:0f:07:a5:d9:a0:ce:94:a1:
         00:54:fc:72:75:d0:44:13:a1:f4:ab:46:4f:d5:be:b8:0f:3b:
         93:4a:a8:ac:40:70:16:f4:a4:4c:13:6a:7f:2b:57:76:67:f9:
         18:a3:3a:22:13:2d:f2:a3:3b:15:43:09:46:39:27:47:7c:3a:
         fe:45:82:68:d8:79:e0:8f:9f:8d:dd:0a:0c:e9:22:c9:68:54:
         64:8b:a5:d6:39:f2:41:19:2f:06:da:35:d1:c4:90:1d:02:7f:
         6a:45:49:a7:3c:47:5a:1e
```

Nel caso in cui il richiedente desideri la pubblicazione delle informazioni inerenti al Ruolo all'interno del proprio certificato di firma digitale, verranno inserite all'interno dei suddetti profili le seguenti informazioni:

- **O** = Organizzazione che rilascia il certificato (ad esempio l'ordine professionale, l'azienda, ecc);
- **OU** = Unità Organizzativa, Dipartimento afferente all'Organizzazione.
- **Title** = Titolo o carica all'interno dell'organizzazione

Eventuali ulteriori informazioni qualificanti potranno essere inserite all'interno dell'attributo **Description** del campo **Subject** (ad esempio il numero di iscrizione all'ordine professionale, la matricola, ecc).

6.3.2 Validità dei certificati

I certificati hanno una validità di 3 anni decorrenti dalla data della loro emissione. In caso di revoca o sospensione, i certificati sono validi sino alla data di pubblicazione della revoca o sospensione, come meglio specificato nei paragrafi che seguono.

Il campo "*validity period"* (periodo di validità) e i relativi attributi *"not after"* (non dopo il) e *"not before"* (non prima del) contengono l'indicazione dell'intervallo temporale all'interno del quale un certificato è da considerarsi valido.

6.4 Interdizione di una CNS

Tramite revoca si attua l'interdizione definitiva della CNS mentre attraverso la sospensione si dà luogo ad una interdizione temporanea. In entrambi i casi, dal momento in cui viene eseguita l'operazione il certificato non viene più riconosciuto come valido.

I certificati revocati o sospesi sono inseriti nella CRL (una lista di revoca e sospensione) firmata dal Certificatore e pubblicata secondo la periodicità stabilita nel registro dei certificati.

È la pubblicazione della revoca e della sospensione nella CRL a dar loro efficacia, invalidando l'utilizzo delle corrispondenti chiavi private da quel momento in poi.La procedura di sospensione provoca l'interruzione temporanea della validità del certificato fino alla sua naturale scadenza o fino alla presentazione di una richiesta di riattivazione o revoca.

La revoca o sospensione dei certificati può avvenire:

- su richiesta del Titolare;
- su iniziativa dell'Ente Emettitore.
- su iniziativa del Certificatore

Per i certificati di ruolo la revoca o sospensione del certificato di sottoscrizione può avvenire anche su iniziativa del terzo interessato. Poiché i certificati presenti sulla smart card seguono lo stesso ciclo di vita, in caso di revoca del certificato di sottoscrizione da parte del terzo interessato, verrà automaticamente revocato anche il certificato CNS.

È il Certificatore a verificare il richiedente la revoca o sospensione. L'Ente Emettitore, direttamente o attraverso personale delegato, autentica il Titolare che richiede la revoca o la sospensione registrandone inoltre la motivazione.

6.4.1 Motivi per la revoca di un certificato

È da richiedersi la revoca nel caso in cui si verifichino le seguenti condizioni:

- una o più chiavi private risultano compromesse come nei casi di seguito riportati:
  - furto o smarrimento CNS;
  - cessata segretezza di una o entrambe le chiavi private e/o del codice di attivazione che ne consente l'accesso;
  - qualsivoglia evento compromettente l'affidabilità delle chiavi private;
- impossibilità da parte del Titolare di utilizzo della CNS (come in caso di guasto del dispositivo);
- cambiamento di dati Titolare presenti all'interno dei Certificati;
- verificata non conformità al presente Manuale Operativo;
- il terzo interessato che ha sottoscritto la richiesta di un certificato di ruolo ritiene che il Titolare non sia più in possesso dei titoli che ne hanno comportato il rilascio.

6.4.2 Procedura per la richiesta di revoca

La richiesta di revoca viene effettuata con modalità diverse a seconda che sia il Titolare, il terzo interessato, il Certificatore o l'Ente Emettitore a richiederla.

6.4.2.1 Revoca su iniziativa del Titolare o del terzo interessato

Il Titolare può richiedere la revoca:

1. utilizzando la funzione di revoca disponibile 7x24 nel sito web del Certificatore, indicando i dati richiesti e utilizzando l'ID scratch e il codice di emergenza fornito in sede di emissione del certificato;
2. recandosi direttamente presso l'Ente Emettitore competente.
3. inviando alla CA, all'indirizzo PEC del QTSP, il modulo presente nel sito id.infocamere.it, compilato e corredato della documentazione necessaria.

Nel caso di richiesta effettuata da parte del Terzo interessato sono applicabili esclusivamente le modalità di cui ai punti 2. e 3.

6.4.2.2 Revoca su iniziativa del Certificatore

Il Certificatore, fatta eccezione per i casi di motivata urgenza, comunica in anticipo al Titolare l'intenzione di revocare il certificato, specificandone il motivo e la data di decorrenza. Il certificato viene inserito nella CRL e da quel momento è da considerarsi revocato.

6.4.2.3 Revoca su iniziativa dell'Ente Emettitore

L'Ente Emettitore, eccetto casi di motivata urgenza, comunica in anticipo al Titolare l'intenzione di revocare il certificato, specificandone il motivo e la data di decorrenza. Il certificato viene inserito nella CRL e da quel momento è da considerarsi revocato.

6.4.3 Motivi per la Sospensione di un certificato

La sospensione deve essere effettuata nel caso si verifichino le seguenti condizioni:

1. è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
2. il Soggetto, il Richiedente o Terzo Interessato, la RA o la CA hanno acquisito elementi di dubbio sulla validità del certificato;
3. è necessaria un'interruzione temporanea della validità del certificato.

In caso di sospetto furto di identità, la CA o la RA, senza preavviso, potrà procedere a una sospensione cautelativa.

6.4.4 Procedura per la richiesta di sospensione

6.4.4.1 Sospensione su iniziativa del Titolare o terzo interessato

Il Titolare può richiedere la sospensione attraverso una delle seguenti modalità:

1. utilizzando la funzione di sospensione disponibile 7x24 nel sito web del Certificatore, indicando i dati richiesti e utilizzando l'ID scratch e il codice di emergenza fornito in sede di emissione del certificato;
2. prenotando un appuntamento telefonico con il Call Center della CA;
3. recandosi direttamente presso l'Ente Emettitore competente;
4. inviando alla CA, all'indirizzo PEC del QTSP, il modulo presente nel sito id.infocamere.it, compilato e corredato della documentazione necessaria.

Nel caso di richiesta effettuata da parte del Terzo interessato sono applicabili esclusivamente le modalità di cui ai punti 3. e 4.

6.4.4.2 Sospensione su iniziativa del Certificatore

Il Certificatore, fatta eccezione per i casi di motivata urgenza, comunica in anticipo al Titolare l'intenzione di sospendere il certificato, specificandone il motivo e la data di decorrenza. Il certificato viene inserito nella CRL e da quel momento è da considerarsi non valido, fino a revoca o riattivazione dello stesso.

6.4.4.3 Sospensione su iniziativa dell'Ente Emettitore

L'Ente Emettitore, eccetto casi di motivata urgenza, comunica in anticipo al Titolare l'intenzione di sospendere il certificato, specificandone il motivo e la data di decorrenza. Il certificato viene inserito nella CRL e da quel momento è da considerarsi non valido, fino a revoca o riattivazione dello stesso.

6.4.5 Procedura di richiesta di riattivazione

La riattivazione può essere richiesta solo dal Titolare.

La richiesta di riattivazione è possibile solamente nei casi in cui un certificato sia stato precedentemente sospeso. Il titolare del certificato sospeso ha tre diverse modalità di riattivazione a sua disposizione:

1. utilizzando la funzione di riattivazione disponibile 7x24 nel sito web del Certificatore, indicando i dati richiesti e utilizzando l'ID scratch e il codice di emergenza fornito in sede di emissione del certificato;

2. prenotando un appuntamento telefonico con il Call Center della CA;
3. recandosi direttamente presso l'Ente Emettitore competente.
4. inviando alla CA, all'indirizzo PEC del QTSP, il modulo presente nel sito id.infocamere.it, compilato e corredato della documentazione necessaria.

La riattivazione di un certificato sospeso comporta la cancellazione dalle liste di revoca (CRL).

6.4.6 Pubblicazione e frequenza di emissione della CRL

Pubblicazione, frequenza e tempistiche della CRL sono riportate nella certificate policy [14] dei Certificatori.

6.5 Attivazione della CNS

La procedura e le modalità di attivazione della CNS seguono quanto descritto all'interno del Manuale Operativo del Certificatore IC-MO-TSP e nelle guide pubblicate nel sito id.infocamere.it

6.6 Rinnovo del Certificato

Il certificato ha una validità di tre anni dalla data di emissione.

La procedura di richiesta di un nuovo certificato, che prevede la generazione di una nuova coppia di chiavi, deve essere avviata da parte del Titolare prima della scadenza del certificato.

Il Titolare che intende rinnovare il suo certificato digitale deve richiedere l'emissione di un nuovo certificato prima della scadenza di quello in suo possesso, restando inteso che la validità del certificato oggetto di rinnovo decorrerà dalla data del rinnovo stesso.

Oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà procedere ad una nuova registrazione.

Le chiavi private di firma di cui sia scaduto il certificato della relativa chiave pubblica, non possono essere più utilizzate.

Il campo "*validity period"* (periodo di validità) e i relativi attributi *"not after"* (non dopo il) e *"not before"* (non prima del) contengono l'indicazione dell'intervallo temporale all'interno del quale un certificato è da considerarsi valido.

Le procedure di rinnovo certificati sono pubblicate sul sito id.infocamere.it.

7 Disponibilità del servizio

Gli orari di erogazione del servizio sono:

Servizio	Orario
Accesso all'archivio pubblico dei certificati (1) (comprende i certificati e le CRL)	Dalle 00:00 alle 24:00 7 giorni su 7 Secondo quanto previsto dal Manuale Operativo IC-MO-TSP
Sospensione, riattivazione e revoca dei certificati (1)	Dalle 00:00 alle 24:00 7 giorni su 7, attraverso il sito web id.infocamere.it e secondo le altre modalità previste dal Manuale Operativo IC-MO-TSP
Altre attività: registrazione, generazione, pubblicazione (2)	Presso la Registration Authority secondo gli orari indicati nei rispettivi siti web.
Rinnovo (1)	Dalle 00:00 alle 24:00 7 giorni su 7, attraverso il sito web id.infocamere.it
Assistenza – Call Center	Dal lunedì al venerdì dalle 08:30 alle 18:30 Esclusi i giorni festivi

(1) Il servizio potrà non essere disponibile nella fascia oraria indicata per fermi di manutenzione o per cause di forza maggiore.
(2) L'attività di registrazione viene svolta presso gli Uffici di Registrazione dell'Ente Emettitore che possono avere diversi orari di sportello.