ENTE CERTIFICATORE
INFOCERT
CERTIFICATI DI AUTENTICAZIONE PER LA CARTA NAZIONALE DEI SERVIZI - CERTIFICATE POLICY

Codice documento: ICERT-INDI-CPCA-CNS
Versione: 8
Data: 26/07/2024

Sommario

1. Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	8
Data Versione/Release:	26/07/2024
Descrizione modifiche:	Indirizzi e riferimenti aziendali, correzione refusi, precisazioni sui servizi di verifica dello stato del certificato, revisione informazioni sugli algoritmi e le chiavi del certificatore.
Motivazioni:	Revisione periodica documento

Versione/Release n°:	7
Data Versione/Release:	18/07/2023
Descrizione modifiche:	Nuovo logo InfoCert
Motivazioni:	Rebranding

Versione/Release n°:	6
Data Versione/Release:	28/09/2021
Descrizione modifiche:	Riferimenti aziendali
Motivazioni:	Revisione e modifica riferimenti aziendali

Versione/Release n°:	5
Data Versione/Release:	07/11/2018
Descrizione modifiche:	Indirizzi e riferimenti aziendali, soppressa parte assicurativa, soppressa pubblicazione certificati (3.3.2 e 6.3), aggiornamento riferimenti normativi garante privacy e GDPR ed aggiornamento relativi paragrafi (7.4 e 7.4.1)
Motivazioni:	Revisione e modifica indirizzi e riferimenti aziendali

Versione/Release n°:	4
Data Versione/Release:	27/01/2014
Descrizione modifiche:	Indirizzi e riferimenti aziendali, polizze assicurative, certificazioni di qualità e sicurezza
Motivazioni:	

Versione/Release n°:	1.3
Data Versione/Release:	20/06/2011
Descrizione modifiche:	Indirizzi e riferimenti aziendali
Motivazioni:	

Versione/Release n°:	1.2
Data Versione/Release:	03/07/2009
Descrizione modifiche:	Eliminazione dell'obbligo per i titolari di non essere in possesso di una Carta d'Identità Elettronica
Motivazioni:	Modifiche normative

Versione/Release n°:	1.1
Data Versione/Release:	15/10/07
Descrizione modifiche:	Indirizzo della sede operativa
Motivazioni:	

Versione/Release n°:	1.0
Data Versione/Release:	01/08/2007
Descrizione modifiche:	Nessuna
Motivazioni:	Prima emissione

1.2 Scopo e campo di applicazione del documento

Il presente documento contiene le regole generali (policy) che governano l'emissione e l'uso dei **Certificati di Autenticazione per la Carta Nazionale dei Servizi (CNS)** sottoscritti dal Certificatore InfoCert. Nel seguito viene indicato per brevità con il termine ″Certificate Policy″. Le procedure operative adottate dall'Ente Emettitore e dal Certificatore stesso per l'erogazione dei servizi di certificazione digitale sono riportate nel Manuale Operativo CNS redatto e reso disponibile dall'Ente Emettitore stesso.

Le indicazioni di questo documento hanno validità per le attività relative ad InfoCert nel ruolo di Certificatore.

1.3 Riferimenti normativi

[1] DECRETO LEGISLATIVO 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) Codice dell'amministrazione digitale e successive modificazioni (nel seguito CAD)

[2] Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 (G. U. del 21/05/2013) (DPCM 22 febbraio 2013)

[3] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) – Codice Privacy e ss.mm.ii e 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 (vigente dal 25 maggio 2018).

[4] Decreto del Presidente della Repubblica 2 marzo 2004, n. 117 (G.U. n. 105 del 06/05/2004) e successive modificazioni

[5] Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi (G.U. n.296 del 18/12/2004)

[6] Linee guida per l'emissione e l'utilizzo della Carta Nazionale dei Servizi, Versione 3.0, del 15 maggio 2006 emanate dal Centro Nazionale per l'informatica nella Pubblica Amministrazione

[7] Determinazione AgID - Aggiornamento documento "Carta Nazionale dei Servizi CNS – File System" v. 11

1.4 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti in [1], [2] e [4] 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. CAD [1]

Certificatore Accreditato – cfr. CAD [1]

Certificatore Qualificato – cfr. CAD [1] Chiave Privata e Chiave Pubblica – cfr. CAD [1]

Dati per la creazione di una firma – cfr. CAD [1]

Dati per la verifica della firma – cfr. CAD [1]

Dispositivo sicuro di firma

Il dispositivo sicuro di firma utilizzato dal Titolare è costituito da una carta di plastica delle dimensioni di una carta di credito o un token USB in cui è inserito un microprocessore. È chiamato anche **carta a microprocessore** o **smart card** oppure **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. CAD [1]

Firma elettronica qualificata – cfr. CAD [1]

Firma digitale*[digital signature]* – cfr. CAD [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.

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 Officer/Operatore di Registrazione

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.

Uffici di Registrazione *[Registration Authority – RA]*/Centro di Registrazione Locale [CDRL]
L'Ente Emettitore o altro Ente delegato dall'Ente Emettitore, previa stipula di accordi di servizio con il Certificatore, svolge le attività necessarie al rilascio, da parte di quest'ultimo, del certificato digitale, nonché alla consegna della CNS.

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.

1.5 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.

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.

IUT – Identificativo Univoco del Titolare
È un codice associato al Titolare che lo identifica univocamente presso il Certificatore; il Titolare ha codici diversi per ogni ruolo per il quale può firmare.

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.

PIN – Personal Identification Number
Codice associato alla CNS, utilizzato dall'utente per accedervi alle funzioni. Altre funzioni installate sulla CNS richiedono PIN specifici della funzione.

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. Altre funzioni installate sulla CNS richiedono PUK specifici della funzione.

RAO – Registration Authority Officer/Operatore di Registrazione (OdR)

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 InfoCert sono emessi su richiesta diretta del Titolare, successivamente all'identificazione fisica dello stesso da parte dell'Ente Emettitore o di altro soggetto da questi delegato, e rilasciati su dispositivo sicuro di firma (smart card o token).

Il presente documento contiene le regole generali che governano l'emissione e l'uso dei Certificati di Autenticazione per la Carta Nazionale dei Servizi CNS (in seguito anche chiamati più brevemente **Certificati**) sottoscritti dal Certificatore InfoCert.

I **Certificati di Autenticazione CNS** sono rilasciati e gestiti da ciascun Ente Emettitore secondo le procedure indicate nel Manuale Operativo della CNS (in seguito anche chiamato più brevemente **Manuale Operativo**) predisposto e reso pubblicamente disponibile dall'Ente Emettitore stesso. I Certificati di Autenticazione CNS sono generalmente utilizzati nell'ambito del protocollo SSL/TLS con strumenti quali i Web browser.

L'Ente Certificatore InfoCert pubblica questa Certificate Policy e inserisce il riferimento a tale documento nel certificato. L'Ente Emettitore pubblica il Manuale Operativo. Insieme, questi documenti consentono ai Richiedenti e agli Utenti di valutare le caratteristiche e l'affidabilità del servizio di certificazione.

2.1 Identificazione del documento

Questo documento è denominato "**Certificati di Autenticazione per la Carta Nazionale dei Servizi – Certificate policy**" ed è caratterizzato dal codice documento: **ICERT-INDI-CPCA-CNS**.

La versione e la data di emissione sono identificabili in calce ad ogni pagina.

L'*object identifier* (OID) di questo documento è il seguente: `1.3.76.36.1.1.4`
Tale OID identifica:

InfoCert	1.3.76.36
Certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
Cp-certificati-di-autenticazione-CNS	1.3.76.36.1.1.4

Questo documento è distribuito in formato elettronico presso il sito Web del Certificatore all'indirizzo https://www.firma.infocert.it/documentazione/

2.2 Attori e Domini applicativi

2.2.1 Certificatore

InfoCert è il **Certificatore Accreditato** che emette, pubblica (se richiesto) nel registro e revoca i **Certificati di Autenticazione CNS**, operando in conformità a quanto descritto nella presente Certificate policy.
Il certificato dell'Autorità di Certificazione InfoCert emittente i certificati CNS, necessario per la verifica della firma apposta sui certificati CNS stessi, è presente in un elenco, firmato digitalmente, sul sito web di AgID. Questo elenco contiene tutti certificati self signed delle Autorità di certificazione italiane che emettono certificati CNS.
I dati completi dell'organizzazione che svolge la funzione di Certificatore sono i seguenti:

Denominazione sociale: InfoCert – Società per azioni - Società soggetta a direzione e coordinamento di Tinexta S.p.A.
Sede legale: Piazza Sallustio n.9, 00187, Roma (RM)
Sedi operative:

- Via Marco e Marcelliano n.45, 00147, Roma (RM)
- Via Fernanda Wittgens n. 2, 20123 Milano (MI)
- Piazza Luigi da Porto n. 3, 35131 Padova (PD)

Rappresentante legale: Danilo Cattaneo, in qualità di Amministratore Delegato
N. di telefono: 06 836691
Codice fiscale e n. Iscrizione Registro Imprese: 07945211006
Numero REA: RM - 1064345
N. partita IVA: 07945211006
Sito web: https://www.infocert.it

2.2.2 Ente Emettitore

L'Ente Emettitore 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.
La registrazione dei dati dei soggetti che richiedono il certificato per la CNS è svolta, direttamente oppure tramite strutture delegate, dall'Ente Emettitore che svolge il ruolo di Ufficio di Registrazione (Registration Authority).
Gli Uffici di Registrazione, eventualmente anche tramite loro incaricati, svolgono, tra l'altro, una funzione di interfaccia tra il Certificatore stesso e il Richiedente. Di seguito è indicata una serie di attività che vengono effettuate presso l'Ufficio di Registrazione:

- Identificazione e registrazione del Richiedente;
- validazione della richiesta del certificato;

- distribuzione ed inizializzazione della CNS;
- attivazione della procedura di certificazione della chiave pubblica del Richiedente/Titolare;
- supporto al Titolare e al Certificatore nel rinnovo, revoca e sospensione dei certificati.

Le procedure operative sono indicate in dettaglio nel Manuale Operativo della CNS a cura dell'Ente Emettitore.

2.2.3 Registro dei Certificati

Le liste di revoca e di sospensione dei certificati sono pubblicate dal Certificatore.

2.2.4 Applicabilità

La CNS è uno strumento di autenticazione in rete. Quindi l'ambito d'utilizzo principale del Certificato di Autenticazione CNS è costituito dai Web browser; esso può essere utilizzato anche dai prodotti di posta elettronica, oltre a specifiche applicazioni rilasciate o approvate dal Certificatore.

Con i Web browser, attraverso lo standard **SSL/TLS**, è possibile verificare l'identità di un soggetto in possesso del Certificato di Autenticazione CNS che si connetta ad un dominio a sua volta certificato.

Più generalmente, un soggetto, attraverso l'utilizzo della chiave privata, per la cui corrispondente chiave pubblica esista un Certificato di Autenticazione CNS, genera una firma elettronica avanzata che assicura l'origine delle informazioni da lui trasmesse in rete e la loro integrità (non alterazione da parte di terzi).

Affinché un Utente possa fare affidamento sull'utilizzo di una chiave privata, il Certificato corrispondente deve essere valido, cioè non scaduto, sospeso o revocato.

Nel caso in cui un certificato di un Titolare venga utilizzato allo scopo di inviare allo stesso un messaggio cifrato (riservatezza del contenuto), la perdita della chiave privata da parte del Titolare comporterà l'impossibilità di decifrare il messaggio: il Certificatore, infatti, **non effettua, in nessun caso, il backup della chiave privata del Titolare**.

2.3 Contatto per utenti finali e comunicazioni

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento. Domande, osservazioni e richieste di chiarimento in ordine al presente Certificate Policy dovranno essere rivolte all'indirizzo e alla persona di seguito indicate:

InfoCert S.p.A.
Responsabile del Servizio di Certificazione DigitalePiazza Luigi da Porto n.3 35131 Padova
Telefono: 06 836691
Call Center: consultare il link https://help.infocert.it/contatti/ per maggiori dettagli
Web: https://www.firma.infocert.it, https://www.infocert.it
e-mail: firma.digitale@legalmail.it

Le comunicazioni del Certificatore verso il Richiedente saranno effettuate via posta elettronica all'indirizzo dichiarato dal Richiedente medesimo al momento della Identificazione.

3. Regole Generali

In questo capitolo sono descritte le condizioni generali con cui il Certificatore eroga il servizio di certificazione descritto in questo manuale.

3.1 Obblighi e Responsabilità

3.1.1 Obblighi del Certificatore

Certificatore è tenuto a garantire:

1. l'associazione tra il Titolare e la chiave pubblica certificata, secondo quanto comunicatogli dall'Ente Emettitore;
2. di non rendersi depositario di chiavi private relative ai corrispondenti Certificati di Autenticazione CNS;
3. il rilascio e il rinnovo di un certificato richiesto secondo le presenti procedure e la sua accessibilità per via telematica;
4. la revoca o la sospensione del certificato dandone tempestiva pubblicità secondo le previsioni della presente Certificate Policy;
5. la protezione accurata delle proprie chiavi private mediante dispositivi hardware e software adeguati a garantire i necessari criteri di sicurezza;
6. la gestione delle operazioni e dell'infrastruttura relativa al servizio di certificazione digitale secondo le regole e procedure previste a carico del Certificatore dalle Regole Tecniche [5] e descritte nella presente Policy;
7. l'adeguamento del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, in conformità a quanto indicato nel Codice dell'Amministrazione Digitale, dal Regolamento UE n. 679/2016 nonché dal Decreto Legislativo 30 giugno 2003, n.196 e ss.mm.ii. [3].

3.1.2 Obblighi dell'Ente Emettitore

L'Ente Emettitore è tenuto a garantire:

1. la verifica d'identità del Richiedente e la registrazione dei dati dello stesso;
2. che lo stesso Richiedente sia espressamente informato riguardo alla necessità di protezione della segretezza della chiave privata e alla conservazione e all'uso dei dispositivi sicuri di firma;
3. la comunicazione al Certificatore di tutti i dati e documenti acquisiti in fase di identificazione allo scopo di attivare la procedura di emissione del certificato;
4. la verifica e l'inoltro al Certificatore delle richieste di revoca o di sospensione attivate dal Titolare presso l'Ufficio di Registrazione;
5. che le operazioni relative al servizio di certificazione digitale, affidate all'Ufficio di Registrazione dal Certificatore, siano effettuate secondo le regole e procedure descritte nel proprio Manuale Operativo e nel rispetto delle regole previste dalla presente policy, nelle modalità specifiche dettagliate negli accordi di servizio;
6. la rispondenza del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, in conformità a quanto previsto dal Regolamento UE n. 679/2016 nonché dal Decreto Legislativo 30 giugno 2003, n.196 e ss.mm.ii. [3].

L'Ente Emettitore, servendosi eventualmente di strutture delegate, terrà direttamente i rapporti con il Richiedente, Titolare del certificato, ed è tenuto ad informarlo circa le disposizioni contenute nella presente Certificate Policy.

3.1.3 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 il codice di attivazione (PIN) utilizzato per l'abilitazione delle funzionalità della CNS, in luogo sicuro e diverso da quello in cui è custodito il dispositivo stesso;

4. proteggere e conservare il codice di sblocco (PUK) utilizzato per la riattivazione della CNS in luogo protetto e diverso da quello in cui è custodito il dispositivo stesso;
5. adottare ogni altra misura atta ad impedire la perdita, la compromissione o l'utilizzo improprio della chiave privata e della CNS;
6. utilizzare le chiavi e il certificato per le sole modalità previste nel presente Certificate Policy;
7. inoltrare all'Ente Emittitore senza ritardo la richiesta di revoca o sospensione dei certificati al verificarsi di quanto previsto nel Manuale Operativo della CNS reso disponibile dall'Ente Emettitore;
8. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.1.4 Obblighi degli Utenti

L'Utente che utilizza un certificato del quale non è il Titolare ha i seguenti obblighi:

1. conoscere l'ambito di utilizzo del certificato e le limitazioni di responsabilità del Certificatore e dell'Ente Emettitore, riportati nel presente Certificate Policy e nel Manuale Operativo;
2. verificare la validità del certificato prima di usare la chiave pubblica in esso contenuta. La validità del certificato viene accertata verificando che questo non sia scaduto, o non sia stato revocato o sospeso;
3. utilizzare i dati contenuti nel registro dei certificati (es. liste di revoca) solo ai fini di verifica di validità del certificato;
4. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

L'Utente è l'unico responsabile per gli utilizzi del certificato posti in essere in maniera non conforme a quanto sopra indicato.

3.2 Responsabilità

3.2.1 Limitazioni di responsabilità

Il Certificatore in nessun caso risponderà di eventi ad esso non imputabili ed in particolare di danni subiti dall'Ufficio di Registrazione, dal Titolare, dal Richiedente, dagli Utenti o da qualsiasi terzo causati direttamente o indirettamente dal mancato rispetto da parte degli stessi delle regole indicate nella presente Certificate Policy ovvero dalla mancata assunzione da parte di detti soggetti delle misure di speciale diligenza idonee ad evitare la causazione di danni a terzi che si richiedono al fruitore di servizi di certificazione, ovvero dallo svolgimento di attività illecite.
Il Certificatore non sarà responsabile di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.

3.2.2 Clausola risolutiva espressa

Il Certificatore ha facoltà di risolvere il rapporto contrattuale, ai sensi dell'articolo 1456 del Codice civile, secondo quanto previsto nel contratto intercorso con la controparte.

3.3 Pubblicazione

3.3.1 Pubblicazione di informazioni relative al Certificatore

La presente Policy è reperibile:

- in formato elettronico presso il sito web del Certificatore (cfr. § 2.1)
- in formato cartaceo presso il Certificatore.

3.3.2 Pubblicazione liste di revoca e sospensione

Le liste di revoca e di sospensione sono accessibili con protocolli LDAP, http e OCSP. Gli indirizzi sono pubblicati direttamente all'interno dei certificati emessi come previsto dallo standard X.509 v3. Tale accesso può essere effettuato tramite i software messi a disposizione dal Certificatore e/o le funzionalità presenti nei prodotti disponibili sul mercato che utilizzano i suddetti protocolli.

Il Certificatore potrà rendere disponibili altre modalità, oltre a quella indicata per verificare la validità dei certificati.

3.4 Tutela dei dati personali

Le informazioni relative al Titolare di cui il Certificatore viene in possesso nell'esercizio delle sue tipiche attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico (es. date di revoca e di sospensione del certificato).
In particolare, i dati personali vengono trattati dal Certificatore in conformità con il Regolamento n. 679/2016 e con il Decreto Legislativo 30 giugno 2003, n.196 e ss.mm.ii. [3].

3.5 Tariffe

3.5.1 Rilascio e rinnovo del certificato

Sono previste tariffe riguardanti l'emissione e il rinnovo del Certificato di Autenticazione CNS. Tali tariffe sono disponibili presso l'Ente Emettitore o le strutture da esso delegate (RA).

3.5.2 Revoca e sospensione del certificato

La revoca e sospensione del Certificato è gratuita.

3.5.3 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.

4. Amministrazione della Certificate Policy

4.1 Procedure per l'aggiornamento

Il Certificatore 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.

Errori, aggiornamenti o suggerimenti di modifiche possono essere comunicati al contatto per gli utenti indicato al § 2.3.
Correzioni editoriali e tipografiche e altre modifiche minori comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative) comportano 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 questa policy verrà prontamente comunicata agli Uffici di Registrazione.

4.2 Regole per la pubblicazione e la notifica

La presente Policy è pubblicata in formato elettronico sul sito Web del Certificatore all'indirizzo https://www.firma.infocert.it/documentazione/.

5. Identificazione e Autenticazione

Il Certificatore predispone un adeguato canale sicuro attraverso il quale riceve la richiesta del certificato CNS da parte dell'Ente Emettitore. Il Certificatore autentica l'Ente Emettitore prima di procedere al rilascio del certificato di Autenticazione CNS richiesto.
L'identificazione del Richiedente il Certificato CNS viene effettuata dall'Ente Emettitore.
Le procedure operative necessarie all'identificazione e autenticazione del Richiedente sono riportate nel Manuale Operativo fornito dall'Ente Emettitore.

5.1 Autenticazione per rinnovo delle chiavi e certificati

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validità" (*validity*) con gli attributi "valido dal" (*not before*) e "valido fino al" *(not after).*

Le date indicate negli attributi suddetti sono espresse nel formato

```
anno-mese-giorno-ore-minuti-secondi-timezone
{AAAAMMGGHHMMSSZ}
```

nella rappresentazione UTCTime prevista dallo standard di riferimento [7].

Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato è da considerarsi non valido.

Il Titolare del certificato può, tuttavia, rinnovarlo, prima della sua scadenza. Il rinnovo richiede la generazione di una nuova coppia di chiavi.
Le procedure di rinnovo sono indicate nel Manuale Operativo dell'Ente Emettitore.

5.2 Autenticazione per richiesta di Revoca o di Sospensione

La revoca o sospensione del certificato può avvenire:

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

Le modalità operative per effettuare la richiesta di Revoca o Sospensione sono indicate nel Manuale Operativo fornito dall'Ente Emettitore.
Il Certificatore verifica la provenienza della richiesta di revoca o di sospensione.

6. Operatività

Questo capitolo descrive le operazioni necessarie per compiere le attività di emissione, revoca, sospensione e rinnovo di un Certificato di Autenticazione CNS dal punto di vista dell'Ente Certificatore. Le fasi operative di registrazione del titolare, di generazione chiavi e di emissione del certificato sono riportate nel Manuale Operativo fornito dall'Ente Emettitore.

6.1 Formato e contenuto del certificato

Il profilo del certificato generato è conforme a quanto pubblicato sul sito dell'AgID http://www.agid.gov.it/.
La conformità alle Regole Tecniche per l'emissione di una CNS è dichiarata nell'estensione Certificate Policy (2.5.29.32) con l'OID 1.3.76.16.2.1.

6.2 Validità del certificato

Il certificato ha validità di tre anni a partire dalla data di emissione ovvero fino alla data di pubblicazione della sua revoca o sospensione se effettuate prima della sua scadenza.

6.3 Uso del Certificato

L'ambito d'utilizzo del certificato di Autenticazione è costituito dai Web Browser oltre a specifiche applicazioni rilasciate dal Certificatore, come descritto al § 2.2.4.

6.4 Revoca e sospensione di un certificato

La revoca o la sospensione di un certificato ne tolgono la validità e rendono **non validi** gli utilizzi della corrispondente chiave privata effettuati successivamente al momento di revoca o sospensione. I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal Certificatore e pubblicata con periodicità prestabilita nel registro dei certificati.
La revoca e la sospensione di un certificato hanno efficacia dal momento di pubblicazione della lista e comportano l'invalidità dello stesso e degli utilizzi della corrispondente chiave privata effettuati successivamente a tale momento.

6.4.1 Motivi per la revoca di un certificato

Il Certificatore può eseguire la revoca del certificato su propria iniziativa, su iniziativa dell'Ente Emettitore o su richiesta del Titolare.

È fatto obbligo di richiedere la revoca nel caso in cui si verifichino le seguenti condizioni:

- la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
  - sia stato smarrito o rubato il dispositivo che contiene la chiave privata di firma;
  - sia venuta meno la segretezza della chiave privata o del codice di attivazione per accedervi;
  - si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave privata;
- il Titolare non riesce più ad utilizzare il dispositivo sicuro di firma contenente la chiave privata in suo possesso (es: guasto del dispositivo sicuro);
- si verifica un cambiamento dei dati del Titolare presenti nel certificato;
- viene verificata una sostanziale condizione di non conformità con il presente manuale oppure con il Manuale Operativo dell'Ente Emettitore.

6.4.2 Procedura per la richiesta di revoca

Le procedure per effettuare la richiesta di revoca del Certificato sono indicate nel Manuale Operativo dell'Ente Emettitore.

Il Titolare può altresì richiedere la revoca del proprio certificato al Certificatore seguendo le modalità operative indicate nel proprio sito www.firma.infocert.it.

Revoca su iniziativa del Certificatore
Il Certificatore comunica al Titolare anticipatamente, salvo casi di motivata urgenza, l'intenzione di revocare il certificato, fornendo il motivo della revoca e la data di decorrenza; la procedura di revoca del certificato viene poi completata con l'inserimento nella lista dei certificati revocati o sospesi (CRL).

6.4.3 Motivi per la Sospensione di un certificato

Il Certificatore esegue la sospensione del certificato su propria iniziativa, su richiesta dell'Ente Emettitore o su richiesta del Titolare.

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 Titolare, l'Ente Emettitore o il Certificatore acquisiscano elementi di dubbio sulla validità del certificato;
3. è necessaria un'interruzione della validità del certificato.

6.4.4 Procedura per la richiesta di sospensione

Le procedure per effettuare la richiesta di sospensione del Certificato sono indicate nel Manuale Operativo dell'Ente Emettitore.

Il Titolare può altresì richiedere la sospensione del proprio certificato al Certificatore seguendo le modalità operative indicate nel proprio sito www.firma.infocert.it.

La sospensione su iniziativa del Certificatore segue lo stesso iter previsto per la revoca.

6.4.5 Pubblicazione e frequenza di emissione della CRL

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL), firmata dal Certificatore, immessa e pubblicata nel registro dei certificati.

La CRL viene pubblicata in modo programmato ogni ora (emissione ordinaria). La CA può, in circostanze particolari, forzare un'emissione non programmata della CRL (emissione straordinaria immediata). L'acquisizione e consultazione della CRL è a cura degli Utenti. La CRL è emessa sempre integralmente. Il Certificatore si riserva la possibilità di pubblicare separatamente altre CRL, sottoinsiemi della CRL più generale, allo scopo di alleggerire il carico di rete. La CRL da consultare per lo specifico certificatoè indicata nel certificato stesso insieme alle informazioni sul protocollo da utilizzare. Ogni elemento della lista CRL contiene nell'apposita estensione la data e l'ora di richiesta della revoca o sospensione. Il formato della CRL è conforme allo standard X.509 V3.

6.4.6 Tempistica

Il tempo di attesa tra la richiesta di revoca o di sospensione e la sua realizzazione tramite pubblicazione della CRL è al massimo di 24 ore.

6.4.7 Servizi online di verifica dello stato di revoca del certificato

Oltre alla pubblicazione della CRL nei registri LDAP e HTTP, InfoCert mette a disposizione anche un servizio OCSP per la verifica dello stato del certificato. L'URL del servizio è indicato nel certificato. Il servizio è disponibile 24 ore 7 giorni la settimana.

La coerenza tra il servizio OCSP e la CRL è garantita entro massimo un'ora. La coerenza del servizio OCSP e dell'aggiornamento delle informazioni emesse dal servizio stesso in relazione agli aggiornamenti della CRL è vincolata dal tempo di attesa necessario all'aggiornamento della CRL stessa come definito nel paragrafo che precede.

Le informazioni sullo stato del certificato saranno rese disponibili fino alla scadenza del certificato di root CA.

6.5 Rinnovo del Certificato

Il certificato ha al massimo 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.

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.

Le modalità operative per effettuare il rinnovo del Certificato sono indicate nel Manuale Operativo dell'Ente Emettitore.

7. Gestione ed operatività della CA

7.1 Gestione della sicurezza

Il Certificatore ha realizzato un sistema di sicurezza del sistema informativo relativo al servizio di certificazione digitale.
Il sistema di sicurezza implementato è articolato su tre livelli:

- un livello fisico che mira a garantire la sicurezza degli ambienti in cui il Certificatore gestisce il servizio,
- un livello procedurale, con aspetti prettamente organizzativi,
- un livello logico, tramite la predisposizione di misure tecnologiche hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio e con l'infrastruttura utilizzata.

Tale sistema di sicurezza è realizzato per evitare rischi derivanti dal malfunzionamento dei sistemi, della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.

7.2 Gestione delle operazioni

Sono predisposte procedure di gestione e sistemi automatici per il controllo dello stato del sistema di certificazione e dell'intera infrastruttura tecnica del Certificatore.
Sono installati strumenti di controllo automatico che consentono al Certificatore di monitorare il sistema valutando gli eventi e gli stati in cui il sistema stesso viene a trovarsi.

7.2.1 Verifiche di sicurezza e qualità

Le procedure operative e di sicurezza del Certificatore sono soggette a controlli periodici legati per le certificazioni di qualità (ISO 9001), di gestione di un Service Management System (ISO 20000), di gestione della sicurezza delle informazioni (ISO 27001) sia a verifiche di auditing interno. Tali verifiche mirano a controllare la corretta applicazione delle procedure previste e la loro effettiva funzionalità in relazione agli obiettivi prefissati.
Oltre alle attività di auditing di processi sono pianificate le analisi e i controlli da effettuare sulle registrazioni prodotte dalle applicazioni e dai sistemi durante il normale funzionamento. Tale attività ha lo scopo di controllare che tutti gli eventi verificatisi rientrino nella normale operatività e che non si verifichino eventi pregiudicanti la sicurezza. La registrazione e la conseguente imputabilità degli eventi verificatisi costituiscono inoltre una valida misura di sicurezza.

Sul sito https://www.infocert.it sono presenti i riferimenti alle certificazioni ottenute dal Certificatore.

7.3 Procedure di Gestione dei Disastri

Il Certificatore ha adottato le procedure necessarie a garantire la continuità del servizio anche in situazioni di elevata criticità, utilizzando componenti ridondanti e sistemi di riserva.
In caso di disastro le operazioni verranno riprese usando le copie di backup dei dati e dei sistemi crittografici contenenti le chiavi di certificazione.

7.4 Dati archiviati

Responsabile del trattamento dei dati personali è l'Ente Emettitore. Il Certificatore tratta i dati personali di cui viene in possesso per l'erogazione del servizio, in modo conforme alla normativa vigente [3] predisponendo tutele rispondenti almeno alle misure minime in essa previste.
Negli archivi gestiti dal Certificatore sono conservati e mantenuti i seguenti dati:

- dati di registrazione dei titolari delle chiavi;
- certificati emessi, sospesi e revocati;
- associazione tra codice identificativo del Titolare e dispositivo di firma;
- dati di sessione al sistema e ai servizi e altri dati necessari a tracciare le operazioni rilevanti ai fini della sicurezza.

L'accesso ai dati contenuti nei diversi archivi è consentito solo a personale opportunamente abilitato, garantendo la riservatezza e l'integrità dei dati. Il Certificatore non tratta dati sensibili [3].

7.4.1 Procedure di salvataggio dei dati

I software e i dati sono soggetti a regolare backup come previsto dalle procedure interne.

7.5 Chiavi del Certificatore

Le chiavi di certificazione sono generate a bordo di un apposito hardware crittografico con caratteristiche di sicurezza conformi ad un accreditamento FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 in Europa. Le chiavi di root CA che firmano l'emissione di nuovi certificati possono essere:

- chiavi asimmetriche RSA con lunghezza non inferiore a 2048 bit;
- chiavi asimmetriche EC su una delle curve ellittiche previste dal documento ETSI TS 119 312 - Cryptographic Suites di lunghezza non inferiore a 256 bit.

7.6 Sistema di qualità

Tutti i processi operativi del Certificatore descritti in questo Manuale Operativo, come ogni altra attività del Certificatore, sono conformi allo standard ISO 9001.

7.7 Disponibilità del servizio

Gli orari di erogazione del servizio, salvo accordi contrattuali diversi, sono:

Servizio	Orario
Accesso all'archivio pubblico dei certificati (1) (comprende i certificati e le CRL e OCSP)	Dalle 00:00 alle 24:00 7 giorni su 7
Revoca e sospensione dei certificati (1)	Dalle 00:00 alle 24:00 7 giorni su 7
Altre attività: registrazione, generazione, pubblicazione, rinnovo (2)	Lun – Ven: dalle 09:00 alle 17:00 Sabato: dalle 09:00 alle 13:00 Festività escluse

(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. In ogni caso il Certificatore garantisce l'erogazione del proprio servizio negli orari sopra riportati.