InfoCert
GRUPPO TECNOINVESTIMENTI

Provincia di Padova

Manuale Operativo
Emissione Carta Nazionale dei Servizi

Questa pagina è lasciata
intenzionalmente bianca

Indice

1 Novità introdotte rispetto alla precedente emissione

***Versione**:*	*1.0*	***Data Versione/Release**:*	*15/04/2013*
Descrizione modifiche:	*Nessuna*		
Motivazioni:	*Prima emissione*		

***Versione**:*	*2.0*	***Data Versione/Release**:*	*15/05/2018*
Descrizione modifiche:	*riferimenti normativi, dati dei responsabili, operatività*		
Motivazioni:			

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 emessi dal Certificatore InfoCert, Trust Service Provider, su affidamento dalla Provincia di Padova.
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 Provincia in qualità di Ente Emettitore, per InfoCert nel ruolo di Certificatore, per gli Uffici di Registrazione, per gli Uffici di registrazione (RA), per i soggetti incaricati ad effettuare l'identificazione/registrazione dei Titolari e/o a consegnare 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:

- Manuale Operativo Certificate Policy - Certificate Practice Statement (ICERT-INDI-MO)
- InfoCert Ente Certificatore - Certificati di Autenticazione per la Carta Nazionale dei Servizi - Certificate Policy (ICERT-INDI-CPCA-CNS)

3 Riferimenti normativi

D.P.R. 445/2000 Testo Unico del Documento Amministrativo
Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale (nel seguito referenziato come CAD) e successive modifiche e integrazioni, comprese le sue Regole Tecniche e Linee Guida
Decreto del Presidente della Repubblica 2 marzo 2004, n.117 Regolamento concernente la diffusione della carta nazionale dei servizi
Regolamento UE eIDAS (electronic IDentification Authentication and Signature) - n° 910/2014
Regolamento UE GDPR (General Data Protection Regulation) - n° 679/2016

3.1 Definizioni e acronimi

AgID - Agenzia per l'Italia Digitale.
CA - Autorità di Certificazione [Certification Authority] - soggetto terzo e fidato che emette, pubblica nel registro e revoca i certificati.
CNS – Carta Nazionale dei Servizi.
CRL – Certificate Revocation List - Lista dei certificati revocati o sospesi.
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.
ERC – Acronimo assegnato al codice di emergenza.
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.
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, 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.
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] - L'Ente Emettitore o altro Ente delegato dall'Ente Emettitore che svolge le attività necessarie al rilascio, da parte di quest'ultimo, dei certificati digitali, nonché alla consegna della CNS.
Utente [Relying Party] – è il soggetto che riceve un certificato digitale e che fa affidamento sul certificato medesimo o sulla firma elettronica avanzata basata su quel certificato.

4 Partecipanti e responsabilità

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 USB).
Sospensione e revoca sono gratuiti.

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, le procedure da seguire in caso di smarrimento, furto o timore di compromissione della CNS, ed è liberamente disponibile sul sito della Provincia.

4.1 Ente Emettitore

L'Ente Emettitore è, in generale, la Pubblica Amministrazione che rilascia la CNS, nel caso specifico la Provincia di Padova, 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	**Provincia di Padova**
Sede legale	Piazza Antenore 3, 35121 Padova
Rappresentante legale	Presidente della Provincia
Numero verde	800800820
PEC	protocollo@pec.provincia.padova.it
N° Codice Fiscale	80006510285
N° partita IVA	00700440282
Sito web	http://www.provincia.pd.it
Sito web per i servizi di certificazione digitale:	http://cst.provincia.padova.it/
Supporto e assistenza	Servizio di supporto per gli utenti dei servizi C.S.T. - Centro Servizi Territoriali - Servizi Informativi (dal lunedì al venerdì delle giornate lavorative) 800.18.50.17 support@provincia.padova.it

4.2 Autorità di Certificazione [Certification Authority]

La Certification Authority (CA) è il soggetto terzo e fidato che emette, pubblica nel registro e revoca i certificati.
I dati completi dell'organizzazione che svolge la funzione di CA sono i seguenti:

Denominazione Sociale	**InfoCert – Società per azioni** **Società soggetta a direzione e coordinamento di Tecnoinvestimenti** **S.p.A.**
Sede legale	Piazza Sallustio n.9, 00187, Roma (RM)
Sede operativa	Piazza Luigi da Porto n.3 35131 Padova
Fax	049 0978914
Call center	199.500.130
Rappresentante legale	Amministratore Delegato
Numero di telefono	06 836691
N° Codice Fiscale	07945211006
N° partita IVA	07945211006
Sito web	https://www.infocert.it https://www.firma.infocert.it
Indirizzo mail	firma.digitale@infocert.it

4.3 Uffici di Registrazione [RA]

L'Ente Emettitore o altro Ente delegato dall'Ente Emettitore che svolge le attività necessarie al rilascio, da parte di quest'ultimo, dei certificati digitali, nonché alla consegna della CNS, sono dislocati nel territorio come RA.
I rapporti tra InfoCert, Provincia e RA sono definiti da appositi accordi di servizio e convenzioni.

4.4 Richiedente [Subscriber]

È il soggetto fisico che richiede all'Ente Emettitore il rilascio della CNS e può coincidere con il Titolare.

4.5 Titolari [Subject]

Il titolare 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.
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 Manuale Operativo;
7. inoltrare all'Ente Emettitore senza ritardo la richiesta di revoca o sospensione dei certificati al verificarsi di quanto previsto nel presente Manuale Operativo;
8. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

L'Ente Emettitore ed il Certificatore in nessun caso risponderanno di eventi ad essi non imputabili ed in particolare di danni subiti dal Titolare o da qualsiasi terzo causati direttamente o indirettamente dal mancato rispetto da parte degli stessi delle regole indicate nel presente Manuale Operativo 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.
L'Ente Emettitore ed il Certificatore non saranno altresì responsabili di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.

5 Operatività

5.1 Identificazione

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.
Le due possibili modalità di identificazione sono:

1. *de visu*
2. mediante certificato di firma qualificata (già in possesso o fornito dalla CA InfoCert prima della richiesta della CNS).

La modalità di identificazione *de visu* prevede un incontro di persona tra il Richiedente e uno dei soggetti abilitati a eseguire il riconoscimento, che provvede ad accertare la sua identità mediante l'esibizione in originale di uno o più documenti in corso di validità.
Il Richiedente deve essere in possesso anche del Codice Fiscale, la cui esibizione può essere richiesta dal soggetto abilitato ad eseguire il riconoscimento.
La procedura di identificazione comporta che il Richiedente sia riconosciuto personalmente attraverso il controllo di uno dei seguenti documenti, secondo il DPR 445/2000:

- Carta d'identità
- Passaporto
- Patente di guida
- Patente nautica
- Libretto di pensione
- Patentino di abilitazione alla conduzione di impianti termici
- Porto d'armi

Sono ammesse ulteriori tessere di riconoscimento oltre a quelle indicate, purché munite di fotografia e di timbro, rilasciate da un'Amministrazione dello Stato.

Ove possibile potranno essere utilizzati, in conformità di quanto previsto nei Manuali Operativi dei Certificatori, ulteriori strumenti di riconoscimento che non prevedano la presenza fisica del Titolare presso gli uffici di registrazione, e che utilizzino, ad esempio strumenti di riconoscimento forte e firma dei contratti mediante certificati di sottoscrizione in corso di validità (il Richiedente è, quindi, già in possesso di un certificato qualificato in corso di validità, che utilizza nei confronti della Provincia per richiedere la CNS).

L'identità del Richiedente può essere accertata dall'Emettitore, dall'Ufficio di Registrazione (RA) o da un loro incaricato.

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

Per ottenere un certificato di sottoscrizione il Soggetto e/o il Richiedente deve:

1. prendere visione del presente Manuale Operativo, della documentazione contrattuale e dell'eventuale ulteriore documentazione informativa;
2. seguire le procedure di identificazione adottate dalla Certification Authority, come descritte nel paragrafo;
3. fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;

4. sottoscrivere la richiesta di registrazione e certificazione, accettando le condizioni contrattuali che disciplinano l'erogazione del servizio, sulla modulistica analogica o elettronica predisposta dalla CA.

Al momento dell'identificazione viene fornito al Richiedente un codice segreto di emergenza (ERC), che costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro tra Certificatore e lo stesso Titolare.
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 sottoscritto dal Richiedente/Titolare.

Sono considerate obbligatorie le seguenti informazioni:

1. Cognome e Nome
2. Data e luogo di nascita
3. Codice fiscale
4. Indirizzo di residenza
5. Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente Emettitore e data di rilascio dello stesso
6. Indirizzo elettronico.

5.2 Registrazione

Per procedere all'emissione del certificato per la CNS è necessario eseguire una procedura di registrazione, successiva all'identificazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del Certificatore.
La registrazione iniziale è effettuata presso l'Ente Emettitore o da suo RA.
Durante questo passaggio iniziale i dati dell'utente vengono inseriti nel sistema in uso al Certificatore.

Conclusasi la fase di registrazione iniziale, per il rilascio dei certificati digitali e la consegna della CNS sono previste due diverse modalità.

La prima modalità (nel seguito **Caso A**) consente al Titolare/Richiedente di concludere la procedura di certificazione entrando in possesso della CNS e del certificato di autenticazione CNS immediatamente dopo la registrazione: in questo caso il RAO avvierà la procedura di generazione della coppia di chiavi e, effettuate le opportune verifiche, di emissione del certificato in presenza del Richiedente/Titolare.

La seconda modalità (nel seguito **Caso B**) prevede una separazione tra la fase di identificazione, effettuata in presenza del Richiedente, Titolare del certificato, e quella di registrazione ed emissione della CNS e del certificato, che viene effettuata successivamente dai RAO. In questo caso la CNS personalizzata è consegnata al Richiedente/Titolare in un secondo momento.

In entrambi i casi la CNS viene personalizzata a cura del Certificatore con il PIN consegnato al Richiedente al momento dell'identificazione.

5.3 Rilascio del certificato

Il RAO seleziona i dati di registrazione di un Richiedente/Titolare e attiva la procedura di richiesta di certificato, che sblocca automaticamente la CNS con il PIN di default, consentendo la generazione della coppia di chiavi di crittografia.

Il RAO, utilizzando il proprio dispositivo, firma la richiesta di certificazione della chiave pubblica corrispondente alla coppia di chiavi crittografiche generate all'interno della CNS e la invia alla Certification Authority (CA), la quale verificata la validità della richiesta e la titolarità del soggetto a inoltrarla, procede alla generazione del certificato e lo invia su canale sicuro all'interno del dispositivo.
Infine, la procedura automatica personalizza la CNS inserendo il PIN consegnato al Richiedente/Titolare in fase di identificazione.
La CNS così personalizzata con la coppia di chiavi generate, è protetta da tale PIN personale, generato in modo casuale, conservato in modo protetto all'interno dei sistemi del Certificatore, e comunicato secondo procedure sicure (crittografiche) al solo Titolare.

Le chiavi sono generate all'interno del microprocessore, veicolato dalla smartcard o dal token USB, e sono lunghe 1024 bit.
La chiave privata del Titolare è generata e memorizzata in un'area protetta del dispositivo che ne impedisce l'esportazione.
Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione rende illeggibile la carta, a protezione dei dati in essa contenuti.
Per utilizzare la chiave privata a bordo della CNS il possessore deve autenticarsi correttamente fornendo il proprio PIN segreto.

5.4 Emissione del certificato

L'emissione del certificato di Autenticazione CNS viene effettuata in modo automatico dalle procedure del Certificatore secondo i seguenti passi:

1) viene verificata la correttezza della richiesta di certificato controllando che:
   - il Richiedente/Titolare sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
   - la chiave pubblica che si intende certificare sia una chiave valida e della lunghezza prevista;
   - la richiesta sia autentica e il Titolare possieda la corrispondente chiave privata;
2) viene controllata la validità della firma dell'incaricato che ha convalidato la richiesta
3) si procede alla generazione del certificato e a pubblicarlo nel registro dei certificati;
4) il certificato viene memorizzato all'interno della CNS dispositivo sicuro di firma del Titolare;
5) si distinguono i due casi:
   (Caso A): il Titolare è già in possesso del dispositivo sicuro di firma, quindi il punto precedente conclude la procedura di rilascio del certificato di autenticazione.
   (Caso B): il dispositivo sicuro di firma, inizializzato e protetto dal PIN, viene consegnato da un incaricato dell'Ufficio di registrazione (RA) personalmente al Titolare.

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 precedentemente a tale data.

5.5 Interdizione di una CNS

L'interdizione della CNS si attua tramite la revoca (interdizione definitiva) o la sospensione (interdizione temporanea) del relativo certificato che 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.

La revoca o sospensione del certificato può avvenire:
- su richiesta del Titolare;
- su iniziativa dell'Ente Emettitore.
- su iniziativa del Certificatore.

Il Certificatore verifica la provenienza della richiesta di revoca o di sospensione.

L'Ente Emettitore, direttamente o tramite strutture all'uopo delegate, autentica il Titolare richiedente la revoca o sospensione e si accerta delle motivazioni della stessa.

Se la richiesta viene effettuata per telefono, il Titolare (per la sola sospensione) si autentica fornendo il codice di emergenza segreto (ERC), consegnato assieme al certificato che si intende sospendere.

Se la richiesta viene fatta presso l'Ufficio di registrazione (RA), l'autenticazione del Titolare avviene con le modalità previste per l'identificazione.

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 stata smarrita o rubata la CNS;
- 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 la CNS 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 del presente Manuale Operativo.

5.6 Procedura per la richiesta di revoca

La richiesta di revoca viene effettuata con modalità diverse a seconda del richiedente. Sono previsti i seguenti casi:

1. **Revoca su iniziativa del Titolare**

L'utente Titolare richiede la revoca tramite l'Ufficio presso cui è stato registrato, il quale, ottenuti i dati necessari (la motivazione della revoca, il codice di emergenza del certificato) ed effettuate tutte le verifiche del caso, procede ad inoltrare la revoca al Certificatore.
Nell'impossibilità di identificare con certezza il Titolare si potrà procedere con una sospensione del Certificato in attesa della corretta identificazione del richiedente (ad esempio mediante richiesta di revoca formulata per iscritto).

2. Revoca su iniziativa del Certificatore

Il Certificatore esegue la sospensione del certificato su propria iniziativa o su richiesta del Titolare.
Il Certificatore attiva una richiesta di revoca con la seguente modalità:
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).

3. Revoca su iniziativa dell'Ente Emettitore

L'Ente Emettitore attiva una richiesta di revoca con la seguente modalità:
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).

5.7 Procedura per la richiesta di sospensione

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

Il Titolare richiede la sospensione tramite l'Ufficio presso cui è stato registrato, il quale, ottenuti i dati necessari (la motivazione della sospensione, il codice di emergenza del certificato) ed effettuate tutte le verifiche del caso, procede ad inoltrare la sospensione al Certificatore.

Se la richiesta di sospensione avviene per telefono, la validità del certificato viene sospesa per un massimo di 10 giorni.

Se la richiesta di sospensione avviene tramite presentazione di una domanda scritta all'Ufficio, il Titolare può indicare una diversa durata del periodo di sospensione.

Alla scadenza dei periodi indicati, se non viene revocato secondo le modalità precedentemente elencate, il certificato si riattiverà automaticamente.

5.8 Rinnovo del Certificato

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validity period" (periodo di validità) con gli attributi " not after" (non dopo il) e "not before" (non prima del).

Al di fuori di questo intervallo di date il certificato è da considerarsi non valido.
Il certificato ha validità di tre anni dalla data di emissione.
La procedura di rinnovo richiede la generazione di una nuova coppia di chiavi: la richiesta di un nuovo certificato deve essere avviata prima della scadenza dello stesso.
La nuova coppia di chiavi è generata all'interno della CNS, l'emissione e la pubblicazione del certificato seguono il procedimento descritto in caso di nuova richiesta.

Le modalità operative per effettuare la procedura di rinnovo del certificato sono indicate dal Certificatore nel proprio sito (http://www.firma.infocert.it).

5.9 Conservazione della contrattualistica

La documentazione tecnica e contrattuale a supporto del riconoscimento e del rilascio della CNS è conservata dalla CA InfoCert in modalità analogica e/o digitale per almeno vent'anni dalla data di emissione, secondo quanto previsto dal Codice dell'Amministrazione Digitale.
In qualsiasi momento l'Ente Emettitore Provincia di Padova può richiederne copia o duplicato scrivendo a infocert@legalmail.it