MANUALE OPERATIVO

CARTA NAZIONALE DEI SERVIZI

Ente Emettitore:
Università degli Studi di Napoli Parthenope

Certificatore:
Uanataca S.A. Unipersonale

INFORMAZIONI GENERALI

Controllo documentale

Livello di sicurezza:	Pubblico
Ente di Emissione:	Università degli Studi di Napoli PARTHENOPE
Versione:	1.1
Data di edizione:	09/09/2025
Codice Documento:	Manuale_Operativo_MOEE_v.1.1

Controllo formale

Redatto da:	Revisionato da:	Approvato da:
UANATACA S.A. UNIPERSONALE (Legal & Compliance)	Università degli Studi di Napoli PARTHENOPE	Università degli Studi di Napoli PARTHENOPE

Controllo delle versioni

Versione	Parti modificate	Descrizione delle modifiche	Data
1.0	Originale	Prima versione del documento	07/07/2021
1.1	Intero documento	Revisione documento; aggiornamento riferimenti certificatore; aggiornamento modalità di identificazione; inserimento "Misure di sicurezza tecnica" e "Disponibilità del servizio"	09/09/2025

INDICE

1. INTRODUZIONE

1.1. AMBITO DI APPLICAZIONE

Il presente manuale operativo (di seguito anche solo "Manuale") descrive le procedure operative disciplinanti l'emissione della Carta Nazionale dei Servizi (di seguito anche solo "CNS") da parte dell'Ente Emettitore Università degli Studi di Napoli "Parthenope" sottoscritta dal Prestatore di servizi fiduciari Uanataca S.A. unipersonale.

L'attività oggetto del presente Manuale rientra in un più ampio progetto di digitalizzazione portato avanti dall'Università degli Studi di Napoli Parthenope la quale, anche con l'obiettivo di perseguire la valorizzazione della ricerca scientifica favorendo l'applicazione delle conoscenze e dei risultati a contesti di utilizzo in ambito amministrativo, produttivo e dei servizi, come ad esempio con iniziative per il trasferimento tecnologico e la digitalizzazione, ha inteso accelerare la transizione al digitale per far diventare cittadini e imprese protagonisti dell'innovazione.

Le regole e le procedure contenute all'interno di questo Manuale si applicano, dunque, in relazione a tutte le attività finalizzate al rilascio della Carta Nazionale dei Servizi nei confronti dell'Ente Emettitore, del Prestatore di servizi fiduciari, degli eventuali Uffici di Registrazione e disciplinano, altresì, il rapporto con gli Utenti del Servizio.

1.2. NOME E IDENTIFICATIVO DEL DOCUMENTO

Il presente Manuale: "Manuale_Operativo_MOEE" è aggiornato alla versione risultante dal Controllo delle Versioni. Nella predetta sezione sarà riportato il *changelog* di eventuali aggiornamenti e la relativa versione, anche visibile in copertina e nell'intestazione del presente documento.

1.3. OID (*Object Identifier*)

Di seguito sono elencati gli OID ("Object Identifier") delle policy supportate da questo Manuale Operativo. Le Policy OID contraddistinguono ciascun profilo di certificato emesso da Uanataca e sono specificate all'interno di ciascun certificato

OID	Tipo di certificato
	Carta Nazionale dei Servizi
1.3.6.1.4.1.47286.10.3.1	Certificato di autenticazione CNS

1.4. RIFERIMENTI NORMATIVI

Di seguito si riportano i riferimenti della normativa applicabile al presente Manuale e, in generale, all'attività di emissione della Carta Nazionale dei Servizi:

- **Decreto Legislativo 7 marzo 2005, n. 82**: Codice dell'amministrazione digitale come modificato dal Decreto Legislativo 4 aprile 2006, n. 159 e dal Decreto Legislativo 30 dicembre 2010, n.235 e s.m.i. (di seguito anche solo "CAD");
- **Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445:** recante "Disposizioni legislative in materia di documentazione amministrativa" e s.m.i. (di seguito anche solo "TU");
- **Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009**: recante Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici;
- **Decreto Legislativo 30 giugno 2003, n. 196**: recante "Codice in materia di protezione dei dati personali" e s.m.i.;
- **Decreto del Presidente della Repubblica 2 marzo 2004, n. 117**: "Regolamento recante disposizioni la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n.3";
- **Decreto interministeriale 9 dicembre 2004**: recante regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi (di seguito anche solo "Regole Tecniche");
- **Decreto del Presidente del Consiglio dei Ministri** del 30 marzo 2009: "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici".
- **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 (di seguito anche solo "Linee Guida CNIPA");
- **Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014** in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (di seguito anche solo "Regolamento eIDAS");
- **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 (di seguito anche solo "GDPR");

1.5. RIFERIMENTI PROCEDURALI

In aggiunta alla normativa sopra richiamata il presente Manuale è redatto in conformità alle politiche di certificazione del Prestatore di servizi fiduciari Uanataca S.A. unipersonale (di seguito anche solo "Uanataca") disponibili nella seguente repository: https://web.uanataca.com/it/politiche-di-certificazione.

1.6. RIFERIMENTI TECNICI

Di seguito si indicano i riferimenti di carattere tecnico applicabili al presente Manuale:

- EN 319 401: "General Policy Requirements for Trust Service Providers";
- RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile;
- RFC 3161: "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)";
- RFC 2527: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework";
- Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8;
- EN 319 411-1: "Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements";

1.7. DEFINIZIONI

All'interno del documento si fa riferimento alle definizioni riportate nella tabella che segue. Per ogni termine non contenuto all'interno della tabella si rimanda alle definizioni di cui alle Regole Tecniche nonché all'art. 4 del GDPR.

AgID	**Agenzia per l'Italia Digitale**
CAD	**Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005 n. 82 e ss.mm.ii.)**
Carta Nazionale dei Servizi - CNS	Documento informatico, rilasciato da una Pubblica Amministrazione, con la finalità di identificare in rete il titolare della carta. Utilizza una carta a microprocessore (smart-card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete.
Certificato di Autenticazione - CdA	L'attestato elettronico che garantisce l'autenticità del circuito che ha emesso la CNS. Certificato X509 v3 della carta, rilasciato da un certificatore accreditato ai sensi dell'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002.
Certificato di Firma	L'attestato elettronico che collega i dati utilizzati per verificare la firma elettronica al titolare e conferma l'identità del titolare stesso. Si tratta di un certificato X509 v3, emesso da un certificatore accreditato ai sensi dell'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002, che può essere utilizzato per la verifica delle firme digitali emesse in aderenza alla vigente normativa.
Certificatore	È la società Uanataca S.A. unipersonale, prestatore di servizi fiduciari qualificati qualificata ex art. 29 del CAD ed opera, per le finalità di cui al presente Manuale, in qualità di "Ente che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche".
Ente Emettitore	Si intende l'Università degli Studi di Napoli Parthenope in qualità di 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.

Uffici di Registrazione	L'Ente Emettitore o altro soggetto giuridico, da questi delegato, che svolge le attività propedeutiche e necessarie al rilascio dei certificati digitali e consegna della Carta Nazionale dei Servizi.
Operatore di Registrazione	Il soggetto, appartenente all'Ufficio di Registrazione o delegato dall'Ente Emettitore a compiere le operazioni di identificazione dei Richiedenti e ad attivare la procedura di certificazione per conto del Certificatore.
GDPR	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016
Codice Privacy	Decreto Legislativo 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali" così come integrato dal Decreto Legislativo 10 agosto 2018, n. 101, recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati)".*
Richiedente	Persona fisica che richiede il rilascio della Carta Nazionale dei Servizi
Manuale Operativo	Il Manuale Operativo dell'Università degli Studi di Napoli Parthenope per l'emissione della Carta Nazionale dei Servizi.
Titolare	Persona fisica titolare della Carta Nazionale dei Servizi e del relativo certificato.
Utente/Interessato	Si riferisce indistintamente al Richiedente e/o al Titolare
Relying Parties	Gli Utenti o i soggetti che fanno affidamento sul certificato.
Identificazione Informatica	L'identificazione di cui all'art. 1 co. 1 lett. u-ter) del Decreto legislativo 7 marzo 2005 n. 82 (CAD)

1.8. ACRONOMI

Di seguito l'elenco degli acronimi utilizzati nel presente Manuale

AgID: Agenzia per l'Italia Digitale

CA: Certification Authority

CAB: Conformity Assessment Body

CAD: Codice dell'Amministrazione Digitale (D.lgs. n.82/2005)

CNS: Carta nazionale dei servizi

CP: Certificate Policy

CRL: Certificate Revocation List

CSP: Certification Practice Statement

DN: Distinguished Name

ETSI: European Telecommunications Standards Institute

FQDN: Fully Qualified Domain Name

GDPR: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;

HSM: Hardware Security Module

HTTP: Hyper-Text Transfer Protocol

I&A: Identificazione e Autorizzazione

ISO: International Organization for Standardization

IR: Incaricato di Registrazione

OCSP: On-line Certificate Status Protocol

OID: Object IDentifier

PKI: Public Key Infrastructure

QSCD: "Qualified Signature-Creation Device"

RA: Registration Authority

TLS: Transport Layer Security

TSL: Trust-service Status List

TSP: Trust Service Provider

QTSP: Qualified Trust Service Provider

1.9. PARTECIPANTI AL SERVIZIO DI CERTIFICAZIONE

1.9.1. ENTE EMETTITORE

L'Ente Emettitore della Carta Nazionale dei Servizi è l'Università degli Studi di Napoli Parthenope.

Di seguito i dati identificativi dell'Ente Emettitore

Nominativo dell'ente: Università degli Studi di Napoli "Parthenope"

Sede Legale: Via Amm. F. Acton, 38 (80133) Napoli – Italia

Partita IVA: 01877320638

Codice fiscale: 80018240632

Con riferimento al ruolo nonché ai diritti e agli obblighi dell'Ente Emettitore si rinvia al paragrafo 2.1.1.

1.9.2. CERTIFICATORE

Il ruolo di Certificatore, per le attività di emissione della Carta Nazionale dei Servizi, in conformità al presente Manuale è la società Uanataca S.A. unipersonale che opera in qualità di Prestatori di servizi fiduciari qualificati in conformità con il Regolamento eIDAS.

Il Certificatore Uanataca S.A. unipersonale, qualificato ai sensi dell'art. 29 del CAD dall'Organismo di Vigilanza (AgID), è iscritta nell'elenco pubblico dei prestatori di servizi fiduciari attivi in Italia consultabile al seguente link.

I dati identificativi del Certificatore sono i seguenti:

Ragione Sociale: Uanataca S.A. unipersonale

Sede legale: Avenida Meridiana no. 350, 3a planta - 08027 Barcellona(Spagna)

Sede Secondaria: Via Diocleziano, 107 - 80125 Napoli (Italia)

P.IVA: 04741241212

Sedi Operative:

- Via Diocleziano, 107 - 80125 Napoli (Italia)
- Avenida Meridiana no. 350, 3a planta - 08027 Barcellona (Spagna)

Sito internet: https://web.uanataca.com/it/

Per la fornitura di servizi fiduciari qualificati in conformità al presente Manuale, Uanataca si avvale della seguente chiave di certificazione, la quale soddisfa i requisiti di cui al Regolamento eIDAS conformandosi *in toto* alle Raccomandazioni di cui alla Determina n. 147/2019 emessa da AgID.

1.9.2.1. UANATACA CNS CA 2020

Si tratta della CA che rilascia il seguente profilo di certificato:

- Certificato di autenticazione CNS;

Il certificato di CA è autofirmato (*self-signed*).

a. **Dati identificativi**:

CN:	**UANATACA CNS CA 2020**
Fingerprint (SHA1):	eae79fa0da7b40c0e180a24ea297b5092755739a
Valido dal:	07/04/2020
Scadenza:	02/04/2040
Lunghezza Chiave RSA	4096

1.9.3. UFFICI DI REGISTRAZIONE (REGISTRATION AUTHORITIES – R.A.)

Lo svolgimento delle attività di identificazione ed autenticazione dei Richiedenti (ovvero i soggetti che richiedono la Carta Nazionale dei Servizi) può essere svolta dai seguenti soggetti:

a. lo stesso Ente Emettitore per il tramite dei suoi dipendenti;
b. dal Certificatore, in considerazione della delega allo svolgimento di tali attività effettuata da parte dell'Ente Emettitore;
c. da Uffici di Registrazione (R.A. - "*Registration Authorities*") delegati dall'Ente Emettitore o direttamente dal Certificatore, attraverso la stipula di appositi mandati.

Gli Uffici di Registrazione nominati dall'Ente Emettitore o dal Certificatore sono adeguatamente formati e sottoposti a tutti i necessari controlli finalizzati alla verifica circa il regolare adempimento degli impegni e degli obblighi derivanti dal mandato.

In particolare, gli Uffici di Registrazione e tutti i soggetti precedentemente indicati svolgono le seguenti attività:

- identificazione e autenticazione dei Richiedenti;
- verifica dei requisiti necessari e dei dati identificativi di colui che figurerà come Titolare del certificato di CNS;
- registrazione dei dati dei Richiedenti;
- autorizzazione all'emissione di certificati digitali attraverso appositi strumenti messi a disposizione dal Certificatore;
- custodia della documentazione relativa: a) all'identificazione del Richiedente; b) alla registrazione del Richiedente; c) alla gestione del ciclo di vita dei certificati.

L'Ente Emettitore, anche tramite l'Ente Certificatore, si impegna a formalizzare contrattualmente ogni tipo di rapporto intercorrente con i soggetti che agiranno per suo conto e svolgeranno le attività di cui sopra in qualità di Uffici di Registrazione.

Se il soggetto deputato a svolgere attività di Ufficio di Registrazione è una persona giuridica, questa potrà, a sua volta, autorizzare una o più persone ad agire come Operatore di Registrazione (o RAO – Registration Authority Officer).

Gli Uffici di Registrazione sono abilitati ad operare solo a seguito di un'opportuna formazione del personale impiegato.

Gli Uffici di Registrazione, inoltre, sono soggetti a verifiche periodiche da parte del Certificatore con lo scopo di verificare il rispetto degli impegni assunti e delle procedure definite nel presente Manuale.

1.9.4. UTENTI FINALI

Gli utenti finali (di seguito anche solo "Utenti") si identificano nelle persone fisiche destinatarie del servizio di emissione, gestione ed utilizzo della Carta Nazionale dei Servizi in conformità al presente Manuale.

In particolare, rientrano tra gli utenti finali le seguenti categorie:

1) **Richiedenti**: persone fisiche che domandano all'Ente Emettitore il rilascio della Carta Nazionale dei Servizi;
2) **Titolari**: persone fisiche titolari del certificato di CNS emesso;
3) **Relying parties**: soggetti che ricevono un documento informatico sottoscritto con il certificato digitale del Titolare o che ricevono richiesta di autenticazione da parte del Titolare per l'accesso ad un servizio e che fanno affidamento sulla validità del certificato per valutare la correttezza e la validità del documento stesso, nei contesti dove esso è utilizzato o dell'identità della persona che richiede l'accesso al servizio.

1.9.5. RICHIEDENTI

Il Richiedente è la persona fisica che domanda all'Ente Emettitore il rilascio della Carta Nazionale dei Servizi. Al momento della richiesta formale di emissione del certificato, il Richiedente dichiara di accettare le Condizioni Generali di contratto stabilite dal Certificatore e, pertanto, acconsente all'esercizio dei diritti e al rispetto degli obblighi dettati da quest'ultimo.

Le condizioni contrattuali contenute nel presente Manuale nonché nelle Condizioni Generali del Certificatore si aggiungono ed integrano i diritti e gli obblighi dei Richiedenti e/o Titolari sanciti nella normativa tecnica, di matrice europea, relativa all'emissione dei certificati qualificati, con particolare riferimento allo standard ETSI EN 319 411.

A seguito dell'emissione del certificato, il Richiedente si identifica nel Titolare.

1.9.6. TITOLARI

Il Titolare è il soggetto che possiede ed utilizza la chiave privata relativa alla Carta Nazionale dei Servizi corrispondente alla chiave pubblica contenuta nel certificato.

Il Titolare è identificato all'interno del certificato attraverso un "Distinguished Name" (DN), nel campo Subject, conforme allo standard ITU-T X.500.

Nel campo Subject sono inseriti i dati identificativi del Titolare del certificato, senza che sia possibile, in genere, l'utilizzo di pseudonimi.

La chiave privata di un Titolare, generata dal Certificatore, non può essere recuperata o ricavata dalla CA una volta consegnata, in quanto i Titolari identificati nei rispettivi certificati sono gli unici responsabili della loro protezione.

Essi, pertanto, sono tenuti a tenere in debita considerazione le conseguenze derivanti dallo smarrimento della chiave privata indicate all'interno del presente Manuale.

1.9.7. RELYING PARTIES (R.P.)

Le Relying Parties si identificano nei soggetti che fanno affidamento sulle informazioni contenute nei certificati di CNS emessi dall'Ente Emettitore.

In particolare, per quanto riguarda il servizio descritto nel presente Manuale, per R.P. si intendono tutti i soggetti che verificano i certificati emessi secondo le modalità descritte nel presente Manuale.

Tutti coloro che devono fare affidamento sulle informazioni contenute nei certificati hanno l'obbligo, prima di accettare un certificato, di effettuare le necessarie verifiche, secondo quanto disposto nel Manuale Operativo del Certificatore, cui si rinvia per ulteriori dettagli.

2. OBBLIGHI E RESPONSABILITA'

2.1. OBBLIGHI DEI SOGGETTI COINVOLTI

2.1.1. ENTE EMETTITORE

Ai sensi del Decreto Interministeriale 9 dicembre 2004 recante regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi, l'Ente Emettitore è responsabile della formazione e del rilascio della CNS; si tratta della 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.

L'Università degli Studi di Napoli Parthenope, in qualità di Ente Emettitore è responsabile:

a) della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione,
b) della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione,
c) della sicurezza delle fasi di produzione, inizializzazione, distribuzione ed aggiornamento/ritiro della carta.

In particolare, le fasi in cui si divide l'attività dell'Ente Emettitore possono essere sintetizzate nelle seguenti:

1. **Individuazione servizi ed infrastruttura**: l'Ente Emettitore analizza ed individua i servizi da rendere disponibili in rete mediante CNS. Valuta le possibilità di mercato offerte per la fornitura delle smart card e decide se far fronte in maniera autonoma all'emissione della CNS, ovvero di utilizzare i servizi di strutture delegate.
2. **Avviamento del processo di emissione**: l'Ente Emettitore avvia la produzione di un lotto di CNS, si dota eventualmente di tutte le risorse *hw* e *sw* necessarie all'emissione della CNS tenendo conto delle direttive e delle norme vigenti, commissiona al produttore individuato la fornitura dei lotti di CNS inizializzate.
3. **Produzione delle CNS**: Il produttore esegue le fasi di produzione ed inizializzazione seguendo le specifiche definite nel presente documento e nel sito AgID. Le carte sono consegnate in modalità protetta all'Ente Emettitore.
4. **Registrazione degli utenti**: l'Ente Emettitore identifica, attraverso un documento di riconoscimento, il cittadino ed attiva la procedura di emissione CNS o in maniera autonoma o rivolgendosi a strutture delegate (v. par. 1.9.3 *infra*). Le attività relative alla registrazione dei dati dei Richiedenti seguono quanto descritto all'interno del Manuale Operativo dell'Ente Certificatore *Manuale_Operativo_Trust_Services_v.X.X_IT* nella sua versione aggiornata e disponibile al sito https://web.uanataca.com/it/politiche-di-certificazione.
5. **Verifica dati identificativi**: la verifica dei dati identificativi avviene tramite gli strumenti messi a disposizione dai soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità.
6. **Generazione del certificato di autenticazione**: Un certificatore accreditato, scelto dall'Ente Emettitore rilascia il certificato che attesta l'autenticità delle informazioni associate ai dati di

autenticazione. L'eventuale colloquio tra l'Ente Emettitore ed il certificatore avviene in modalità protetta.

7. **Personalizzazione della CNS**: l'Ente Emettitore, tramite strutture proprie o esterne, esegue la personalizzazione della CNS, inserendo i dati personali del cittadino ed il certificato di autenticazione, stampa gli stessi sulla carta, produce il PIN ed il PUK necessari all'utilizzo della CNS in rete ed il PIN necessario per l'eventuale installazione della firma digitale.
8. **Consegna della CNS**: l'Ente Emettitore, tramite strutture proprie o esterne, consegna la CNS al titolare. L'ente emettitore illustra al titolare le modalità di uso della carta e le procedure che dovranno essere utilizzate in caso di problemi. Fornisce al titolare le informazioni necessarie per l'assistenza sul dispositivo e i canali predisposti per la revoca e sospensione del certificato.
9. **Gestione della CNS**: l'Ente Emettitore provvede alla gestione delle CNS emesse predisponendo le strutture per l'assistenza agli utenti, la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza. Per le funzioni di gestione delle carte l'ente può avvalersi di strutture delegate. L'eventuale software consegnato al cittadino deve garantire l'interoperabilità con la CIE.

L'Ente Emettitore ha delegato al Certificatore, tramite la stipula di apposita convenzione, lo svolgimento delle attività di cui sopra, fermi restando in regimi di responsabilità previsti dalla normativa vigente.

2.1.2. CERTIFICATORE

Il Certificatore Uanataca S.A. è l'ente che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche abilitato ai sensi dell'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002.

Come anticipato nel paragrafo precedente l'Ente Emettitore ha delegato al Certificatore lo svolgimento di parte delle attività relative al ciclo di vita del certificato di CNS, per i cui dettagli si rimanda.

Il Certificatore è responsabile della generazione del certificato di autenticazione e di firma nella CNS.

2.1.3. UFFICI DI REGISTRAZIONE

Per la gestione del ciclo di vita della Carta Nazionale dei Servizi l'Ente Emettitore si avvale del Certificatore, cui delega, altresì, le attività degli Uffici di Registrazione (per maggiori informazioni v. par. 1.9.3).

Il Richiedente che intenda domandare il rilascio della Carta nazionale dei Servizi può rivolgersi indifferentemente sia all'Ente Emettitore che al Certificatore: saranno poi questi ultimi ad indirizzare il Richiedente presso gli Uffici di Registrazione abilitati ad effettuare le operazioni di riconoscimento e gestione del ciclo di vita del certificato di CNS.

Maggiori informazioni in merito agli Uffici di Registrazione saranno disponibili sul sito web dell'Ente Emettitore.

2.1.4. TITOLARE

Il Titolare della Carta Nazionale dei Servizi 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 con le sole modalità previste nel presente Manuale;
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.

2.2. LIMITAZIONI DI RESPONSABILITA'

L'Ente Emettitore ed il Certificatore non saranno tenuti a rispondere di quegli eventi a loro non direttamente imputabili, inclusi i danni che direttamente o indirettamente saranno riconducibili:

a) all'inosservanza del presente Manuale;
b) allo svolgimento di attività illecite;
c) a comportamenti del fruitore di servizi di certificazione privi delle richieste misure di diligenza atte ad evitare danni a terzi;

e subiti dal Titolare, dal Richiedente, dagli utenti o da terzi.

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

3. IDENTIFICAZIONE ED AUTENTICAZIONE

L'Ente Emettitore, anche per il tramite del Certificatore o di un Ufficio di Registrazione autorizzato, verifica con certezza l'identità di ogni Richiedente al momento della richiesta di emissione di un certificato di CNS al fine di assicurare che quel certificato possa riferirsi in maniera accurata e completa al soggetto Richiedente.

L'identità dei Richiedenti viene verificata tramite un documento di identità o tramite una delle modalità alternative previste dal Certificatore e condivise con l'Ente Emettitore, che garantiscono l'identificazione certa del Richiedente (cfr. §3.2 *Manuale_Operativo_Trust_Services_v.X.X_IT* nella sua ultima versione pubblicata).
Tutta la documentazione acquisita durante il processo di riconoscimento e verificata sarà conservata dall'Ente Certificatore per conto dell'Ente Emettitore, per tutto il tempo necessario ad assicurare la fruizione e la continuità del servizio richiesto, in ogni caso in conformità a quanto disposto dal Regolamento (UE) 2016/679 – GDPR - del Parlamento Europeo e del Consiglio del 27 aprile 2016.
Per garantire la tutela e la gestione dei dati personali acquisiti nel corso delle procedure di registrazione, inoltre, sarà preventivamente fornita ad ogni Richiedente l'informativa sulla privacy, pubblicata sul sito del Certificatore https://web.uanataca.com/it/condizioni-generali-del-servizio.

3.1. PROCEDURA DI IDENTIFICAZIONE DE VISU

Tale procedura di identificazione prevede la presenza fisica del Richiedente dinnanzi ad un operatore o al personale autorizzato dall'Ente Emettitore, il quale provvede (avendo ricevuto apposita formazione in precedenza) ad accertare l'identità del Richiedente attraverso la verifica dei corrispondenti documenti di identità esibiti in originale.
È specifico onere dell'operatore accertarsi che il documento di identità esibito risulti in corso di validità (e, dunque, che non sia scaduto al momento della presentazione della richiesta di emissione del certificato) e che quest'ultimo rechi in maniera chiara la fotografia del soggetto da identificare.
È necessario che il Richiedente sia in possesso del Codice Fiscale (Tessera Sanitaria, Tessera del Codice Fiscale, Certificato di attribuzione di Codice Fiscale ecc..) la cui esibizione può essere richiesta dai soggetti abilitati ad eseguire il riconoscimento.
Il personale incaricato ed addetto all'identificazione provvederà all'accertamento delle seguenti tipologie di dati:

- Nome completo (prenome, nome e cognome);
- data e luogo di nascita;
- indirizzo di residenza e di domicilio;
- codice fiscale o altro codice identificativo univoco;
- indirizzo di posta elettronica, numero di telefono e facoltativamente p.e.c.;
- tipo e numero del documento di identità esibito;
- Autorità che ha rilasciato il documento, data e luogo di rilascio, data di scadenza;
- ogni altro dato ritenuto utile ai fini dell'identificazione;

L'Ufficio di Registrazione verificherà, mediante la visualizzazione di documenti o attraverso le proprie fonti di informazione, il resto dei dati e degli attributi da includere nel certificato.

Una volta terminata la procedura di identificazione da parte di un Operatore a ciò autorizzato, questi è tenuto a raccogliere e ad archiviare in maniera precisa ed ordinata, gli originali di tutta la documentazione inerente ogni singola richiesta di emissione dei certificati nonché tutta la documentazione relativa all'identificazione dei Richiedenti che sarà comunicata all'Ente Emettitore e al Certificatore, anche in formato elettronico, al fine di attivare correttamente la procedura di emissione dei certificati.

L'Ente Emettitore e il Certificatore si impegnano a conservare e ad archiviare tutte le informazioni relative ai Dati Personali dei Titolari, in conformità con il Regolamento (UE) n. 679/2016 e alla propria Politica sulla Privacy.

3.2. PROCEDURA DI IDENTIFICAZIONE DA REMOTO

In alternativa alla procedura di identificazione "*de visu*", l'Ente Emettitore ha previsto una procedura di identificazione dei Richiedenti da remoto, tramite utilizzo di una apposita piattaforma telematica di video-identificazione, messa a disposizione dal Certificatore.

L'Ente Emettitore garantisce l'utilizzo di procedure e strumenti in grado di garantire, sul piano giuridico, l'identificazione "certa" del Richiedente il certificato di CNS, in piena conformità a quanto richiesto dall'art. 19 del CAD secondo cui il certificatore che "rilascia […] certificati qualificati deve […] provvedere con certezza alla identificazione della persona che fa richiesta della certificazione" e dal successivo art. 32 co. 3 lett. a).

Una volta effettuata la richiesta di emissione di un certificato digitale qualificato da parte del Richiedente, l'Ente Emettitore o un suo Ufficio di Registrazione (RA) autorizzato, provvederà alla fissazione della data e dell'ora del primo appuntamento disponibile, la quale sarà comunicata al Richiedente tramite i canali di comunicazione da quest'ultimo indicati in fase di richiesta.

Prima di procedere con tale modalità di identificazione il Richiedente viene informato che dovrà disporre di un Personal Computer, di uno smartphone o di un Tablet dotato di webcam (ovvero di videocamera che consenta la visualizzazione e l'ascolto di tutto ciò che avviene nel suo campo visuale) e, successivamente, gli verranno fornite le opportune indicazioni in relazione alla piattaforma da utilizzare per la video-identificazione

Il sistema per la video-identificazione è messo a disposizione direttamente dal Certificatore o anche da terzi e comunque deve essere in grado di garantire che le modalità di registrazione delle immagini e dei video assicurino la non alterabilità e/o sostituibilità del soggetto ripreso e di tutte le immagini e/o suoni che vengono rilevati nel corso della sessione di ripresa tramite webcam.

Inoltre, è necessario che, durante la sessione di ripresa, l'immagine video sia a colori e consenta una chiara visualizzazione dell'interlocutore.

L'operatore, al fine di assicurare quanto sopra, potrà non avviare o sospendere in qualsiasi momento la procedura di identificazione qualora la qualità audio/video risulti tale da non garantire i requisiti sopra indicati nonché quelli di cui all'art. 32 comma 3 lett. a) del CAD.

Scegliendo di proseguire nella procedura di identificazione da remoto il Richiedente sarà informato sulle modalità e sul Trattamento dei Dati Personali, in conformità alla Privacy Policy prevista nel Manuale e che la sessione di identificazione tramite webcam sarà registrata; in questo modo il Richiedente potrà così scegliere se fornire o meno il consenso al Trattamento: resta inteso che, in caso di mancato consenso circa il Trattamento dei Dati Personali da parte del Richiedente, l'operatore non potrà procedere alla successiva identificazione.

In caso di manifestazione espressa del consenso, che potrà avvenire anche a seguito di esplicita richiesta dell'operatore incaricato all'inizio di ogni sessione si potrà procedere con l'identificazione da remoto.

A questo punto, avviata la sessione tramite webcam, l'operatore incaricato, ai fini di una corretta identificazione personale tramite il documento di identità, provvederà, innanzitutto a verificare se:

a. il documento è stato rilasciato da un'Amministrazione dello Stato;
b. il documento reca la fotografia del soggetto;
c. nel documento sono presenti i dati anagrafici del soggetto;
d. il documento presenta il seriale identificativo;
e. il documento presenta idonei segni di anticontraffazione;

L'Ente Emettitore garantisce che gli operatori incaricati di effettuare le operazioni sopra descritte sono adeguatamente formati; è facoltà dell'operatore, dunque, escludere l'ammissibilità dei documenti esibiti dai Richiedenti, se carenti di una delle caratteristiche sopra elencate.

Una volta completata e chiusa la sessione di identificazione da remoto, il video così realizzato sarà conservato e protetto in modo adeguato, in conformità al Trattamento dei dati personali di cui alla Privacy Policy adottata dall'Ente Emettitore.

3.3. PROCEDURA DI IDENTIFICAZIONE TRAMITE CIE

L'Ente Emettitore ha previsto, quale ulteriore modalità di identificazione, la possibilità di utilizzare la CIE "Carta di Identità Elettronica" per l'acquisizione certa dei dati identificativi dei Richiedenti.

Per CIE, ai sensi dell'art. 1 del D.M. 23 dicembre 2015 si intende: "il documento di identità personale rilasciato dal Ministero dell'Interno denominato "Carta di Identità Elettronica", mezzo di identificazione elettronica, di livello significativo, notificato ai sensi dell'articolo 9 del Regolamento eIDAS.

Il Richiedente, previo inserimento del PIN, effettua l'autenticazione sul portale del Certificatore o del CIE ID Server (caso CIE). Il sistema recupera le informazioni anagrafiche inserite nel certificato digitale e le associa a quelle relative al certificato di sottoscrizione in oggetto di richiesta.

A seguito della corretta esecuzione della procedura di identificazione sopra descritta sarà possibile, per l'Ente Emettitore emettere il certificato digitale di autenticazione richiesto dal Richiedente, previa sottoscrizione, da parte di quest'ultimo, delle Condizioni Generali di Contratto.

3.4. PROCEDURA DI IDENTIFICAZIONE TRAMITE IDENTITA' DIGITALE SPID

Ai sensi dell'art. 64 co. 2-bis del Codice dell'Amministrazione Digitale "per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)".

Il Richiedente, che sia in possesso di credenziali di autenticazione tramite SPID (di livello 2 o superiore), potrà richiedere a Uanataca previa accettazione, da parte di quest'ultimo, delle Condizioni Generali di Contratto, l'emissione di certificati digitali di autenticazione senza effettuare una nuova procedura di identificazione secondo le norme del presente Manuale.

In tali casi, infatti, l'identità del Richiedente è già stata previamente accertata da uno dei Fornitori dell'Identità Digitale SPID accreditato dall'Agenzia per l'Italia Digitale, per la gestione dell'identità digitale dei propri utenti.

In ogni caso, l'Ente Emettitore, anche tramite l'Ente Certificatore, si riserva la facoltà di rifiutare le richieste di emissione qualora, a seguito di adeguate verifiche, risultino incongruenze tra i dati identificativi forniti dal Richiedente al momento della richiesta di emissione del certificato e quelli risultanti dall'identità digitale SPID da questo utilizzata.

Il richiedente è chiamato ad effettuare un'autenticazione su di un portale del Certificatore attraverso meccanismi del circuito SPID, in tale processo di autenticazione, sono richiesti i seguenti dati minimi:

- Nome;
- Cognome;
- Codice Fiscale;
- Sesso;
- Data di nascita;
- Luogo di nascita.

I dati di registrazione sono conservati esclusivamente in formato elettronico.

3.5. PROCEDURA DI IDENTIFICAZIONE TRAMITE FIRMA DIGITALE

La seguente procedura di identificazione consente al Richiedente di identificarsi in maniera certa mediante l'utilizzo di certificati qualificati rilasciati da altri prestatori di servizi, in conformità al Regolamento eIDAS.

In questo caso, il Richiedente è stato già previamente identificato da un prestatore di servizi fiduciari qualificato, che ha rilasciato il certificato digitale e utilizzerà quest'ultimo, se ancora in corso di validità, per firmare il modulo di richiesta di emissione del certificato CNS.
Ricevuta la richiesta di emissione, sottoscritta digitalmente da parte del Richiedente, l'Ente Emettitore, anche tramite il Certificatore, effettuerà adeguati controlli al fine di verificare la validità del certificato utilizzato per la firma riservandosi di rifiutare la richiesta di emissione in caso di esito negativo di questa.

3.6. IDENTIFICAZIONE ED AUTENTICAZIONE PER LE RICHIESTE DI RINNOVO

3.6.1. RINNOVO PERIODICO DEI CERTIFICATI

La procedura di identificazione ed autenticazione nei casi in cui sia richiesto il rinnovo dei certificati di CNS si svolge in maniera più semplice rispetto a quella relativa alla richiesta di prima emissione.
Prima di rinnovare un certificato, l'operatore verifica che le informazioni utilizzate per l'identificazione del Titolare continuino ad essere valide e non abbiano subito cambiamenti.
I metodi per effettuare tale verifica sono:

- l'utilizzo del codice riservato di emergenza ("codice utente") relativo al certificato precedente, o di altri mezzi di autenticazione personale, che consistono in informazioni note solo alla persona fisica identificata nel certificato e che consentono di riemettere automaticamente il certificato, a condizione che il periodo massimo stabilito dalla legge non sia stato superato;
- l'uso dell'attuale certificato, purché quest'ultimo non abbia superato il periodo massimo stabilito dalla legge per il rinnovo.

Se le informazioni del Titolare identificato nel certificato hanno subito variazioni, non sarà possibile procedere con il rinnovo, ma sarà necessario effettuare un'identificazione completa, conformemente alle disposizioni della sezione precedente.

3.6.2. RINNOVO DOPO LA REVOCA

Nel caso in cui sia richiesto un rinnovo del certificato dopo la sua revoca è necessario, per il Titolare, ripetere la procedura di validazione dell'identità di cui al presente capitolo (v. par. 3.1 ,3.2, 3.3, 3.4 e 3.5. *infra*).
Prima di generare un certificato per un Titolare il cui certificato precedente sia stato revocato, l'operatore o il personale autorizzato da una R.A. di Uanataca verificherà che le informazioni utilizzate per validare l'identità e le ulteriori informazioni del Richiedente e/o del Titolare siano valide, in quel caso si applicheranno le disposizioni della sezione precedente.
Dopo la revoca del certificato non sarà possibile la riemissione dei certificati, qualora ricorra uno dei seguenti casi:

- il certificato è stato revocato in quanto erroneamente emesso per una persona diversa da quella identificata nel certificato;
- il certificato è stato revocato in quanto emesso senza l'autorizzazione del soggetto identificato nel certificato;
- il certificato revocato contiene informazioni errate o false.

Se le informazioni del Titolare identificato nel certificato hanno subito variazioni, le nuove informazioni verranno correttamente registrate e sarà effettuata un'identificazione completa, conformemente alle disposizioni del presente capitolo.

3.6.3. IDENTIFICAZIONE PER LE RICHIESTE DI REVOCA

L'identificazione dei Titolari nel processo di revoca dei certificati può essere effettuata:

- dal Titolare: tramite l'uso del codice di revoca ERC attraverso il sito Web di Uanataca https://www.uanataca.com/lcm/ disponibile 7 giorni su 7 e 24 ore su 24 o invio dell'apposito modulo di richiesta tramite indirizzo PEC del Certificatore;
- dagli Uffici di Registrazione: questi devono identificare il Titolare prima di approvare una richiesta di revoca.

In tutte le ipotesi in cui sussistano dei dubi sull'identità del Titolare il certificato entrerà in stato di sospensione.

4. OPERATIVITA'

Nella presente sezione sono descritte le fasi relative al ciclo di vita del certificato di CNS che possono riassumersi nelle seguenti: emissione, sospensione, revoca, riattivazione e rinnovo.

4.1. DOMANDA DI EMISSIONE DEL CERTIFICATO

4.1.1. LEGITTIMAZIONE ALLA RICHIESTA

Il Richiedente del certificato è tenuto a sottoscrivere il modulo di richiesta del servizio predisposto dal Certificatore e ad accettare la documentazione contrattuale predisposta dall'Ente Emettitore comprendente le condizioni generali di fornitura del servizio e la politica in materia di protezione di dati personali.

4.1.2. PROCEDURE E RESPONSABILITA'

L'Ente Emettitore riceve le richieste di emissione della Carta Nazionale dei Servizi: tali richieste vengono inoltrate tramite un modulo, in formato cartaceo o digitale, singolarmente o in lotti, o collegandosi a database esterni o tramite appositi servizi Web predisposti dall'Ente Emettitore.

La domanda deve essere accompagnata da una documentazione di supporto relativa all'identità e da altre informazioni sulla persona fisica identificata nel certificato, in conformità alle disposizioni della sezione 3.

4.2. ELABORAZIONE DELLA RICHIESTA

4.2.1. SVOLGIMENTO DELLE FUNZIONI DI IDENTIFICAZIONE E AUTENTICAZIONE

Ricevuta una richiesta di emissione del certificato CNS, l'Ente Emettitore verifica che quest'ultima sia completa, accurata e debitamente autorizzata, prima di elaborarla.

In caso di esito positivo, l'Ente Emettitore analizza le informazioni fornite, verificandone la compatibilità con gli aspetti descritti nella sezione 3.

4.2.2. APPROVAZIONE O RIFIUTO DELLA RICHIESTA

Nel caso in cui la verifica dei dati forniti abbia esito positivo, l'Ente Emettitore o un suo delegato, Ente Certificatore o RA, approverà la richiesta di certificato e procederà alla sua emissione e consegna.

Se dalla verifica effettuata emerge che le informazioni fornite sono errate, o nel caso in cui tali informazioni vengano giudicate non affidabili, inesatte, incomplete o incoerenti, l'Ente Emettitore o un suo delegato, Ente Certificatore o RA, rigetterà la richiesta o interromperà la sua approvazione fino a quando non avrà effettuato i controlli che riterrà necessari.

Se, a seguito dell'ulteriore verifica, dovesse risultare che le informazioni fornite non sono corrette, l'Ente Emettitore rifiuterà definitivamente la richiesta.

L'Ente Emettitore è in grado di automatizzare le procedure che permettono di verificare la correttezza delle informazioni contenute nei certificati e i processi di approvazione delle domande.

4.3. EMISSIONE DEL CERTIFICATO

4.3.1. PROCESSO DI EMISSIONE

A seguito dell'approvazione della richiesta, il certificato viene generato in modo sicuro e reso disponibile al Titolare per l'accettazione.

Le procedure stabilite in questa sezione si applicano anche in caso di rinnovo dei certificati, poiché quest'ultimo implica, comunque, l'emissione di un nuovo certificato.

Durante il processo di emissione l'Ente Emettitore:

- garantisce la riservatezza e l'integrità dei dati di registrazione forniti;
- utilizza sistemi e prodotti affidabili che siano protetti da qualsiasi alterazione possibile e che garantiscono la sicurezza, dal punto di vista tecnico, dei processi in cui vengono adoperati;
- produce una coppia di chiavi, tramite una procedura sicura di generazione;
- implementa un processo di generazione di certificati che collega in modo sicuro il certificato alle informazioni di registrazione, inclusa la chiave pubblica certificata;
- assicura che il certificato sia rilasciato da sistemi protetti da ogni possibile contraffazione e che garantiscono la riservatezza delle chiavi durante il processo di generazione di queste ultime;
- indica la data e l'ora in cui è stato emesso un certificato;
- garantisce il controllo esclusivo delle chiavi da parte dell'utente, di modo che terzi non possano detrarle o utilizzarle in alcun modo.

4.3.2. GENERAZIONE DEL CERTIFICATO DI AUTENTICAZIONE

L'attività di generazione del certificato di autenticazione CNS viene svolta dal Certificatore secondo quanto previsto nel proprio Manuale Operativo disponibile al seguente percorso: https://web.uanataca.com/it/

4.3.3. GENERAZIONE DEL CERTIFICATO DI FIRMA

L'attività di generazione del certificato di firma digitale viene svolta dal Certificatore secondo quanto previsto nel proprio Manuale Operativo disponibile al seguente percorso: https://web.uanataca.com/it/

4.4. RILASCIO DEL CERTIFICATO

A seconda della modalità di identificazione prescelta il certificatore procederà al rilascio della Carta Nazionale dei Servizi con le modalità di seguito descritte.

4.4.1. EMISSIONE DEL CERTIFICATO

L'emissione del certificato di autenticazione CNS avviene su dispositivi sicuri (QSCD), che garantiscono i elevati standard di sicurezza, mentre differiscono unicamente per le interfacce offerte: Smartcard, Token USB e DNA Key (con doppia interfaccia USB e Bluetooth Low Energy).

La generazione della coppia di chiavi crittografiche avviene, a cura della R.A. di riferimento, direttamente sul dispositivo sicuro di firma prescelto, tramite l'utilizzo di appositi programmi per elaboratore, forniti da Uanataca, che garantiscono adeguate misure di sicurezza.
In seguito, la RA invia a Uanataca la richiesta di certificazione, in formato PKCS#10, della chiave pubblica firmata digitalmente affinché quest'ultima, verificata la validità della firma e la provenienza della richiesta da soggetto a ciò autorizzato, genera il certificato, successivamente importato all'interno del dispositivo tramite canale sicuro.

4.5. USO DELLA COPPIA DI CHIAVI E DEL CERTIFICATO

Il Titolare del certificato di CNS è tenuto a:

- leggere ed accettare integralmente il contenuto del presente documento prima di richiedere il certificato;
- fornire all'Ente Emettitore informazioni esatte, complete e veritiere in fase di richiesta del certificato;
- esprimere il suo consenso preventivamente all'emissione e alla consegna di un certificato;
- utilizzare la propria chiave privata e il proprio certificato unicamente per gli scopi previsti dal presente documento;
- adottare misure di sicurezza atte a prevenire l'uso non autorizzato della propria chiave privata;
- assicurare la confidenzialità dei codici riservati ricevuti dall'Ente Emettitore;
- richiedere tempestivamente all'Ente Emettitore la revoca del certificato nel caso di sospetta compromissione della propria chiave privata;
- nel caso di accertata compromissione della propria chiave privata, richiedere tempestivamente all'Ente Emettitore la revoca del certificato;
- prima di cominciare ad utilizzare la chiave privata, controllare attentamente che il corrispondente certificato di CMS abbia il profilo previsto e contenga informazioni corrette, incluse le eventuali limitazioni d'uso;
- fino alla data di scadenza o di eventuale revoca del proprio certificato, informare prontamente la l'Ente Emettitore nel caso in cui: il proprio dispositivo sia andato perso, sia stato sottratto o si sia danneggiato; abbia perso il controllo esclusivo della propria chiave privata, per esempio a causa della compromissione dei dati di attivazione (PIN o password) della propria chiave privata; alcune informazioni contenute nel certificato siano inesatte o non più valide;
- nel caso di compromissione della propria chiave privata (per esempio, a causa dello smarrimento del PIN o della sua rivelazione a terzi non autorizzata), cessare immediatamente l'utilizzo della stessa ed assicurarsi che non venga più utilizzata: in tale situazione l'Ente Emettitore revoca immediatamente il certificato.

A seguito della richiesta del certificato il Titolare assume consapevolmente le seguenti responsabilità affinché:

- tutte le informazioni fornite contenute nel certificato siano corrette;
- il certificato sia utilizzato esclusivamente per usi legali e autorizzati, in conformità con il presente Manuale;
- nessuna persona non autorizzata abbia accesso alla chiave privata del certificato, assumendosi, inoltre, l'esclusiva responsabilità per i danni causati dalla mancata protezione della chiave privata;
- non cedere o concedere in uso in nessuna circostanza la chiave privata (trattandosi di un elemento strettamente personale) a terzi.

4.6. VALIDITA' DELLA CARTA NAZIONALE DEI SERVIZI

I certificati presenti all'interno della CNS hanno validità 3 (tre) anni e possono essere rinnovati per ulteriori 3 anni a partire dalla data di rinnovo, in conformità alle disposizioni del presente Manuale.
Il rinnovo dei certificati è consentito entro e non oltre il giorno lavorativo precedente alla data di scadenza.
La validità del certificato perdura sino alla data di scadenza, salvo revoca o sospensione mediante pubblicazione nella CRL.

4.7. INTERDIZIONE DELLA CNS

L'interdizione della Carta Nazionale dei Servizi si verifica attraverso la revoca del relativo certificato; nell'ipotesi di sospensione si avrà, invece, un caso di interdizione temporanea che perdura sino alla riattivazione del certificato.
Quando un certificato di CNS si trova in stato di interdizione (sia per essere stato revocato sia per essere stato sospeso) esso non sarà più riconosciuto come valido.
La revoca e la sospensione di un certificato comportano la cessazione della sua validità. La revoca comporta la cessazione anticipata e definitiva della validità del certificato. È pertanto una condizione irreversibile.
La sospensione comporta l'interruzione momentanea della validità di un certificato e consente la successiva riattivazione oppure la revoca definitiva.
La revoca o sospensione del certificato si materializzano con l'inserimento del numero di serie del certificato all'interno della CRL – *Certificate Revocation List*, vale a dire una lista dei certificati revocati.
Questa viene pubblicata e firmata dal Certificatore per consentire agli interessati la consultazione necessaria alla determinazione dello stato di validità dei certificati (v. par. 4.9. *infra*).

4.8. REVOCA E SOSPENSIONE DEL CERTIFICATO

4.8.1. IPOTESI DI REVOCA DI UN CERTIFICATO

L'Ente Emettitore revoca un certificato quando si presenta una delle seguenti cause (elenco non esaustivo):

1. **circostanze che influenzano le informazioni contenute nel certificato:**
   a. modifica di alcuni dei dati contenuti nel certificato, successivamente all'emissione del certificato corrispondente;
   b. prova della non correttezza dei dati contenuti nella richiesta di certificato;
2. **circostanze che influiscono sulla sicurezza della chiave o del certificato**:
   a. compromissione della chiave privata, dell'infrastruttura o dei sistemi del Certificatore, a condizione che ciò influisca sull'affidabilità dei certificati rilasciati;
   b. violazione dei requisiti previsti nelle procedure di gestione dei certificati;
   c. sospetto o prova di compromissione della sicurezza della chiave o del certificato emesso;
   d. accesso o uso non autorizzato, da parte di terzi, della chiave privata corrispondente alla chiave pubblica contenuta nel certificato;
   e. uso improprio del certificato da parte della persona fisica identificata nel certificato o mancanza di diligenza nella custodia della chiave privata.
3. **circostanze che riguardino il Richiedente e/o il Titolare**:
   a. cessazione del contratto tra l'Ente Emettitore e il Titolare;
   b. modifica o risoluzione anticipata del contratto tra l'Ente Emettitore e il Titolare;
   c. violazione da parte del Richiedente dei requisiti prestabiliti per la sua richiesta;
   d. violazione da parte del Titolare degli obblighi contrattuali;
   e. incapacità sopravvenuta del Titolare;
   f. richiesta esplicita di revoca del certificato da parte del Titolare e/o del suo rappresentante.
4. **altre circostanze:**
   a. cessazione del servizio di certificazione da parte del Certificatore;
   b. utilizzo del certificato non conforme e pregiudizievole per l'Ente Emettitore o per il Certificatore, specie in modo continuativo;
   c. provvedimento dell'Autorità giudiziaria.

In questo caso, un utilizzo è considerato dannoso in base ai seguenti criteri:

- la natura e il numero di reclami ricevuti;
- l'identità dei soggetti che presentano i reclami;
- la legislazione applicabile;
- la risposta fornita dal Titolare rispetto ai reclami ricevuti.

4.8.2. CHI PUÒ RICHIEDERE LA REVOCA

La revoca del certificato di autenticazione può essere inoltrata dal Titolare del certificato o in determinati cas da un Terzo Interessato, oltre che dall'Ente Emettitore e dal Certificatore laddove ne ravvisino la necessità.

Inoltre, la revoca può essere richiesta dall'Autorità Giudiziaria e tali segnalazioni, vista la specifica identità del segnalatore, saranno trattate con maggiore priorità rispetto alle altre.

4.8.3. PROCEDURA DI REVOCA

Il soggetto che richiede la revoca di un certificato può farlo rivolgendosi direttamente all'Ente Emettitore, al Certificatore, ad un Ufficio di Registrazione oppure, in prima persona, attraverso il servizio online disponibile sulla pagina web del Certificatore.

La richiesta di revoca dovrà includere le informazioni seguenti:

- data della richiesta di revoca;
- dati identificativi del Titolare;
- recapiti della persona che chiede la revoca;
- motivazione dettagliata relativa alla richiesta di revoca.

Prima di procedere alla revoca, la richiesta deve essere validata dall'Ente Emettitore o dal Certificatore o dall'Operatore di Registrazione, demandato e formato per svolgere le presenti attività.

In seguito all'elaborazione della richiesta di revoca, il cambio di stato del certificato verrà notificato al Titolare.

4.8.4. TEMPI ESECUZIONE RICHIESTA DI REVOCA

Il Certificatore esegue la revoca con la massima tempestività e attenzione, garantendo che il tempo necessario per l'elaborazione dell'operazione di revoca o sospensione e il conseguente aggiornamento dello stato del certificato (effettuato tramite pubblicazione di una nuova lista di revoca CRL) sia il più ridotto possibile.

Se effettuata per mezzo di un operatore, la richiesta di revoca sarà elaborata entro il consueto orario d'ufficio del Certificatore o laddove applicabile dall'Ufficio di Registrazione che ha proceduto all'emissione del certificato. Se effettuata online, avrà effetto immediato.

4.8.5. PUBBLICAZIONE E FREQUENZA DI EMISSIONE DELLA CRL

La periodicità della pubblicazione delle CRL è definita dal Certificatore nelle proprie politiche di certificazione, disponibili al seguente percorso: https://web.uanataca.com/it/politiche-di-certificazione.

4.9. CIRCOSTANZE PER LA SOSPENSIONE

La sospensione del certificato di autenticazione CNS è prevista nelle seguenti circostanze:

1. circostanze che influenzano le informazioni contenute nel certificato;
2. sospetta non correttezza dei dati contenuti nella richiesta di certificato;
3. circostanze che influiscono sulla sicurezza della chiave o del certificato;
4. sospetta violazione dei requisiti previsti nelle procedure di gestione dei certificati;
5. sospetto accesso o uso non autorizzato, da parte di terzi, della chiave privata corrispondente alla chiave pubblica contenuta nel certificato;

6. sospetto uso improprio del certificato da parte della persona fisica identificata nel certificato o mancanza di diligenza nella custodia della chiave privata;
7. circostanze che riguardino il Titolare: richiesta esplicita di revoca del certificato da parte del Titolare e/o del suo rappresentante;

4.9.1. CHI PUÒ RICHIEDERE LA SOSPENSIONE

La sospensione del certificato di autenticazione può essere inoltrata dal Titolare del certificato o in determinati cas da un Terzo Interessato, oltre che dall'Ente Emettitore e dal Certificatore laddove ne ravvisino la necessità. Inoltre, la sospensione a scopo cautelativo può essere richiesta dall'Autorità Giudiziaria e tali segnalazioni, vista la specifica identità del segnalatore, saranno trattate con maggiore priorità rispetto alle altre.

4.9.2. PROCEDURA LA SOSPENSIONE

La sospensione dei certificati qualificati è effettuata dal Certificatore mediante l'inserimento del codice identificativo in una delle liste dei certificati revocati e sospesi (CRL).
Il termine di durata massima del periodo di sospensione è stabilito dal Certificatore; al termine del periodo di sospensione, senza che sia intervenuta indicazione contraria da parte del Titolare, il Certificatore provvederà alla revoca del certificato.
Per la restante parte, la procedura di sospensione si effettua in maniera equivalente a quanto avviene per la revoca, così come descritto nei paragrafi precedenti.

4.9.3. PROCEDURA DI RIATTIVAZIONE

La riattivazione del certificato può essere richiesta dal soggetto che ha richiesto la sospensione e non è consentita nell'ipotesi in cui il certificato è stato revocato.

La riattivazione del certificato, che avviene su intervento dell'operatore di registrazione, comporta la cancellazione dalle liste di revoca CRL e la conseguente acquisizione della piena validità.

4.9.4. PROCEDURA DI RINNOVO

Il rinnovo del certificato richiede la generazione di una nuova coppia di chiavi e può essere attuato con una procedura che viene avviata dal Titolare prima della scadenza del certificato.
Se il Titolare non richiede il rinnovo prima della scadenza del certificato dovrà richiedere l'emissione di un nuovo certificato.

4.9.5. SERVIZI INFORMATIVI SULLO STATO DEI CERTIFICATI

Lo stato dei certificati è messo a disposizione attraverso la pubblicazione della CRL mediante protocollo http ed https ed in formato conforme alla specifica [RFC 5280].

Lo stato dei certificati è inoltre reso disponibile online dal Certificatore attraverso un servizio basato sul protocollo OCSP (*On-line Certificate Status Protocol*) in conformità con la specifica [RFC6960].

Gli indirizzi per l'accesso ai servizi di revoca sono inseriti all'interno dei certificati. L'indirizzo delle CRL è inserito nell'estensione CRLDistributionPoints.

L'indirizzo del server OCSP viene inserito nell'estensione *AuthorityInformationAccess*.

I Servizi sono ad accesso pubblico.

Per ulteriori informazioni si invita a consultare le politiche di certificazione del Certificatore al seguente percorso: https://web.uanataca.com/it/politiche-di-certificazione.

5. DISPONIBILITA' DEL SERVIZIO

Gli orari di disponibilità e di erogazione del servizio da parte del Certificatore sono stabiliti nei paragrafi successivi.

5.1. ACCESSO ALLE LISTE DEI CERTIFICATI

L'accesso alle CRL è disponibile 24h/24h in conformità alle politiche di certificazione del Certificatore, disponibili al seguente percorso: https://web.uanataca.com/it/politiche-di-certificazione.

5.2. SOSPENSIONE E RIATTIVAZIONE

Le procedure per la sospensione e riattivazione dei certificati di CNS sono attivabili sul sito del Certificatore secondo le proprie politiche di certificazione e presso gli Uffici di Registrazione nei rispettivi orari di ufficio.

5.3. REVOCA

La revoca dei certificati di CNS può essere richiesta, in conformità al presente Manuale tramite il sito del Certificatore e presso gli Uffici di Registrazione nei rispettivi orari di ufficio.

5.4. REGISTRAZIONE, GENERAZIONE, PUBBLICAZIONE E RINNOVO

La richiesta di rilascio e rinnovo dei certificati di CNS può essere presentata presso gli Uffici di Registrazione a ciò abilitati.

6. CONDIZIONI ECONOMICHE E LEGALI

6.1. TARIFFE

6.1.1. EMISSIONE O RINNOVO DEL CERTIFICATO

L'Ente Emettitore ha previsto delle tariffe per l'emissione e per il rinnovo dei certificati di CNS. Le tariffe vigenti sono disponibili sul sito web dell'Ente Emettitore e sono comunque comunicate al Richiedente al momento della richiesta di emissione o di rinnovo sui canali di distribuzione.

6.1.2. REVOCA E SOSPENSIONE DEL CERTIFICATO

La revoca e la sospensione del certificato di CNS non prevede alcuna tariffa.

6.1.3. ACCESSO AI CERTIFICATI E ALLE CRL

L'accesso al pubblico registro dei certificati revocati è libero e gratuito: per tale motivo non è stata prevista alcuna tariffa economica per l'accesso alla lista di tali certificati.

6.2. POLITICA PER IL RIMBORSO - RECESSO

Ai sensi e per gli effetti degli artt. 49 e ss. del D.lgs. 6 settembre 2005 n. 206 e s.m.i. (Codice del Consumo) il Titolare ha diritto di recedere dal contratto, anche senza indicarne le ragioni, entro il termine di 14 (quattordici) giorni decorrenti dalla data della sua conclusione e di ottenere il relativo rimborso.

Il diritto di recesso può essere esercitato unicamente dai Titolari che, nella stipulazione del contratto, hanno agito per scopi estranei all'attività imprenditoriale (e, dunque, da coloro che sono qualificabili come consumatori ai sensi dell'art. 3 co. 1 lett. a) del Codice del Consumo).

Per poter esercitare il diritto di recesso il Titolare è tenuto ad informare l'Ente Emettitore della sua decisione di recedere dal contratto tramite una dichiarazione esplicita.

Per ulteriori contatti è possibile consultare il sito web dell'Ente Emettitore.

6.3. TUTELA DELLE INFORMAZIONI TRATTATE

6.3.1. INFORMAZIONI CONFIDENZIALI

L'Ente Emettitore si impegna, insieme con il Certificatore, a trattare e a gestire, qualificandole come confidenziali, tutte le seguenti informazioni:

- richieste di emissione certificati, approvate o negate, nonché tutti i dati personali ottenuti per l'emissione e il mantenimento dei certificati, ad eccezione delle informazioni che devono essere inserite nei certificati o che per altre ragioni, ai sensi del paragrafo seguente, sono da considerarsi non confidenziali;
- chiavi private dei Titolari qualora siano generate e/o memorizzate dal Certificatore;
- log dei sistemi di elaborazione del Certificatore;
- contratti stipulati tramite gli Uffici di Registrazione;
- documenti di controllo, interni ed esterni, creati e/o gestiti dal Certificatore e dai suoi auditor;
- business continuity e piani di emergenza;
- piani di sicurezza;

- ogni altra informazione identificata come "Confidenziale".

Tutte le informazioni confidenziali sono trattate dall'Ente Emettitore e dal Certificatore nel rispetto delle norme applicabili, in particolare del D.lgs. 196/03 e s.m.i. e del Regolamento (UE) 2016/679, in conformità alle rispettive poliche in materia di trattamento dei dati personali.

Per l'informativa sul trattamento dei dati personali ai sensi dell'art. 13 del Regolamento (UE) 2016/679 effettuata dal Certificatore si rinvia al seguente sito web: https://web.uanataca.com/it/condizioni-generali-del-servizio.

L'Ente Emettitore e il Certificatore assicurano che le informazioni confidenziali siano adeguatamente protette fisicamente e/o logicamente dagli accessi non autorizzati nonché dal rischio di perdita a seguito di disastri (si veda a tal riguardo la sezione apposita presente del Manuale Operativo del Certificatore).

6.3.2. INFORMAZIONI NON CONFIDENZIALI

Non sono considerate confidenziali le seguenti informazioni:

- certificati emessi o in corso di emissione;
- periodo di validità del certificato, nonché la data di emissione del certificato e la data di scadenza;
- numero di serie del certificato;
- differenti stati del certificato (ad esempio: in attesa di generazione e/o consegna, valido, revocato, sospeso o scaduto), la data di inizio di ciascuno di essi e il motivo che ha determinato il cambiamento di stato;
- liste dei certificati sospesi o revocati (CRL), nonché le altre informazioni sullo stato di revoca;
- informazioni contenute all'interno del certificato;
- informazioni sui Titolari ottenibili dalla consultazione delle fonti pubbliche;
- informazioni che il Titolare stesso ha chiesto al Certificatore di rendere pubbliche;
- qualsiasi altra informazione che non rientri nell'ambito di applicazione nel paragrafo precedente.

7. MISURE DI SICUREZZA TECNICA

Uanataca utilizza sistemi e tecniche affidabili atte a garantire la sicurezza tecnica dei processi implementati.

Tutte le misure di sicurezza tecnica impiegate da Uanataca sono descritte nel documento Manuale_Operativo_Trust_Services_v.X.X_IT, pubblicato sul sito https://web.uanataca.com/it/politiche-di-certificazione nella sua versione aggiornata.

7.1. GENERAZIONE DELLA COPPIA DI CHIAVI

7.1.1. COPPIA DI CHIAVI DELLA CA

La coppia di chiavi delle CA è generata seguendo una procedura di "cerimonia di chiavi" che avviene in un ambiente protetto, all'interno di un perimetro di elevata sicurezza specificatamente destinato a tale scopo.
Le attività svolte durante la "cerimonia" di generazione delle chiavi di certificazione sono registrate, datate e firmate da tutte le persone coinvolte.
Inoltre, l'esecuzione di tali attività avviene in presenza dell'auditor interno ed è documentata in un apposito verbale redatto dal responsabile della sicurezza.
I verbali sono conservati per scopi di controllo e monitoraggio, per un periodo appropriato definito da Uanataca. Per la generazione delle chiavi sono stati utilizzati dispositivi HSM conformi FIPS 140-2 livello 3 e Common Criteria EAL4 +.

UANATACA CNS CA 2020	4.096 bits	20 anni
- Certificati di entità finale	2.048 bits	Fino a 3 anni

7.1.2. CHIAVI DEI TITOLARI

Le chiavi dei Titolari sono generate tramite dispositivi hardware sicuri (QSCD – Qualified Signature Creation Device), in maniera conforme a quanto indicato nel "security target" del dispositivo stesso e attraverso le librerie software fornite dal produttore del dispositivo.
Gli algoritmi e le suite crittografiche utilizzate sono conformi alle specifiche ETSI TS 119 312.
In particolare, le chiavi vengono generate utilizzando l'algoritmo a chiave pubblica RSA, con una lunghezza minima di 2048 bit o chiavi ECDSA equiparabili.

8. DISPONIBILITA' DEL SERVIZIO

Funzionalità del Servizio	**Livello di disponibilità**	**Modalità**
Accesso all'archivio dei certificati	24x7	Fino a 3 anni
Sospensione/Revoca/ Riattivazione	24x7	Servizio di assistenza dalle ore 9 alle ore 18 (lun.-ven), esclusi i festivi. Presso gli Uffici di registrazione secondo gli orari da essi indicati.
Rilascio	Orario di ufficio	Presso gli Uffici di registrazione secondo gli orari da essi indicati.

Con riferimento alle modalità di contatto del Centro Assistenza di Uanataca è possibile inoltrare tutte le richieste al seguente indirizzo di posta elettronica: assistenza@uanataca.com.