Manuale Operativo CNS

Versione 1.0

20 dicembre 2019

INTESI GROUP S.p.A. Via Torino, 48 - 20123 Milano – Italia - Tel: +39 02 676064.1 – www.intesigroup.com

1 Indice

Revisioni

Rev.	Date	Author	Description
1.0	20/12/19	Francesco Barcellini	Prima versione.

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 del “Convitto nazionale Carlo Alberto” di Novara (da ora CNCA).

La CNS è emessa dal CNCA ed i relativi certificati di autenticazione sono emessi dal Certificatore accreditato Intesi Group S.p.A. Le indicazioni di questo documento hanno validità per le attività relative al CNCA in qualità di Ente Emettitore, ad Intesi Group nel ruolo di Certificatore, per gli stessi Titolari e per gli Utenti.

2.1 Riferimenti

[1] “Manuale CP (TSP_Policy)”

Certificate Policy dei certificati qualificati di Intesi Group scaricabile dall’URL

https://www.intesigroup.com/it/documenti/

[2] “Manuale CPS (TSP_Practice_Statements)”

Certificate Practice Statement dei certificati qualificati di Intesi Group scaricabile dall’URL https://www.intesigroup.com/it/documenti/

[3] “Certificati_Qualificati_Termini_Condizioni”

Termini e condizioni di utilizzo dei certificati di Intesi Group scaricabile dall’URL https://www.intesigroup.com/it/documenti/

[4] “Informativa sul trattamento dei dati personali”

Informativa al trattamento dei dati personali di Intesi Group

https://www.intesigroup.com/it/documenti/

2.2 Acronimi

Acronimi	Definizione
AGID	Agenzia per l'Italia Digitale
CA	Certification Authority
CAO	Certificate Authority Officer
CNS	Carta Nazionale dei Servizi
TSPP	TSP Policy
TSPPS	TSP Practice Statement
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IR	Incaricato alla registrazione
PIN	Personal Identification Number
PKI	Public Key Infrastructure – componente per l'emissione dei certificati
PUK	Pin Unblocking key
RAO	Registration Authority Officer
RFC	Request For Comments
TA	Trusted Agent
TIN	Tax Identification Number
TLS	Transport Layer Security
TSP	Trust Service Provider

3 Generalità

3.1 Versione del manuale operativo

La versione del presente “Manuale Operativo” è indicata sul frontespizio. La sola versione da ritenersi valida è quella pubblicata sul sito web della CA https://www.intesigroup.com e sul sito dell’Ente Emettitore.

3.2 Contatti

Intesi Group S.p.A.
Via Torino, 48
20123 Milano (MI) – ITALY
Telefono: +39 02 6760641
Fax: +39 02 67606437
Indirizzo web: http://www.intesigroup.com
Indirizzo e-mail: intesi@intesigroup.com

3.3 Riservatezza delle informazioni personali

L’informativa sul trattamento dei dati e la modalità di elaborazione dei dati degli utenti dei servizi è pubblica e liberamente scaricabile dal sito istituzionale di Intesi Group all’url:

https://www.intesigroup.com/it/privacy/

4 Ruoli previsti

4.1 Certificatore

È l'azienda che fisicamente emette i certificati Certification Authority (CA) svolto dalla società Intesi Group S.p.A accreditata come Qualified Trust Service Provider dal 19/01/2018.

4.2 Ente Emettitore

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

Per questo documento l'Ente emettitore della Carta Nazionale dei Servizi è il "Convitto nazionale Carlo Alberto" di Novara

4.3 Local Registration Authority

La Local Registration Authority (LRA) è una terza parte delegata da Intesi Group a svolgere attività di:

- identificazione e autenticazione (I&A) dei soggetti;
- trasmissione, con procedure sicure, delle informazioni dei soggetti riconosciuti alla CA.
- registrazione dei dati del richiedente e della autorizzazione all'emissione di certificati attraverso appositi strumenti messi a disposizione da Intesi Group.
- validazione e gestione di eventuali richieste di sospensione, revoca e riattivazione;

4.4 Richiedente

Per richiedente si intende la persona che richiede la CNS.

4.5 Titolare

Per titolare si intende la persona che ha in uso le chiavi la CNS.

4.6 RAO

I RAO sono addetti della LRA preposti alle attività di Identificazione, raccolta e trasmissione documentazione e alla registrazione.

4.7 IR

Gli IR sono addetti della LRA preposti alle attività di Identificazione e raccolta della documentazione.

4.8 Relying parties o utilizzatori

Le “Relying Parties” sono tutti i soggetti che fanno affidamento sulle informazioni contenute nei certificati.

4.9 Altri partecipanti

Le attività svolte dalla CA qualificata Intesi Group sono soggette alla supervisione di Agid (Agenzia per l’Italia Digitale).

5 Obblighi del certificatore, del titolare e dei richiedenti

5.1 Obblighi del titolare

Il titolare deve:

- garantire la completezza e la correttezza delle informazioni fornite all'Ente Emettitore o alla LRA per la richiesta della CNS.
- conservare con la massima diligenza la carta CNS al fine di garantire di essere il solo utilizzatore delle chiavi private in essa contenute.
- mantenere in modo esclusivo la conoscenza dei dati per lo sblocco della firma (PIN, PUK) conservandoli con la massima diligenza.
- astenersi dall'utilizzare in modo improprio o fraudolento le chiavi ed i certificati in suo possesso.
- chiedere il blocco della carta se ha fondate ragioni di credere che i dati di sblocco della chiave privata (ad es. codice PIN) siano stati compromessi.
- chiedere la revoca della carta CNS se i dati in esso contenuti sono cambiati o errati.

6 Responsabilità

6.1 Responsabilità dell'Ente emettitore

L'ente emettitore è responsabile

- Della correttezza dei dati identificativi contenuti nella carta CNS e nel certificato di autenticazione (responsabilità delegata ad Intesi Group).
- Della correttezza del codice fiscale e dei dati del titolare contenuti nella carta CNS e riportati nel certificato (responsabilità delegata ad Intesi Group).

- Della sicurezza della produzione, inizializzazione, attivazione e distribuzione della carta (responsabilità delegata ad Intesi Group).

6.2 Responsabilità del produttore

Il produttore deve garantire la sicurezza del circuito di produzione e della conformità della carta in base alla normativa esistente.

6.3 Responsabilità del certificatore

Il certificatore è responsabile della generazione del certificato di autenticazione CNS e dell'eventuale certificato di firma digitale qualificata inserito all'interno della smartcard CNS. Per maggiori dettagli riferirsi ai documenti [1], [2], [3] e [4].

7 Amministrazione del manuale operativo

Il presente Manuale operativo viene redatto, revisionato e aggiornato per conto dell'Ente Emettitore da personale incaricato di Intesi Group S.p.A. Richieste di informazioni o chiarimenti riguardo al presente 'Manuale Operativo' possono essere inviate scrivendo una e-mail all'indirizzo tsp@intesigroup.com.

Ogni versione di questo manuale operativo viene approvato dal dirigente del "Convitto nazionale Carlo Alberto" di Novara.

8 Identificazione del titolare

In questo capitolo sono contenute le procedure per la verifica dell'identità del titolare necessarie per procedere all'emissione della CNS e dell'eventuale certificato di firma digitale.

8.1 Validazione delle identità individuali

Il processo di Identificazione viene condotto dai RAO che devono operare secondo le procedure di identificazione applicate da Intesi Group. Il processo di Identificazione applicato per l'emissione delle carte CNS è il processo "de-visu" che avviene con un incontro fisico tra un RAO ed il richiedente.

8.2 Identificazione de-visu

Il certificatore Intesi Group, in qualità di struttura delegata dall'Ente Emettitore, verifica l'identità del richiedente attraverso un proprio RAO od un RAO di una propria LRA.

8.3 Soggetti abilitati ad effettuare l'identificazione

I soggetti abilitati ad effettuare il riconoscimento sono:

1. Il Certificatore attraverso uno dei propri incaricati (RAO o IR);
2. Un LRA attraverso uno dei propri incaricati (RAO o IR);
3. Pubblico Ufficiale;

8.4 Procedura per l'identificazione

L'identificazione è effettuata da uno dei soggetti elencati al par. 8.3 ed è richiesta la presenza fisica del Richiedente che deve esibire al RAO o all'IR un documento di riconoscimento tra:

1. Carta d'Identità;
2. Passaporto;

Il RAO o l'IR deve verificare che il documento sia valido (non scaduto) e, nel limite del possibile, che non sia falso.

8.5 Richiesta di rilascio della CNS e dei Certificati

Un Titolare per richiedere il rilascio di una CNS e di un eventuale certificato di firma deve:

1. Incontrare il RAO incaricato del riconoscimento.
2. Prendere visione del manuale operativo [1]e [2]
3. Leggere i termini e condizioni del servizio [3].
4. Seguire le procedure di riconoscimento adottate dal Certificatore esibendo il documento di riconoscimento e fornendo i dati personali richiesti.
5. Firmare la richiesta di registrazione con cui richiede l'emissione della CNS, accettare i termini e condizioni del servizio e il consenso al trattamento dei dati personali.

8.6 Informazioni del soggetto richieste

Per richiedere una smartcard CNS il richiedente deve fornire le seguenti informazioni:

- Nome e cognome;
- Data di nascita, città di nascita, provincia di nascita e stato di nascita;
- Stato, provincia, città e indirizzo di residenza;
- Numero di telefono;
- Indirizzo e-mail;
- Codice fiscale;
- Documento di identità valido;

9 Operatività

Questo capitolo descrive le operazioni relative all'emissione, rinnovo, revoca e sospensione dei certificati contenuti nella CNS.

9.1 Emissione e consegna della CNS al Titolare

Il processo di personalizzazione è avviato dal RAO alla presenza del titolare attraverso il processo di personalizzazione della CNS e svolto in seguito al processo di identificazione e registrazione del titolare della CNS.

Il processo di emissione è svolto in conformità a quanto descritto nel documento [2].

9.2 Registrazione dei dati dei Titolari

Le attività di registrazione dei dati dei Titolari seguono quanto descritto all'interno del documento [2].

9.3 Generazione e protezione delle coppie di chiavi

Le coppie di chiavi per i certificati di autenticazione CNS e la coppia di chiavi per i certificati per la Firma Digitale sono generate in fase di personalizzazione attraverso gli strumenti software messi a disposizione del produttore della smartcard che utilizzano funzionalità messe a disposizione della smartcard CNS.

Le chiavi generate sono di lunghezza di almeno 2048bit.

9.4 Rilascio dei certificati di Autenticazione CNS e di Firma Digitale

Completata la fase di creazione delle coppie di chiavi si procede all'emissione dei certificati attraverso le applicazioni informatiche messe a disposizione del RAO dal certificatore e dal produttore delle smartcard. Queste procedure:

1. Verificano la correttezza delle richieste di certificato assicurandosi:
    - Il titolare sia in possesso delle relative chiavi private;
    - Le chiavi siano valide e conformi alla normativa vigente;

- I dati necessari per l'emissione dei certificati siano completi e corretti;

2. Generano i certificati di firma e autenticazione;
3. Salvano i certificati generati all'interno della smartcard CNS;

Le procedure seguite per la generazione dei certificati rispettano e sono coerenti con quanto scritto all'interno del documento [2] di Intesi Group.

9.5 Validità dei certificati

I certificati vengono emessi con validità di tre anni a partire dalla data di emissione della smartcard CNS. In caso di revoca della smartcard la validità del certificato cessa alla data di revoca contenuta all'interno delle CRL pubblicate dal certificatore.

9.6 Interdizione della CNS

Una CNS può essere interdetta temporaneamente oppure definitivamente revocando o sospendendo i certificati in essa contenuti. L'interdizione viene resa pubblica attraverso la pubblicazione della CRL che contiene il riferimento al certificato e la data da cui i certificati non devono più essere considerati validi.

La procedura di revoca è irreversibile mentre la procedura di sospensione è un blocco temporaneo che può essere tolto attraverso la riattivazione oppure reso definitivo attraverso una successiva revoca.

Le CRL sono gestite e pubblicate dal certificatore secondo le modalità descritte nel documento [2] di Intesi Group. Il certificato può essere revocato o sospeso su richiesta del:

1. titolare della smartcard;
2. dal RAO su richiesta del titolare;
3. dal Certificatore;

4. dall'Ente Emettitore;

È onere del Certificatore, attraverso le proprie procedure, di identificare ed autenticare il richiedente della revoca e sospensione.

9.6.1 Revoca dei Certificati

Le condizioni che possono causare una revoca di una smartcard CNS sono:

1. Il titolare richiede la revoca del certificato;
2. la chiave privata viene persa, rubata o potenzialmente compromessa;
3. il titolare non ha più il controllo esclusivo della chiave privata perché i dati di attivazione della chiave privata (codice PIN e PUK) sono stati compromessi.
4. l'utente non può più utilizzare la chiave del dispositivo protetto (ad. esempio nel caso in cui la smartcard sia guasta).
5. le informazioni del Titolare contenute nei Certificati sono variate.
6. vi è una condizione di non conformità del presente manuale operativo.

Le procedure e le modalità di richiesta di revoca dei Certificati sono conformi a quanto descritto all'interno del documento [2] di Intesi Group.

9.6.2 Sospensione dei Certificati

La sospensione in una delle seguenti circostanze:

1. Il Certificatore riceve una richiesta di revoca contenente informazioni incomplete.
2. Il Titolare, il Certificatore o l'Ente Emettitore acquisiscono elementi che mettono in dubbio la validità del certificato;
3. Sono presenti dubbi riguardanti la salvaguardia del dispositivo di conservazione delle chiavi e delle quantità di autenticazione;
4. È necessaria un'interruzione della validità del certificato.

Le procedure e le modalità di richiesta di sospensione dei Certificati sono conformi a quanto descritto all'interno del documento [2] di Intesi Group.

9.6.3 Riattivazione dei Certificati

La riattivazione di una smartcard CNS può essere fatta solamente se i certificati in essa contenuti sono sospesi e consiste nelle procedure di riattivazione dei certificati messa a disposizione del Certificato.

Le procedure e le modalità di richiesta di riattivazione dei Certificati sono conformi a quanto descritto all'interno del documento [2] di Intesi Group.

10 Disponibilità del servizio

Servizio di registrazione e generazione:

- richiesto attraverso i RAO e gli IR, in base agli orari forniti dalle LRA di appartenenza.

Servizio di revoca delle smartcard CNS:

- In modalità self-service sono disponibili 24 ore al giorno, 7 giorni a settimana.
- richiesto attraverso i RAO, in base agli orari forniti dalle LRA di appartenenza.

Servizio di sospensione e riattivazione delle smartcard CNS:

- In modalità self-service sono disponibili 24 ore al giorno, 7 giorni a settimana.
- richiesto attraverso i RAO, in base agli orari forniti dalle LRA di appartenenza.

Pubblicazione stato dei certificati

- Le CRL sono disponibili 24 ore al giorno, 7 giorni a settimana.
- Il servizio OCSP è disponibile 24 ore al giorno, 7 giorni a settimana.

Documenti di servizio

- sono disponibili 24 ore al giorno, 7 giorni a settimana sul sito istituzionale del certificatore.