Allegato 1 del Capitolato Tecnico

INFOCAMERE S.C.P.A.

"Servizi di Certification Authority"

*** *** ***

CAPITOLATO TECNICO - Specifiche tecniche CMS

*** *** ***

INDICE

1 Introduzione al documento 3
1.1 Scopo e campo di applicazione del documento 3
1.2 Termini e definizioni ..... **Errore. Il segnalibro non è definito.**
2 Card Management System 4
3 Funzionalità del CMS 5
3.1 Configurazione Camere di Commercio 5
3.1.1 Uffici di Registrazione 5
3.1.2 Operatori 5
3.1.3 Esportazione e importazione incaricati tra uffici 5
3.2 Servizi per il rilascio e la gestione dei certificati 5
3.2.1 Gestione del ciclo di vita delle richieste CNS e Firma Digitale 5
3.2.2 Emissione CNS e Firma Digitale 6
3.2.3 Rinnovo CNS e Firma Digitale 6
3.3 Funzionalità di servizio per gli operatori in CMS 6
3.3.1.1 Registrazione della richiesta e stampa del modulo 7
3.3.1.2 Produzione dei certificati e assegnazione dei dispositivi 8
3.3.1.3 Operazioni sui certificati 8
3.4 Funzionalità utente da Sito WEB 8
3.4.1 Rilascio in modalità remota 9
3.4.1.1 Piattaforma WebID 9
3.4.2 Interazioni con il Card Management System 10

1 Introduzione al documento

1.1 Scopo e campo di applicazione del documento

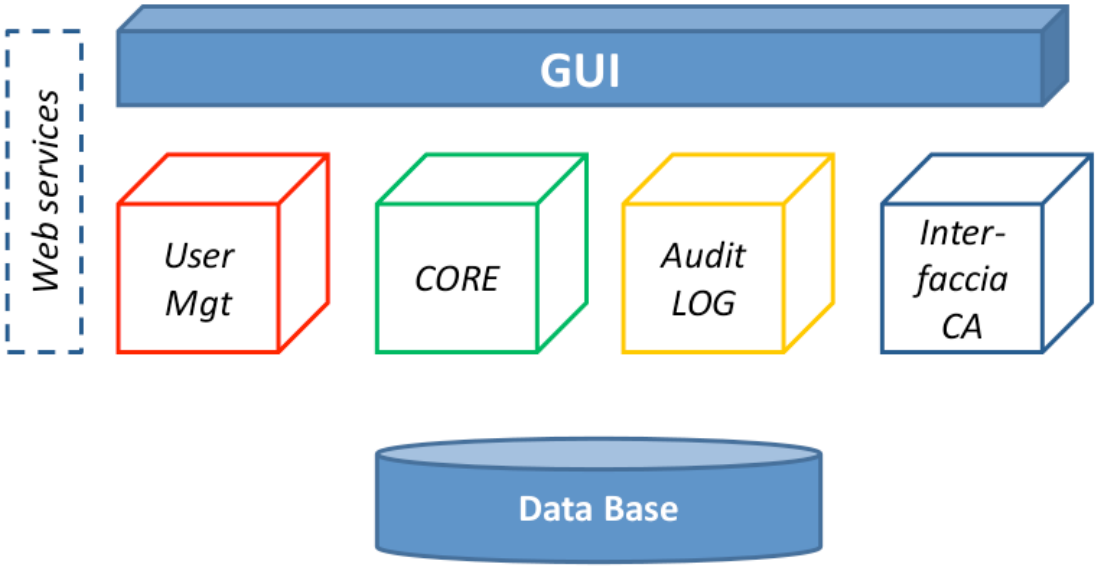
Il documento ha l'obiettivo di descrivere il Card Management System di InfoCamere, per la gestione del ciclo di vita di smart card e token per la firma digitale, fruibile dal Sistema Camerale.

2 Card Management System

Il CMS è un sistema informatico fruibile attraverso una web application che permette la gestione completa del processo di rilascio della firma digitale. In particolare il CMS gestisce la registrazione degli utenti, l'emissione dei certificati digitali e dei dispositivi di firma digitale qualificata ed il loro ciclo di vita.
La web application mantiene organizzati in un database tutti i dati relativi alle Camere di Commercio fruitrici del servizio, dei titolari richiedenti i certificati e dei dispositivi di firma.

Il CMS, grazie ad un gateway (Interfaccia CA), permette l'emissione di certificati digitali da diversi Trusted Service Providers a seconda dell'esigenza dell'organizzazione cliente.

Di seguito viene riportata l'architettura applicativa del sistema.



Il CMS è un'applicazione modulare composta dai seguenti componenti:

- **Database** che immagazzina tutte le informazioni relative al ciclo di vita dei certificati, ai dati anagrafici dei titolari, agli operatori di registrazione ed incaricarti, agli uffici, ecc. Contiene inoltre una serie di tabelle di sistema e dizionari utilizzati per la corretta esecuzione delle procedure (ad esempio le tabelle istat dei comuni, le tabelle relative alle emissioni pregresse ecc.
- **Core** che costituisce il motore del sistema e gestisce le interazioni con i vari moduli e l'accesso al database.
- **User management** che si occupa della creazione degli utenti del sistema e la relativa associazione ai profili e agli sportelli.
- **Interfaccia C**A che è il modulo contenente le interfacce verso la CA per le operazioni di enrollment, sospensione, riattivazione, revoca, verifica stato corrente. Il modulo contiene anche le funzionalità di interazione con altri sistemi esterni camerali, quali Diritto Annuo, Sistema Pagamenti, ecc
- **Web service** che permette ai cittadini di richiamare alcune funzionalità del CMS dal portale informativo www.card.infocamere.it. Tali operazioni sono la sospensione dei certificati, la riattivazione, la richiesta di emisione in modalità remota (dal portale).
- **Interfaccia grafica GUI** per la fruizione di tutte le funzionalità da parte degli utenti.

L'accesso all'applicazione è profilato in base al ruolo ed ai privilegi dell'utente:
- nelle funzionalità, cioè mostrando all'utente solamente le funzioni da esso attuabili;
- nella vista dei dati, cioè permettendo l'accesso ai soli dati di diretta competenza.

3 Funzionalità del CMS

3.1 Configurazione Camere di Commercio

Il CMS è in grado di gestire l'anagrafica di ogni Camera di Commercio e la sua afferenza alle CA per l'emissione dei certificati e la loro configurazione.

Ogni Camera di Commercio (o altro soggetto equiparato) può essere configurata perché rispecchi la propria struttura logistico-organizzativa (sedi/uffici/operatori e relativi mandati. La struttura logistico-organizzativa di ogni Camera di Commercio o altro soggetto equiparato è la seguente:

- l'Ente può avere più sedi;
- ogni sede può avere più uffici;
- in ogni ufficio possono operare più soggetti, anche con ruoli diversi;
- ad ogni soggetto viene assegnato uno specifico mandato, con durata e profilo propri, ovvero specifiche abilitazioni.

Ogni Ente è totalmente autonomo nel definire il numero di operatori addetti al servizio, che può variare dalle poche unità alle decine (e centinaia in riferimento agli Incaricati alla Registrazione).

3.1.1 Uffici di Registrazione

A livello di singolo Ufficio di Registrazione, il CMS permette l'estrazione degli operatori afferenti e i dati di produzione/approvazione/registrazione delle richieste effettuate dalla stessa.

3.1.2 Operatori

Il CMS prevede la gestione di operatori per ogni ufficio di registrazione, la loro prototipazione nei seguenti gruppi:

- Incaricato al Riconoscimento (IR)
- Addetti alla registrazione RAO
- Help Desk

e la gestione granulare per operatore dei loro permessi. Inoltre il sistema è in grado di assegnare e far gestire ad un operatore piu' incarichi su uffici di registrazione o su Camere di Commercio diverse.

3.1.3 Esportazione e importazione incaricati tra uffici

In caso di chiusura di un ufficio di registrazione o di un suo spostamento sono disponibili delle procedure per la movimentazione degli operatori da un ufficio ad un altro in maniera rapida.

3.2 Servizi per il rilascio e la gestione dei certificati

Il paragrafo descrive le principali caratteristiche dei servizi di rilascio e gestione dei certificati di sottoscrizione ed autenticazione CNS, attraverso il CMS InfoCamere.

3.2.1 Gestione del ciclo di vita delle richieste CNS e Firma Digitale

Attraverso l' interfaccia di amministrazione gli operatori hanno la possibilità di registrare le richieste CNS e Firma Digitale, precompilare i dati del titolare interrogando specifici servizi InfoCamere collegati al Registro Imprese, gestire il pagamento attraverso chiamata a servizio specifico. La procedura di Approvazione impedisce i cambiamenti dei dati di un titolare per evitare qualsiasi modifica prima della produzione.

Attraverso l'interfaccia di amministrazione LCM (Life Cycle Management) gli operatori abilitati possono effettuare la revoca e la sospensione dei certificati.

Il CMS espone inoltre delle API che permettono le stesse operazioni in maniera autonoma (self-service) ai clienti attraverso il portale di card.infocamere.it.

3.2.2 Emissione CNS e Firma Digitale

Il CMS consente di emettere certificati per nome e per conto del titolare richiedente. Grazie alla presenza delle buste cieche o scratchcard e ad un particolare workflow di emissione che protegge i segreti, le carte non possono essere né utilizzate né recuperate da nessun operatore del CMS o di sistema se non correttamente prodotte. Una volta che la carta sia stata correttamente prodotta, solo il cliente finale in possesso dei segreti è in grado di accedere ed utilizzare il token o la smartcard. Di seguito si riportano i passi:

a) l'operatore camerale si collega al CMS tramite il browser;
b) l'operatore sceglie il lettore; quindi, viene verificato che il dispositivo da inizializzare sia associato alla CA che dovrà produrre il certificato; i PIN e PUK di trasporto vengono sostituiti da due PIN e PUK random;
c) viene creata una Certificate Signing Request prelimirare contente i dati del titolare;
d) sulla carta vengono generate le coppie di chiavi;
e) le CSR vengono finalizzate con le chiavi pubbliche e con la chiave privata; vengono firmate le CSR (prova di possesso);
f) tramite CMS, le due CSR firmate vengono inviate alla CA, secondo modalità specifiche per ogni CA;
g) la CA restituisce i certificati debitamente firmati, secondo modalità specifiche;
h) i certificati sono inseriti nel CMS ed inviati alla componente del sistema che si incarica di acquisirli nel dispositivo;
i) il CMS conferma che l'operazione di enrollment ha avuto successo;
j) i PIN e PUK vengono sostituiti con quelli della scratch card.

3.2.3 Rinnovo CNS e Firma Digitale

Attraverso uno specifico software di Gestione Rinnovi (scaricabile direttamente dal sito card.infocamere.it) è possibile rinnovare un certificato appartenente al circuito Camerale in modalità Desk, ovvero in Camera, o in modalità Self-Service, in autonomia. In quest'ultima modalità un titolare in possesso della carta e del PIN è in grado, in completa autonomia, dopo aver effettuato il pagamento, di effettuare il rinnovo da casa, senza doversi recare in Camera. In particolare la procedura di
rinnovo avviene secondo i seguenti step:

a) verifica che il CMS sia attivo e i sistemi di enrollment funzionino (ad esempio non è possibile fare enrollment dopo le 21);
b) richiesta dell'inserimento del dispositivo e sblocco tramite PIN;
c) riepilogo dei passi che si stanno per compiere per avere conferma;
d) richiesta del pagamento (tramite sistema Pagamenti InfoCamere oppure con carta di credito);
e) esecuzione delle operazioni di enrollment, in modo simile all'emissione, gestendo le diverse modalità proprie di ogni CA;
f) scrittura del certificato rinnovato sul dispositivo.

3.3 Funzionalità di servizio per gli operatori in CMS

Le funzioni principali del CMS sono: registrazione della richiesta e produzione cartacea o PDF dei relativi moduli, produzione di certificati e rilascio dei dispositivi, verifica della validità dei certificati, sospensione ed eventuale riattivazione dei certificati, revoche dei certificati, rinnovi dei certificati.

Gli operatori fanno uso di un sistema di autenticazione con dispositivo CNS (Smart card / Token USB). Ogni Camera di Commercio (o altro soggetto equiparato) vede e interviene solo sui dati di propria competenza.

Di seguito una descrizione dei ruoli coinvolti nei diversi processi:

- **Gli incaricati** al riconoscimento (IR) sono abilitati solo alle funzioni di data entry dei dati dei richiedenti, stampa/produzione pdf dei moduli e consegna dei dispositivi, ma non alle funzioni di emissione /rinnovo dei certificati e dei dispositivi. Deve inoltre essere possibile profilare ciascun mandato a ciascun incaricato in modo che sia possibile gestire sia la durata dell'incarico che come questi operi, ovvero se telematicamente o meno, sia in relazione alle funzioni di data entry, che di pagamento.
- **Gli addetti RAO** intervengono sulle proprie registrazioni e lavorano sulle registrazioni effettuate da qualsiasi incaricato al riconoscimento della propria Camera. Oltre alle funzioni degli incaricati al riconoscimento, essi emettono certificati e dispositivi e, sulla base del proprio profilo, svolgono tutte le funzioni necessarie alla corretta gestione del servizio.
- **Gli Operatori di Help Desk** operano analogamente agli Addetti in un ambiente loro riservato, analogo a quello di produzione, mentre nell'ambiente di produzione agiscono come Addetti ma solo in modalità di visualizzazione, escludendo qualsiasi forma di registrazione che non attenga il supporto diretto all'utente finale.

3.3.1.1 Registrazione della richiesta e stampa del modulo

La registrazione della richiesta avvenire come segue:
- inserendo online i dati scritti in un modulo compilato precedentemente in forma cartacea;
- inserendo online i dati per poi stampare il modulo di richiesta con i dati;

La funzione consente l'inserimento dei seguenti dati:
- i principali dati anagrafici del richiedente, tra cui codice fiscale, nome, cognome, data e luogo di nascita, indirizzo di residenza, estremi documento riconoscimento.
- la chiave (CCIAA + numero REA) e altri dati dell'impresa per cui viene richiesto il rilascio del dispositivo:
  - la funzione verifica, nel Registro delle Imprese, se il richiedente è legale rappresentante dell'impresa tenendo conto della facoltà di ciascuna Camera di Commercio di identificare le cariche da includere anche ai fini della determinazione del "primo rilascio all'impresa";
  - la funzione verifica nel Diritto Annuale se l'impresa ha pagato il diritto previsto alla Camera di Commercio e segnalarlo all'addetto / incaricato, tenendone conto per la determinazione del "primo rilascio all'impresa" secondo quanto indicato dalla Camera; la funzione verifica, controllando l'archivio dei rilasci precedenti (anche di diversi fornitori), se sia il "primo rilascio per l'impresa" (in assoluto o per tipologia di dispositivo CNS, a seconda delle indicazioni della Camera) e segnalarlo all'addetto / incaricato; infatti per il primo rilascio sono previste, per i richiedenti, tariffe particolari praticate dalla Camera.
  - Se la Camera lo richiede, il sistema impone, per uno o più uffici, la determinazione del "primo rilascio all'impresa" o del rilascio normale sulla base degli elementi indicati nei punti precedenti.

In caso di richiedente presente nel Registro delle Imprese la funzione riporta automaticamente i dati ufficiali (anagrafica e residenza) ricavati dal Registro delle Imprese, evitando la necessità di effettuare un data entry manuale di tutti i dati. Nel caso la persona non sia presente nel Registro delle Imprese ma abbia effettuato una richiesta di prenotazione tramite funzionalità online, la funzione acquisisce i dati anagrafici inseriti con la richiesta prenotazione. Nel caso in cui il richiedente sia già titolare di altri certificati la funzione consente di acquisire le informazioni relative all'ultimo precedente certificato.

Le informazioni acquisite dalle varie fonti sono comunque essere modificabili, nella nuova richiesta.

La funzione permette inoltre l'inserimento di un indirizzo email del richiedente per cui il certificato di autenticazione CNS deve poter firmare / cifrare / decifrare i messaggi, secondo gli standard previsti per la posta elettronica.

L'indirizzo email del richiedente per comunicazioni, invece, è invece previsto come dato obbligatorio al fine di agevolare l'invio degli avvisi di scadenza dei certificati. Tale indirizzo è modificabile in qualsiasi momento anche direttamente dal titolare e può essere diverso da quello contenuto nel certificato.

La funzione consente la produzione dei moduli da far firmare al richiedente, sia in forma cartacea, sia in forma digitale. Per la Camera di Bolzano tale funzionalità consente la produzione del modulo nella versione in tedesco.

3.3.1.2 Produzione dei certificati e assegnazione dei dispositivi

La funzione presenta all'addetto le registrazioni online effettuate dagli operatori afferenti alla propria Camera di Commercio, attraverso opportune ricerche basate almeno su nominativo dell'operatore, ufficio e periodo di registrazione (e qualsiasi combinazione di questi).

La funzione consente:

- la verifica, la modifica (nel rispetto della vigente normativa), l'approvazione o l'annullamento della registrazione effettuata,
- l'emissione dei certificati previsti (certificato di autenticazione CNS e certificato qualificato di sottoscrizione per firma digitale) sulla tipologia di dispositivo prescelta: Smart card o Token USB, (v. par 3.2.2).
- la registrazione delle operazioni con tutti i dati necessari, ad esempio l'assegnazione del dispositivo,
- la stampa del modulo previsto in fase di registrazione con l'eventuale aggiunta di informazioni relative al rilascio,
- la stampa di una ricevuta di consegna da far firmare al titolare nel momento della consegna.

Il servizio, in particolare:

- controlla che la tipologia di dispositivo inserito corrisponda a quello previsto nella richiesta;
- opera a livello di dispositivo, ovvero tratta contemporaneamente ed in modo equivalente i certificati in esso contenuti;
- fornisce chiara evidenza dell'esito della produzione di un dispositivo, indicando nel dettaglio i dati significativi del dispositivo stesso e dei certificati in esso presenti;
- in caso di errore: consente agli addetti di resettare il dispositivo e ripetere la fase di produzione sullo stesso dispositivo;
- consente la stampa della lettera di accompagnamento del dispositivo.

Il servizio gestisce l'interazione facoltativa, se consentita dalle abilitazioni assegnate dalla Camera a ciascun operatore, con uno o più dei seguenti sistemi:

- pagamenti elettronici InfoCamere o con carta di credito,
- gestione documenti degli incassi.

3.3.1.3 Operazioni sui certificati

Sospensione/Riattivazione

La funzione consente all'addetto e all'operatore di Help Desk di sospendere i certificati (CNS e firma digitale), su dispositivi (Smart card o Token USB) rilasciati dalla Camera di Commercio.

Rinnovo

La funzione consente all'addetto di rinnovare i certificati (CNS e firma digitale), su dispositivi (Smart card o Token USB) rilasciati dalla Camera di Commercio.

Revoca

La funzione consente all'addetto di revocare i certificati (CNS o firma digitale), su dispositivi (Smart card o Token USB) rilasciati dalla Camera di Commercio.

3.4 Funzionalità utente da Sito WEB

Il sito web **card.infocamere.it**, erogato dall'infrastruttura di InfoCamere che ne cura la manutenzione e la gestione, è interamente dedicato ai servizi di Firma Digitale; contiene i documenti, i software e le altre

informazioni correlate ai certificati e ai dispositivi, ad esempio: l'installazione, l'utilizzo, le procedure, tutte le normative di riferimento, tutti i manuali e la documentazione di riferimento, la modulistica etc.

All'interno del sito, il colloquio con i sistemi di Certification Authority, per le funzionalità LCM (Life Cicle Management) (es. richiesta di sospensione, riattivazione, ecc.) è mediato dal CMS, per tramite di web-services.

Il sito rende disponibili tutte le funzioni operative direttamente destinate a richiedenti e titolari, che si identificano mediante il proprio certificato di autenticazione, quali:

- sospensione / riattivazione diretta dei propri certificati;
- funzione di modifica del proprio indirizzo di posta elettronica per le comunicazioni;
- funzione di rilascio in modalità remota;

Il sito consente all'utente, tramite richiesta e verifica delle informazioni necessarie (es. codici segreti), di **sospendere**, ed eventualmente **riattivare** (se previsto), i propri certificati con una funzione che effettua automaticamente tale operazione senza la necessità di intervento umano. Il sito avvisa l'utente del tempo massimo che intercorre tra la richiesta e l'effettiva efficacia della sospensione.

Il servizio via portale consente di **modificare la casella email** del Titolare, comunicata in fase di richiesta e necessaria per le comunicazioni allo stesso (es. servizio avvisi a scadenza).

Le funzionalità di rilascio in **modalità remota** sono trattate nel paragrafo successivo.

A titolo puramente informativo, si evidenzia che il sito offre funzionalità connesse all'attivazione e gestione della Firma Digitale Remota, non oggetto della presente gara.

3.4.1 Rilascio in modalità remota

Nel sito web **card.infocamere.it** sono disponibili le funzionalità connesse al rilascio di dispositivi in modalità "remota", ovvero con riconoscimento a distanza del titolare, attraverso l'accesso a funzionalità on-line presente sul portale card.infocamere.it.

Tramite le funzionalità online, è consentito al titolare:

- di accedere all'area dedicata alla richiesta di una CNS
- di scegliere la Camera di Commercio, tra quelle aderenti, a cui richiede il nuovo dispositivo e la tipologia del dispositivo;
- di scegliere la modalità di consegna (Spedizione a Domicilio o Ritiro in Camera con prenotazione)
- di identificarsi mediante il proprio dispositivo CNS, in corso di validità, ovvero tramite sistema basato sull'utilizzo di webcam (WebID) per il riconoscimento del richiedente (v par 3.4.1.1);
- di inserire le informazioni previste per la registrazione; nel caso di autenticazione via CNS, alcuni dei dati identificativi dell'utente sono precaricati a sistema;
- di firmare digitalmente la richiesta di nuovi certificati nel nuovo dispositivo;
- di pagare online il dispositivo tramite analoghi sistemi di pagamento elettronico previsti per i rinnovi;
- di acquisire tutta la contrattualistica e la documentazione prevista.

A completamento della fase di registrazione e pagamento utente, l'operatore RAO della CCIAA selezionata dall'utente si ritroverà una richiesta di rilascio proveniente dal portale, in stato "pronta per essere prodotta"; e procede con l'emissione del dispositivo; parallelamente il CMS procede con l'invio via email al titolare della scratch card con le credenziali.

In funzione della scelta operata nelle fasi precedenti, il dispositivo sarà spedito all'operatore, piuttosto che reso disponibile in Camera per il ritiro da parte del Titolare alla data fissata, tramite apposita funzionalità calendario.

3.4.1.1 Piattaforma WebID

Nel caso in cui il richiedente non sia in possesso di dispositivo CNS in corso di validità, il sistema di rilascio con modalità remota consente l'utilizzo di una piattaforma basata su webcam (WebID), per il riconoscimento.

Per effettuare il riconoscimento online con la piattaforma WebID, il richiedente potrà prendere appuntamento con un operatore incaricato. Al giorno ed all'orario prestabilito si collegheranno entrambi alla piattaforma e seguiranno un processo ben definito che consentirà all'operatore:

- di acquisire il consenso da parte del richiedente;
- di visualizzare la faccia della persona con sufficiente dettaglio;
- di confrontare la persona con il documento di identità che sarà acquisito mediante la piattaforma.

Una volta completata la procedura di riconoscimento WebID online, il sistema genera un codice che verrà inviato all'utente mediante email. Attraverso tale codice il richiedente potrà accedere al portale di servizio ad un'apposita sezione per la richiesta del dispositivo CNS.

Questo processo ricalca il processo precedentemente descritto per i possessori di CNS ad esclusione del primo passo di autenticazione con CNS che, in questo caso, è sostituito dall'autenticazione con il codice (generato dalla piattaforma) e dalla firma della richiesta con un certificato temporaneo, valido per tutta la durata dell'operazione (certificato one-shot). A conclusione del processo, l'utente riceverà via email la scratch card con le credenziali.

3.4.2 Interazioni con il Card Management System

Il portale card.infocamere.it prevede le seguenti interazioni con il sistema di gestione dei certificati, che risulta trasparente per l'utente finale. Tali interazioni riguardano alcuni specifici momenti della gestione dei certificati:

Sospensione diretta dei certificati
A seguito della richiesta Titolare, il portale, con protocollo HTTPS propone un form di sottomissione dati con campi identificativi dello stesso, il codice di revoca e la causale, richiesti per la sospensione.

Questi dati sono passati al CMS tramite l'invocazione di un servizio e serviranno a far attivare la procedura di sospensione del certificato. Il servizio comunica in modalità sincrona l'esito dell'operazione (OK/KO con messaggio di errore) in modo da permettere alla pagina del sito informativo di mostrare all'utente un feedback.

Riattivazione di un certificato sospeso
Lo schema è lo stesso di quello riportato nel caso precedente. I dati di riattivazione sono passati al CMS tramite invocazione di apposito servizio.

Cambio email
Il dato aggiornato è registrato nel CMS, tramite invocazione di apposito servizio.

Rilascio dispositivo in modalità remota
Rispetto al processo sopra descritto, che prevede 2 diverse modalità di riconoscimento e autenticazione dell'utente Titolare, è prevista interazione con il sistema CMS relativamente a:

- Configurazione CMS, in funzione della tipologia di servizio di *rilascio in modalità remota*, a seconda del tipo di autenticazione (CNS/WebID) e della modalità di ritiro (a domicilio/presso la Camera).
- Controllo in fase di richiesta, sul CMS di eventuali altre richieste pendenti.
- Recupero dei dati anagrafici, in presenza di registrazioni in archivio CMS.
- Registrazione dati richiesta sul CMS.