MANUALE OPERATIVO PER L'EMISSIONE E L'UTILIZZO DELLA CARTA NAZIONALE DEI SERVIZI DELLA REGIONE MARCHE

CARTA RAFFAELLO

Versione 1.0 - novembre 2005

SOMMARIO

Capitolo 1

Introduzione

La progressiva disponibilità di servizi on-line erogati dalla pubblica amministrazione rende necessarie modalità di accesso sicure, facili da utilizzare per i servizi di tutte le amministrazioni.

Lo standard di riferimento che deve essere rispettato per l'accesso a tali servizi è "Carta Nazionale di accesso ai Servizi" o "Carta Nazionale dei Servizi".

La Carta Nazionale dei Servizi della Regione Marche è denominata "Carta Raffaello".

1.1 Obiettivi e contenuto del documento

Questo documento è il **Manuale Operativo** relativo al circuito di emissione della Carta Raffaello.

1.2 Quadro normativo di riferimento

I documenti di riconoscimento in formato elettronico compaiono nel nostro ordinamento giuridico con la legge 15 maggio 1997 n. 127 che all'articolo 2, comma 10, successivamente sostituito dall'articolo 2 comma 4 della legge 16 giugno 1998 n. 191, stabilisce: "*con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, sono individuate le caratteristiche e le modalità per il rilascio della carta di identità e di altri documenti di riconoscimento muniti di supporto magnetico o informatico. La carta di identità e i documenti di riconoscimento devono contenere i dati personali e il codice fiscale e possono contenere anche l'indicazione del gruppo sanguigno, nonché delle opzioni di carattere sanitario previste dalla legge. Il documento, ovvero il supporto magnetico o informatico, può contenere anche altri dati, al fine di razionalizzare e semplificare l'azione amministrativa e l'erogazione dei servizi al cittadino, nel rispetto della legge 31 dicembre 1996, n. 675, e successive modificazioni, nonché le procedure informatiche e le informazioni, che possono o debbono essere conosciute dalla pubblica amministrazione o da altri soggetti, ivi compresa la chiave biometrica, occorrenti per la firma digitale ai sensi dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59, e dei relativi regolamenti di attuazione; analogo documento contenente i medesimi dati è rilasciato a seguito della dichiarazione di nascita. La carta di identità potrà essere utilizzata anche per il trasferimento elettronico dei pagamenti tra soggetti privati e pubbliche amministrazioni. Con decreto del Ministro dell'interno, sentite l'Autorità per l'informatica nella pubblica amministrazione e la Conferenza Stato-città ed autonomie locali, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione delle carte di identità e dei documenti di riconoscimento di cui al presente comma. Le predette regole sono adeguate con cadenza almeno biennale in relazione alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche. La carta di identità può essere rinnovata a decorrere dal centottantesimo giorno precedente la scadenza, ovvero, previo pagamento delle spese e dei diritti di segreteria, a decorrere dal terzo mese successivo alla produzione di documenti con caratteristiche tecnologiche e funzionali innovative. Nel rispetto della disciplina generale fissata dai decreti di cui al presente comma e nell'ambito dei rispettivi ordinamenti, le*

pubbliche amministrazioni possono sperimentare modalità di utilizzazione dei documenti di cui al presente comma per l'erogazione di ulteriori servizi o utilità".

Il decreto del Presidente del Consiglio dei Ministri del 22 ottobre 1999, n. 437 ha quindi definito il regolamento per il rilascio della carta di identità elettronica e del documento di identità elettronico, mentre il decreto del Ministro dell'interno del 19 luglio 2000 ha fissato le relative regole tecniche e di sicurezza.

La Carta Nazionale dei Servizi è introdotta nel quadro normativo italiano dal Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica 28 dicembre 2000, n. 445), modificato dal decreto legislativo 23 gennaio 2002 n.10 e dal decreto del Presidente della Repubblica 7 aprile 2003 n. 137, in attuazione della direttiva europea 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.

Nel Testo unico la Carta Nazionale dei Servizi è definita come "*il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalla pubblica amministrazione*" (articolo 1 lettera bb). L'articolo 36 del citato testo tratta, al comma 4, l'utilizzo della carta per i pagamenti informatici(1) ed al comma 5 le regole tecniche(2). Il comma 2 dell'articolo 38 del Testo unico sancisce il valore legale del riconoscimento mediante carta elettronica nell'ambito dei servizi on-line:

Le istanze e le dichiarazioni inviate per via telematica sono valide:
a) se sottoscritte mediante la firma digitale, basata su di un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura;
b) ovvero quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi.

Con tale comma viene così delineato il campo di utilizzo della firma digitale e delle carte elettroniche nei rapporti con la pubblica amministrazione: la prima è lo strumento per la validazione di atti informatici in analogia alla sottoscrizione autografa, CIE e CNS sono strumenti che consentono di utilizzare i servizi di e-government e di inoltrare istanze e dichiarazioni nell'ambito di tali servizi.

1.3 Regolamento di attuazione

L'attuazione di quanto previsto nel Testo unico è disciplinata dal 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".

In tale decreto si precisa che la Carta Nazionale dei Servizi è emessa dalle pubbliche amministrazioni interessate "*al fine di anticiparne le funzioni di accesso ai servizi in rete delle pubbliche amministrazioni*" (art. 2 comma 1). Quindi la CNS è intesa quale strumento "ponte" verso la carta d'identità elettronica, che resta il mezzo nazionale per l'identificazione in rete.

La CNS viene emessa se l'utente non è in possesso della Carta d'Identità Elettronica(3). Al momento dell'emissione l'amministrazione, oltre a verificare tale condizione, controlla i dati identificativi utilizzando i servizi telematici resi disponibili dall'Indice nazionale delle anagrafi(4). Se i controlli hanno esito positivo, l'amministrazione emette la CNS ed

aggiorna l'indice inviando il codice numerico identificativo della carta e le date di rilascio e di scadenza (art. 2 comma 3).

Strutturalmente, la CNS è una smart card che contiene un certificato elettronico per l'autenticazione in rete del titolare. Tale certificato deve essere emesso da un certificatore abilitato al rilascio dei certificati per la firma digitale[5] (art. 3 comma 1).

Il decreto rinvia alle regole tecniche la definizione delle proprietà informatiche della carta, mentre, per quanto concerne l'aspetto esteriore, impone unicamente che sul dorso sia presente la dicitura "CARTA NAZIONALE DEI SERVIZI" ed il nome della pubblica amministrazione che l'ha emessa (art. 3 comma 4).

Oltre ai dati comuni a tutte le CNS (descritti nelle regole tecniche), la carta può contenere informazioni aggiuntive, ossia *indicazioni di carattere individuale generate, gestite e distribuite dalle pubbliche amministrazioni per attività amministrative e per l'erogazione dei servizi al cittadino*, con l'eccezione dei dati personali sensibili (art. 4 comma 1).

Il comma 2 dell'articolo 4 stabilisce il principio secondo cui i dati personali presenti nella carta (compreso il codice fiscale) devono essere utilizzati esclusivamente per la finalità di *identificare in rete il titolare della carta nazionale dei servizi e per verificare la sua legittimazione al servizio*. Questo comma contestualizza il principio di necessità introdotto dal Codice in materia di protezione dei dati personali[6] (DL 30 giugno 2003, n. 196, art. 3) chiarendo che le informazioni personali presenti sulla carta devono essere utilizzate esclusivamente per la finalità di abilitare l'accesso ai servizi. E' opportuno osservare che, in conseguenza del principio di necessità espresso dal Codice della privacy, non sono consentite applicazioni che leggono i dati personali sulla carta e quindi li trasmettono via rete allorché sono disponibili tecniche che permettono l'identificazione e l'autorizzazione attraverso il codice di identificazione (codice fiscale) presente nel certificato digitale.

Particolarmente importante è il comma 2 dell'articolo 5 che recita: *tutte le pubbliche amministrazioni che erogano servizi in rete devono consentirne l'accesso ai titolari delle carta nazionale dei servizi indipendentemente dall'ente di emissione, che è responsabile del suo rilascio*. Questa norma impone che i servizi in rete delle pubbliche amministrazioni siano progettati in modo da accettare l'identificazione e l'autenticazione tramite la Carta nazionale dei Servizi, qualunque sia l'ente che l'ha emessa.

In pratica tutti i servizi della pubblica amministrazione dovranno prevedere una doppia modalità di autenticazione:

- tramite le carte per l'accesso ai servizi in rete (Carta d'identità elettronica e Carta nazionale dei servizi);
- con modalità alternative (PIN, password, ecc.) per gli utenti che ancora non dispongono di tali strumenti.

Il regolamento prevede inoltre la presenza di un sistema per interdire l'operatività della carta nazionale dei servizi in caso di smarrimento o furto della stessa. In sostanza viene prevista la presenza di un sistema di liste di revoca accessibili per via telematica, rimandando alle regole tecniche la definizione della modalità di accesso alle stesse (art. 6 ed art. 7 comma 1).

La competenza in merito ai controlli di qualità sulle procedure e sui dati utilizzati per l'emissione delle carte nazionali è assegnata al *Centro nazionale per l'informatica nella pubblica amministrazione* (CNIPA). Quest'ultimo ha anche il compito di definire le iniziative atte a migliorare il sistema dei servizi accessibili in rete (art. 7 comma 2).

Le disposizioni transitorie sono rivolte principalmente a regolamentare l'allineamento dell'Indice Nazionale delle Anagrafi fino a quando tale sistema non sarà nella fase di regime, ossia in attesa della sottoscrizione delle convenzioni previste dal regolamento. Durante tale fase l'allineamento dell'indice delle anagrafi avverrà in modalità differita attraverso la procedura di seguito descritta.

Le amministrazioni, all'atto dell'emissione, effettuata la verifica dei dati identificativi del titolare della carta, rilasceranno la CNS ed invieranno all'Indice nazionale delle anagrafi i dati identificativi della persona, il codice numerico identificativo della carta, la data del rilascio e la data di scadenza. Successivamente l'Indice nazionale delle anagrafi verificherà la correttezza di tali dati e, se la verifica avrà esito positivo, inserirà nella propria banca dati le informazioni relative all'emissione della CNS. Nel caso la verifica manifesti l'assenza delle informazioni anagrafiche presso dell'Indice nazionale delle anagrafi, quest'ultimo trasmetterà i dati anagrafici al comune competente affinché li convalidi[(7)] e, ricevuta la convalida, aggiornerà l'Indice. Nel caso in cui la verifica evidenzi l'inesattezza dei dati anagrafici, l'Indice nazionale delle anagrafi segnalerà all'amministrazione emittente la necessità di attivarsi nei confronti del titolare per interdire la carta emessa (art. 8 commi 2 e 3).

Al fine di assicurare l'aggiornamento delle informazioni presenti nella carta, l'Indice nazionale delle anagrafi segnalerà all'amministrazione che ha emesso la CNS eventuali variazioni dei dati identificativi del titolare comunicate dal Comune di residenza del titolare all'Indice nazionale delle anagrafi; a seguito di ciò l'amministrazione di emissione dovrà interdire la carta emessa (art. 8 comma 4).

Un'ulteriore norma transitoria riguarda la verifica preventiva del possesso della carta d'identità elettronica: fintantoché il sistema di allineamento dell'Indice nazionale delle anagrafi non sarà nella fase di regime (e comunque non oltre il 31 dicembre 2005) tale verifica potrà essere effettuata *limitatamente ai residenti nei comuni che diffondono la carta d'identità elettronica, previo accordo con i comuni interessati* (art. 8 comma 5).

1.4 Visione tecnologica della CNS

La CNS è una carta a microprocessore che, per quanto concerne la parte elettronica, presenta le stesse caratteristiche funzionali della CIE, ma mentre quest'ultima contiene gli elementi di sicurezza necessari per il riconoscimento a vista del titolare (in particolare gli ologrammi prodotti dall'Istituto Poligrafico dello Stato e la banda ottica inserita sul retro della carta), la CNS non contiene gli elementi "esterni" tipici di una carta d'identità.

Questa semplificazione permette di adottare un circuito di emissione più snello e flessibile di quello della CIE, infatti gli enti emettitori potranno rivolgersi a strutture esterne accreditate per quanto attiene le attività di produzione/inizializzazione delle smart card e di emissione dei certificati digitali.

La CNS è, quindi, principalmente uno strumento di identificazione in rete. Sfruttando le capacità di memorizzazione della carta stessa è possibile ospitare informazioni necessarie per altre funzionalità.

Il modello tecnologico della CNS consente anche l'inserimento delle informazioni crittografiche necessarie per la firma digitale. In tal modo il titolare della CNS ha la possibilità di sottoscrivere documenti elettronici.

Naturalmente, per assicurare la fruizione dei servizi garantendone la sicurezza e l'interoperabilità è necessario non solo che l'utente disponga di strumenti per

l'identificazione in rete, ma anche che i servizi siano progettati e realizzati secondo precise regole che permettono di garantire il rispetto dei principi di sicurezza enunciati.

1.5 Definizioni ed acronimi

Voce o acronimo	Descrizione
CNS	Carta Nazionale dei Servizi - 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.
CIE	Carta di Identità elettronica - Documento di riconoscimento personale a fini di Polizia rilasciato dal comune su supporto informatico. Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete. All'esterno contiene gli elementi necessari per l'identificazione a vista.
TS	Tessera Sanitaria contenente il codice fiscale in formato barcode, utilizzabile per l'accesso alle prestazioni del servizio sanitario regionale nazionale.
Firma digitale	E' un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Firma elettronica avanzata	La firma elettronica avanzata che sia basata su un certificato qualificato, creata mediante un dispositivo sicuro per la creazione della firma
Certificato di autenticazione	L'attestato elettronico che garantisce l'autenticità del circuito che ha emesso la CNS. E' un 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.
Certificato qualificato	Insieme di informazioni che creano una stretta ed affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. Sono certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.
Documento informatico	E' costituito da qualunque oggetto informatico (file) che contenga atti, fatti o dati giuridicamente rilevanti
Ministero dell'Interno CNSD	Centro Nazionale dei Servizi Demografici - Il Ministero dell'Interno, con DM del 23 aprile 2002 ha costituito il Centro

	Nazionale dei Servizi Demografici, per gestire in modo integrato e razionale i flussi delle informazioni anagrafiche necessari al mantenimento dell'allineamento dei dati delle anagrafi comunali. Gli enti emettitori si collegano su rete Internet o Rete unitaria al CNSD attraverso la porta applicativa.
Ministero dell'Interno INA	Indice Nazionale delle Anagrafi. In attuazione alla legge 28 febbraio 2001, n. 26, il Ministero dell'Interno rende disponibile il collegamento telematico al backbone INA/SAIA di sicurezza e certificazione, per la convalida delle informazioni anagrafiche dei cittadini
PIN	Personal Identification Number. E' il codice utilizzato per svolgere operazioni privilegiate sulla CNS
Posta elettronica Certificata	Posta Elettronica Certificata - Si intende un servizio basato sulla posta elettronica, come definito dallo standard SMTP e sue estensioni, che consenta la trasmissione di documenti prodotti mediante strumenti informatici nel rispetto dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
IRUW	Indice Regionale degli Utenti del Welfare.
Titolare	Il soggetto cui sono attribuite le firme digitali generate attraverso una determinata chiave associata ad un determinato certificato

Capitolo 2

Carta Raffaello

La Carta Raffaello nasce con l'intento di essere la Carta Nazionale dei Servizi e divenire uno strumento diffuso all'intera cittadinanza delle Marche e riconosciuto da tutte le amministrazioni per:

- l'autenticazione forte finalizzata all'identificazione in rete per accedere ai servizi
- la sottoscrizione digitale qualificata dei documenti

Con la scelta del nome, ispirato a Raffaello Sanzio, pittore rinascimentale fortemente legato per origini ed opere alle Marche, si intende dare alla carta una chiara connotazione regionale.

La Carta Raffaello soddisfa tutti i requisiti di sicurezza che permettono di utilizzare in rete le informazioni con la massima garanzia di sicurezza e tutela dei diritti personali

La Carta Raffaello rappresenta quindi lo strumento principale che abilita il cittadino all'accesso ai servizi telematici di eGovernment e all'inoltro di istanze e dichiarazioni nell'ambito di tali servizi. La Carta Raffaello aderisce allo standard Carta Nazionale dei Servizi e si conforma a tutti i requisiti tecnologici, organizzativi e di sicurezza previsti dalla normativa in termini di CNS e dispone di capacità di firma digitale qualificata.

2.1 Caratteristiche tecniche

La Carta Raffaello è una carta a microprocessore che aderisce allo standard CNS e quindi, per quanto concerne la parte elettronica, presenta le stesse caratteristiche funzionali della CIE, ma mentre quest'ultima contiene gli elementi di sicurezza necessari per il riconoscimento a vista del titolare, la CNS-Carta Raffaello non contiene gli elementi "esterni" tipici di una carta d'identità.

La Carta Raffaello ha le seguenti funzionalità principali:

- è uno strumento di identificazione in rete. E' dotata di un certificato di autenticazione rilasciato da un certificatore accreditato.
- ospita il servizio di firma digitale qualificata, fornendo al titolare la possibilità di sottoscrivere documenti elettronici.

La Carta Raffaello rispetta i vincoli imposti dagli standard internazionali sulle smart card, con particolare attenzione alle norme che regolamentano i documenti di identità (ISO/IEC 7816-1-2). Le dimensioni, lo spessore e le tolleranze sono conformi a quanto specificato dalla norma ISO/IEC 7810: 1995 per la carta di tipo ID-1.
E' dotata di una memoria EEPROM di almeno 32 KB. Il microprocessore é conforme agli standard ISO/IEC 7816 parte 3, 4 e 8.
La struttura della memoria interna della carta è conforme al file system pubblicato sul sito del Centro nazionale per l'informatica nella pubblica amministrazione e aderente a quanto stabilito dalle regole tecniche per l'emissione della CNS.

La struttura del file system, concepita per consentire un uso flessibile della CNS, è suddivisa in:

- un'area necessaria per la gestione della carta (DF0, DF1, PIN, PUK, Id_carta, PIN_SO);
- un'area contenente le informazioni necessarie per l'autenticazione in rete (Kpri, c_carta, Dati_personali);
- un'area predisposta per le funzioni di firma digitale (Firma_digitale);
- un'area disponibile per eventuali servizi aggiuntivi (Memoria_residua).

Inoltre, in aggiunta a quanto prescritto dallo standard ISO/IEC 7816 parte 4 circa i comandi del sistema operativo, la carta rispetta le specifiche del sistema operativo (APDU) oggetto del protocollo d'intesa per la realizzazione dei progetti Carta d'identità elettronica e Carta nazionale dei servizi.

Sulla carta, in accordo alle regole tecniche è presente la scritta "Carta Nazionale dei Servizi" ed il logo dell'Ente emettitore Regione Marche.

2.2 Il Layout

Il layout della Carta Raffaello è riportato nella figura seguente.

Figura 1 - Layout Carta Raffaello

L'immagine in semitrasparenza sullo sfondo è quella di Raffaello Sanzio a cui si ispira la carta.

I dati riportati sul fronte della CNS sono in Formato "Verdana True Type", stile normale dimensione 7 punti.

Le informazioni riportate sul fronte sono:

- codice fiscale 16 caratteri alfanumerici;
- cognome dimensionato per una lunghezza di 40 caratteri alfabetici;
- nome dimensionato per una lunghezza di 35 caratteri alfabetici;
- provincia di nascita per una lunghezza di 2 caratteri alfabetici;
- sesso, 1 carattere (M/F);

- data di nascita (GG/MM/AAAA) per una lunghezza di 10 caratteri alfanumerici;
- luogo di nascita, comune di nascita dimensionato per una lunghezza di 35 caratteri alfabetici;
- data di scadenza (GG/MM/AAAA) per una lunghezza di 10 caratteri alfanumerici;

La Carta Raffaello riporta sul retro le seguenti informazioni:

- banda magnetica ad ossidi rigidi e a tre tracce;
  - la prima traccia è personalizzata all'atto dell'emissione e contiene: codice fiscale 16 caratteri, cognome e nome separati da 2 spazi per una lunghezza complessiva di 60 caratteri. Le informazioni registrate sono precedute da un carattere denominato «Start sentinel» e seguite da un carattere denominato «End sentinel».

    Le informazioni sono registrate secondo la codifica IATA (International Air Transport Association) e il metodo di registrazione è AIKEN con densità 210 bpi.
  - la seconda traccia è personalizzata all'atto dell'emissione e contiene il codice fiscale convertito secondo tabella di conversione (caratteri numerici per una lunghezza complessiva di 34 caratteri comprensivi di start e end sentinel).

    Le informazioni sono registrate secondo la codifica ABA (American Bankers Association) e il metodo di registrazione è AIKEM con densità 75 bpi.
  - la terza traccia è a disposizione per ulteriori sviluppi e non viene personalizzata all'atto dell'emissione.
- Codice a barre del codice fiscale secondo lo standard di codifica 39 (oppure in modalità "128 code);

Il layout della Carta Raffaello contenente i dati di un utente è riportato nella figura seguente.

Figura 2 - Layout compilato della Carta Raffaello

2.3 Ruoli previsti nel circuito di emissione

2.3.1 Il Produttore

Il **produttore**, è l'azienda che provvede alla fornitura delle carte a microprocessore con un chip compatibile con quello previsto dalla CNS, che predispone opportunamente gli spazi dedicati alla firma digitale, applica al supporto fisico l'artwork e gli elementi costanti;

2.3.2 Il Certificatore

Il **certificatore**, è il soggetto che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche (sono abilitati a prestare servizi di certificazione per la CNS i soggetti di cui all'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002 per le informazioni relative all'autenticazione o alla firma elettronica).

2.3.3 L'ente Emettitore

L'**ente emettitore è** la Pubblica Amministrazione che emette la CNS e nel caso della Carta Raffaello è la Regione Marche ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta garantendo la corretta gestione del ciclo di vita della Carta Raffaello.

2.3.4 Il titolare

Il **titolare** è il proprietario della Carta Raffaello e quindi l'utente utilizzatore della stessa come strumento di identificazione in rete e per la sottoscrizione dei documenti informatici.

2.4 Obblighi e responsabilità

2.4.1 Obblighi del certificatore

Il certificatore è responsabile della generazione del certificato di autenticazione e di firma. Le informazioni anagrafiche ottenute in fase di registrazione, congiuntamente con le chiave pubbliche generate in fase di personalizzazione, sono utilizzate dal certificatore per generare i certificati secondo le specifiche disponibili presso il sito del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (www.cnipa.gov.it).

Possono operare come emettitori dei certificati di autenticazione e di firma della CNS esclusivamente i certificatori accreditati di cui all'articolo 5 del Decreto Legislativo 23 gennaio 2002, n.10, iscritti in un elenco consultabile in via telematica, tenuto dal CNIPA.

Tali soggetti devono operare in aderenza alle vigenti norme che regolano l'emissione e la gestione dei certificati qualificati.
L'ente certificatore per la Regione Marche è:

- denominazione sociale: Actalis S.p.A
- indirizzo della sede legale: via Torquato Taramelli, 26 – 20124 Milano
- n° partita Iva:03358520967

2.4.2 Obblighi e responsabilità dell'ente emettitore

L'ente emettitore della Carta Raffaello è la Regione Marche.

Come evidenziato in precedenza la parte elettronica della CNS, quindi della Carta Raffaello, presenta le stesse caratteristiche funzionali della CIE, ma mentre quest'ultima contiene gli elementi di sicurezza necessari per il riconoscimento a vista del titolare (in particolare gli ologrammi prodotti dall'Istituto Poligrafico dello Stato e la banda ottica inserita sul retro della carta), la CNS non contiene gli elementi "esterni" tipici di una carta d'identità.

Questa semplificazione permette di adottare un circuito di emissione più snello e flessibile di quello della CIE, infatti gli enti emettitori potranno rivolgersi a strutture esterne accreditate per quanto attiene le attività di registrazione/personalizzazione delle smart card e di emissione dei certificati digitali.

L'ente emettitore ha la responsabilità della sicurezza del circuito di emissione e del rispetto delle normative vigenti in merito alla tutela dei dati personali e ha comunque la facoltà di trasferire, nei termini di legge, tale responsabilità a terzi.

L' **ente emettitore** è responsabile:

- della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione e di firma;
- della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione;
- della sicurezza delle fasi di produzione, inizializzazione, distribuzione ed aggiornamento/ritiro della carta;
- dell'invio dei dati identificativi al Ministero dell'interno, Centro Nazionale Servizi Demografici, per l'aggiornamento dell'INA, secondo le modalità previste dal regolamento di attuazione, con procedure operative e formati che saranno definiti da apposita circolare del Ministero dell'interno.

2.4.3 Obblighi e responsabilità del titolare

Il titolare della Carta Raffaello ha l'obbligo e responsabilità di:

- fornire all'ente emettitore o struttura delegata, informazioni esatte e veritiere in fase di registrazione
- custodire con la massima diligenza i codici riservati ricevuti dall'ente emettitore, al fine di preservarne la riservatezza
- conservare con la massima diligenza la Carta Raffaello contenente le proprie chiavi private
- conservare le informazioni di abilitazioni all'uso delle chiavi private in luogo diverso dal dispositivo che le contengono
- richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute nel dispositivo di cui abbia perduto il possesso o difettosi.

Capitolo 3

Aspetti organizzativi

La Regione Marche, al fine di distribuire su tutto il territorio la Carta Raffaello, delega a strutture esterne accreditate le attività di registrazione/personalizzazione delle smart card.

Il personale preposto all'emissione e distribuzione della Carta Raffaello è organizzato secondo le seguenti figure organizzative:

- responsabile della registrazione
- responsabile della personalizzazione
- responsabile della sicurezza

Le figure sopra elencate possono avvalersi, per lo svolgimento delle funzioni di loro competenza di addetti e operatori.

Al fine di ampliare le possibilità operative, le funzioni di registrazione possono essere svolte anche da strutture, con sedi distribuite sul territorio, sulla base di apposite convenzioni stipulate con la Regione Marche. In tal caso, tali strutture (in seguito chiamate **Local Registration Autority** – **LRA**) operano secondo procedure concordate con la Regione Marche; tali procedure, descritte nelle specifiche convenzioni stipulate tra la Regione Marche e le LRA, potranno differire, da quelle descritte nei successivi paragrafi del presente documento, ma comporteranno i medesimi livelli di accuratezza ed affidabilità.

Analogamente le funzioni di personalizzazione della Carta Raffaello possono essere svolte anche da strutture, con sedi distribuite sul territorio, sulla base di apposite convenzioni stipulate con la Regione Marche. In tal caso, tali strutture (in seguito chiamate **Centro Servizi**) operano secondo procedure concordate con la Regione Marche; tali procedure, descritte nelle specifiche convenzioni stipulate tra la Regione Marche e Centro Servizio, potranno differire, da quelle descritte nei successivi paragrafi del presente documento, ma comporteranno i medesimi livelli di accuratezza ed affidabilità. Un Centro Servizio può svolgere l'attività di personalizzazione di carte provenienti da uno o più LRA e lo scambio di informazioni avviene mediante **canali di comunicazione sicuri**.

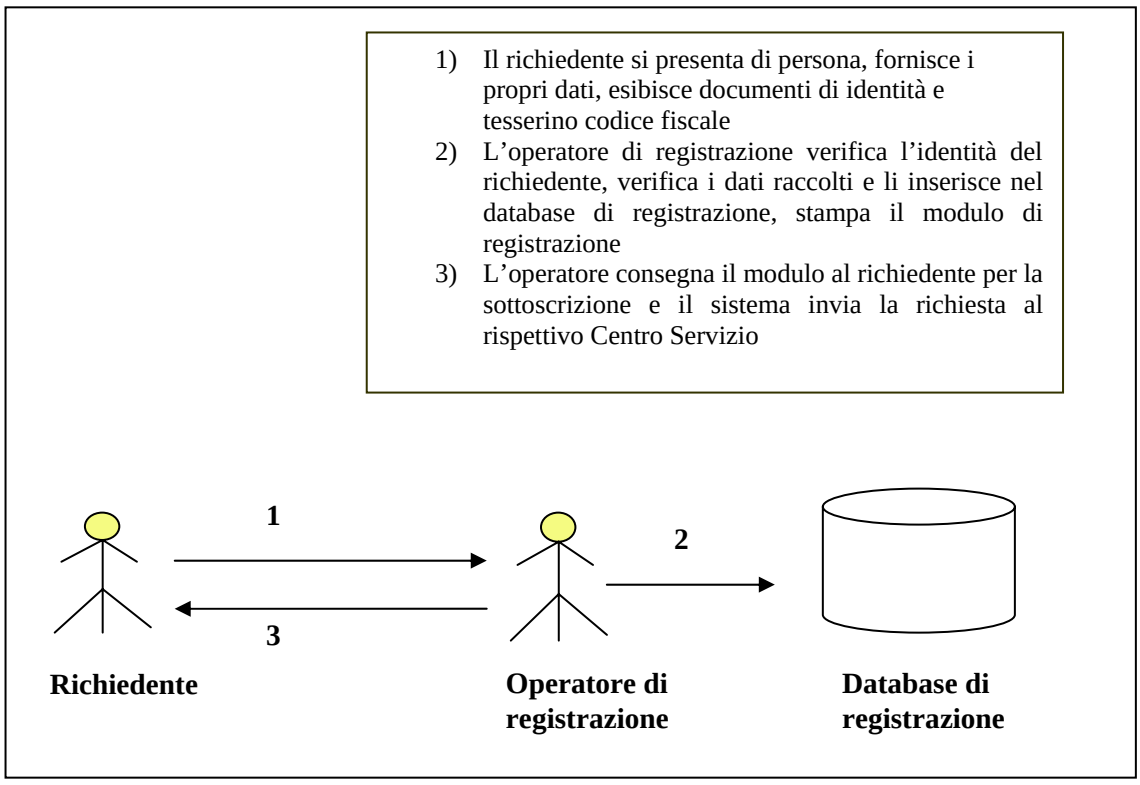
Gli LRA e i Centri Servizi debbono utilizzare il software messo a disposizione della Regione Marche per svolgere le attività di registrazione e personalizzazione, mentre devono dotarsi delle attrezzature hardware necessarie per la personalizzazione della Carta Raffaello, indicate dall'ente emettitore.

3.1 Modalità di identificazione e registrazione degli utenti

La procedura di identificazione e registrazione degli utenti si articola nelle seguenti fasi:

- sottomissione della richiesta, corredata della necessaria documentazione,
- verifica delle informazioni fornite ed accettazione o rifiuto della richiesta.

In questa procedura, il richiedente interagisce con un operatore di registrazione, il quale opera per conto del responsabile di registrazione presso una struttura LRA.



3.1.1 Identificazione dei richiedenti

Il richiedente deve **recarsi di persona** davanti all'operatore di registrazione e dimostrare la propria identità fornendo:

- la propria carta d'identità (o altro documento valido di riconoscimento)
- il proprio tesserino fiscale rilasciato dal Ministero delle Finanze

L'operatore di registrazione verifica/inserisce le seguenti informazioni, attraverso il software regionale, nel database di registrazione:

- cognome
- nome
- sesso
- data di nascita
- comune di nascita
- stato di nascita

- codice fiscale
- indirizzo di residenza
- cap
- comune di residenza
- stato
- numero di telefono
- numero di telefono
- numero di fax
- documento
- numero di documento
- luogo di rilascio
- data emissione
- data scadenza
- iscrizione a Cohesion
- eventuale assegnazione di account di posta elettronica certificata – PostaRaffaello

il sistema stampa il modulo di registrazione che deve essere firmato dal richiedente in presenza dell'operatore di registrazione.

Le informazioni sopra elencate sono da considerarsi obbligatorie ai fini della registrazione dell'utente e del rilascio del certificato di autenticazione e di firma.

E' responsabilità del richiedente fornire un indirizzo valido di posta elettronica, poiché il certificatore userà in seguito tale indirizzo per comunicare con il richiedente.

Firmando il modulo di registrazione, il richiedente:

- fornisce tutti i dati personali necessari alla registrazione
- esprime di fornire il proprio consenso al trattamento dei propri dati personali solo ed esclusivamente ai fini del servizio di autenticazione e di firma

3.1.2 Verifiche svolte dall'operatore di registrazione

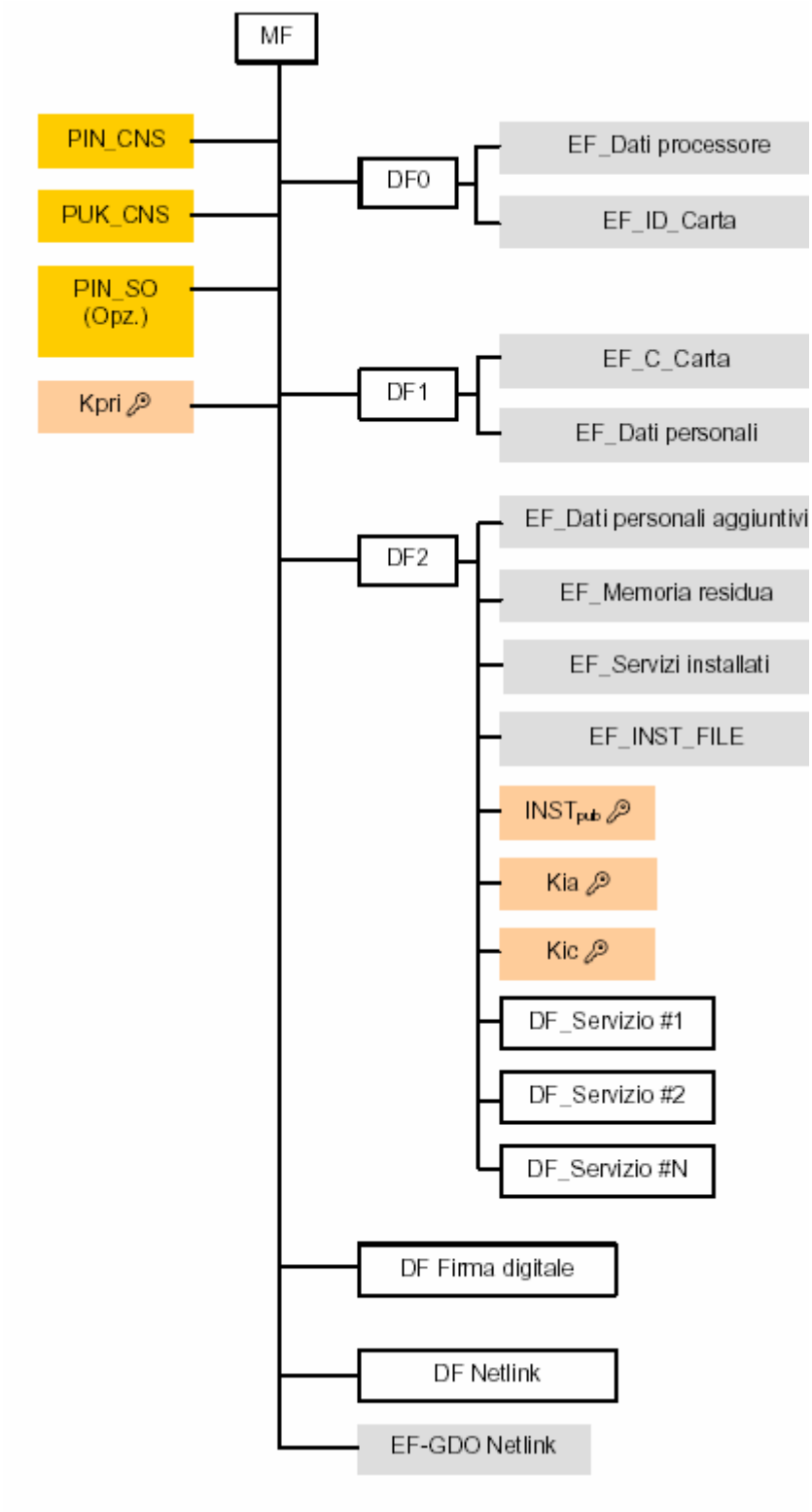
A fronte della richiesta di registrazione, l'operatore di registrazione svolge le seguenti verifiche:

- verifica l'identità del richiedente (mediante ispezione dei documenti di identità)
- verifica il codice fiscale (comparando il tesserino del codice fiscale con quello generato dal software)
- stampa il modulo di registrazione e verifica la sottoscrizione del richiedente
- riporta nel database di registrazione tutte le informazioni raccolte.
- Verifica se il richiedente vuole un account di posta certificata PostaRaffaello se richiesta
- Inoltra la richiesta di personalizzazione della Carta Raffaello al rispettivo Centro Servizio.

3.2 Modalità di personalizzazione della Carta Raffaello

La Carta Raffaello deve essere "personalizzata" con modalità stabilite dalla CA, attraverso iterazioni sicure, protette da SSL con l'applicativo del certificatore stesso.

Struttura file system



1. Scrittura del chip

I dati presenti all'interno della CNS:

Dati personali

- dati personali (MF/DF1/EF.DatiPersonali)
- dati personali aggiuntivi (MF/DF2/EF.Dati_Personali_Aggiuntivi)
- certificato utente (MF/DF1/EF.C_Carta)

Dati carta

- Dati processore (MF/DF0/EF.Dati_Processore)
- ID_Carta (MF/DF0/EF.ID_Carta)

Dati di servizio

- Card Status (MF/EF.CardStatus)
- Memoria residua (MF/DF2/EF.MemoriaResidua)
- Servizi installati (MF/DF2/EF.ServiziInstallati)
- InstFile (MF/DF2/EF.InstFile)

Label

- Chiavi di autenticazione

Dati Personali

EF: MF/DF1/EF.DatiPersonali
Dimensione file: 400 bytes

Contiene i dati dell'utente. I campi per identificazione personale (altezza, atto di nascita,...) non sono utilizzati. Alcuni campi sono opzionali nelle specifiche CNS, come indicato dalla colonna (M(obbligatorio)/O(opzionale)/V(vuoto)).

Dato	Codifica	M/O/V	Dimensione Max	Descrizione
Emettitore	ASCII	M	4	Codice derivante dai seriali standard; es. per la CNS della Lombardia "6030".
Data di emissione del documento	ASCII	M	8	Formato GGMMAAAA
Data di scadenza del documento	ASCII	M	8	Formato GGMMAAAA
Cognome	ASCII	M	26	
Nome	ASCII	M	26	
Data di Nascita	ASCII	M	8	Formato GGMMAAAA
Sesso	ASCII	M	1	'M' per maschio, 'F' per femmina
Statura (cm)	ASCII	O	0	Presente per compatibilità CIE
Codice fiscale	ASCII	M	16	
Cittadinanza (codice)	ASCII	O	0	Presente per compatibilità CIE
Comune di Nascita	ASCII	M	4	
Stato estero di Nascita	ASCII	O	0	Presente per compatibilità CIE
Estremi atto di nascita	ASCII	O	0	Presente per compatibilità CIE
Comune di residenza al momento dell'emissione	ASCII	M	4	
Indirizzo di residenza	ASCII	O	80	
Eventuale annotazione in caso di non validità del documento per l'espatrio	ASCII	V	0	Presente per compatibilità CIE

Tabella Definizione Dati Personali

Dati Personali aggiuntivi

MF/DF2/EF.DatiPersonaliAggiuntivi
Dimensione: 100 bytes

Il file, presente per back compatibility con la CIE, è vuoto, con l'intero contenuto posto a 00h.

Certificato Utente

MF/DF1/EF.C_Carta
Dimensione: 2048

Identifica l'utente in un'autenticazione.
Il formato è PKCS#1, codificato ASN.1.
Il Common Name ha la struttura:

CF/ID.Hash(DatiPersonali)
dove:
CF = codice fiscale
ID = 16 caratteri di ID carta, come definito più avanti in questa specifica
Hash = operazione di hash SHA-1
DatiPersonali = dati personali come presenti nel file EF.DatiPersonali. Vanno considerati solo i dati utili (escludendo quindi la parte finale riempita a 00h), nella stessa sequenza in cui appaiono nel file, includendo tutti i campi Len.

Dati Processore

MF/DF0/EF.DatiProcessore
Dimensione: 54 byte

Questo file contiene i dati di tracciabilità del chip. Una prima parte viene normata per identificare il produttore del chip e del sistema operativo. Altri campi restano a discrezione del produttore della carta.
All'interno del record i campi sono fissi e il loro significato applicativo è definito dalla posizione.

Dato	Codifica	Y/N	Dimensione (bytes)	Descrizione
Chip Manufacturer	ASCII	Y	2	Definita in ISO 7816
OS Manufacturer	ASCII	Y	2	Definita nelle specifiche governative delle APDU per la CNS
Personalizer	ASCII	Y	2	A partire da '01'
Chip Tracing Data	ASCII	Y	2	'00'
Personalizer Specific Data	Libera	Y	10	Dati di competenza del personalizzatore (es stato carta, lotto,...) - TBD
OS Specific Data	Libera	Y	10	Dati di competenza del produttore del sistema operativo - TBD
Free Data	Libera	N	0	Area libera - Assente

ID Carta

MF/DF0/EF.ID_Carta
Dimensione: 16 bytes

L'ID Carta della CNS.

Card Status

MF/EF.CardStatus
Dimensione file: 20

Utilizzato per marcare lo stato della carta. L'intero file è riempito con 00h.

Memoria Residua

MF/DF2/EF.MemoriaResidua
Dimensione file: 2

Mantiene la dimensione della memoria ancora non utilizzata.
Il valore è in byte, e la codifica è binaria.
Questo valore viene inizializzato in emissione con un valore che potrà dipendere dal fornitore e dal lotto di emissione.

Servizi Installati

MF/DF2/EF.ServiziInstallati
Dimensione file: 160
Mantiene la lista dei servizi installati. In fase di emissione il file è riempito con 00h.
Questo file viene utilizzato per visualizzare la lista dei servizi installati e per la gestione delle applicazioni. Viene scritto dalle applicazioni di caricamento servizi.
Il contenuto del file non è definito da questa specifica ma viene lasciato al gestore dei servizi aggiuntivi.

InstFile

MF/DF2/EF.Inst File
Dimensione file: 128
Contiene le chiavi da utilizzare per l'installazione dei servizi aggiuntivi.
Il contenuto di questo file è

$RSA_{InstPubKey}$(KIC | KIA)

Il padding usato è BT02.
La codifica è binaria.

Label

Sulla carta è presente all'emissione solo la coppia di chiavi di autenticazione.
La label delle chiavi di autenticazione deve essere nota per poter essere usata dagli applicativi o dagli strati software intermedi.
Si fissa il valore della label delle chiavi di autenticazione uguale a "CNS0".

Attività dell'operatore di personalizzazione

A fronte delle richieste di personalizzazione, l'operatore di personalizzazione che opera per conto del responsabile di registrazione presso il Centro Servizio, svolge le seguenti attività:

1. Scrittura dei dati personali all'interno del chip
2. Scrittura dei dati personali sulla banda magnetica
3. Stampa dati personali sul fronte e retro della Carta Raffaello rispettando il layout stabilito.

L'attività n°1 prevede:

- L'invia i dati personali del richiedente alla CA attraverso un canale di trasmissione sicuro SSL.

- La memorizzazione all'interno del chip della carta, rispettando quanto indicato nel documento "Linea Guida per l'emissione della CNS" redatto del Cnipa ossia:
  - si genera un Hash dei dati personali da inserire nel subjectname del certificato di autenticazione.
  - si inserisce i dati personali all'interno della Carta

- Richiesta e importazione del Certificato di Autenticazione e di Firma (tale step viene ripetuto per ogni richiesta di certificato)
  - si invia, tramite canale sicuro, alla CA le informazioni per la creazione dei certificato
  - si generano le coppie di chiavi all'interno della smart-card
  - si genera la richiesta di certificato e si invia alla CA
  - si importa il certificato all'interno della smart-card utilizzando il PIN di fabbrica della carta

- Generazione nuovo PIN in maniera random e memorizzato criptato nel database

L'attività n°2 prevede:

- La scrittura della prima e seconda traccia della banda magnetica e precisamente, viene scritto il codice fiscale dell'utente sulla prima traccia e nella seconda la conversione nel formato ABA dello stesso codice.

L'attività n°3 prevede:

- La stampa del fronte e del retro della carta riportando i dati del richiedente rispettando il layout indicato nel paragrafo 2.2 del presente documento

La richiesta di certificazione viene inviata al certificatore attraverso un "canale telematico sicuro, ottenuto con l'uso del protocollo SSL (Secure Sockets Layer)

Il periodo di validità del certificato di autenticazione e di firma è di 5 anni.

La seguente figura mostra, in modo semplificato, la procedura di richiesta ed emissione di un certificato.

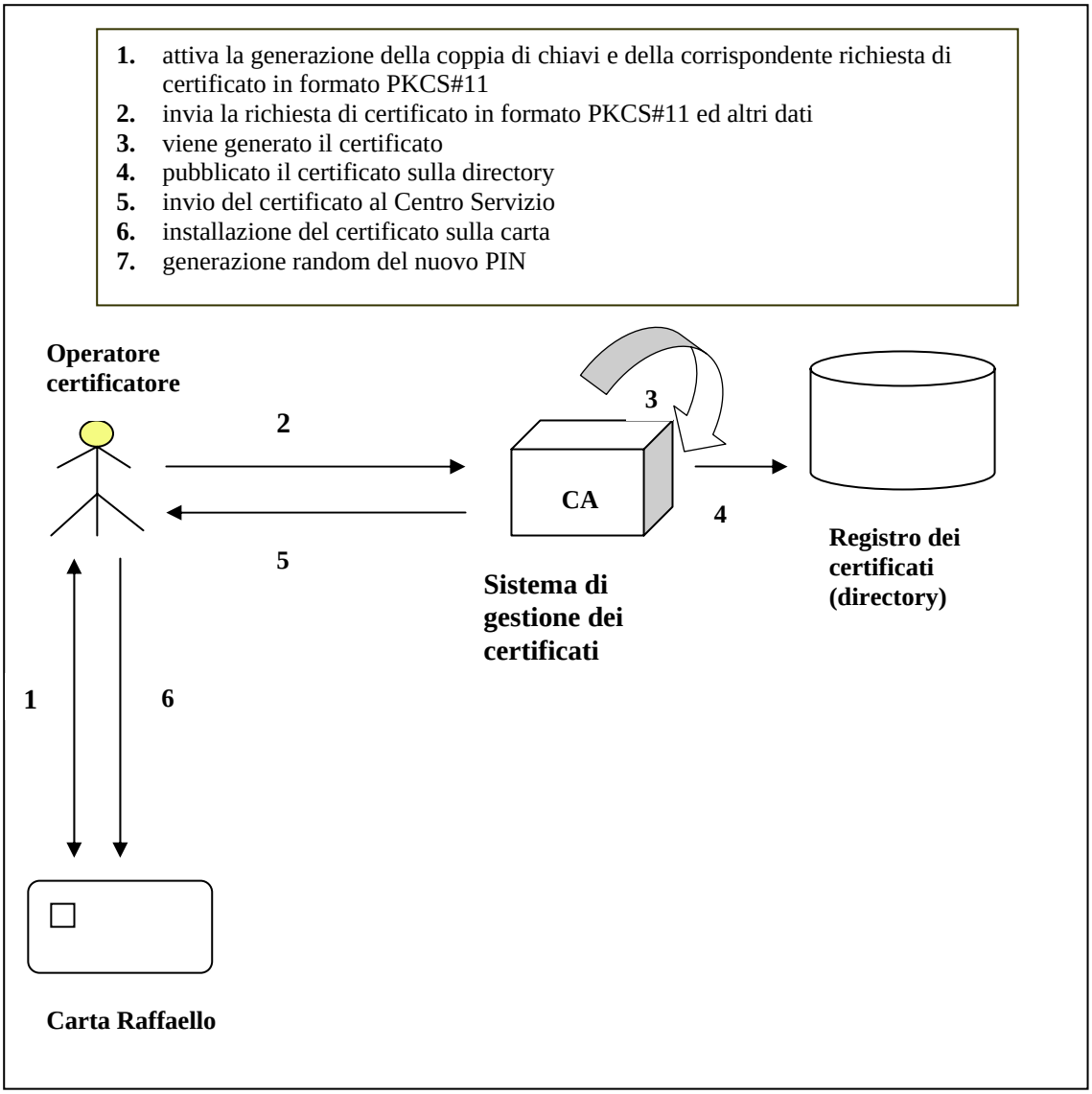


Figura 3- richiesta, generazione e rilascio certificati di autenticazione e di firma

3.2.1 Pubblicazione certificato

La pubblicazione del certificato di firma avviene nel seguente modo:

- Il certificato viene pubblicato nel registro dei certificati; il momento (data/ora) della pubblicazione viene attestato con la richiesta di una marca temporale, ottenuta mediante interazione col sistema di marcatura temporale predisposto dal certificatore
- Il certificato e la relativa marca temporale vengono inviati all'utente, tramite posta elettronica, all'indirizzo fornito in fase di registrazione;
- Viene generato e fornito all'utente un **codice riservato di revoca certificato.**

3.2.3 Conservazione e trasporto delle Carte Raffaello

Quando le carte non sono in lavorazione, devono essere conservate in locali in grado di assicurare adeguati livelli di sicurezza. Ogniqualvolta le carte devono transitare tra siti diversi (dal Centro Servizi al rispettivo LRA per la consegna al richiedente), devono utilizzare un trasporto sicuro verificato dal responsabile della Sicurezza.

Il Responsabile della Sicurezza ha l'obbligo di mantenere in appositi registri di entrata/uscita, elettronici e/o cartacei, riportando ogni singolo movimento, con l'indicazione della data e d ora sottoscritto dal responsabile stesso.

3.2.4 Consegna della Carta Raffaello al titolare

Il richiedente deve **recarsi di persona** davanti all'operatore di registrazione per ritirare la Carta Raffaello.

L'operatore, accertata l'identità del richiedente consegna la Carta Raffaello dopo aver stampato su una busta retinata il codice PIN e PUK che l'operatore di certificazione aveva provveduto a generare in maniera random e a criptarlo.

Effettuata tale operazione il PIN viene cancellato dal Database.

- Il richiedente deve sottoscrivere un ulteriore modulo dell'avvenuta consegna.

3.3 Modalità di sospensione e revoca della Carta Raffaello

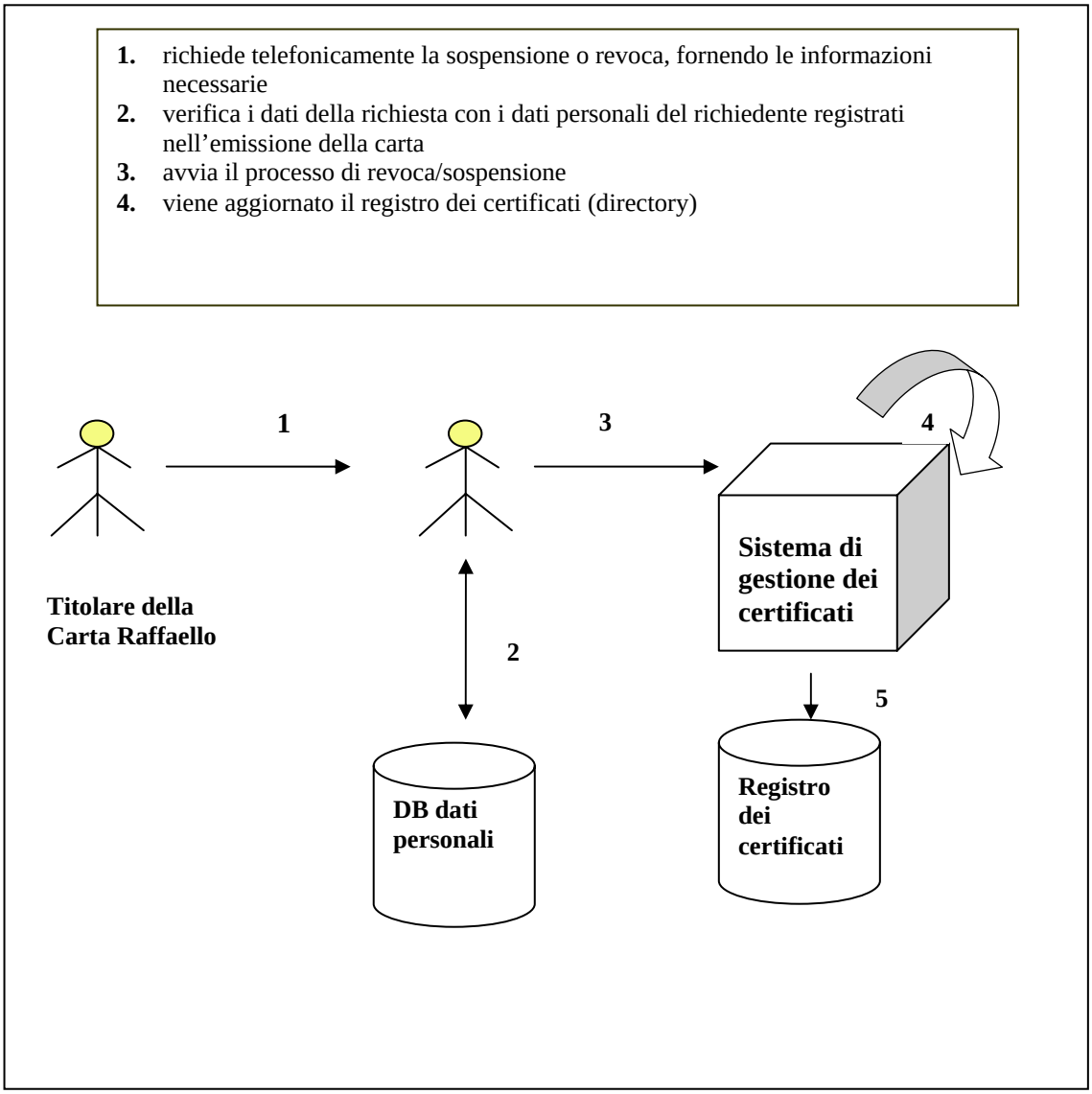
Il certificatore procede tempestivamente alla sospensione o revoca del certificato nelle seguenti circostanze:

- Richiesta da parte del titolare;
- Perdita del possesso della chiave

3.3.1 Richiesta di sospensione o revoca da parte del titolare

Si mostra di seguito, in modo semplificato, la procedura di richiesta ed effettuazione della sospensione o revoca dl certificato su richiesta del titolare; la procedura si articola nelle seguenti fasi:

- Inoltro della richiesta da parte del titolare;
- Verifica, da parte del certificatore, dell'autenticità e correttezza della richiesta;
- Effettuazione della revoca



Il titolare può telefonare al **numero verde 800.077.407** del call center regionale fornendo le seguenti informazioni:

- Tipo di intervento richiesto (sospensione o revoca)
- L'apposito codice riservato di revoca del certificato (paragrafo "Pubblicazione del certificato")
- Il proprio nome e cognome
- Ulteriori dati identificativi (es. codice fiscale) nel caso in cui si debbono risolvere omonimie
- La motivazione per la richiesta di sospensione o revoca
- La data e l'ora di decorrenza della sospensione o revoca, in ogni caso non inferiore a tre giorni prima della data corrente
- Nel caso di richiesta di sospensione la durata della sospensione.