LINEE GUIDA PER L'EMISSIONE E L'UTILIZZO DELLA CARTA NAZIONALE DEI SERVIZI

Versione 3.0
15 maggio 2006

Ufficio Standard e tecnologie d'identificazione
Centro Nazionale per l'informatica nella Pubblica Amministrazione

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.

L'accesso a tali servizi deve essere garantito indipendentemente dallo strumento di identificazione digitale utilizzato dall'utente. Parallelamente è indispensabile evitare la proliferazione di strumenti di identificazione digitale per l'accesso ai servizi delle amministrazioni, garantendo, invece, la convergenza verso uno standard unitario, le cui caratteristiche di realizzazione, distribuzione e gestione siano largamente condivise, rapidamente realizzabili su tutto il territorio nazionale in modo economicamente sostenibile.

Il nome di questo standard è "Carta Nazionale di accesso ai Servizi" o "Carta Nazionale dei Servizi".

Il presente documento contiene le Linee guida per l'emissione, la gestione e l'utilizzo della Carta Nazionale dei Servizi (nel seguito CNS).

1.1 Obiettivi e contenuto del documento

Obiettivo di questo documento è quello di fornire indicazioni ai comuni, alle province, alle comunità montane, alle regioni e alle amministrazioni centrali sull'emissione e utilizzo della CNS. Nei vari capitoli vengono presentati l'ambito politico nel quale ci si muove ovvero quello della visione condivisa; il contesto normativo al quale la CNS deve conformarsi; le tecnologie ICT di riferimento necessarie per un corretto e omogeneo funzionamento nell'ambito del controllo d'accesso ai servizi in rete erogati dalla pubblica amministrazione. Vengono anche descritti sinteticamente gli obiettivi sanitari cha la CNS si pone in conformità con quelli della CIE; le possibilità di integrazione con i sistemi di pagamento in linea.

Infine vengono date le specifiche generali per consentire alla CNS di essere utilizzata dalle applicazioni sulle postazioni client e alle applicazioni server di gestire l'ambiente di autenticazione e autorizzazione in conformità alle regole di cooperazione applicativa.

Si è ritenuto opportuno ricordare anche le regole di sicurezza del circuito di produzione e emissione della CNS, secondo quanto stabilito nelle regole tecniche di riferimento.

1.2 La visione condivisa

Il documento "L'E-GOVERNMENT PER UN FEDERALISMO EFFICIENTE - UNA VISIONE CONDIVISA, UNA REALIZZAZIONE COOPERATIVA"[1], come recita il suo sottotitolo, contiene le "Note di riferimento per lo sviluppo dell'e-government nelle Amministrazioni Centrali, nelle Regioni e negli Enti Locali." Questo documento ha l'obiettivo di formulare una visione comune

[1] Disponibile sul sito del Ministro per l'innovazione e le tecnologie (www.innovazione.gov.it), nella sezione "Enti locali".

nell'ambito delle pubbliche amministrazioni coinvolte nel percorso di innovazione del paese che ha come impegnativo processo la riorganizzazione della Stato in senso federale.

Come già evidenziato in precedenza l'efficacia, l'efficienza e l'economicità dei processi di e-government richiedono scelte omogenee nelle visione tecnologica per evitare inutili sprechi di risorse economiche.

A tal proposito è stata sviluppata una visione comune tra i diversi livelli di governo e di responsabilità amministrativa sui seguenti temi:

1. l'interconnessione tra tutte le Pubbliche amministrazioni e tra le Pubbliche amministrazioni i cittadini e le imprese;
2. gli strumenti di accesso ai servizi erogati sul canale telematico;
3. le modalità di erogazione dei servizi sul canale telematico;
4. i requisiti per garantire la sicurezza;
5. le architetture che garantiscono l'interoperabilità dei servizi sul territorio nazionale;
6. sistemi federati e riuso delle soluzioni;
7. le strutture organizzative per l'attuazione dell'e-government;
8. verso architetture condivise di sistema.

La CNS, ovviamente, è contemplata nell'ambito degli strumenti di accesso ai servizi on-line. Le carte per l'accesso ai servizi in rete sono diverse tipologie di smart card che hanno in comune le seguenti caratteristiche:

- sono emesse da un ente pubblico che convalida le informazioni di rilevanza sociale in esse contenute;
- hanno requisiti di sicurezza che permettono di utilizzare in rete queste informazioni con la massima garanzia di sicurezza e tutela dei diritti personali.

Con questi strumenti si supera il modello di interazione tradizionale che costringe gli utenti a fornire una serie di dati in rete e soprattutto a gestire un numero elevato (circa 40) di pin o password per accedere ai servizi erogati on-line dalle diverse pubbliche amministrazioni.

Le carte per l'accesso ai servizi sono riconducibili a due tipologie:

- la Carta d'Identità Elettronica (CIE), emessa dai comuni in sostituzione della carta d'identità tradizionale;
- le altre carte per accedere ai servizi in rete (carta sanitaria, tributaria, carte regionali e cittadine dei servizi, etc.), che devono essere conformi a un unico standard denominato "Carta Nazionale dei Servizi".

La CNS rappresenta uno standard per le carte di accesso ai servizi in rete rilasciate dalla Pubblica amministrazione.

La descrizione della CIE non è tra gli obiettivi del presente documento.

1.3 La 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. Infine, l'apertura al libero mercato delle smart card avrà come immediata conseguenza le economie indotte dalla concorrenza e dalla molteplicità delle offerte.

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

In ogni caso, il quadro normativo di riferimento è la base di partenza alla quale attenersi. Questo è l'argomento del prossimo capitolo.

Capitolo 2

Il 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 la 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 e' 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). Tale definizione è rimasta inalterata (articolo 1, comma 1, lettera d)) nel decreto legislativo 4 aprile 2006, n. 159 recante "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale".

Il medesimo decreto legislativo aggiorna anche le regole per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni. L'articolo 64 contiene queste regole e di seguito lo si riporta per comodità in modo integrale:

"64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'autenticazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

3. Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi. E' prorogato alla medesima data il termine relativo alla procedura di accertamento preventivo del possesso della Carta di identità elettronica (CIE), di cui all'articolo 8, comma 5, del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, limitatamente alle richieste di emissione di Carte nazionali dei servizi (CNS) da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE."

2.1 Il 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[2]. 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[3]. 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). In questo contesto è importante tenere in conto quanto disposto nell'articolo 64, comma 3 del decreto legislativo 4 aprile 2006, n. 159 cioè le "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale".

Esso tra l'altro stabilisce che "…*è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi. E' prorogato alla medesima data il termine relativo alla procedura di accertamento preventivo del possesso della Carta d'identità elettronica (CIE), di cui all'articolo 8, comma 5, del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, limitatamente alle richieste di emissione di Carte nazionali dei servizi (CNS) da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE.*

[2] Le funzioni telematiche della CNS sono le stesse della Carta d'Identità Elettronica, dunque è superfluo fornire la prima a chi è già in possesso della seconda.

[3] I servizi di validazione dei dati sono erogati dal Centro Nazionale per i Servizi Demografici, ai sensi dell'art. 2-*quater* del decreto legge 27 dicembre 2000, n.392, convertito dalla legge 28 febbraio 2001. Il regolamento di attuazione prevede la stipula di convenzioni tra il Ministero dell'interno ed i Comuni per l'accesso all'Indice Nazionale delle Anagrafi (INA), con la finalità di garantire a livello nazionale la congruenza e la correttezza delle informazioni anagrafiche.

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[4] (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 inserisce nel giusto contesto il principio di necessità introdotto dal Codice in materia di protezione dei dati personali[5] (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, confermata nel Codice dell'amministrazione digitale, conferma e ribadisce che i servizi in rete erogati dalle 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

[4] Il certificatore deve essere iscritto nell'elenco pubblico secondo quanto disposto dall'articolo 29, comma 6 del decreto legislativo 4 aprile 2006, n. 159.

[5] *I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*

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[6] 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 riguardava 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). Tale norma è stata modificata nel Codice dell'amministrazione digitale aggiornato nel 2006 (cfr. art. 64, comma 3).

2.2 Le regole tecniche

Le regole tecniche individuano le caratteristiche informatiche della Carta Nazionale dei Servizi e la modalità di gestione del ciclo di vita della stessa.

Esse sono definite nel decreto del Presidente del Consiglio dei ministri 9 dicembre 2004 "Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi".

Nel seguito vengono sintetizzati alcuni aspetti essenziali per la caratterizzazione della CNS.

In particolare la CNS è caratterizzata da tre funzionalità principali:

- la CNS è uno strumento di identificazione in rete;
- la CNS può essere predisposta per operare come carta sanitaria (Netlink);
- la CNS deve essere predisposta per ospitare il servizio di firma digitale, fornendo al titolare la possibilità di sottoscrivere documenti informatici.

Queste tre funzionalità devono essere comuni a tutte le CNS, anche se le ultime due possono non essere attive al momento dell'emissione della carta.

2.2.1 Caratteristiche della carta e standard di riferimento

La CNS non presenta particolari restrizioni per quanto riguarda la struttura del supporto fisico, dovranno essere comunque rispettati 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 devono essere conformi a quanto specificato dalla norma ISO/IEC 7810: 1995 per la carta di tipo ID-1.

Sulla carta deve essere presente la scritta Carta Nazionale dei Servizi ed è consigliato l'inserimento del logo dell'Ente emettitore. I dati da stampare sulla CNS e l'eventuale loro memorizzazione sul microchip sono decisi e disposti dall'Ente emettitore che la rilascerà.

[6] Si noti che non è detto che l'amministrazione emittente coincida con il comune di residenza del titolare della carta, per cui è necessaria questa fase di convalida da parte di quest'ultimo.

Le regole tecniche precisano comunque che l'aspetto della CNS deve essere tale da evitare che la carta possa essere scambiata per un documento di riconoscimento a vista, per cui *sulla CNS non devono essere presenti dei dati utilizzabili in alcun modo per il riconoscimento a vista del titolare, come per esempio la fotografia.*

Per quanto concerne le caratteristiche interne della carta, le regole tecniche stabiliscono che deve essere presente una memoria EEPROM della capacità non inferiore a 32 KB.

Inoltre, il microprocessore deve essere conforme agli standard ISO/IEC 7816 parte 3, 4 e 8.

Inoltre, in aggiunta a quanto prescritto dallo standard ISO/IEC 7816 parte 4 circa i comandi del sistema operativo, dovranno essere rispettate 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 (cfr. il sito Internet del CNIPA www.cnipa.gov.it).

2.2.2 La certificazione della smart card

Dall'obbligo relativo alla predisposizione per la funzionalità di firma digitale derivano alcune caratteristiche fondamentali delle smart card. Infatti, per poter ospitare la firma digitale, la smart card deve essere conforme a quanto stabilito dal più volte citato Codice dell'amministrazione digitale.

In particolare, la smart card dovrà avere le caratteristiche di un "*dispositivo sicuro per la generazione della firma*" basata su quanto stabilito nell'articolo 35 del Codice dell'amministrazione digitale[7]. Le regole tecniche per la firma digitale precisano che *i dispositivi sicuri di firma di cui all'articolo 29-sexies del testo unico, devono essere conformi alle norme generalmente riconosciute a livello internazionale o individuate dalla Commissione europea secondo la procedura di cui all'articolo 9 della direttiva n. 1999/93/CE.*

La decisione della Commissione europea del 14 luglio 2003 circa i riferimenti a standard generalmente riconosciuti per i prodotti di firma elettronica ha riportato, relativamente ai dispositivi sicuri per la creazione della firma, lo standard CWA 14169 (marzo 2002) che dunque costituisce il riferimento (peraltro non esclusivo)per la certificazione delle smart card che possono ospitare la firma elettronica[8]. Potranno essere anche accettati dispositivi dichiarati conformi alle caratteristiche di sicurezza di un dispositivo sicuro di firma, mediante apposita dichiarazione e certificazione da parte di un "certification body" accreditato operante anche all'interno dell' Unione Europea.

2.2.3 Le informazioni registrate nella memoria della carta

La struttura della memoria interna della carta è conforme al file di sistema (file system) pubblicato sul sito del Centro nazionale per l'informatica nella pubblica amministrazione.

La struttura del file di sistema è stata concepita per consentire un uso flessibile della CNS e può essere 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 carta sanitaria (Carta_sanitaria);
- un'area predisposta per le funzioni di firma digitale (Firma_digitale);

---

[7] Si riportano i primi due commi dell'articolo 35 :*1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata: a) sia riservata; b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni; c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.*
2. I dispositivi sicuri di cui al comma 1 devono garantire l'integrità dei dati elettronici a cui la firma si riferisce. I dati devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma.
3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del titolare.
4. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.

[8] In sostanza per la CNS si deve utilizzare una smart card certificata in base alla norma ISO/IEC 15408 (Common Criteria) secondo il Protection Profile riportato nell'allegato A dello standard CWA 14169.

- un'area disponibile per eventuali servizi aggiuntivi (Memoria_residua).

La tabella 1 delle regole tecniche riporta la descrizione dei campi elencati e, per ogni campo, le responsabilità in merito alla generazione, la predisposizione e la registrazione dell'informazione.

Il file elementare dei dati personali è codificato secondo le modalità previste per la Carta d'Identità Elettronica, riportate nella tabella 2 delle regole tecniche.

Viene inoltre precisato che, nel contesto della Carta Nazionale dei Servizi, in aggiunta a quanto definito per la CIE, la locuzione "dati identificativi della persona" si riferisce ai dati anagrafici ed al codice fiscale, dove, per dati anagrafici si intende il nome, il cognome, il sesso, la data, il luogo di nascita e il comune di residenza al momento dell'emissione.

2.2.4 L'emissione della CNS

Le regole tecniche chiariscono che la CNS può essere emessa da tutte le pubbliche amministrazioni. La Pubblica Amministrazione che emette la CNS è definita **ente emettitore** ed è responsabile:

- della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione;
- 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.

Si osservi che non è richiesto che l'Ente emettitore effettui in proprio le attività necessarie alla personalizzazione, al rilascio ed alla successiva gestione della carta, esso comunque, anche nel caso queste attività vengano delegate ad altre strutture, ne mantiene le responsabilità ed è il referente diretto nei confronti del Ministero dell'interno - Centro Nazionale Servizi Demografici.

Durante la fase preparatoria, l'ente emettitore analizza ed individua i servizi da rendere disponibili in rete mediante CNS, valuta l'offerta di mercato relativa alla fornitura delle smart card e decide se far fronte in maniera autonoma all'emissione della CNS, ovvero utilizzare servizi di strutture delegate. Eventualmente stipula accordi con le Regioni per la predisposizione delle carte con le funzionalità di tessera sanitaria.

L'ente emettitore avvia la produzione di un lotto di CNS, si dota eventualmente di tutte le risorse hardware e software necessarie all'emissione della CNS, tenendo conto delle direttive e delle norme vigenti[9], commissiona quindi al produttore individuato la fornitura dei lotti di CNS inizializzate.

L'Ente emettitore non è l'unico soggetto che concorre al processo di emissione della CNS. Gli altri soggetti sono:

il **produttore**, ossia 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 carta sanitaria (Netlink) ed alla firma digitale, che applica al supporto fisico l'artwork e gli elementi costanti;

il **certificatore**, cioè 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).

[9] In generale si dovrà ricorrere ad una procedura di appalto concorso di tipo aperto. Nel disciplinare di gara dovranno quindi essere indicati gli elementi di conformità alle caratteristiche ed agli standard della CNS (norme di riferimento, APDU, file system, criteri di sicurezza, certificazione, ecc.)

2.2.5 Il circuito della CNS

Le regole tecniche stabiliscono le modalità con cui deve essere prodotta, rilasciata emessa e gestita la Carta Nazionale dei Servizi.

Attività a carico del produttore

Il produttore della CNS è responsabile della produzione della carta plastica, della sua inizializzazione tramite la generazione del file system, e della creazione delle condizioni necessarie per controllare l'accesso ai file.

L'operazione di inizializzazione è finalizzata a produrre in maniera sicura delle carte che siano pronte ad essere personalizzate, ossia risultino in uno stato definito "Attivate".

Attività a carico dell'ente emettitore

L'ente emettitore è responsabile della registrazione degli utenti, dell'aggiornamento dell'Indice Nazionale delle Anagrafi, della personalizzazione e consegna della CNS e della successiva gestione della carta.

La registrazione consiste nell'identificazione del cittadino attraverso un documento di riconoscimento valido. Al momento della registrazione, il cittadino deve dichiarare di non possedere la Carta d'Identità Elettronica.

Prima di personalizzare la CNS, l'ente emettitore verifica i dati identificativi ed aggiorna l'Indice Nazionale delle Anagrafi, direttamente o tramite struttura delegata, mediante i servizi del sistema informativo del Ministero dell'Interno – Centro Nazionale dei Servizi Demografici (in via transitoria potrà essere utilizzata la procedura differita prevista dall'articolo 9 del regolamento attuativo).

La personalizzazione delle carte ed il loro rilascio è condotta dagli enti emettitori per mezzo di strutture proprie o esterne. Nel corso dell'attività di personalizzazione, vengono inserite le informazioni utente necessarie per l'identificazione in rete e per gli altri servizi previsti, viene inoltre generato il PIN_utente ed il PUK, utilizzabile per lo sbocco della carta nel caso di iterata digitazione errata del PIN. Il PIN ed il codice PUK sono stampati in buste retinate atte a garantire la riservatezza di tali informazioni.

Dopo la personalizzazione, la CNS viene consegnata al titolare, previa verifica dell'identità, unitamente alla busta contenente il PIN ed il codice PUK. L'ente emettitore deve illustrare al titolare le modalità di uso della carta e le procedure che dovranno essere utilizzate in caso di anomalie o disservizi. Deve fornire al titolare un numero telefonico per l'assistenza in caso di problemi ed il numero telefonico utile per richiedere la sospensione o la revoca.

L'ente emettitore provvede inoltre 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 (anche per le funzioni di gestione delle carte l'ente può avvalersi di strutture delegate), provvede inoltre al ritiro della CNS a seguito di problemi di funzionamento della smart card o allorché questa abbia raggiunto il naturale termine di scadenza. L'ente emettitore è tenuto al ritiro della CNS prima dell'emissione di una nuova carta o del suo rinnovo.

Attività a carico del certificatore

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

2.2.6 La gestione della CNS

L'ente emettitore è responsabile della gestione del circuito di emissione che a lui fa capo. L'ente dovrà definire le procedure di gestione, personalizzazione e rilascio delle carte CNS e descriverle in un apposito manuale operativo accessibile al pubblico, dovrà inoltre predisporre, eventualmente avvalendosi di terzi, le strutture per l'assistenza agli utenti, per la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza, infine, è responsabile di definire un servizio di "contact center" per l'assistenza, nonché la revoca o sospensione della CNS.

L'ente emettitore può distribuire software di complemento alla CNS, tenendo in conto che il software per la CIE è distribuito dal Ministero dell'Interno.

L'ente emettitore ha la facoltà di procedere di propria iniziativa alla revoca della CNS; in tal caso ha l'obbligo di avvertire il titolare esplicitando le motivazioni della revoca.

2.2.7 Requisiti per la partecipazione al circuito della CNS

Produttori

Ai fini della sicurezza dell'intero circuito di emissione, i fornitori di smart card che intendono offrire i propri servizi agli enti emettitori per le fasi di inizializzazione delle smart card, devono rispettare le specifiche previste nel presente documento.

In particolare, i fornitori sono vincolati al rispetto delle specifiche del sistema operativo (APDU) e della struttura interna della carta (file system) pubblicate sul sito del Centro Nazionale per l'informatica nella pubblica amministrazione.

Ogni consegna di lotti di CNS dovrà essere accompagnata da distinta cartacea o elettronica, da consegnare all'ente emettitore richiedente, dalla quale si evinca il numero di CNS inizializzate ed i relativi numeri seriali.

Enti emettitori

Per quanto riguarda gli enti emettitori, essi devono rispettare caratteristiche di qualità e di affidabilità tali da garantire la sicurezza dell'intero circuito.

In particolare devono:

- definire le procedure del sistema di emissione e gestione della CNS in modo conforme alle specifiche di qualità previste dalla norma ISO 9000;
- soddisfare i requisiti di sicurezza del circuito della CNS;
- definire modalità di interazione con i produttori ed i certificatori che forniscano adeguate garanzie di affidabilità e sicurezza;
- predisporre un manuale operativo che evidenzi le procedure seguite per la gestione di tutte le fasi del processo di emissione e di gestione della CNS;
- predisporre un manuale utente che illustri le modalità d'uso della CNS, i modi per usufruire dei servizi in rete e le procedure da seguire in caso di smarrimento, furto o timore di compromissione della carta;
- organizzarsi in modo da costituire il riferimento per ogni problema di funzionalità, disponibilità o sicurezza del circuito di emissione, rendendo disponibile un recapito telefonico costantemente attivo;
- predisporre il piano della sicurezza relativo all'intero circuito di emissione.

L'ente emettitore può avvalersi di servizi di terzi per lo svolgimento delle funzioni di emissione della CNS o di parte di esse, purché questi assicurino il rispetto dei requisiti di cui ai precedenti punti.

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

Certificatori

Possono operare come emettitori dei certificati di autenticazione della CNS esclusivamente i certificatori accreditati di cui all'articolo 5 del Decreto Legislativo 23 gennaio 2002, n.10.

Tali soggetti devono operare in aderenza alle vigenti norme che regolano l'emissione e la gestione dei certificati qualificati.

I certificatori che rilasciano certificati di autenticazione CNS sono iscritti in un elenco consultabile in via telematica, tenuto dal CNIPA in perfetta analogia con la normativa sulla firma digitale.

2.2.8 La sicurezza

La sicurezza della CNS dipende:

- dalle caratteristiche intrinseche della carta;
- dalla modalità con cui questa viene utilizzata e gestita;.
- dalla sicurezza del ciclo di produzione e del circuito della CNS.

Per quanto concerne il primo punto, le regole tecniche fanno riferimento a standard che assicurano un elevato livello di protezione delle carte nei confronti di possibili attacchi.

Il secondo aspetto viene demandato alla responsabilità dell'ente emettitore che ha il compito di fornire una adeguata informativa all'utente sulle regole per il corretto uso della carta e sulle procedure da seguire in caso di problemi.

Per quanto concerne l'ultimo aspetto, va osservato che il modello adottato permette diverse soluzioni organizzative. Infatti, in funzione delle strategie e delle scelte di mercato dell'ente emettitore, le strutture che concorrono alla produzione e gestione della CNS possono far capo ad un diverso numero di organizzazioni, non escludendosi il caso che una stessa organizzazione gestisca l'intero ciclo di vita della CNS.

Le regole tecniche forniscono dunque delle indicazioni di carattere generale che devono trovare corretta applicazione nell'effettivo contesto operativo. Tali indicazioni saranno esposte in un successivo capitolo del presente documento.

L'ente emettitore potrà definire varianti alle linee guida che consentano una maggiore flessibilità, mantenendo livelli di sicurezza equivalenti. L'Ente emettitore, peraltro, può adempiere a tali requisiti utilizzando fornitori già in possesso di idonea certificazione o accreditamento nazionale o internazionale.

Capitolo 3

Interoperabilità tra le carte

La proliferazione non controllata di carte di differenti produttori, anche se omogenea con gli standard di riferimento, comporta un elevato rischio di interoperabilità anche tra applicazioni coerenti. Ne consegue che l'interoperabilità deve essere garantita, al fine di evitare sprechi di risorse, tramite ulteriori regole.

Tali regole possono essere il risultato di due scelte architetturali:

- uniformità del sistema operativo della smart card, della sua organizzazione e struttura interna dei dati;
- appropriato riconoscimento della carta da parte dell'applicazione che gestisce quest'ultima.

Nei paragrafi successivi viene trattata in dettaglio la tematica dell'interoperabilità, approfondendo gli aspetti tecnici e funzionali e fornendo delle motivazioni relative alla scelta effettuata.

Prima di entrare nel dettaglio delle possibili soluzioni, saranno esaminati gli standard riconosciuti a livello internazionale che disciplinano la materia delle smart card (carte a microcircuito).

E' bene, inoltre, ricordare che i progetti che utilizzano pienamente la specifica Netlink (descritta nel capitolo successivo), devono prevedere due distinte tipologie di carte: la carta del cittadino (CNS) e la carta dell'operatore sanitario.

La carta del cittadino, che ha la funzione di carta sanitaria, contiene le informazioni di carattere sanitario e le chiavi simmetriche segrete, derivate dalle chiavi di gruppo custodite dalle strutture del Ministero della salute, al fine di custodire le informazioni sensibili. Essa contiene inoltre la chiave asimmetrica privata e il certificato digitale del cittadino utilizzate per i processi di autenticazione e attestazione che saranno descritti nel seguito. La carta dell'operatore sanitario contiene le chiavi di gruppo del Ministero della salute per accedere ai dati protetti della carta del cittadino, certificato e chiave asimmetrica privata per la firma digitale. Infine contiene il certificato e la chiave asimmetrica privata per i processi di autenticazione e cifratura dei dati.

E' bene anche ricordare che la descrizione successiva è svolta per completezza descrittiva, ma la soluzione di riferimento è quella presentata nel successivo capitolo relativo al Protocollo d'intesa 13 maggio 2003.

3.1 Standard di riferimento

Lo standard internazionale che definisce, nell'ambito delle carte a microcircuito, le caratteristiche fisiche ed elettriche, il protocollo di comunicazione, il protocollo applicativo, l'organizzazione dei dati e gli aspetti di sicurezza è la norma ISO/IEC 7816. Essa è suddivisa nelle seguenti parti:

- Parti 1 e 2 per la definizione delle dimensioni, delle caratteristiche meccaniche ed elettriche, le condizioni ambientali di funzionamento e la disposizione dei contatti elettrici;

- Parte 3 che disciplina in merito ai seguenti temi :
  - le caratteristiche elettriche dell'interfaccia;
  - il protocollo di comunicazione per il trasferimento dei comandi tra lettore e carta;
  - la risposta al comando di "reset" (ATR) in cui sono contenute le informazioni atte ad individuare il tipo di carta ed il costruttore della stessa.

- Parte 4 che disciplina in merito ai seguenti temi :
  - il formato dei comandi applicativi (APDU) per accedere ai dati ed alle funzioni di sicurezza interne della carta;
  - le modalità per costruire ed organizzare le strutture dati (file system);
  - le modalità di accesso;
  - la tipologia delle strutture dati ovvero la tipologia dei file che conterranno i dati.

- Parte 5 che disciplina in merito alle procedure per l'ottenimento degli "application identifiers";

- Parte 6 che disciplina in merito allo "Inter-industry data element" cioè la modalità con cui descrivere e codificare i dati all'interno della smart card;

- Parte 7 (non pubblicata);

- Parte 8 che disciplina in merito ai seguenti temi :
  - protocolli di sicurezza ed estensioni del secure messaging definito nella parte 4 della norma;
  - la definizione degli ambienti di sicurezza e la loro gestione;
  - l'estensione dei comandi applicativi (APDU), definiti nella parte 4, per la gestione degli ambienti di sicurezza e l'espletamento delle funzioni di sicurezza (es.: gestione della chiave privata di firma, comando di firma digitale,etc.).

- Parte 9 che disciplina in merito ai seguenti temi :
  - la gestione del ciclo di vita della carta e degli oggetti ad essa correlati;
  - definizione degli attributi di sicurezza degli oggetti crittografici;
  - formalizzazione, rispetto a quanto definito nella parte 4, delle condizioni di accesso;
  - estensione dei comandi applicativi (APDU), rispetto a quanto definito nella parte 4 e 8, sopratutto per ciò che concerne la gestione del ciclo di vita della carta e degli oggetti ad essa correlati.

Le parti 3,4,8 e 9 definiscono il sistema operativo della smart card e come questa si interfaccia ai dispositivi di lettura e scrittura, mentre le parti 5 e 6 specificano come definire gli identificativi delle applicazioni e come strutturare i dati contenuti nei file.

Altre parti come la 10, la 11 e la 15 sono in sviluppo o già pubblicate ma il loro contenuto è al di fuori degli scopi del presente documento.

Nei paragrafi successivi sarà fornita una panoramica sull'applicazione di tale norma da parte dei produttori di carte a microcircuito.

3.1.1 Carte e norme ISO, lo stato dell'arte

La norma ISO 7816 può essere considerata la specifica di riferimento per la progettazione delle smart card soprattutto per le carte che in gergo sono chiamate *ID-Card*, ovvero le carte di identificazione come, la Carta Nazionale dei Servizi e la Carta di Identità Elettronica. E' doveroso osservare che le varie parti della norma sono state emesse in tempi differenti e, a volte, tali da poter essere recepite solo dai fornitori che si accingevano a progettarne una nuova e tali da scoraggiare le aziende che avevano da poco immesso una carta sul mercato (ad esempio la parte 9 è stata emessa solo un anno dopo la parte 8). Un altro aspetto consiste nella libertà di interpretazione che viene lasciata in alcuni punti della norma e che spinge i produttori ad adottare soluzioni quanto più possibile vicine a quelle adottate nelle precedenti realizzazioni.

L'effetto di tutto ciò è riassumibile nel seguente modo:

- sino alla parte terza la norma è rispettata praticamente da tutti i fornitori e questo implica che a livello di protocollo fisico esiste interoperabilità e, grazie alla standardizzazione della risposta all'inizializzazione (ATR), le applicazioni sono in grado di capire con quale carta stanno interagendo e chi ne è il produttore;
- la parte quarta è ampiamente rispettata almeno per ciò che concerne l'organizzazione delle strutture dati (file system) e l'implementazione dei comandi applicativi per la creazione, cancellazione, lettura e scrittura dei file; non si può dire altrettanto per i comandi relativi alla gestione ed utilizzo delle chiavi asimmetriche utilizzati nei processi di autenticazione e di firma digitale; tali comandi sono implementati in modo proprietario;
- la parte 8 è recepita da un numero ristretto di fornitori e nella maggior parte dei casi limitatamente all'estensione dei comandi applicativi e con differenti livelli di conformità;
- la parte 9 è rispettata solo da pochissimi fornitori e da questi solo parzialmente.

Da quanto esposto si evince che l'esigenza di interoperabilità tra le carte non può essere soddisfatta solamente con la richiesta di dispositivi conformi alla norma ISO 7816 in quanto questa è soggetta ad implementazioni parziali, ma deve essere affrontata secondo le modalità anticipate nel presente capitolo.

3.1.2 Interoperabilità a livello applicativo

Questo livello di interoperabilità, come anticipato precedentemente, non pone vincoli restrittivi sul sistema operativo delle smart card, salvo la presenza di comandi consoni alle applicazioni che si vogliono sviluppare (es.: presenza di motori crittografici se devono essere attivati processi di autenticazione o di firma digitale). L'interoperabilità è garantita dagli strati Software di interfaccia. mostrati nella figura 1. Questi, che chiameremo Software di Gestione Unificata (**SGU**), consentono di utilizzare smart card di differenti fornitori senza vincoli restrittivi sul sistema operativo. L'architettura descritta si presta a processi di Autenticazione e Firma Digitale ma è carente per quanto concerne la gestione dei dati sanitari o dei servizi erogati dalle Pubbliche Amministrazioni Locali (es.: applicazioni qualificate dei Comuni). Dopo aver esaminato nel dettaglio l'architettura SW saranno mostrati gli ampliamenti per la gestione di dati non strettamente crittografici.

Inoltre, in appendice 3, vengono descritti i dati presenti sulla CNS, descrivendone contenuto e codifica.

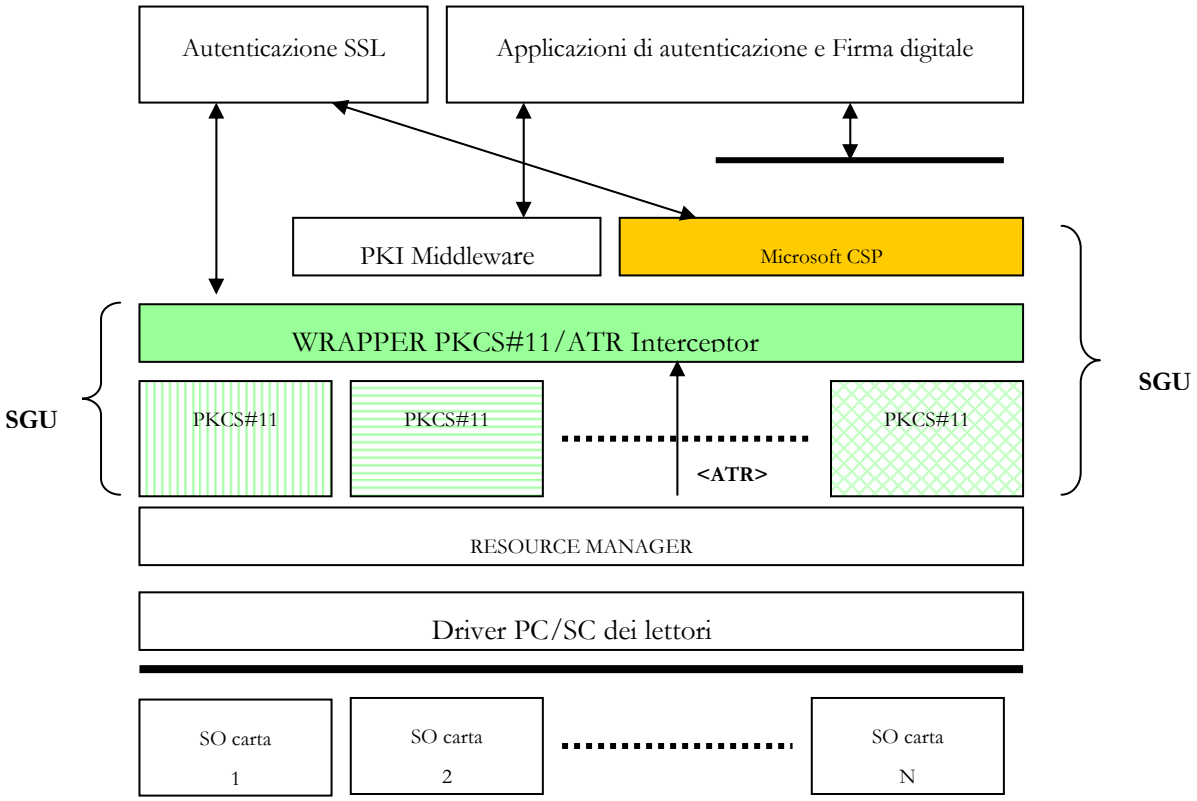


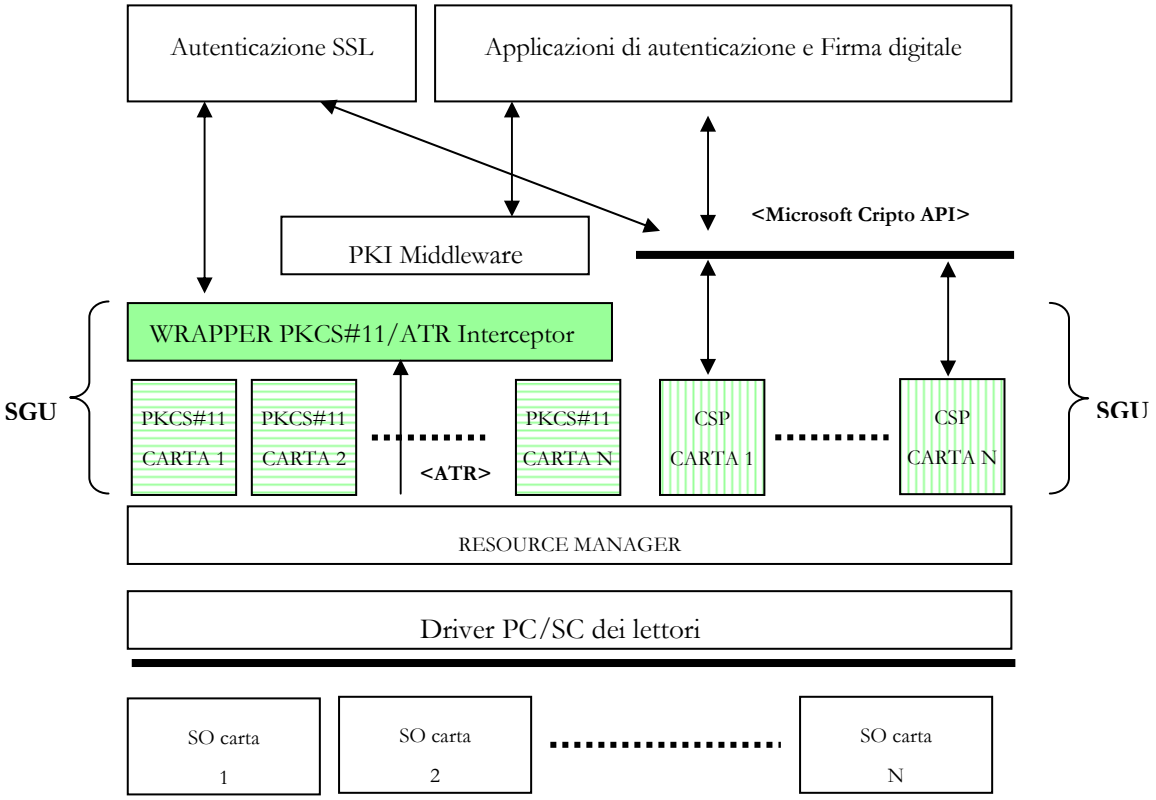
Fig. 1

In questo scenario ogni fornitore, oltre alla smart card, deve rendere disponibile anche la libreria crittografica PKCS#11, realizzata in funzione dei comandi applicativi (APDU) della propria smart card; tale libreria deve essere integrata nel Software di Gestione Unificata (**SGU**). All'atto dell'inserzione di una smart card il Resource Manager dell'ambiente Windows rende disponibili le informazioni della risposta al reset (ATR), fornendo quindi uno strumento per attivare la libreria PKCS#11 specifica della carta (se questa è stata prevista nel modulo **SGU)**. L'attivazione della libreria può essere fatta dal PKCS#11 WRAPPER al quale è anche affidato il compito di rendere omogenee le funzioni esposte da ciascuna libreria.

A valle di questa operazione sarà possibile attivare i processi di autenticazione SSLv3 con i BROWSER che utilizzano le librerie PKCS#11 e processi di Firma digitale tramite applicazioni che si appoggiano a middleware crittografici di mercato (PKI Middleware).

Per consentire l'utilizzo di Browser di grande diffusione presso l'utenza, come Internet Explorer, è necessario disporre di un ulteriore strato SW esclusivo dell'ambiente Microsoft, il Crypto Service Provider (CSP). Attraverso questo strato sono possibili processi di autenticazione in modalità SSLv3 oppure applicazioni di Firma Digitale che utilizzano le Cryptographic API di Microsoft (C-API).

In genere i fornitori di carte, insieme alle librerie PKCS#11 forniscono anche le librerie CSP, necessarie per interfacciarsi con l'ambiente Microsoft (Browser IE, Outlook, OutlookExpress …).



Le applicazioni risiedenti su PC (Application) sono messe in comunicazione con applicazioni sulla carta per mezzo del gestore delle risorse ICC (ICC Resource Manager) ed un fornitore di servizi.

Resource Manager

È il modulo più utilizzato anche in contesti e piattaforme non Microsoft e si occupa di tre aspetti legati alla gestione di lettori e carte multipli. Il componente fa parte del Sistema Operativo del PC.

Identificazione ed indirizzamento delle risorse disponibili
Contiene una lista dei lettori installati e delle carte per cui esiste un fornitore dei servizi. Identifica le interfacce supportate, sia comuni (accesso ai file e autenticazioni) che appartenenti a standard di dominio ristretto (EMV, GSM). Mantiene informazioni sulle carte inserite nei lettori e segnala inserimenti o rimozioni. Si occupa della connessione logica tra funzioni offerte dalle carte e fornitore dei servizi (Service provider).

Allocazione delle risorse tra applicazioni multiple
Permette alle applicazioni l'accesso esclusivo o condiviso a dati e funzioni della carta e fornisce lo stato delle risorse. Si occupa di accessi concorrenti a risorse in mutua esclusione.

Controllo delle transazioni per specifiche carte
Assicura che particolari sequenze di comandi siano portate a termine senza interruzioni, come avviene in contesto transazionale.

Crypto Service Provider

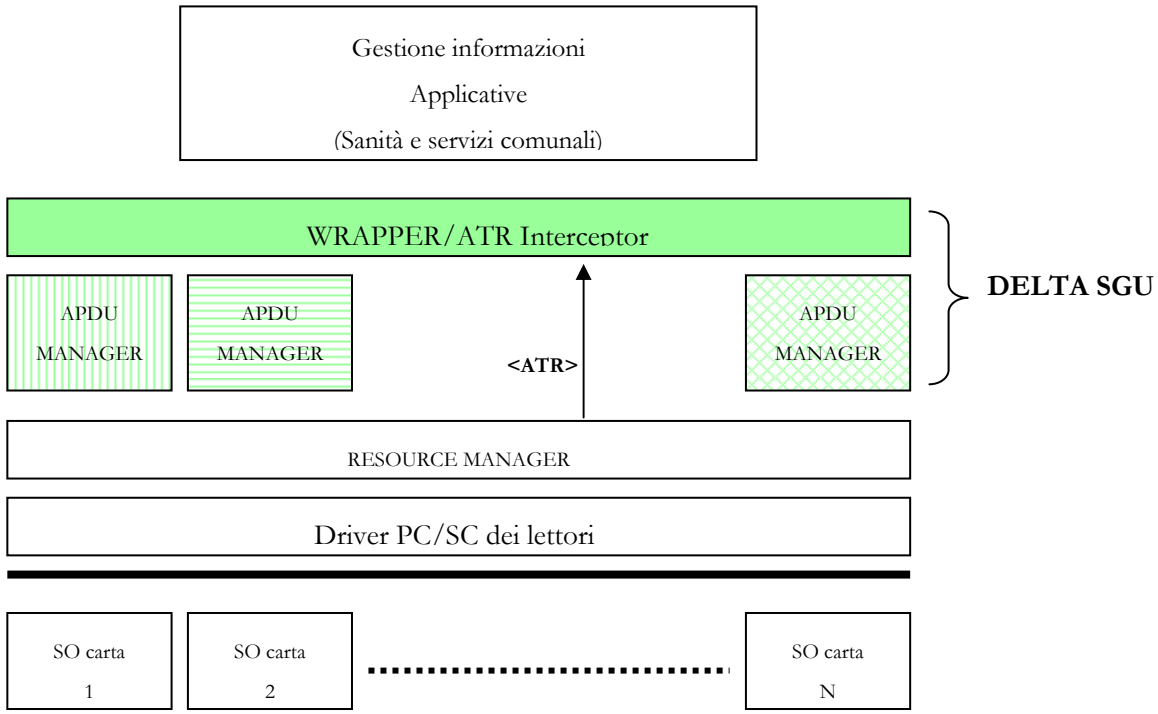
Questo componente, fornito dagli sviluppatori della carta, fornisce un'interfaccia di alto livello che definisce le funzioni supportate da una specifica carta, ed in particolare fornisce servizi crittografici, che presentano particolari condizioni di Input/Output. Contiene le specifiche di componenti opzionali dipendenti dalla specifica carta (per esempio coprocessori crittografici). Le interfacce supportate sono definite per:

- Generazione e gestione di chiavi crittografiche
- Generazione di numeri casuali
- Firme digitali
- Scambio di chiavi e gestione dati crittografati

Per poter gestire le informazioni sanitarie contenute nella smart card del cittadino, ad esempio i dati di emergenza, ed effettuare processi di autenticazione locale tra la carta dell'operatore sanitario e la carta del cittadino è necessaria. una visibilità "fine" dei comandi APDU rispetto a quella offerta dalle librerie crittografiche. In questo caso i fornitori di smart card dovranno rendere disponibili ulteriori moduli SW, che chiameremo APDU Manager, allo scopo di poter intervenire sulle strutture dati delle smart card. Il Modulo Wrapper , che oltre alla libreria crittografica attiverà anche il modulo APDU Manager, dovrà esser tale da fornire alle applicazioni una visione unificata dei comandi APDU (questo modulo è più di un semplice Wrapper ed è relativamente sofisticato). La figura seguente mostra come deve essere arricchito il modulo **SGU**.

Il discorso vale anche nel caso delle librerie CSP, che inglobano il modulo ICC Service Provider. Questo componente, fornito dagli sviluppatori della carta, fornisce un'interfaccia di alto livello che definisce le funzioni supportate da una specifica carta. In generale contiene i comandi specificati dalla 7816-4, ma può includere anche particolari funzionalità personalizzate. Prima di potere fornire il servizio alle applicazioni deve essere inizializzato presso il Resource Manager.

Per quanto riguarda il WRAPPER /ATR Interceptor, in ambiente Microsoft è il resource manager che, inserita una carta del lettore, riceve la stringa ATR e la passa al servizio di winlogon. Il servizio, ricerca nel registry del S.O.la corrispondenza con gli ATR registrati e, se presente, attiva il CSP relativo.



I punti a favore di questa soluzione sono rilevanti, in quanto questa consente, entro ragionevoli limiti, di non essere condizionati dai fornitori di carte e può essere considerata uno strumento di standardizzazione. Tuttavia presenta alcuni punti a sfavore:

- se non ci si limita alla Firma Digitale o a processi di autenticazione basati sull'utilizzo di Infrastrutture a Chiave Pubblica non è sufficiente disporre delle librerie PKCS#11 /CSP e del

modulo APDU Manager, ma è necessario definire il File System delle carte, le sue modalità di navigazione e le condizioni di accesso; da questo punto di vista non è a priori certo che una carta valga l'altra anche se entrambe sono dotate di motori crittografici indispensabili nei processi di Firma ed Autenticazione;

- l'architettura SW descritta è efficiente nella fase di utilizzo delle smart card ma non considera in modo esaustivo le fasi di inizializzazione ed emissione che restano vincolate al sistema operativo della Carta; questo aspetto deve essere valutato con attenzione quando si intenda distribuire sul territorio milioni di carte come nel caso del progetto CRS-SISS.

Il modulo **SGU** precedentemente descritto ha un discreto livello di sofisticazione e deve essere mantenuto aggiornato in termini di librerie PKCS#11, CSP e moduli APDU manager. Questa soluzione potrebbe rivelarsi uno strumento poco efficiente nell'ottica di una distribuzione capillare ai cittadini che intendano utilizzare la smart card sul proprio Personal Computer per accedere ai servizi resi disponibili dalle Pubbliche Amministrazioni.

3.1.3 Interoperabilità a livello di sistema operativo della carta

Questo livello di interoperabilità, come anticipato precedentemente, prevede l'omogeneità dei sistemi operativi delle carte a microcircuito e della struttura del file system. Lo standard internazionale a cui riferirsi è la norma ISO 7816 e nell'ambito di tale norma devono essere fatte le scelte che condizionano il sistema operativo. I principi che devono guidare nella scelta delle funzionalità del sistema operativo, compatibilmente con le esigenze applicative, sono:

- completa conformità con la parte 3 in quanto adottata praticamente da tutti i produttori e indispensabile sia per l'interoperabilità a livello di sistema operativo che a livello di applicazione;
- conformità con la parte 4 almeno per quanto concerne i comandi APDU inerenti la gestione del file system della carta;
- conformità con la parte 8 almeno per quanto concerne i comandi APDU che trattano gli oggetti di sicurezza;
- conformità con la parte 9 almeno per quanto concerne le condizioni di accesso e i comandi APDU per la gestione del ciclo di vita.

Per gestire una situazione di mercato non perfettamente conforme alle esigenze appena esposte è stato insediato un gruppo di lavoro, coordinato dalla allora attiva Autorità per l'informatica nella pubblica amministrazione, composto da tutti i maggiori produttori di sistemi operativi per carte.

Tale tavolo di lavoro ha sviluppato una soluzione tecnica che soddisfa i requisiti imposti e che è stata formalizzata in un protocollo d'intesa tra i fornitori stessi e il Ministero dell'interno e il Ministro per l'innovazione e le tecnologie. Il paragrafo successivo fornisce una serie di dettagli su questo protocollo d'intesa disponibile in appendice.

3.2 Carte "dual interface"

Alcune tipologie di applicazione rendono non consigliabile l'utilizzo di una carta a contatti. Si pensi ad esempio ai servizi di bigliettazione elettronica (e-ticketing) basati sull'uso di carte a microchip. Queste carte richiedono la capacità di eseguire un numero elevato di interazioni nel tempo più breve possibile e secondo modalità che garantiscano una sufficiente durata del supporto costituito dalla carta.

Come si può intuire, l'interfacciamento tra i terminali di accettazione e le carte attraverso i normali contatti elettrici presenta il duplice inconveniente di un alto tempo di transazione, dovuto sostanzialmente anche al tempo necessario per il corretto inserimento della carta nel lettore, e all'usura dei contatti elettrici che porta a conseguenti malfunzionamenti.

Le smartcard, tuttavia, possono anche essere dotate di un'interfaccia a radiofrequenza (si parla in tal caso di tecnologia RFID e di carte "contactless"), che permette il colloquio tra carta e lettore senza alcun contatto fisico, entro una distanza di alcuni centimetri. Il principale standard di riferimento è quello noto come ISO 14443 che prevede l'uso di una segnale radio con frequenza di 13.56 MHz. Il criterio di modulazione del segnale radio può variare secondo due schemi noti rispettivamente come "Tipo A" e "Tipo B".

L'utilizzo di una carta contactless riduce il tempo complessivo di transazione in quanto la carta dev'essere semplicemente avvicinata al terminale; la transazione può inoltre essere effettuata anche senza estrarre la carta da un portafoglio o da un'apposita custodia. Anche l'usura si riduce ai minimi termini, per evidenti ragioni.

Dal punto di vista della fabbricazione, la plastica di una carta contactless contiene un'antenna necessaria per catturare l'energia del campo elettromagnetico emesso dal terminale (energia che serve anzitutto per alimentare il microprocessore) nonché per scambiare dati col terminale.

Le specifiche tecniche della Carta Nazionale dei Servizi prevedono come obbligatoria l'interfaccia a contatti, nel rispetto dello standard ISO 7816-3, ma non escludono che la CNS sia anche dotata di un'interfaccia contactless. Le carte dotate di entrambe le interfacce (a contatti e contactless) sono chiamate "dual interface".

Si noti che una carta dual interface è sostanzialmente diversa da una carta "ibrida", dove con questo termine si intende una normale carta a contatti il cui supporto plastico contiene anche un "transponder" separato. Solo nel caso di una carta dual interface è possibile interagire coi medesimi dati previsti dalle specifiche CNS (chiavi crittografiche, certificati, dati anagrafici, servizi aggiuntivi, ecc) anche in modalità RFID.

Una CNS di tipo dual interface è evidentemente più versatile di una CNS dotata dei soli contatti elettrici, perché ne consente l'uso anche in applicazioni di bigliettazione elettronica e in ogni altro contesto caratterizzato da esigenze analoghe (per es. rilevazione presenze in azienda, accesso a parcheggi, mense, etc).

3.3 La piattaforma JAVACARD

Una carta CNS deve ovviamente rispettare le specifiche tecniche definite a livello normativo e pubblicate sul sito internet del CNIPA. Queste specifiche non pongono restrizioni sulle caratteristiche del sistema operativo (purché siano garantite le funzionalità delle APDU), quindi la carta può essere dotata di un sistema operativo "nativo" oppure di un sistema JavaCard (Java Card Technology, http://java.sun.com/products/javacard/, Sun Microsystems).

A parità di altre condizioni, l'utilizzo di una carta con tecnologia Javacard offre alcuni vantaggi:

- un supporto multi-applicazione nel senso più pieno del termine: la carta può contenere molteplici applicazioni che rispondono ciascuna ai propri comandi (che possono anche essere proprietari, secondo le esigenze dell'applicazione); applicazioni aggiuntive possono essere installate in modo sicuro sulla carta anche dopo l'emissione;
- la portabilità delle applicazioni sulle carta Javacard di molti differenti produttori (vedere il sito http://www.javacardforum.org/) e dunque anche la possibilità di installare sulla carta applicazioni già pronte (es. applicazioni di pagamento in standard EMV, borsellini elettronici, schemi di loyalty, ecc);
- una maggiore economicità e semplicità nello sviluppo delle applicazioni (applet); poiché un'applet è scritta in linguaggio Java, lo sviluppo può essere realizzato in modo autonomo

dall'Amministrazione emittente, senza necessità di coinvolgimento del produttore della carta, utilizzando strumenti standard di sviluppo software.

Una CNS realizzata con tecnologia Javacard offre dunque più "gradi di libertà" alle Amministrazioni. Per contro, dato che un'applicazione Java tende ad occupare più memoria sul microchip rispetto a quanto richiesto da una carta "nativa", una Javacard deve avere una maggiore capacità di memoria e quindi un prezzo tendenzialmente maggiore di quello di una carta nativa.

Non bisogna dimenticare che bisogna applicare i requisiti di sicurezza che si applicano a tutte le CNS. Pertanto, anche una carta CNS basata su tecnologia Javacard dev'essere sottoposta alla certificazione di sicurezza secondo i criteri indicati dalla normativa sulla firma digitale.

3.4 Il protocollo d'intesa 13 maggio 2003

Essendo passati 36 mesi dalla sottoscrizione del protocollo d'intesa, questo è scaduto alla data di pubblicazione del presente documento. Ma nonostante ciò la sua importanza è stata cruciale per garantire un modello di riferimento nell'ambito dell'interoperabilità delle smart card. Per tali motivi viene lasciato pressoché inalterato, rispetto alle versioni precedenti, il presente paragrafo e di conseguenza il testo del protocollo d'intesa in allegato.

L'appena citata scadenza del Protocollo d'intesa rende necessario una nuova tipologia di aggregazione tra gli enti governativi di riferimento e i produttori di smart card. Sono in fase di studio alcune ipotesi tra le quali quella della costituzione di un tavolo permanente di concertazione tecnica sotto la probabile presidenza del Ministero dell'Interno e il coordinamento tecnico del CNIPA.

Nell'ambito della diffusione degli strumenti d'accesso ai servizi in rete sia di tipo CIE che di tipo CNS si deve garantire la totale e completa interoperabilità delle carte utilizzate su tutto il territorio nazionale. L'interoperabilità è condizione primaria per la diffusione del modello CIE/CNS e dei servizi erogabili ai cittadini, garantendo nello stesso tempo il contenimento dei costi per le pubbliche amministrazioni nel progettare l'infrastruttura di accesso ai servizi. Alla base dell'interoperabilità è il processo di standardizzazione del microprocessore presente sulla smart card, che è previsto essere dello stesso tipo e con analoghe funzionalità sia per la CIE, che per la CNS. A tal fine si è definito uno standard "aperto" che consenta a tutti i produttori di carte di poter fornire microchip conformi ai requisiti previsti.

Come già detto, un apposito gruppo di lavoro ha elaborato, con i produttori di microchip e le pubbliche amministrazioni direttamente interessate al progetto, specifiche comuni e standard che il microprocessore deve possedere. E' necessario ricordare che, allo stato attuale, gli standard internazionali non garantiscono funzionalità di interoperabilità dei microprocessori per quanto riguarda proprio le funzioni di sicurezza nell'accesso ai servizi in rete.

Il gruppo di lavoro ha concluso le sue attività alla fine di gennaio 2003 e il documento finale, accluso in allegato al protocollo di intesa, è stato accettato da tutte le aziende.

Tale documento aggiornato recentemente alla versione 1.1.3 per renderne più chiare alcune parti e eliminare dei refusi è stato considerato anche la base tecnologica per le specifiche tecniche del microchip della CIE.

Ovviamente questo accordo ha costituito un passo fondamentale per l'attuazione dell'e-government, paragonabile alla definizione degli standard GSM per la telefonia mobile o EMV per la carte bancarie di debito e credito. Va ulteriormente ricordato che tale accordo costituisce un'assoluta novità a livello internazionale che può essere proposta in sede comunitaria quale possibile standard da adottare nei progetti e-Europe.

Tra gli elementi fondamentali del protocollo d'intesa è bene mettere in evidenza che i produttori di microchip si impegnano reciprocamente a garantire lo standard tecnologico definito nel progetto

CIE/CNS (art. 2 e art. 4) e a consultarsi periodicamente per la definizione e approvazione di eventuali variazioni indotte dallo sviluppo tecnologico (art. 3).

Una copia del protocollo d'intesa è allegata al presente documento. Le specifiche tecniche contenute nel protocollo sono disponibili sul sito del Centro nazionale per l'informatica nella pubblica amministrazione.

Hanno aderito successivamente al protocollo d'intesa le società:

GEP S.p.A. via Ferrante Imparato, 190 80146 Napoli (in data 20/09/2004);

EPS Engineering And Professional Services Incorporated, Via C. Fracassini, 25 00196 (in data 08/11/2004).

La società Schlumberger ha comunicato in data 09/12/2004 di aver cambiato la denominazione sociale in AXALTO SA.

La società CardNet Group S.p.A. ha comunicato in data 21/02/2005 di aver cambiato denominazione sociale in Kaitech S.p.A.

La società Ghirlanda S.p.A. ha comunicato in data 05/08/2005 di essersi trasformata in Ghirlanda Smart Card Solutions S.p.A. (dopo una scissione parziale delle attività in Ghirlanda Smart card Solutions S.r.l.).

Capitolo 4

L'identificazione e l'autenticazione in rete

L'identificazione è il processo con cui l'utente si dichiara a un sistema o a un'applicazione, l'autenticazione è il processo che consente al sistema o all'applicazione di accertare l'identità dell'utente. I metodi convenzionali sono basati sull'utilizzo della coppia "Username" e "Password", dove il primo elemento è fornito dall'utente per farsi riconoscere ed il secondo elemento viene fornito, sempre dall'utente, come prova di identità. Facendo un paragone con le tecniche moderne che fanno uso di infrastrutture a chiave pubblica e di dispositivi sicuri come le smart card si può sostenere che:

- lo "Username" è sostituito da un certificato digitale;
- la "Password" è sostituita da un crittogramma prodotto per mezzo della chiave privata di autenticazione contenuta nella smart card.

Nei paragrafi successivi vengono descritti in dettaglio i processi di autenticazione basati sull'utilizzo di smart card e di infrastrutture a chiave pubblica (PKI).

4.1 I processi di identificazione e autenticazione

Prima di affrontare il dettaglio dei processi di Identificazione/Autenticazione, che sfruttano la tecnologia PKI, è opportuno considerare le modalità con cui l'utente interagisce con le applicazioni, ovvero se opera in modalità WEB/Browsing oppure Client/Server.

Nel primo caso esiste la possibilità di utilizzare il protocollo TLS/SSL che è uno standard in ambito Internet, mentre nel secondo caso ci si deve riferire a procedure, chiamate Challenge/Response (CH/R), che definiscono il processo di autenticazione dal punto di vista funzionale, per le quali non esistono prodotti standard ma solo realizzazioni di tipo proprietario strettamente integrate con l'applicazione per cui sono state scritte e quindi difficilmente riusabili.

I successivi paragrafi tratteranno dettagliatamente questi aspetti. In particolare un capitolo sarà dedicato all'ambiente software sul client e un altro all'ambiente di accesso sul server.

4.1.1 Mutua autenticazione tramite il protocollo SSL/TLS

Il protocollo SSL/TLS è garantito da una libreria di programmi che consentono di stabilire un canale di comunicazione tra Browser e WEB Server che può garantire:

- riservatezza del contenuto dei messaggi;
- integrità dei messaggi;
- mutua autenticazione delle parti coinvolte.

Tali caratteristiche vengono ottenute con i seguenti procedimenti:

- per la riservatezza ed integrità dei messaggi:

- il protocollo che prevede l'autenticazione tra server e client, può basarsi su diversi meccanismi (RSA, Fortezza, alcune versioni dell'algoritmo di Diffie-Hellman);
- dopo l'iniziale fase di negoziazione della chiave di sessione, tutti i dati trasmessi sono crittografati, la crittografia è di tipo simmetrico;
- la connessione garantisce l'integrità dei messaggi utilizzando funzioni di hash .

- Per l'autenticazione delle parti:

SSL/TLS prevede l'uso di certificati digitali del tipo X509v3 e di coppie di chiavi asimmetriche utilizzate sia dal web server che dal browser e quindi si presta ad essere utilizzato con smart card crittografiche quali la Carta Nazionale dei Servizi (CNS) e la Carta di Identità Elettronica (CIE).

Il grosso vantaggio offerto da SSL/TLS risiede nel fatto che web browser e web server sono già predisposti per utilizzare tale protocollo e quindi qualunque applicazione WEB può sfruttare le caratteristiche di sicurezza sopra esposte. Occorre solo configurare opportunamente le opzioni di sicurezza del browser e del web server. Nei successivi paragrafi saranno fornite le caratteristiche dei certificati X509v3 adatti al protocollo SSL/TLS.

L'applicazione web, dopo la fase di autenticazione, può procedere a successive fasi di autorizzazione all'accesso ai servizi in funzione degli specifici diritti e privilegi dell'utente. Per fare ciò ha la necessità di riconoscere l'utente estraendo lo "Username" e eventualmente altre informazioni dal certificato.

4.2 L'autenticazione del server

Nello scenario dell'erogazione dei servizi in rete il cittadino deve essere tutelato che chi sta erogando il servizio richiesto sia proprio la pubblica amministrazione competente e responsabile del servizio da erogare. Ciò significa che ogni server della pubblica amministrazione abilitato ad erogare un servizio deve possedere un certificato identificativo.

A tale esigenza organizzativa bisogna aggiungere che sono proprio i meccanismi SSL ad avere bisogno che sul web server sia necessariamente installato un certificato identificativo.

Esistono tre possibilità:

- i siti vengono autenticati da una struttura governativa (Es. SSCE);
- i siti vengono autenticati dai certificatori di firma digitale;
- i siti vengono autenticati da soggetti autorizzati generici.

Nel primo caso va definita e costruita una struttura ad hoc presso un qualche settore governativo; inoltre c'è il rischio che la centralità di questo servizio possa creare problemi di competenza con gli enti locali.

Nel secondo caso si deve garantire un livello di fiducia adeguato dei certificati che queste strutture utilizzano per la loro attività. Il modello che appare adeguato, perché poco invasivo e già sperimentato per la firma digitale, è quello dell'elenco pubblico dei certificatori di autenticazione".

La catena di fiducia rimane sotto il controllo centrale (è indispensabile per garantire integrità ed autenticità dell'elenco stesso) mediante la firma digitale di tale elenco, che può essere effettuata dal Ministero dell'Interno.

Lo stesso vale per la terza ipotesi, anche se in questo caso bisognerebbe discriminare sui servizi offerti. L'autenticazione dei siti non dovrebbe essere effettuata da un soggetto generico se sono offerti servizi di pagamento o comunque servizi ad elevato rischio informatico dal punto di vista dell'analisi del rischio effettuata.

Esistono soluzioni alternative ma come variazione di dettaglio di quelle presentate.

Deve essere risolto il problema delle liste di revoca. Se operano i certificatori, non è efficiente far gestire ai web server le oltre dieci CRL/CSL necessarie. E' invece sicuramente opportuno utilizzare un server , ad esempio di tipo OCSP, che garantisce informazioni applicative sullo stato della revoca e si alimenta per proprio conto con i dati dei certificatori.

Anche in questo esistono soluzioni analoghe ma comunque basate su un server (logicamente) centrale.

4.2.1 Configurazione del client Internet Explorer

Se si dispone della CNS (o della CIE), il client potrà utilizzare la coppia di chiavi contenute nella carta a microprocessore con le modalità che saranno illustrate di seguito[10].

Nel sistema operativo Windows, le funzioni di crittografia sono gestite dal modulo CSP (Cryptographic Service Provider). Quando le chiavi di cifratura sono memorizzate su smart card, il CSP deve essere in grado di interagire con quest'ultima.

Sul sito del CNIPA sono descritte le modalità mediante le quali, quest'ultimo rende disponibile il software di supporto all'uso della CNS da parte dei cittadini e delle amministrazioni.

Con questa soluzione il browser Explorer può utilizzare le funzioni di sicurezza della CNS in modalità nativa.

Sullo stesso sito è anche riportato il manuale utente per l'attivazione della protezione SSL (CIE_CSP Guida Utente)[11].

4.2.2 Configurazione di browser open source (Netscape, Mozilla, ecc.)

I browser Netscape e Mozilla non utilizzano le funzioni del CSP ma interagiscono con le librerie della smart card in modalità PKCS #11.

Anche in questo caso sul sito del CNIPA sono descritte le modalità mediante le quali, quest'ultimo rende disponibile il software di supporto all'uso della CNS da parte dei cittadini e delle amministrazioni.

4.2.3 Configurazione del server

Il responsabile dell'erogazione del servizio dovrà invece provvedere alla generazione di una coppia di chiavi sul web server, nonché alla pubblicazione della chiave pubblica utilizzando un certificato for-

10 Per queste funzioni viene utilizzata la coppia di chiavi, presente sulla smart card, che identifica univocamente la CNS o CIE. Le operazioni crittografiche avvengono all'interno della smart card, in modo che la chiave segreta non possa essere in alcun modo estratta.

11 Le modalità operative per l'installazione e l'utilizzo delle funzioni SSL/TLS dipendono anche dalle caratteristiche del browser e quindi possono variare in funzione della versione utilizzata. Sulla documentazione pubblicata nel sito è riportata la modalità operativa relativa alla versione più recente.

mato X.509 v.3[12]. Dovrà inoltre provvedere ad inserire il certificato utente, reperibile dalla CNS, nell'elenco dei certificati abilitati ad usufruire del servizio.

Il web server dovrà infine essere configurato in modo da gestire la lista dei certificati revocati (CRL)[13].

4.2.4 Installazione del certificato del server

Indipendentemente dal browser utilizzato è necessario che sullo stesso sia presente il certificato che contiene la chiave pubblica del server. Ciò può ottenersi nei seguenti modi:

- il certificato viene preinstallato sul browser (ad esempio con un opportuno kit di installazione);
- il certificato viene scaricato ed installato sul browser al momento del primo utilizzo della funzione protetta (in tal caso uno specifico messaggio chiederà all'utente se intende installare ed utilizzare il certificato);
- il certificato del server è firmato da una certification authority il cui certificato è presente per default sul browser, in tal caso non è necessaria alcuna installazione.

Ovviamente l'ultima soluzione è quella più semplice sotto l'aspetto operativo, ma richiede che si utilizzino i servizi di una certification authority appartenente ad una ristretta rosa di società i cui certificati sono inseriti «all'origine» nei browser.

4.3 Personalizzazione delle funzioni di sicurezza

La soluzione esposta ha il vantaggio di non richiedere la scrittura di software aggiuntivo, ma presenta le seguenti limitazioni:

- è adatta solo ad applicazioni di tipo web (ad esempio non è utilizzabile per applicazioni client server tradizionali);
- non permette di realizzare funzioni di sicurezza diverse da quelle standard SSL/TLS;
- le modalità operative sono rigidamente condizionate dai prodotti browser e web server utilizzati.

In tutti quei casi in cui tali limitazioni non sono accettabili, è possibile utilizzare funzioni di sicurezza «ad hoc».

In generale sono possibili due strade:

- l'impiego di funzioni di sicurezza proprie dell'ambiente client Windows (ad esempio le funzioni del CIE_CSP utilizzabili con le CryptoApi o l'interfaccia standard PKCS#11);
- l'interazione con il middleware che gestisce la smart card attraverso i Metacomandi.

12 Ciò può essere fatto sfruttando le caratteristiche del web server oppure ricorrendo ai servizi di un certificatore. Nel caso di ricorso a certificati acquisiti da terzi, è necessario che gli stessi consentano la crittografia simmetrica con chiavi lunghe 128 bit.

13 La verifica della validità del certificato mediante accesso alla CRL è gestita in modo differente dai web server.

Tra le due possibilità deve essere preferita la seconda, in quanto consente l'interazione con l'ambiente di sicurezza attraverso una modalità standard indipendente dallo specifico ambiente software.

Utilizzando i Metacomandi è infatti possibile combinare le funzioni di sicurezza in modo semplice ed integrato con le altre funzioni applicative. In ogni caso tali funzioni applicative devono essere sviluppate secondo il modello di autenticazione Challenge/Response (CH/R).

4.4 Autenticazione in modalità Challenge/Response(CH/R)

Questa modalità di autenticazione consente di accertare l'identità dell'utente tramite un processo relativamente semplice, che non ha impatti di tipo computazionale sia sul client che sul server erogatore del servizio, ma deve essere appositamente sviluppata in conformità con l'ambiente operativo sia del client che del server.

Il processo di autenticazione in modalità CH/R segue i seguenti passi funzionali:

- dopo una fase iniziale di identificazione, eseguita verificando il certificato dell'utente, il server produce un messaggio di autenticazione (Challenge), in generale diversificato da un numero pseudocasuale per evitarne possibili riutilizzi, e lo invia al client;
- il client, tramite la chiave privata dell'utente, effettua un'operazione di "signature" del Challenge producendo il Response che rinvia al server;
- il server, per mezzo della chiave pubblica contenuta nel certificato dell'utente ne accerta l'identità verificando l'autenticità del Response.

Dopo la fase di autenticazione il server può procedere a successive fasi di autorizzazione all'accesso ai servizi in funzione degli specifici diritti e privilegi dell'utente.

La coppia di chiavi ed il certificato di autenticazione specifici per il protocollo SSL/TLS possono essere utilizzati anche per i processi di autenticazione in modalità CH/R.

Il processo di autenticazione in modalità CH/R, da un punto di vista strettamente tecnico, può essere effettuato tramite la coppia di chiavi e il certificato destinati alla Firma Digitale, ma è doveroso osservare che ciò è espressamente vietato dalle norme che disciplinano la Firma Digitale in ambito Nazionale ed Europeo per pericolosi rischi che questa pratica comporta.

Bisogna considerare che la firma digitale è un processo che un utente attiva su un documento elettronico a lui noto, che intende firmare digitalmente e che è conscio di non poter ripudiare. A discrezione dell'utente, questo processo può essere effettuato anche in modalità stand alone.

Il processo di autenticazione CH/R è strettamente on line e induce l'utente a firmare un messaggio che è, in generale, non visibile e prodotto nell'ambito stesso del processo di autenticazione.

È possibile utilizzare l'autenticazione CH/R anche utilizzando un browser. In questo caso su di esso, in base al tipo di browser, deve essere caricato un "Plugin", un'Applet oppure un ActiveX al fine di attivare la componente client del processo.

Capitolo 5

I Certificati digitali

I processi di autenticazione descritti nei precedenti paragrafi fanno uso di tecniche PKI e quindi impiegano chiavi asimmetriche e certificati digitali. Queste quantità di sicurezza non sono utilizzate solamente per l'autenticazione in rete, ma anche per l'apposizione di firme digitali e per la produzione di buste crittografiche. Per questa ragione, nel seguito, saranno esaminate le caratteristiche dei certificati digitali e il formato dei dati da sottoporre sia ai processi di autenticazione che alle operazioni di firma digitale e crittografia.

5.1 Certificati e formati per la Firma Digitale

In accordo con quanto previsto dalla normativa vigente, il certificato di firma digitale per l'utilizzo di una smart card (come strumento di *sottoscrizione* di documenti elettronici) deve essere conforme allo standard RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (alla data sostituito da RFC 3280) e contenere almeno le seguenti informazioni:

- numero di serie del certificato di sottoscrizione;
- ragione o denominazione sociale del certificatore;
- codice identificativo del titolare presso il certificatore (campo **subject** del certificato = **common name + description**);
- nome cognome e data di nascita del titolare;
- valore della chiave pubblica;
- tipo di algoritmi di generazione e verifica della sottoscrizione del titolare;
- inizio e fine del periodo di validità della coppia di chiavi;
- tipo di algoritmo di sottoscrizione utilizzato dal certificatore;
- eventuali limitazioni nell'uso della coppia di chiavi.

In particolare il **common name**, (object ID = 2.5.4.3), ha la seguente struttura:
<cognome>/<nome>/<codice fiscale>/<identificativo titolare presso il certificatore>.

Il campo **description** (object ID = 2.5.4.13), ha la seguente struttura:

*"**C="**<cognome esteso>"/**N="**<nome esteso>"/**D="**<data di nascita>["/**R="**<ruolo titolare>]*

Le estensioni necessariamente presenti nei certificati e quindi, secondo la specifica pubblica RFC 3280, sono:

- Authority Key Identifier: identifica la chiave pubblica corrispondente alla chiave privata utilizzata dal Certificatore per sottoscrivere il certificato;
- Subject Key Identifier: identifica certificati che contengono una particolare chiave pubblica;
- Key usage (estensione critica): indica l'uso delle chiavi (**non repudiation**);
- Certificate Policies: specifica la policy di riferimento del certificato ed il sito di distribuzione del manuale operativo;
- CrlDistributionPoint: contiene l'indirizzo che indica dove reperire la Certificate Revocation List che eventualmente conterrà le informazioni di revoca relative al certificato.

Questi certificati devono essere utilizzati per verificare la firma di documenti prodotti con la chiave privata a cui fanno riferimento. Il tentativo di usarli in un browser con il protocollo di mutua autenticazione SSL/TLS produrrebbe il rifiuto del certificato da parte del browser, causato dal **Key Usage** che, essendo una estensione critica, è obbligatoriamente verificata.

Il formato dei dati e le buste crittografiche utilizzate per la firma digitale fanno riferimento ai seguenti standard:

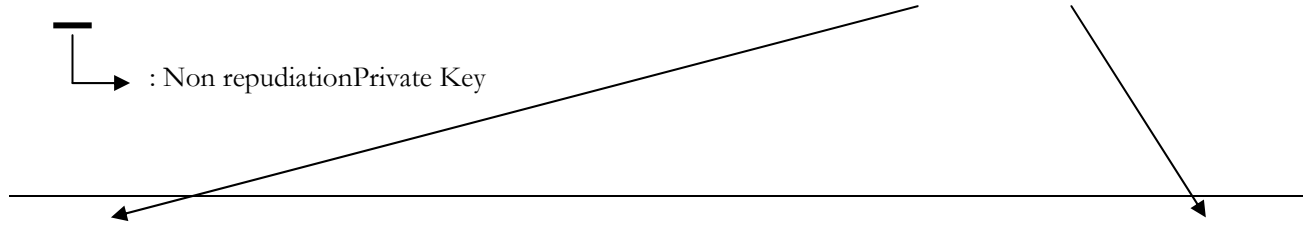
- PKCS#1 (RSA Laboratories - RSA Cryptography Standard);
- PKCS#7 (RFC 2315).

PKCS#1 è lo standard di riferimento per la crittografia a chiave pubblica applicata, fra gli altri, alla Firma Digitale di documenti elettronici e per i processi di autenticazione e crittografia in rete Internet.

PKCS#7 è lo standard di riferimento per le buste crittografiche create per contenere la firma e il documento al quale si riferisce.

Dato un messaggio "M", la componente che deve essere firmata digitalmente è l'impronta di "M" ed il formato dei dati da sottoporre al processo di firma secondo lo standard PKCS#1 è rappresentato nella figura seguente:

Key Identifier	**Padding**	**Delimiter**	**ID_Hash**	**Message Hash**
00 01h	FF FF FF FFh.....FF FF FF FFh	00		Hash(M)



ID HASH_SHA-1 (Codifica BER della sintassi ASN.1)						
Tag	LL	Tag	LL	ID encapsulation	Hash Tag	Hash LL (20 byte)
30	21h	**30**	09h	06 05 2B 0E 03 02 1A 05 00	**04**	14h

Le smart card conformi allo standard ISO 7816-8/9 (vedere paragrafo relativo agli standard di interoperabilità tra le carte) ammettono il formato PKCS#1 e, nei confronti delle operazioni di Digital Signature, si comportano nel seguente modo:

- controllano che l'oggetto chiave privata sia identificabile come chiave di firma digitale e non come chiave di autenticazione o di crittografia;
- se la precedente condizione è verificata forzano automaticamente il formato dei dati di firma secondo lo standard PKCS#1 descritto nella figura precedente.

Se si tentasse di utilizzare una chiave di autenticazione o di "encryption" con un comando di Signature la smart card restituirebbe un codice di errore.

5.2 Certificati di autenticazione e crittografia

Sono di seguito rappresentate le caratteristiche salienti dei certificati di autenticazione e crittografia secondo lo standard X509v3, soprattutto per ciò che concerne le differenze con i certificati per la firma digitale. Le differenze salienti, cioè quelle che ne vincolano l'utilizzo, sono contenute nelle estensioni ed in particolare nel **Key Usage** e nello **Extended Key Usage**.

Sono previste dallo standard X509v3 le seguenti estensioni:

- **Key Usage** (critica) ::= Authentication, Encryption, Signature;
- **Extended Key Usage** ::= Client Authentication, Secure e-mail (non previste nel certificato di firma digitale);

Le precedenti estensioni consentono di utilizzare il certificato e la coppia di chiavi a cui esso si riferisce, nei seguenti ambienti:

- Browser WEB per l'autenticazione tramite il protocollo SSLv3;
- User Agent di posta elettronica per la produzione di e-mail cifrate e firmate elettronicamente secondo il formato standard S/MIME.

La componente Signature del **Key Usage** non è riferita alla Firma Digitale ma alla firma elettronica del formato S/MIME 2.

Ricordiamo infatti che il **Key Usage** per la firma digitale è : **non repudiation**.

La Carta di Identità Elettronica e Carta Nazionale dei Servizi usano, per i processi di autenticazione in rete, un certificato con le caratteristiche sopra descritte. Il profilo dettagliato, facente parte delle regole tecniche descritte nel capitolo 2 viene riportato in appendice.

5.3 Processo di attestazione

Nell'ambito del progetto CRS LOMBARDIA– SISS della Regione Lombardia la carta specifica del progetto è anche utilizzata per attestare la presenza del cittadino durante l'erogazione di un servizio

sanitario. Per Attestazione si intende la firma elettronica di un documento effettuata con la chiave privata e certificato di autenticazione a bordo della carta del cittadino.

L'attestazione non ha di per sé valore legale ma è considerata valida solo nell'ambito del progetto CRS LOMBARDIA-SISS e per i fini sopra detti.

Capitolo 6

Le applicazioni sanitarie della carta

L'installazione facoltativa della componente sanitaria (Netlink) sulla CNS avviene in due fasi distinte:

- inizializzazione della CNS a cura dei produttori;
- formazione della CNS e caricamento dei dati sanitari.

Nella prima fase i produttori, delegati dall'Ente emettitore, predispongono le strutture dati sanitarie (secondo le specifiche Netlink), compilano i file elementari che non contengono dati specifici del cittadino e caricano le quantità di sicurezza derivate dalle chiavi di gruppo fornite dal Ministero della Salute.

I produttori devono garantire la segretezza delle chiavi di gruppo, conservandole in dispositivi che ne consentano l'utilizzo al solo fine di inizializzare le carte, ma ne impediscano la lettura o l'esportazione dei dati contenuti. L'Ente emettitore renderà disponibili, in modo sicuro, le chiavi di gruppo previa autorizzazione del Ministero della Salute.

Per la gestione della seconda fase (personalizzazione e caricamento dei dati sanitari), le Regioni possono costituire Centri Servizi Regionali omologati per il territorio di competenza.

La realizzazione della seconda fase può avvenire secondo le modalità che sono di seguito brevemente descritte e che possono essere liberamente scelte dagli enti emettitori:

- si utilizza un Centro Servizi Regionale il quale, per gli Enti emettitori che effettuano questa scelta, effettua la fase di formazione della CNS, l'installazione dei dati sanitari ed eventualmente il rilascio;
- gli Enti emettitori gestiscono autonomamente la formazione della CNS oppure si avvalgono di un Centro Servizi diverso da quello Regionale; in questo caso durante la fase di formazione sono installati i dati sanitari tramite collegamento con le ASL con cui gli Enti Emettitori avranno stabilito una opportuna convenzione;
- gli Enti emettitori gestiscono autonomamente la formazione della CNS oppure si avvalgono di un Centro Servizi diverso da quello Regionale e , dopo la fase di formazione e prima del rilascio della carta ai cittadini, inviano i lotti di CNS al Centro Servizi Regionale affinché possano essere caricati i dati sanitari;
- gli Enti emettitori gestiscono autonomamente la formazione della CNS predisponendo le strutture dati secondo quanto specificato in questo paragrafo e la rilasciano senza dati sanitari; i cittadini si recano presso gli sportelli delle amministrazioni competenti con cui l'ente emettitore avrà preventivamente stabilito accordi.

6.1 Il modello di sanità basato sulla Carta Sanitaria.

Nell'ambito dei vari progetti di e-government, che vengono sperimentati a livello nazionale, regionale e locale, è particolarmente interessante, per numero di attori coinvolti e per ampiezza del progetto, quello del Sistema Informativo Socio-Sanitario (CRS-SISS) in Lombardia.

Nel corso del 2001 è stata progetta e sperimentata con successo in provincia di Lecco, una carta dal formato e aspetto simile a un bancomat, con cui è possibile accedere, per via telematica, ai servizi integrati in Rete a livello regionale, con paradigmi e modelli mutuati dalla tecnologia web. La sperimentazione della Carta in provincia di Lecco ha coinvolto 306.000 cittadini, 1.500 operatori sanitari, 275 medici di base e pediatri e 88 farmacie. Nel corso della sperimentazione oltre il 35% delle prescrizioni di farmaci, visite ambulatoriali e richieste di ricoveri –con punte del 52% per le prescrizioni di farmaci- avviene con l'uso della Carta.

Inizialmente il Progetto supporta servizi in ambito socio-sanitario, ma prevede già da ora l'analisi delle modalità di coinvolgimenti di altri settori della pubblica amministrazione.

Il 15 marzo del 2002 la Regione Lombardia ha deliberato l'estensione del progetto CRS-SISS su tutto il territorio regionale. In questo ambito è prevista entro la metà del 2006 la diffusione della carta in tutta la Lombardia (9.000.000 cittadini, 100.000 operatori sanitari, 8500 medici di base e pediatri, 2500 farmacie e 15 Aziende Sanitarie Locali).

La sottoscrizione di un protocollo d'intesa tra il Ministro per l'innovazione e le tecnologie e il Governatore della Regione Lombardia in data 12 novembre 2002 ha, tra l'altro, determinato la convergenza del progetto CRS-SISS con gli obiettivi della CNS.

Alla fine di marzo 2005 è stata completata la distribuzione delle 9.255.000 smart card previste.

Altre regioni stanno utilizzando questo modello di Carta Sanitaria basato sulle specifiche Netlink.

6.2 Le specifiche Netlink

Il progetto Netlink ha rappresentato il pilota europeo di un modo innovativo di fare sanità nella gestione del rapporto paziente, operatore sanitario e, specificamente, il medico di base. I suoi meccanismi applicativi garantiscono un efficace controllo e gestione dell'offerta e della fruizione dei servizi socio-sanitari.

Le specifiche di Netlink sono pubbliche e si basano su principi di sicurezza che utilizzano mutua autenticazione tra due soggetti mediante meccanismi di crittografia simmetrica. Vista la struttura applicativa prevista la mutua autenticazione è tra il paziente e l'operatore sanitario rispetto al sistema informativo socio-sanitario con una elevata quantità di sicurezza anche nei confronti di quanto previsto dalla normativa vigente sulla privacy.

Sempre in quest'ottica e nell'ambito delle specifiche Netlink (tracciato record definito) la carta contiene una serie di informazioni sanitarie che consentono di gestire in modo più mirato le prestazioni sanitarie mediante la maggiore integrazione tra i diversi attori del processo di diagnosi, cura, riabilitazione e assistenza.

Ovviamente la tipologia dello strumento garantisce anche un più efficace controllo della spesa e costituisce la base per l'uso marginale di documenti cartacei.

Non è obiettivo del presente documento dare il dettaglio delle specifiche operative Netlink, ma è opportuno ricordare che i processi di gestione socio-sanitari basati su queste specifiche sono complessi e basati su un sistema informativo già pronto e rodato a prescindere dall'utilizzo dalla carta.

Il progetto CNS, peraltro, consente di predisporre gli spazi all'interno della smart card e di attivarli al momento opportuno, cioè quando le strutture informatiche di supporto sono popolate con un numero di dati sufficiente e funzionale agli obiettivi di efficacia e efficienza di questo tipo di progetti.

In ogni caso la struttura interna della carta conforme alle specifiche Netlink viene resa disponibile nell'ambito della pubblicazione delle specifiche del file system "multiservizi" previsto per la CNS.

Capitolo 7

La firma digitale

La firma digitale è stato il primo strumento introdotto per la semplificazione dei processi amministrativi.

Il compito di questo strumento è di consentire la stipula di atti basati su processi informatici, fornendo evidenza e prova della sottoscrizione, da parte del firmatario, degli atti, fatti o dati che il documento firmato rappresenta.

La firma digitale è dunque soprattutto uno strumento amministrativo, ma è anche in grado di assicurare l'integrità del documento firmato, infatti protegge il documento da contraffazioni anche se quest'ultimo viene conservato in un ambiente non sicuro.

La firma digitale è dunque uno strumento chiave dei processi di e-government e trova proficua applicazione in tutti i casi in cui il servizio comporta un atto amministrativo.[14]

E' evidente come l'integrazione di questo strumento nella CNS consenta al titolare di disporre di uno strumento utile non solo per identificarsi ed autenticarsi in rete, accedendo quindi ai servizi in rete, ma per sottoscrivere, con pieno valore legale, una propria volontà, una dichiarazione, un'istanza.

7.1 La firma digitale nella CNS

La CNS deve essere predisposta per accogliere le funzionalità di firma digitale. E' quindi indispensabile che la smart card utilizzata rispetti le norme relative al cosiddetto "dispositivo sicuro per la generazione delle firme" ed in particolare le caratteristiche previste dall'allegato III della Direttiva europea 1999/93/CE. Tali caratteristiche possono essere dimostrate come previsto dalla "Decisione della Commissione europea del 14 luglio 2003" (Gazzetta ufficiale dell'Unione europea n. L175/45 del 154 luglio 2003): valutazione EAL 4+ della norma ISO/IEC 15408 secondo le modalità previste nel CWA 14169 (marzo 2002). Sono ammessi livelli di valutazione internazionalmente riconosciuti come equivalenti.

La predisposizione della firma digitale può avvenire con due diverse modalità:

a) il soggetto responsabile della certificazione delle chiavi di firma è stabilito dall'ente emettitore, nell'ambito dei soggetti accreditati ai sensi dell'articolo 29 del decreto legislativo 4 aprile 2006, n. 159;
b) il titolare della CNS può scegliere il Certificatore responsabile dell'erogazione dei servizi suddetti tra quelli accreditati o notificati secondo la normativa vigente.

[14] Tratto dal documento "L'e-government per un federalismo efficiente". Documento elaborato dal Comitato Tecnico della Commissione permanente per l'Innovazione e le Tecnologie

Nel primo caso l'ente emettitore predispone una procedura atta a far sì che il titolare della CNS possa disporre della firma digitale al momento del rilascio della carta o in una fase successiva. A tale scopo l'ente emettitore sceglie almeno un soggetto responsabile della certificazione fra quelli iscritti nell'elenco pubblico dei certificatori previsto dall'art. 29, comma 6 del decreto legislativo 4 aprile 2006, n.159.

Nel secondo caso , attuabile solo se l'ente emettitore non predispone la CNS nella modalità di cui al punto a), l'ente emettitore deve consegnare al cittadino, al momento del rilascio della CNS, le modalità operative da utilizzare per la predisposizione della carta quale dispositivo per generare firme digitali. Il titolare della CNS, tramite queste modalità, può successivamente richiedere l'installazione delle componenti inerenti l'utilizzo della firma digitale rivolgendosi ad uno dei certificatori accreditati secondo la normativa vigente. Sono ammessi metodi alternativi a quello appena indicato, con l'unico vincolo che questo metodo sia tale da non modificare la certificazione di sicurezza della smart card ai fini del dispositivo sicuro per la creazione della firma.

Più in dettaglio, il titolare della CNS, provvisto di un documento di identità e utilizzando le modalità stabilite dall'ente emettitore per l'attivazione del servizio di firma digitale, si mette in contatto con un certificatore che procede ad impostare la smart card in modo che possa essere utilizzata per i processi di firma. Si sottolinea che queste informazioni dedicate all'installazione della firma digitale sono necessarie per attivare i diritti di scrittura sulla directory dedicata a tale servizio.

Nel caso in cui l'ente emettitore attivi delle convenzioni con i certificatori di firma, non si esclude la possibilità che lo stesso ente emettitore svolga le funzioni di "registration authority" per le fasi di identificazione del cittadino.

In entrambi i casi, le procedure di predisposizione della carta, di gestione del certificato di firma digitale e delle relative chiavi, dovranno essere conformi alla normativa vigente in materia di firma digitale.

Capitolo 8

Altre applicazioni nella CNS

Un servizio essenziale nell'ambito dell'offerta di servizi in rete è quello dei sistemi di pagamento in linea. Un elevato numero di transazioni, infatti, si completa con una operazione di pagamento. E' ovvio che una operazione direttamente fruibile all'interno del servizio in rete è più efficace e efficiente nei confronti del fruitore. Nel seguito vengono descritte le modalità prescelte per sperimentare un servizio di pagamenti in linea con l'utilizzo della CNS.

Altri servizi possono essere erogati tramite la CNS su base locale, utilizzando lo spazio libero memoria permanente della CNS (EEPROM). In generale è il fornitore di carte che definisce le modalità del servizio, coordinandosi con la pubblica amministrazione cliente. Il CNIPA, comunque, offre supporto tecnico e organizzativo al fine di garantire la coerenza con il progetto globale e la sicurezza delle scelte effettuate rispetto all'emissione della carta.

8.1 I servizi aggiuntivi

La Carta Nazionale dei servizi può contenere anche i cosiddetti "servizi aggiuntivi". Con tale termine ci si riferisce ai dati memorizzati sulla smart card al fine di consentire l'erogazione di ulteriori servizi applicativi, oltre a quelli già previsti come standard per le carte CNS cioè l'autenticazione, più le opzionali firma digitale e carta sanitaria basata sulle specifiche Netlink.

I servizi aggiuntivi possono essere installati sulla carta al momento dell'emissione oppure essere installati successivamente. In ogni caso, essi vengono installati in un'apposita area della CNS nota come "DF2".

Per installare i servizi aggiuntivi è necessario inviare alla carta opportuni comandi in modalità protetta ("secure messaging"); ciò richiede l'impiego di apposite chiavi crittografiche detenute dall'Amministrazione emittente la CNS. L'Amministrazione può eventualmente delegare la creazione di servizi aggiuntivi ad altri soggetti coi quali abbia rapporti di collaborazione a diverso titolo, purché nel rigoroso rispetto delle specifiche e delle necessarie misure di sicurezza.

Ogni servizio aggiuntivo dev'essere contenuto in una specifica DF ("Dedicated File") all'interno di DF2. Una DF è in pratica una directory nella quale è contenuto l'insieme dei file necessari per un particolare servizio aggiuntivo: può trattarsi di una combinazione di file elementari (EF), oggetti di sicurezza (BSO) e ulteriori DF.

L'insieme degli identificatori (FID) dei servizi aggiuntivi presenti in una carta CNS è mantenuto in un apposito file anch'esso presente in DF2.

L'unica limitazione alla creazione di un servizio aggiuntivo è data dalla disponibilità di memoria residua sulla carta CNS. La memoria residua dipende a sua volta dalla capacità della carta, dallo spazio occupato dalle (eventuali) aree di firma digitale e Netlink e dallo spazio occupato dai servizi aggiuntivi già presenti.

L'allocazione di un identificatore (FID) univoco necessario per poter creare un servizio aggiuntivo in una carta CNS può essere ottenuta inviando una richiesta al CNIPA contenente una descrizione del

servizio che si intende registrare. L'elenco dei servizi registrati è reperibile sul sito del CNIPA alla pagina http://www.cnipa.gov.it/site/it-IT/Attivit%C3%A0/Certificatori_accreditati/Carta_Nazionale_dei_Servizi/Servizi_aggiuntivi/

I servizi aggiuntivi installabili sulla carta CNS possono rispondere alle più diverse esigenze applicative; ecco alcuni esempi significativi:

- rilevazione presenze in azienda,
- pagamenti (secondo vari schemi),
- memorizzazione di informazioni personali,
- bigliettazione elettronica (e-ticketing),
- raccolta e consumo di "punti fedeltà" (loyalty),
- ricarica ed utilizzo di "buoni" (pasto, carburante, ecc).

Ogni servizio può avere differenti requisiti per quanto riguarda le caratteristiche del lettore o terminale di "accettazione"; alcuni servizi potranno essere fruiti da differenti piattaforme (es. il normale PC, il decoder della TV digitale terrestre, terminali POS, ecc).

8.2 I sistemi di pagamento in linea

L'obiettivo principale di questo tipo di progetto è di consentire a cittadini e imprese di usufruire di servizi in rete offerti dalle pubbliche amministrazioni effettuando, anche in modo contestuale, i pagamenti eventualmente necessari.

Un secondo obiettivo è quello di utilizzare la carta CNS per l'identificazione dell'utente nella transazione relativa ai pagamenti in oggetto.

Un terzo obiettivo, non meno importante, è quello di rendere possibile al cittadino fruitore del servizio di utilizzare una gamma di strumenti di pagamento diversificati, largamente diffusi e soprattutto non legati a un singolo emettitore.

Un sistema di pagamento in linea deve obbligatoriamente fare riferimento a un circuito virtuale di pagamento. E' opportuno che tale circuito virtuale sia tale da rendere il cliente indipendente dal possesso di uno specifico strumento di pagamento e dal rapporto con una particolare banca o emettitore di carte di debito o credito.

L'indagine effettuata ha evidenziato che l'unico circuito rispondente ai requisiti indicati sia attualmente il sistema BANKPASS Web.

Tale circuito nasce all'interno dell'e-Committee, costituita da un'associazione di banche, promossa dall'ABI, nata per assumere il ruolo di motore per l'innovazione bancaria nell'ambito dell'ICT.

All'e-Committee oggi aderiscono 240 banche in rappresentanza di oltre il 90% del sistema.

BANKPASS Web è stato lanciato sul mercato il 28 gennaio 2002, nasce con l'obiettivo di rendere sicuri e flessibili gli acquisti in rete e dare impulso al commercio elettronico.

Il sistema si avvale di operatori tecnologici di tipo interbancari come SSB, SECETI e Consorzio Triveneto. Gli utenti aderenti a BANKPASS Web possono utilizzare una varietà di strumenti di pagamento (carte di credito, carte di debito e a breve bonifici).

Per operare gli utenti utilizzano un "portafoglio virtuale" in cui il consumatore può inserire tutti i propri strumenti di pagamento che può utilizzare per effettuare i propri acquisti in linea in totale sicurezza. L'esercente in rete può acquisire pagamenti con tutte le carte di credito (Visa, MasterCard, Amex, Diners, JCB, ecc.) e anche con il PagoBANCOMAT.

Associando alla categoria "esercente" la pubblica amministrazione che eroga il servizio in rete è possibile associare alle operazioni di acquisizione pagamenti il servizio in rete offerto dall'amministrazione stessa.

E' possibile a questo punto, realizzando un'opportuna interfaccia software, far colloquiare il portale di servizi con il circuito virtuale di pagamento.

8.3 La CNS e la televisione digitale terrestre.

Il decoder della Televisione Digitale Terrestre (DTT) rappresenta una piattaforma molto interessante per l'utilizzo della CNS. In tal senso è importante sottolineare che, a differenza dei PC, tutti i decoder interattivi ovvero la maggioranza di quelli presenti presso le famiglie, sono equipaggiati con un lettore di carte.

Il decoder della Televisione Digitale Terrestre (DTT) rappresenta una piattaforma molto interessante per l'utilizzo della CNS. Si noti infatti che, a differenza dei PC, tutti i decoder interattivi (la maggioranza) sono equipaggiati con un lettore di carte.

Il lettore di carte del decoder è stato inizialmente previsto per la fruizione delle trasmissioni TV a pagamento (Pay-TV), mediante l'inserimento di una carta di "accesso condizionato". Tuttavia, nulla vieta di usare quel lettore anche per utilizzare una carta di altro tipo, come per es. una CNS.

I decoder interattivi sono dotati di un ambiente di elaborazione basato sullo standard MHP (Multimedia Home Platform). Si tratta in pratica di un ambiente Java, per il quale è possibile scrivere applicazioni dotate di interfaccia grafica, in grado anche di collegarsi ad Internet (attraverso il cosiddetto "canale di ritorno" rappresentato dal modem interno) e di interagire con una carte. Queste possibilità permettono quindi alle Amministrazioni di realizzare servizi on-line fruibili anche attraverso il decoder DTT. Laddove sia necessaria l'interattività, questa è supportabile dal "canale di ritorno" attraverso il quale è possibile effettuare comunicazioni anche col protocollo HTTP.

Le applicazioni sono inviate in modalità "broadcast" a tutti gli utenti, utilizzando il medesimo segnale radio che veicola la trasmissione TV. Su ogni canale DTT possono essere trasmesse diverse applicazioni, in orari diversi del giorno. Le Amministrazioni interessate a diffondere le proprie applicazioni MHP alla cittadinanza devono prendere accordi con un operatore di rete DTT al fine di accedere ad una "banda" di trasmissione.

Di seguito descriviamo le particolarità del colloquio con la carta in ambiente MHP.

8.4 Modalità di colloquio con la smartcard

Il parco di decoder installati in Italia al termine dell'anno 2005 risulta essere equipaggiato con un'implementazione di MHP v1.0.2 o v1.0.3. Buona parte di questi decoder consentono l'accesso alla smartcard tramite l'interfaccia "OCF" sviluppata dal consorzio Open Card (http://www.opencard.org); il colloquio avviene in modo conforme a quanto previsto dallo standard ISO 7816-4.

Anche la v1.1.1 delle specifiche MHP (l'ultima versione ufficiale pubblicata) prevede l'uso di OCF per il colloquio con la smartcard, ma tale versione di MHP non è ancora presente nei decoder sul mercato. La v1.1.2 delle specifiche MHP, ancora allo stato di bozza, prevede invece l'utilizzo del pacchetto "SATSA" della Sun Microsystems.

Al momento non è chiaro se la prossima generazione di decoder DTT che sarà immessa sul mercato sarà conforme alla specifica MHP v1.1.1 oppure alla specifica MHP v1.1.2. In ogni caso, le particolari API utilizzate per colloquiare con la smartcard (OCF, SATSA) possono essere mascherate alle applicazioni MHP tramite l'adozione di un opportuno layer di astrazione.

8.5 Possibili utilizzi della CNS in ambiente MHP

8.5.1 Identificazione ed autenticazione in rete

Anche in ambiente MHP è possibile effettuare l'identificazione ed autenticazione in rete, in quanto su ogni decoder è presente un "canale di ritorno" (modem interno) che permette la comunicazione TCP/IP con elaboratori raggiungibili su Internet. Sul canale di ritorno si possono utilizzare i classici protocolli Internet, tipicamente HTTP ed HTTPS (ovvero HTTP protetto con SSL).

Si possono adottare almeno due diverse tecniche per l'identificazione in rete:

8.5.1.1 Autenticazione in modalità Challenge/Response (CH/R)

Analogamente a quanto descritto nel paragrafo 4.4 del presente documento, il processo si articola nei seguenti passi:

- il client invia al server il proprio certificato di autenticazione (estratto dalla CNS);
- il server verifica il certificato utente, produce un messaggio randomico di autenticazione (Challenge) e lo invia al client;
- il client "firma" il Challenge con la chiave privata di autenticazione dell'utente (tramite la CNS) ottenendo un messaggio (Response) che viene inviato al server;
- il server verifica l'autenticità della Response tramite la chiave pubblica contenuta nel certificato utente;
- se la verifica ha successo, il server ha ottenuto l'identità certa dell'utente.

In questo caso, i dati scambiati tra client e server nei vari passaggi sono *veicolati a livello applicativo*, ossia sopra il livello dei sockets TCP (per esempio a livello HTTP, ma non necessariamente).

8.5.1.2 Autenticazione in modalità SSL Client Authentication

Il supporto per la *client authentication* SSL è solo opzionale nelle specifiche MHP v1.0.x e v1.1.1. Di fatto, negli attuali decoder, la SSL client authentication non è disponibile come funzionalità nativa. Chi desidera usare tale meccanismo, alla stregua di quanto si fa in ambiente PC, deve quindi utilizzare del software aggiuntivo.

Ricordando che l'ambiente MHP si basa sulle specifiche Java, per gestire la SSL client authentication è necessario disporre di un opportuno "provider crittografico" nei termini previsti dalla Java Cryptography Architecture (JCA) della Sun. Tale provider crittografico deve evidentemente interagire con la CNS se si desidera che la SSL client authentication utilizzi la chiave privata di autenticazione dell'utente.

8.6 Dati personali e servizi aggiuntivi

La digitazione di numeri e lettere tramite i tasti del telecomando di un decoder DTT è un'operazione piuttosto scomoda rispetto all'uso di una normale tastiera di PC: ci vuole più tempo ed è più facile commettere errori. L'uso delle cosiddette "tastiere virtuali", visualizzate sullo schemo TV, risolve il problema solo in parte.

Ogni qual volta un'applicazione MHP debba ottenere i dati anagrafici dell'utente, risulta molto più efficiente leggerli dalla CNS piuttosto che chiederne la digitazione. Alcuni dati potranno sempre essere

letti dal file *EF_DatiPersonali* presente su tutte le CNS: nome, cognome, codice fiscale, data di nascita, località di residenza, ecc.

Altri dati personali (es. numeri di telefono, numeri di conto corrente, userid/password, ecc) potranno invece essere letti da appositi "servizi aggiuntivi" sulla CNS, secondo le esigenze di ogni particolare applicazione. In un tale contesto, la disponibilità sulla CNS di un servizio che consenta la scrittura e lettura di dati generici può risultare molto utile ed efficiente, considerando che i decoder non consentono l'uso di memorie di massa rimovibili come floppy disk, chiavi USB, ecc.

Più in generale, i "servizi aggiuntivi" possono rappresentare la base per un'ampia gamma di possibili applicazioni interattive fruibili in ambiente MHP.

8.7 Una nota sulla sicurezza delle applicazioni MHP

Lo standard MHP prevede che l'accesso alle "risorse critiche" del decoder, quali il canale di ritorno e la smartcard, venga concesso solo ad applicazioni *firmate digitalmente dall'autore* e provviste dei necessari privilegi di accesso alla risorsa richiesta. Tuttavia, negli attuali decoder, tale meccanismo di sicurezza è disabilitato.

Il consorzio dei broadcaster italiani (DGTVi) intende abilitare la sicurezza nei decoder quanto prima, ma per il momento occorre ricordare che tutte le applicazioni MHP (firmate o non) possono accedere alla smartcard e al canale di ritorno.

D'altra parte, va detto che la particolare modalità di distribuzione delle applicazioni MHP rende molto più difficile e quindi più improbabile la circolazione di applicazioni "maligne" rispetto al caso di Internet. Lo stesso ambiente MHP impone molti più vincoli alle applicazioni di quanto non accada sui PC. Queste considerazioni, insieme al fatto che la CNS è per definizione una smartcard molto sicura, portano a ritenere che l'uso della CNS sul decoder DTT sia più sicuro che non sui normali PC, anche con la sicurezza MHP disabilitata.

8.8 Lo stato dell'arte

Sono state condotte numerose sperimentazioni sull'utilizzo della CNS nell'ambito dei sistemi di pagamento, del digitale terrestre e del contactless tramite l'interfaccia esterna dell'antenna.

Nei sistemi di pagamento sono significative le esperienze del Progetto TESEO (collegato a un gruppo di comuni guidati dal Comune di Verona che ha sperimentato il Sistema BankPass Web per i pagamenti online di una serie di servizi locali erogati in rete) e della Regione Lombardia (che ha installato un sistema di pagamento elettronico nella CNS emessa su l'intero territorio regionale nell'ambito del Progetto CRS-SISS).

Significativi i numerosi esperimenti condotti sull'utilizzo della CNS nei decoder interattivi nell'ambito dei progetti cofinanziati dal CNIPA e dal Ministero delle Comunicazioni.

Infine è importante citare anche le sperimentazioni della CNS come controllo accesso ai varchi, biglietto elettronico, strumento per il controllo presenze e supporto per la gestione di informazioni biometriche.

Capitolo 9

L'ambiente software sul client

L'utilizzo della carta sul client differisce in base al sistema operativo installato sulla macchina ove opera l'utente (client). Inoltre, se la carta viene utilizzata come token crittografico per l'autenticazione o la firma digitale, la configurazione differisce se si opera in ambiente open source piuttosto che in ambiente win32 con Explorer.

L'utilizzo dell'applicazione sanitaria basata su Netlink è basata su software specifico che utilizza i comandi di sistema operativo della carta (APDU) e quindi le librerie di corredo della carta (PKCS#11 e CSP - Cryptographic Service Provider) non sono di alcuna utilità per tale specifica applicazione.

Le librerie PKCS#11 vengono interfacciate direttamente da questa tipologia di codice. La stessa libreria in ambiente Microsoft deve essere mediata rispetto all'utilizzo crittografico (autenticazione e firma digitale) da uno specifico modulo denominato, come già detto, CSP.

9.1 Modalità di utilizzo della CNS in ambiente open source (Netscape, Mozilla, ecc.)

Per tranquillità dell'utente e del gestore locale del progetto è bene precisare che pur trattandosi di tecnologie complesse, l'onere sull'utente finale è minimo. Ogni carta viene fornita di una libreria PKCS#11 in grado di utilizzarne le caratteristiche di token crittografico. In particolare se si utilizza la CNS come token di accesso ai siti sicuri, la libreria deve essere installata sul sistema client e il browser configurato per poter "vedere" il nuovo modulo crittografico.

Ovviamente l'utilizzo della carta per la firma digitale può avvenire con la stessa libreria ma con un software specifico per l'operazione diverso da quello del browser. Per tale circostanza, in alcune configurazioni, è accettabile la disponibilità di due librerie. La prima solo per l'autenticazione in rete in modalità "autenticazione forte" e l'altra, da installare eventualmente in seguito, per le operazioni di firma digitale.

In ogni caso il client deve disporre di software (driver) conforme allo standard PC/SC. Tale software è indispensabile per utilizzare il lettore/scrittore di smart card.

Le modalità di configurazione ed utilizzo di tali librerie non è tra gli scopi del documento, ma sarà oggetto di specifica documentazione.

9.2 Modalità di utilizzo della CNS in ambiente Microsoft

L'unica differenza con quanto descritto nel paragrafo precedente è che per utilizzare la libreria PKCS#11 fornita a corredo della carta bisogna disporre di un ulteriore software denominato CSP.

In realtà il CSP non utilizza le PKCS#11 ma, per eseguire operazioni crittografiche, si poggia sull'uso delle Microsoft Cypto API. Come detto nei capitoli precedenti, anche la libreria CSP viene fornita a corredo della carta e risulta essere l'alternativa alla libreria PKCS#11 in ambiente Microsoft.

Anche in questo caso le operazione di autenticazione e firma utilizzano software di supporto specifico (il browser e il software di firma).

Le modalità di configurazione e utilizzo del CSP non è tra gli scopi del presente documento, ma sarà oggetto di specifica documentazione.

9.3 Modalità di utilizzo della CNS in modo semplificato

Anche se ben documentate le librerie PKCS#11 e CSP non sono di facile utilizzo per uno sviluppatore medio. Per limitare i disagi si può prevedere di sviluppare un'ulteriore libreria per rendere direttamente fruibili allo sviluppatore funzionalità complesse. Una tale libreria, che possiamo definire di metacomandi, una volta referenziata, può direttamente attivare le funzioni di lettura della carta, di firma digitale o altre specifiche funzioni come l'estrazione del codice fiscale dalla carta stessa.

Sul sito web del CNIPA è disponibile una libreria di riferimento definita nell'ambito di una fornitura aggiudicata tramite una gara d'appalto comunitaria.

9.4 Modalità di utilizzo della CNS in ambiente Linux o MACOS X

La possibilità di utilizzo della CNS da parte di titolari che non utilizzano la piattaforma Windows non deve essere trascurata in considerazione del fatto che il numero di utenti che utilizzano piattaforme Linux piuttosto che MAC è tutt'altro che trascurabile.

Si deve tenere in conto anche degli aspetti relativi all'accessibilità dei siti web, alle norme di tutela degli utenti e alla corretta concorrenza sul mercato.

Per queste tipologie di utenti, titolari di CNS, non vi sono particolari ostacoli al suo utilizzo. Sul mercato, sono disponibili da tempo, lettori di carte dotati di librerie software per interfacciare gli ambienti operativi Linux e MacOS X. Entrambi i sistemi operativi consentono di connettersi ai lettori con le stesse modalità utilizzate in ambiente Windows (cfr. la sezione 3.1.2 del presente documento). Tale funzionalità è offerta da pacchetti open source che hanno raggiunto un adeguato livello di stabilità e che sono in grado di funzionare nelle applicazioni tradizionali.

In tale contesto è anche necessario disporre delle librerie software che garantiscono il colloquio con browser come Netscape e Mozilla/Firefox. Tale libreria è in genere realizzata dal produttore della CNS, dal certificatore accreditato che genera i certificati di autenticazione o da una generica terza parte, avendo a disposizione le specifiche funzionali e del file system della CNS.

Capitolo 10

L'ambiente di accesso sul server

Il modello di autenticazione introdotto dalle carte di accesso ai servizi si basa su meccanismi di "strong authentication" che sfruttano i certificati digitali X.509 all'interno dei meccanismi di sicurezza SSL/TLS. Questi meccanismi di sicurezza, nelle situazioni funzionali più comuni, sono associati al protocollo http.

Il modello funzionale dei certificatori di firma digitale accreditati secondo la normativa vigente in Italia, realizza un modello di tipo paritario, nel quale il singolo certificatore, non è in relazione gerarchica con altre infrastrutture ma opera in un dominio indipendente e interoperabile con gli altri.

Questo modello, particolarmente efficiente all'interno del dominio del singolo certificatore, introduce criticità rispetto all'interoperabilità pressoché assenti in un modello gerarchico. In particolare, deve essere gestito il numero massimo di certificati root che il server web può gestire come pure la modalità di verifica di validità del certificato a fronte di CRL emesse da certificatori diversi.

In questo contesto è bene descrivere i principi generali ai quali attenersi per garantire le funzionalità necessarie all'ambiente di controllo dell'autenticazione sul server, per utilizzare i certificati di autenticazione installati nelle carte di accesso.

Le problematiche di dettaglio delle configurazioni del web/application server sono specifiche dei singoli prodotti ma comunque non si discostano in modo significativo da quanto esposto nel seguito.

Qualora necessario verrà garantito il supporto per specifiche architetture.

10.1 L'ambiente di accesso in modalità web

Per non appesantire il documento con informazioni non strettamente pertinenti ai suoi scopi, non viene inserita una descrizione, seppur sintetica, del protocollo SSL/TLS. Tale conoscenza deve essere quindi un prerequisito per la lettura del seguito.

Si ipotizza quindi che il processo di autenticazione "forte" avvenga mediante i meccanismi standard previsti dalle applicazioni basate sulle tecnologie web ovvero mediante il protocollo SSL/TLS.

Come evidenziato in un precedente capitolo, l'autenticazione "forte" è un meccanismo di sicurezza che, nelle architetture considerate, utilizza i certificati digitali. Praticamente significa che una postazione utente (il client) quando richiede l'accesso a una applicazione accessibile esclusivamente a seguito di autenticazione, invia tramite il protocollo SSL/TLS le credenziali dello specifico titolare in forma di certificato digitale. Il server web è in grado di gestire le informazioni presenti nel certificato e in particolare quelle presenti nel campo "common name". La presenza del codice fiscale in questo campo rende immediatamente disponibile questa informazione ai meccanismi di sicurezza e qualora le verifiche siano positive, il server web connette l'utente all'applicazione da lui richiesta.

Come si vede il codice fiscale è indispensabile per attivare l'associazione tra il titolare della carta e l'applicazione alla quale egli è autorizzato ad accedere (nel seguito daremo dei dettagli sul processo di

autorizzazione). In altre parole, il codice fiscale costituisce lo username dell'utente. La sua unicità è indispensabile e questa viene garantita mediante i meccanismi stabiliti nella legislazione vigente.

E' bene ricordare che, per completare il processo di scambio delle credenziali di sicurezza, il titolare della carta di accesso deve digitare il PIN di sblocco. Inoltre, poiché vengono prima completate le operazioni di crittografia tra client e server e poi si prosegue con lo scambio di credenziali per l'autenticazione, tutte le informazioni non viaggiano in chiaro sulla rete nella tratta coinvolta.

10.1.1 Il processo di autorizzazione

Una volta che il server web ha autenticato il titolare della carta di accesso, si devono definire le autorizzazioni alle quali il titolare ha diritto. Ovviamente le cosiddette ACL (Access Control List) sono fortemente dipendenti dalla realizzazione dell'ambiente di accoglienza sul server e dalle modalità di accesso alla banca dati da parte delle applicazioni invocate dagli utenti.

Ovviamente esistono dei principi di carattere generale sempre applicabili quando si descrive un ambiente operativo dotato di controllo d'accesso. In particolare è possibile, senz'altro in tutti i contesti, considerare gli utenti singolarmente o per gruppo omogeneo. Prendendo come riferimento l'ambiente Java 2 Enterprise Edition (J2EE) possiamo considerare quanto segue (non esistono differente sostanziali in ambiente .Net, salvo ovviamente la non interoperabilità di alcune componenti).

La sicurezza, nel contesto Web Application Server J2EE consiste di due parti principali: autenticazione e autorizzazione (il termine autenticazione va inteso nella sua espressione tecnica classica per evitare ambiguità con l'ordinamento giuridico dove "autenticazione" ha un altro significato). L'autenticazione viene delegata in modo pressoché totale ai certificati digitali e al protocollo http nell'ambito delle funzionalità tipiche dei server web di front-end. I meccanismi differiscono in base al server utilizzato. I più diffusi tra i server web sono I-Planet, Apache e Internet Information Server. Ognuno di loro utilizza modalità specifiche di gestione dei certificati digitali, anche se i vari ambienti non differiscono in modo sostanziale. La parte più critica è quella della gestione delle liste di revoca (CRL) o, in alternativa, dell'interrogazione di server OCSP (Online Certificate Status Protocol). Non è obiettivo di questo documento fornire i dettagli tecnici di queste operazioni. Naturalmente a richiesta verrà fornito tutto il supporto necessario per l'armonizzazione delle soluzioni che le amministrazioni intendono realizzare.

I meccanismi di autorizzazione sono realizzati all'interno dell'application server.

Il modello di sicurezza J2EE consente di costruire uno schema per le autorizzazioni delle utenze referenziate via web garantendo granularità per l'accesso e l'utilizzo delle singole applicazioni fino alle singole funzioni ("metodi" nell'ambiente J2EE).

Durante la fase di sviluppo dell'applicazione vengono creati ruoli e permessi, in modo tale che i permessi di esecuzione siano assegnati a uno o più ruoli di sicurezza. A questa fase segue, al momento della messa in linea dell'applicazione, l'associazione dei ruoli di sicurezza a utenti singoli o gruppi di utenti.

A un utente possono essere assegnati più ruoli e quindi i suoi permessi sono l'unione dei permessi dei singoli ruoli; l'associazione di un gruppo a un ruolo equivale all'assegnazione di tutti i suoi utenti a tale ruolo.

E' ovvio che questo tipo di approccio a due fasi consente elevati gradi di portabilità e flessibilità nell'amministrazione della sicurezza. I responsabili dell'applicazione possono controllare come gli utenti o gruppi di utenti sono associati ai ruoli di sicurezza definiti per l'applicazione e sui meccanismi di autorizzazione e di autenticazione usati per determinare l'appartenenza ai ruoli.

La gestione della sicurezza effettuata in questo modo consente di gestire le politiche relative a una applicazione in modo tale che possano essere realizzate senza vincoli all'interno del codice applicativo (sicurezza di tipo dichiarativo). Da questo aspetto si deduce che possono essere radicalmente cambiati gli aspetti di sicurezza senza che sia necessario agire sul software applicativo.

In alcune transazioni può accadere che il livello di autorizzazione all'azione su una specifica funzione si debba spingere fino a considerare il contenuto del dato trattato. Il modello di autorizzazione J2EE prevede che l'applicazione possa ottenere informazioni, sia sul ruolo sia sull'identità di chi sta richiedendo una certa operazione, al fine di prendere le opportune decisioni derivanti dalle politiche di si-

curezza da garantire. Questo tipo di approccio viene generalmente indicato come sicurezza di tipo programmatico.

10.1.2 Tecnologie per un'identità federata

Si stanno diffondendo alcune architetture tecnologiche per la gestione di identità federate. Una fa riferimento all'ambiente Microsoft e si chiama Passport.

L'altra è la Liberty Alliance Project supportata da un consorzio di industrie con la specifica di realizzare un protocollo per le funzionalità di autenticazione e autorizzazione tra le istituzione coinvolte, indipendentemente dai meccanismi di sicurezza interni alle istituzioni stesse.

L'utilizzo di questi meccanismi in un ambiente federato può essere opportuno nei seguenti casi:

- pubblica amministrazione centrale o locale non dotata di meccanismi in grado di verificare le credenziali degli utenti;
- integrazione con la verifica dell'identificativo elettronico fornito dalle carte di accesso.

Il primo caso rappresenta lo scenario tipico in cui una pubblica amministrazione non è in grado di identificare gli utenti perché non possiede i dati di autenticazione. Attraverso un processo di federazione dell'identità si stabilisce una relazione di fiducia tra diverse istituzioni in modo che una o più organizzazioni possano fornire i dati d'autenticazione a un terzo ente che li richiede.

Il secondo caso rappresenta lo scenario più diretto a risolvere, nell'utilizzo delle carte d'accesso, il problema della non immediata disponibilità delle informazioni sull'identità dell'utente attraverso il meccanismo dei certificati digitali. In questo caso, uno o più enti possono fungere sia da "Authentication authority" che da "Attribute authority" per fornire i dati relativi all'identità e eventuali altre informazioni sull'utente, come ad esempio il codice fiscale.

Tali processi si basano su meccanismi standard di sicurezza (Liberty/SAML) che rispettano i principi di riservatezza/privacy, integrità e disponibilità dei dati.

Il SAML (Security Assertion Markup Language) è uno standard aperto per la realizzazione delle funzionalità di autenticazione, autorizzazione e single sign on sul web. Esso si basa sul linguaggio XML e utilizza un modello di servizio composto da 5 entità:

- Principal
- Authentication authority
- Attribute authority
- Policy decision point (PDP)
- Policy enforcement point (PEP)

Alcuni dei principali fornitori di application server utilizzano questo tipo di tecnologia e, in particolare, delle estensioni del SAML.

Capitolo 11

La sicurezza del circuito della CNS

Ai fini della sicurezza del circuito, l'intero ciclo di vita della CNS deve essere opportunamente tracciato, dal momento di inizio della produzione della carta, fino al ritiro della CNS. Ciascuna attività elementare (produzione, inizializzazione, registrazione, emissione del certificato, personalizzazione, ecc.) deve essere registrata in appositi registri che devono essere sottoscritti dal responsabile dell'attività e conservati in modo protetto.

11.1 La sicurezza della fase di produzione

La produzione delle smart card destinate ad operare come CNS deve avvenire con criteri che garantiscano la segretezza delle informazioni presenti nelle carte inizializzate.

E' opportuno scegliere produttori che abbiano provata esperienza nella produzione di carte con elevati requisiti di sicurezza (ad esempio carte di credito e di debito).

Di seguito vengono esposti alcuni criteri di sicurezza che dovranno essere seguiti dal produttore delle CNS. Tali criteri devono essere considerati come indicativi e non esaustivi, per cui il rispetto di tali criteri non solleva il fornitore dalle responsabilità circa la sicurezza del processo produttivo.

11.1.1 Fasi di lavorazione della carta

Durante l'intero processo di lavorazione, le strutture interne della smart card devono essere protette mediante opportuni codici (PIN, codici di trasporto, ecc.) finalizzati a consentire al solo personale autorizzato la modifica di tali strutture.

I codici di protezione devono essere generati in modo casuale, quindi trasmessi e memorizzati in forma cifrata, con modalità tale da rendere possibile il loro utilizzo esclusivamente agli apparati preposti alla lavorazione della carta.

Questi apparati devono inoltre poter operare unicamente sotto il controllo di operatori muniti di opportuna smart card personale (smart card operatore, di seguito specificata) ovvero di altri sistemi di controllo accesso di paragonabile sicurezza.

Il sistema di sicurezza che governa il processo produttivo (fasi di produzione ed inizializzazione) deve assicurare:

- l'autenticazione certa dell'operatore;
- la registrazione di tutte le operazioni effettuate e dei dati utili alla tracciatura del processo;
- la protezione delle informazioni di tracciatura in modo tale da garantirne integrità e non ripudio.

11.1.2 Conservazione e trasporto delle carte

Quando le carte non sono in lavorazione, devono essere conservate in locali (di tipo caveau) in grado di assicurare adeguati livelli di sicurezza. Ogniqualvolta le carte devono transitare tra siti diversi, devono utilizzare un trasporto con regolare bolla di consegna che deve essere verificata dal responsabile della Sicurezza della sede di arrivo.

11.1.3 Gestione degli scarti

Ogni lavorazione deve tenere traccia degli eventuali scarti ed i moduli utilizzati per tracciare le attività devono riportare sia il numero delle smart card utili, sia il numero degli scarti non utilizzabili. Sia le smart card utili che le non utilizzabili devono essere conservate nel Caveau. Al centro di emissione devono pervenire sia le smart card utili che gli scarti in modo da poter verificare la corrispondenza con il numero delle carte complessive previste. La distruzione degli scarti può essere effettuata solo da un'apposita commissione con procedura verbalizzata.

11.1.4 Generazione delle chiavi

Il software presente sul sistema di personalizzazione dovrà provvedere a tale operazione in modalità sicura.

A tal fine il sistema dovrà leggere l'identificativo della carta ed accedere all'archivio cifrato contenente i PIN di personalizzazione.

A questo punto sarà possibile attivare la generazione delle coppie di chiavi RSA relative all'autenticazione e, eventualmente, alla firma digitale.

Durante questa operazione saranno creati i PIN utente di attivazione delle relative chiavi private.

Tali PIN dovranno essere memorizzati in un archivio cifrato.

11.1.5 Tracciatura delle operazioni

Tutte le operazioni di inizializzazione dovranno essere tracciate in appositi registri elettronici o cartacei. I registri dovranno essere conservati per un periodo non inferiore a 10 anni a decorrere dalla data dell'ultima registrazione inserita. In particolare, il registro di entrate/uscite delle smart card dovrà essere compilato per ogni singolo movimento, con indicazione della data ed dell'ora e dovrà essere firmato sia dal Responsabile della Sicurezza sia dal Responsabile della fase produttiva.

11.1.6 Protezione delle informazioni di tracciatura

La smart card operatore dovrà essere dotata anche di una coppia di chiavi con relativo certificato di crittografia. Occorrerà predisporre un archivio protetto in grado di contenere tutti i record relativi alle carte prodotte, cifrati con la chiave di crittografia presente nella smart card operatore.

La chiave utilizzata per proteggere tali record dovrà essere tenuta in modalità "memorizzazione protetta" all'interno della smart card dell'operatore.

Gestione della smart card dell'operatore

La Smart Card Operatore deve essere generata, attraverso l'uso di software dedicato di generazione, mediante una procedura che assicuri la massima sicurezza del processo. In fase di generazione della carta, saranno registrate su di essa le informazioni di sicurezza (chiavi crittografiche) necessarie per l'accesso ai file protetti e la firma elettronica dei record di tracciatura.

Tale smart card dovrà essere consegnata al responsabile del processo produttivo, od a persona da lui delegata, e conservata in cassetta di sicurezza all'interno di un locale accessibile solo dal responsabile della sicurezza.

L'apertura della cassetta di sicurezza contenente tale smart card di firma dovrà avvenire con una procedura che preveda la presenza congiunta del responsabile della sicurezza e del responsabile del processo produttivo ovvero della persona da lui delegata..

Ogni accesso alla cassetta contenete la smart card dovrà essere documentato firmando opportuni registri.

11.1.7 Misure organizzative

Dovranno essere previste opportune misure organizzative finalizzate a gestire in modo efficace la sicurezza dei siti.

In particolare, dovrà essere presente in ogni sito una opportuna organizzazione della sicurezza che deve prevedere almeno un Responsabile di Sicurezza per turno che risponderà al Responsabile della Sicurezza dell'Organizzazione.

I responsabili della sicurezza dovranno garantire il rispetto di tutte le procedure e le norme previste dall'organizzazione.

11.1.8 Misure di sicurezza fisiche

L'esterno dello stabilimento deve essere recintato e controllato tramite telecamere.

I cancelli devono essere sempre chiusi e gli utenti, i fornitori e gli spedizionieri non devono avere accesso ai locali interni se non dopo essersi presentarsi alla *reception* per il riconoscimento.

Nel caso di ingresso automezzi, il personale addetto alla *reception* deve avvertire il Responsabile di Sicurezza o il magazziniere, i quali ricevono all'esterno gli automezzi dopo che il personale addetto alla *reception* ha azionato il pulsante di apertura cancelli che si richiuderà automaticamente dopo un tempo predeterminato.

Tutti i dipendenti, anche quelli facenti capo ad uffici non inerenti la produzione o la personalizzazione, devono avere a disposizione un badge di ingresso con accesso limitato ad aree ben definite. Gli uffici devono essere protetti da intrusioni esterne, almeno tramite sensori alle finestre.

Gli impianti di sicurezza devono essere attivati dopo l'orario di chiusura e disattivati prima dell'orario di apertura degli uffici.

Nel caso in cui si debba protrarre l'orario di chiusura o anticipare l'orario di apertura, si dovrà necessariamente avvertire il Responsabile di Sicurezza che opererà di conseguenza.

L'accesso all'edificio in cui si svolge la produzione delle carte dovrà essere possibile solo dopo aver superato una bussola di sicurezza. Dovrà inoltre essere previsto un servizio di guardiania che consentirà l'accesso ai reparti o agli uffici solo dopo le operazioni di riconoscimento o registrazione.

L'ingresso dovrà essere suddiviso tra:

- dipendenti con badge nominativi il cui passaggio è registrato dalla bussola e dal sistema di monitoraggio basato su telecamere;
- visitatori che si qualificano al citofono e accedono alla hall tramite la bussola operata dalla guardiola.

La qualificazione e la registrazione in guardiola dei visitatori deve basarsi su un documento di identità valido, di cui deve essere prodotta una fotocopia che sarà archiviata per un anno. Il personale addetto alla *reception* dovrà avvertire il dipendente a cui il visitatore fa riferimento. Questi dovrà prendere in consegna il visitatore, che verrà munito di un badge personale che verrà restituito alla fine della visita. Su apposito registro verrà registrato l'orario di ingresso e di uscita che verrà firmato dal dipendente con funzione di accompagnatore.

11.2 La sicurezza della fase di emissione

La fase di emissione comprende la personalizzazione della carta, la verifica dei dati anagrafici e la consegna della carta al titolare, unitamente ai codici segreti PIN e PUK.

Queste attività possono essere svolte con modalità e tempi diversi, in ogni caso devono essere seguiti criteri di sicurezza volti ad evitare il furto e la personalizzazione criminosa di carte inizializzate o la consegna della carta a persone diverse dal legittimo titolare.

Presso i centri di personalizzazione e di emissione dovranno essere attuate le misure tecniche ed organizzative previste per la tutela dei dati personali (Codice in materia di protezione dei dati personali – DL 30 giugno 2003, n. 196).

In particolare, il documento programmatico per la sicurezza dovrà indicare le azioni messe in atto per proteggere le carte nei confronti del rischio di furto o di utilizzo improprio.

11.2.1 Protezione delle carte inizializzate

E' necessario predisporre opportune misure di sicurezza fisica per la protezione delle carte. Nel caso di spostamento delle carte tra locali o siti diversi, deve essere utilizzato un trasporto con regolare bolla di consegna che deve essere verificata dal responsabile della Sicurezza della sede di arrivo

Tutte le operazioni di personalizzazione dovranno essere tracciate in appositi registri elettronici o cartacei. I registri dovranno essere conservati per un periodo non inferiore a 10 anni. In particolare, il registro di entrate/uscite delle smart card dovrà essere compilato per ogni singolo movimento con data ed ora e firmato dal responsabile della struttura di personalizzazione.

11.2.2 Protezione dei flussi di dati

I flussi informativi che durante il processo produttivo si generano tra la struttura di registrazione, il certificatore e la struttura di personalizzazione, devono utilizzare esclusivamente canali sicuri, utilizzanti sistemi di crittografia simmetrica di lunghezza almeno pari a 128 bit..

Nel caso di utilizzo di una sessione SSL, dovranno essere impiegati sia i meccanismi di autenticazione del server, sia quelli relativi alle postazioni client.

Capitolo 12

Conclusioni

Con l'avanzare degli sviluppi dei "cantieri" dell'e-government, aumenta con significativa consistenza il numero dei progetti che intende utilizzare la CNS. Per concludere queste linee guida facciamo il punto sullo stato di avanzamento lavori dei progetti al momento della pubblicazione del presente documento. Naturalmente lo stato dell'arte costituirà un paragrafo in costante evoluzione. Di tale evoluzione si darà evidenza nell'ambito delle riunioni istituzionali previste nell'ambito della "visione condivisa".

12.1 Lo stato dell'arte

Al momento vi sono in corso vari progetti di rilascio di CNS. Oltre al progetto del Sistema Informativo Socio Sanitario della Regione Lombardia che completerà la distribuzione delle smart card entro la primavera del 2005, sono in fase di sviluppo una serie di altri progetti di distribuzione della CNS nell'80% delle regioni italiane.

Importanti progetti sono stati sviluppati anche nei comuni di Bologna, Verona e S. Giorgio a Cremano e altri sono in fase di studio di fattibilità.

Tra i sottoscrittori del protocollo d'intesa del 13 maggio 2003, solo due soggetti supportano le specifiche previste da tale protocollo. Altri quattro prevedono di supportarle nel breve periodo, mentre ulteriori due, utilizzando tecnologia dei primi due citati possono di fatto definirsi conformi.

I restanti soggetti stanno predisponendo un piano di convergenza.

Nell'attesa di alcune decisioni del Ministro dell'Interno sulla CIE, si stanno valutando le migliori soluzioni per interfacciare dal terminale utente la CNS. Ovviamente, tali soluzioni sono conformi a quelle descritte nel presente documento.

Come più volte ribadito nel documento non sono stati approfonditi alcuni aspetti tecnici non perché di scarsa rilevanza nell'ambito dei progetti, ma a causa delle numerose specificità dei progetti territoriali. In ogni caso non è certamente oneroso gestire le eccezioni per garantire, nel quadro complessivo, la loro coerenza con le specifiche di riferimento del progetto.

Appendice 1

Profilo di certificato digitale per l'autenticazione mediante Carta Nazionale dei Servizi (CNS)

Per ragioni di chiarezza nell'interpretazione del profilo il testo è stato redatto secondo le indicazioni della specifica pubblica RFC 2119.

1 Scopo

Nel presente documento viene definito il profilo del certificato di autenticazione per l'utilizzo nell'ambito dell'emissione della Carta Nazionale dei Servizi (CNS) [9].

Il profilo proposto consente di individuare lo specifico circuito di emissione che ha generato il certificato.

2 Riferimenti

I seguenti documenti contengono definizioni e indicazioni di riferimento che sono citate all'interno del testo e che costituiscono parte integrante della proposta.
I riferimenti sono specifici (identificati dalla data di pubblicazione e/o numero di versione o dal numero di versione) oppure non specifici. Per i riferimenti specifici le revisioni successive non sono applicabili mentre lo sono per i riferimenti non specifici.

[1] CIRCOLARE n. AIPA/CR/24, "Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513", 19 giugno 2000, (G.U. 30 giugno 2000, Serie generale n. 151).

[2] RFC 1778, "The String Representation of Standard Attribute Syntaxes", IETF, March 1995.

[3] RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", IETF, March 1997.

[4] RFC 2246, "The TLS Protocol Version 1.0", IETF, January 1999.

[5] RFC 2255, "The LDAP URL Format", IETF, December 1997.

[6] RFC 2560, "Online Certificate Status Protocol – OCSP", IETF, June 1999.

[7] RFC 3039, "Qualified Certificates Profile", IETF, January 2001.

[8] RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF, April 2002 (rende obsoleto l'RFC 2459).

[9] CNS/CIE, documentazione tecnica per la Carta d'Identità Elettronica (CIE) e per la Carta Nazionale dei Servizi (CNS), http://www.cartaidentita.it, http://www.cnipa.it .

3 Introduzione

Le parole chiave "*DEVE*", "*DEVONO*", "*NON DEVE*", "*NON DEVONO*", "*E' RICHIESTO*", "*DOVREBBE*", "*NON DOVREBBE*", "*RACCOMANDATO*", "*NON RACCOMANDATO*" "*PUO'*" e "*OPZIONALE*" nel testo del documento debbono essere interpretate come descritto nel seguito, in conformità alle corrispondenti traduzioni contenute nel documento IETF RFC 2119 [3].

Le parole chiave "*DEVE*" o "*DEVONO*" o "*E' RICHIESTO*" stanno a significare che l'oggetto in questione è un requisito assoluto della definizione.
Le parole chiave "*NON DEVE*" o "*NON DEVONO*" stanno a significare che l'oggetto in questione è un divieto assoluto per la definizione.
Le parole chiave "*DOVREBBE*" o "*RACCOMANDATO*" stanno a significare che, in particolari circostanze, possono esistere valide motivazioni per ignorare la particolare specifica, ma le complete implicazioni di tale scelta debbono essere comprese e pesate con cautela prima di scegliere per un'altra soluzione.
Le parole chiave "*NON DOVREBBE*" o "*NON RACCOMANDATO*" stanno a significare che, in particolari circostanze, possono esistere valide motivazioni perché la specifica sia accettabile o anche utile, ma le complete implicazioni debbono essere comprese e pesate con cautela prima di implementare una soluzione corrispondente.
Le parole chiave "*PUO'*" o "*OPZIONALE*" stanno a significare che una specifica è puramente opzionale. Un soggetto può scegliere di includere l'oggetto perché un particolare mercato lo richiede o perché ritiene che il prodotto finale ne risulti migliorato, mentre è possibile che un altro soggetto ometta tale oggetto. Un'implementazione che non include una particolare opzione, *DEVE* essere preparata ad interoperare con un'altra implementazione che la include, anche se con ridotte funzionalità. Allo stesso modo, un'implementazione che include una particolare opzione, *DEVE* essere preparata ad interoperare con un'altra implementazione che non la include (eccetto per la particolare funzionalità che l'opzione consente).

Così come definito in IETF RFC 3280 [8], si rammenta che per ogni estensione usata all'interno di un certificato va definito se essa vada marcata "critica" oppure "non critica". Un sistema che utilizzi il certificato *DEVE* rifiutare il certificato stesso se esso incontra un'estensione marcata "critica" che non riconosce od interpreta correttamente, d'altra parte un'estensione non marcata "critica" può essere ignorata.

4 Certificato di autenticazione

Nel presente documento viene definito il profilo del certificato di autenticazione per l'utilizzo nell'ambito dell'emissione della Carta Nazionale dei Servizi (CNS) [9].
Il profilo del certificato di autenticazione è basato sugli standard IETF RFC 3039 [7] e RFC 3280 [8].

5 Certificato di autenticazione per CNS

5.1 Informazioni relative al titolare (subject)

Le informazioni relative al titolare del certificato *DEVONO* essere inserite nel campo Subject (Subject DN).
In particolare l'attributo commonName (Object ID: 2.5.4.3) *DEVE* contenere il codice fiscale del titolare (nel seguito: codiceFiscale). Esso *DEVE* inoltre contenere l'identificativo univoco del dispositivo (ID_Carta) e il valore dell'hash calcolato sul file elementare contenente i dati personali del titolare così come memorizzato nel dispositivo (EF_Dati_Personali).
La valorizzazione dei sottocampi relativi all'identificativo del dispositivo e ai dati personali DEVE essere effettuata in conformità con le specifiche della CNS e con lo scopo di garantire l'interoperabilità con la CIE.
In conformità con quanto definito per la CNS e per compatibilità con i certificati inseriti all'interno della CIE (CNS/CIE [9]), il carattere separatore dei sottocampi codiceFiscale e ID_Carta dell'attributo commonName *DEVE* essere il carattere "/" (slash, ASCII 0x2F) mentre il carattere separatore dei sottocampi ID_Carta e hashDatiPersonali *DEVE* essere il carattere "." (dot, ASCII 0x2E).
(ad es.: "DMMRNT63H14H501T/123322123123.cd3fdfdfeH2Duoewf5oasookDHo=" è un valore corretto per il commonName).
L'attributo countryName DEVE contenere il *Country Code* ISO 3166 dello Stato in cui è residente il titolare.
L'attributo organizationalUnitName DEVE contenere la denominazione dell'Amministrazione che ha rilasciato la carta.
La valorizzazione di altri attributi nel Subject DN *DEVE* essere eseguita in conformità allo RFC 3280 [8].

5.2 Estensioni del certificato

Le estensioni che *DEVONO* essere presenti nel certificato di autenticazione sono:

Key Usage, Extended Key Usage, Certificate Policies, CRL Distribution Points, Authority Key Identifier, Subject Key Identifier;

L'estensione Basic Constraints *NON DEVE* essere presente.

La valorizzazione delle estensioni elencate per il profilo descritto è riportata nel seguito.

L'estensione Key Usage (Object ID: 2.5.29.15) *DEVE* avere attivato il bit di digitalSignature (bit 0) e *DEVE* essere marcata critica. L'estensione *PUO'* contenere altri bit attivati corrispondenti ad altri Key Usage, purché ciò non sia in contrasto con quanto indicato in RFC 3280 [8] e in RFC 3039 [7]. L'estensione *NON DEVE* avere attivato il bit di nonRepudiation (bit 1).

L'estensione Extended Key Usage (Object ID: 2.5.29.37) *DEVE* contenere l'object id previsto per lo scopo di "TLS WWW Client Authentication" (Object ID 1.3.6.1.5.5.7.3.2) e *NON DEVE* essere marcata critica. L'estensione *PUO'* contenere altri valori che indicano altri scopi, purché non in contrasto con quanto indicato in RFC 3280 [8].

L'estensione Certificate Policies (Object ID: 2.5.29.32) *DEVE* contenere l'object id della Certificate Policy (CP) e l'URI (Uniform Resource Identifier) che punta al Certificate Practice Statement (CPS) nel rispetto del quale il certificatore ha emesso il certificato. Detto object id è definito e pubblicizzato dal certificatore. A far data dal mese di maggio 2005 l'estensione DEVE inoltre contenere l'object id "1.3.76.16.2.1" e il qualifier "userNotice" di tipo "explicitText" con il seguente contenuto: "Identifies X.509 authentication certificates issued for the italian National Service Card (CNS) project in according to the italian regulation".
Considerato che la regione Lombardia, nell'ambito del progetto CRS SISS, ha già emesso certificati di autenticazione e smart card comunque conformi alle norme sulla CNS, che dette carte

costituiscono quindi delle CNS, si rendono pubblici i valori che l'object id può assumere nei suddetti certificati: "1.3.159.6.1.3.2.10" e "1.3.76.12.1.1.10.2.2.10".
Nel caso specifico di certificati emessi per il circuito della CNS la correttezza del valore contenuto nel campo codiceFiscale viene sempre verificata dall'ente emettitore (la Pubblica Amministrazione) come specificato in CNS/CIE [9].L'estensione Certificate Policies *NON DEVE* essere marcata critica.

L'estensione CRL Distribution Points (Object ID: 2.5.29.31) *DEVE* contenere l'URI che punta alla CRL/CSL pubblicata dal certificatore e utilizzabile per effettuare la verifica del certificato. In conformità a quanto definito in IETF RFC 3280 [8] par. 4.2.1.14 e par. 5.2.5, l'URI *DEVE* configurare un percorso assoluto per l'accesso alla CRL e non un percorso relativo ed inoltre *DEVE* specificare anche il nome del server.
Lo schema da utilizzare per l'URI *DEVE* essere l'http oppure l'ldap (IETF RFC 1778 [2] e RFC 2255 [5]) e consentire il download anonimo della CRL.
Costituiscono esempio valido i seguenti valori possibili:

"http://www.cns_crl.it/CRL/Autenticazione/crlauth"
"ldap://dir.cns_crl.it/cn=CA%20Autenticazione,o=Servizi%20di%20Certificazione,c=IT?certificateRevocationList;binary"

L'estensione CRL Distribution Points *NON DEVE* essere marcata critica.

L'estensione Authority Key Identifier (Object ID: 2.5.29.35) *DEVE* contenere almeno il campo keyIdentifier e *NON DEVE* essere marcata critica.
L'estensione Subject Key Identifier (Object ID: 2.5.29.14) *DEVE* contenere almeno il campo keyIdentifier e *NON DEVE* essere marcata critica.

Se il certificatore mette a disposizione delle cosiddette "relying parties" (i terzi che effettuano la verifica della validità del certificato) un sistema di Online Certificate Status Protocol (OCSP, definito in IETF RFC 2560 [6]), ha la necessità di indirizzarle correttamente sui sistemi che forniscono tali informazioni (OCSP Responders).
In tal caso il certificato *DEVE* contenere l'estensione Authority Info Access (Object ID: 1.3.6.1.5.5.7.1.1). Tale estensione *DEVE* contenere almeno un campo AccessDescription valorizzato con l'OID 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) nel campo accessMethod e l'URI che punta all'OCSP Responder del certificatore, utilizzabile per effettuare la verifica del certificato stesso, nel campo accessLocation. In conformità a quanto definito in IETF RFC 3280 [8] par. 4.2.2.1 e IETF RFC 2560 [6], l'URI *DEVE* configurare un percorso assoluto per l'accesso all'OCSP Responder ed inoltre *DEVE* specificare anche il nome del server.
Lo schema da utilizzare per l'URI *DEVE* essere almeno l'http e consentire l'interrogazione mediante il protocollo OCSP definito in IETF RFC 2560 [6].
Nel caso vengano valorizzati più di un AccessDescription per l'estensione, tali indicazioni debbono configurare diversi percorsi alternativi per lo stesso risultato, ossia l'interrogazione tramite OCSP dello stato del certificato al momento della richiesta.
Il valore "http://www.cns_ocsp.it/OSCPResponderOne" costituisce un esempio valido per l'accessLocation.

L'estensione Authority Info Access *NON DEVE* essere marcata critica.

L'aggiunta delle altre estensioni anche private non contenute in questo documento è *OPZIONALE* purché in conformità allo IETF RFC 3280 [8].

APPENDICE A. Esempio

Nel seguito è riportato un esempio di certificato digitale di autenticazione conforme.

a. Certificato per CNS in versione annotata

L'esempio riporta un certificato per CNS, i valori in esso contenuti sono immaginari e utilizzati a puro scopo di esempio.

```
 VERSION:  3
 SERIAL:  7510 (0x1d56)
 INNER SIGNATURE:
  ALG. ID:    id-sha1-with-rsa-encryption
  PARAMETER:  0
 ISSUER:
  Country Name:             IT
  Organization Name:        Certificatore accreditato
  Organizational Unit Name: Servizi di certificazione
  Common Name:              Certification Authority Cittadini
 VALIDITY:
  Not Before:  Oct 28, 03 09:59:55 GMT
  Not After:   Oct 27, 09 09:58:42 GMT
 SUBJECT:
  Country Name:             IT
  Organization Name:        Nome convenzionale di progetto
  Organizational Unit Name: Nome dell'amministrazione
  Common Name:              LGRDNT63H14H501T/1234567890123456.hRfo7thkjYF45tF40v0t8DkgiIG=
 PUBLIC KEY:  (key size is 1024 bits)
 ALGORITHM:
  ALG. ID:    id-rsa-encryption
  PARAMETER:  0
 MODULUS:  0x00a209b4 65f57559 1f699938 e29a27b3
           13a30893 7379cb22 37a6380e 9dd48c4d
           c9057d01 1039dd56 a55e9940 76c68c50
           069a25b5 d777ffc4 d8c56ca2 fc3163e0
           279d919f 0bb1d22d bb07d923 9e972ff3
           252ed27a 4781bccd 99d7b76d 149d08cd
           057f4b9d 9b04ddcb 76e1029e 16e0067f
           f7407553 01aa513e 126ae6b1 2977ea16
           b3
 EXPONENT:  0x010001
 EXTENSIONS:
  Authority Information Access:
   Method:                 id-ad-ocsp
   Location:
    Uniform Resource ID:   http://www.capki.it/OCSP/ResponderOne
  Certificate Policies:
   Policy 1:
   ID:                     1.3.76.16.2.1
   Qualifier 1:            unotice (id-qt-unotice)
   userNotice:
        explicitText: Identifies X.509 authentication certificates issued for the italian National Service Card (CNS) project in ac-
cording to the italian regulation
   Policy 2:
   ID:                     OID del Certificatore
   Qualifier 1:            cps (id-qt-cps)
   CPS uri:                https://www.capki.it/PrivateCA/CNSCPS
  Key Usage*:              Digital Signature
  Extended Key Usage:      Client Authorization
  Authority Key Identifier:  0xea3e2ce0 c724083f 97563685 e8b85cbd 4bba9e30
  CRL Distribution Points:
  Distribution Point 1:
   Uniform Resource ID:    https://www.capki.it/Certificatore/CRL3
  Subject Key Identifier:  0x44a0ff7c f5592ca6 63da6059 490ac1ce 337ecc2a
SIGNATURE:
 ALG. ID:    id-sha1-with-rsa-encryption
 PARAMETER:  0
 VALUE: 0x6c3e208d 1d9bea97 31757b54 b752678f
        1002426b a5e403d5 f5368d51 fce72a97
        4040731e e0601ead e1e34a46 a7d0c305
```

***Appendice* 2**

Protocollo d'intesa del 13 maggio 2003

Protocollo d'intesa
per la realizzazione dei progetti
Carta d'identità elettronica e Carta nazionale dei servizi

Vista la legge 16 giugno 1998, n.191 e, in particolare, l'art.2, comma 4, che ha sostituito l'art.2, comma 10, della legge 15 maggio 1997, n.127;

Visto il regolamento, emanato con decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437, che disciplina le caratteristiche e le modalità per il rilascio "della carta di identità elettronica e del documento elettronico" ;

Visto il decreto del Ministro dell'interno 19 luglio 2000, recante: "Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici";

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante: **"**Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" e, in particolare, l'art.36, concernente la carta di identità e i documenti elettronici;

Vista la direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche;

Visto il decreto legislativo 23 gennaio 2002, n.10, recante: "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche"

Considerato che:

- il Governo ha posto la realizzazione dell'e-Government tra gli obiettivi primari da raggiungere;
- la prima fase di sperimentazione del progetto "Carta d'identità elettronica", nel corso della quale sono state rilasciate 170.000 carte, si è conclusa con successo nel 2001 e il Ministero dell'interno ha varato la seconda fase;
- il Ministro per l'innovazione e le tecnologie ha avviato il progetto "Carta nazionale dei servizi" per accelerare la diffusione dei servizi in rete, offrendo agli Enti pubblici l'opportunità di fornire ai cittadini carte a microcircuito che consentano l'identificazione "*on line*" e siano pienamente compatibili con la carta d'identità elettronica

Ritenuto che:

- è essenziale, per lo sviluppo dei progetti di e-Government, l'identificazione in rete dei cittadini attraverso carte a microcircuito (carta d'identità elettronica e carta nazionale dei servizi);

- è necessario assicurare l'accesso ai servizi in rete attraverso l'utilizzo di carte diverse, prodotte secondo i principi della libera concorrenza, assicurando, nel contempo, la piena interoperabilità tra le funzioni proprie delle carte e i servizi;
- il progetto pilota Netlink ha posto le basi per lo sviluppo della carta sanitaria, che consentirà di usufruire dei servizi sanitari nazionali utilizzando le carte a microcircuito;
- in ambito comunitario, nel contesto del piano d'azione eEurope, l'iniziativa eEurope Smart Cards (eESC) ha studiato le problematiche inerenti le carte a microcircuito multi-uso e ha prodotto la documentazione "eESC Common Specifications for interoperable multi-application secure smart cards v2.0";
- le imprese che hanno sottoscritto il presente Protocollo d'intesa rappresentano il mercato europeo delle carte a microcircuito e sono impegnate a sostenerne la crescita, nonché ad assicurare l'interoperabilità tra le carte partecipando attivamente ai lavori in materia di standardizzazione in ambito europeo e nel più ampio contesto internazionale.

tutto ciò premesso e considerato

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE
Dott. Lucio Stanca

IL SOTTOSEGRETARIO DI STATO ALL'INTERNO
Sen. Antonio D'Alì

e

la società CardNet Group S.p.A. , Via Marconi, 8 - 20020 Arese (MI), nella persona del Presidente, Dott. Stefano Camilleri, nato a Joppolo Giancaxio (AG) il 1 gennaio 1935, residente in Milano;

la società Gemplus SA, Avenue du Pic de Bertagne, Parc d'activitè de Gemenos, 13881 Gemenos (France),
nella persona del FSS Sales Manager Italy, Dott. Paolo Magri, nato a Milano il 16 settembre 1960, residente in Milano;

la società Ghirlanda S.p.A., Via Gonzaga, 7 - 20123 Milano,
nella persona dell'Amministratore Delegato, Sig. Ettore Ghirlanda, nato a Magenta (MI) il 15 giugno 1967, residente in Milano;

la società Giesecke & Devrient GmbH, Prinzregentenstrasse, 159, D-81677 München,
nella persona dell'Executive Senior vice President, Dott. Jürgen Moll, nato a Urach-Wittlingen (Germany) il 27 ottobre del 1952, residente in Sauerlach;

la società Incard S.p.A., Via F. Caracciolo, 15 - 80122 Napoli,
nella persona dell'Amministratore Delegato, Ing. Simone Cavallo, nato a S. Nicola la Strada (CE) il 19 giugno 1962, residente in Caserta;

la società Oberthur Card Systems Italia s.r.l., Via Monte Spluga, 58 - 20021 Baranzate di Bollate (MI),
nella persona dell'Amministratore Delegato, Dott. Angelo Giuseppe Cogliati, nato a Milano il 28 settembre 1966, residente in Milano;

la società Orga Card Systems (Italia) s.r.l., Via Benedetto Croce, 19 - 00142 Roma,
nella persona dell'Amministratore Delegato, Dott. Gilberto Tonali, nato a Roma il 24 agosto 1948, residente in Roma;

la società SEMA S.p.A., Viale Carlo Viola, 76 – 11026 Pont-Saint-Martin (AO),
nella persona del Vice President & Managing Director Mediterranean Geo-Market, Ing. Luigi Giacalone, nato a Firenze il 20 novembre 1955, residente in Roma;

la società Siemens Informatica S.p.A., Via Vipiteno, 4 – 20128 Milano,
nella persona dell'Amministratore Delegato, Sig. Valentino Bravi, nato a Pavia il 10 marzo 1957, residente in Pavia.

CONVENGONO QUANTO SEGUE

ART. 1 – AMBITO DI APPLICAZIONE

Il presente Protocollo d'intesa riguarda la fornitura di carte a microcircuito destinate ad essere utilizzate nei progetti Carta d'Identità Elettronica (di seguito denominato "CIE") e Carta Nazionale dei Servizi (di seguito denominato "CNS"), nonché in ogni altro progetto che faccia riferimento alle specifiche tecniche relative alla CIE e alla CNS.
Il presente protocollo è aperto all'adesione di tutti i soggetti interessati.

ART. 2 – OGGETTO DELL'ACCORDO

Il Ministero dell'interno e il Ministro per l'innovazione e le tecnologie e le imprese firmatarie stabiliscono di avviare una comune azione per lo sviluppo di servizi nel campo della identificazione e della autenticazione elettronica.

A tal fine:

- il Ministero dell'interno e il Ministro per l'innovazione e le tecnologie si impegnano a sostenere lo sviluppo di progetti concernenti la CIE e la CNS, promuovendone la diffusione e offrendo un supporto ai fini dell'efficienza dei servizi connessi da erogare
- le imprese firmatarie si impegnano a garantire l'indipendenza tra i servizi e i dispositivi (carte a microcircuito), al fine di incoraggiare il più possibile l'adesione generale ai sistemi di identificazione e di autenticazione in rete, nonché ad altri servizi basati su carte a microcircuito evitando, in pari tempo, di vincolare sviluppatori e utenti all'uso di specifici dispositivi.

ART. 3 – GRUPPO DI LAVORO

Le imprese firmatarie concordano sull'opportunità che il Ministero dell'interno e il Ministro per l'innovazione e le tecnologie istituiscano un apposito Gruppo di lavoro - del quale saranno chiamate a fare parte - con il compito di sviluppare regole comuni orientate a garantire l'indipendenza tra le applicazioni e i sistemi operativi delle carte e l'efficacia dei servizi connessi.

Nello svolgimento della propria attività detto Gruppo di lavoro organizzerà periodiche riunioni che si svolgeranno a Roma.

Le decisioni del Gruppo di lavoro terranno conto degli *standard* disponibili e degli orientamenti propri di altri progetti presenti nell'ambito dell'Unione europea relativi allo stesso settore, nonché dei vincoli che hanno caratterizzato la fase di avvio dei progetti CIE e CNS.

I risultati conseguiti dal Gruppo di lavoro potranno essere utilizzati ai fini della definizione di ulteriori specifiche relative ai progetti CIE e CNS che dovranno, comunque, essere rispettate per poter partecipare alle procedure di gara per la fornitura di carte a microcircuito per i progetti CIE e CNS.

ART. 4 – SPECIFICHE DEL SISTEMA OPERATIVO DELLE CARTE A MICROCIRCUITO

Le imprese firmatarie convengono di implementare le specifiche del sistema operativo della carta a microcircuito (APDU) riportate in allegato.

Le imprese firmatarie riconoscono che i documenti allegati accolgono le indicazioni del Gruppo di lavoro previsto dal precedente art.3 e tengono, altresì, conto dello stato dell'arte della tecnologia e degli orientamenti del mercato.

Il Ministero dell'interno, il Ministro per l'innovazione e le tecnologie e le imprese firmatarie, si impegnano a promuovere la diffusione delle specifiche allegate, quali modello per la realizzazione di progetti cooperativi nell'ambito dell'Unione europea.

ART. 5 – DIRITTI E OBBLIGHI DELLE IMPRESE FIRMATARIE

Le imprese firmatarie che intendono partecipare alla realizzazione dei progetti CIE e CNS devono pianificare le attività concernenti la realizzazione e la fornitura delle carte a microprocessore in accordo con le indicazioni che verranno date dal Gruppo di lavoro previsto dal precedente art.3 e in conformità alle specifiche APDU allegate.

Le imprese firmatarie cooperano al fine di raggiungere e garantire la piena interoperabilità tra i servizi che si basano su differenti carte a microcircuito.

Le imprese firmatarie riceveranno dai gruppi di progetto governativi informazioni in merito ai tempi di realizzazione e alle linee di indirizzo dei progetti.

Le imprese firmatarie, in sede di partecipazione a procedure concorsuali per la fornitura di carte a microcircuito relative a progetti CIE e CNS potranno dichiarare di aver sottoscritto il presente Protocollo d'intesa, attestando, con l'occasione, l'elevato livello di conoscenza del progetto e la sua aderenza alle specifiche tecniche riportate in allegato.

Le imprese firmatarie saranno debitamente e tempestivamente informate dai gruppi di progetto governativi in merito ad eventuali modifiche relative alle specifiche tecniche riguardanti i progetti CIE e CNS.

ART. 6 – RECESSO

Ciascuna impresa può recedere unilateralmente dall'adesione al presente Protocollo d'intesa dandone formale comunicazione al Ministero dell'interno e al Ministro per l'innovazione e le tecnologie, nonché a tutte le altre imprese firmatarie.

In esito al recesso vengono meno i diritti e gli obblighi previsti al precedente art.5.

ART. 7 – PERIODO DI VALIDITA'

Il presente Protocollo d'intesa sarà efficace per 36 mesi, a partire dalla data di sottoscrizione.

Roma, 13 maggio 2003

IL MINISTRO
PER L'INNOVAZIONE E LE TECNOLOGIE
Dott. Lucio Stanca

IL SOTT. DI STATO ALL'INTERNO
Sen. Antonio D'Alì

La SOCIETA' CardNet Group S.p.A.
(Il Presidente)
Dott. Stefano Camilleri

La SOCIETA' Gemplus SA
(per l'Amministratore Delegato)
Dott. Paolo Magri

La SOCIETA' Ghirlanda S.p.A.
(L'Amministratore Delegato)
Sig. Ettore Ghirlanda

La SOCIETA' Giesecke & Devrient GmbH
(L'Executive Senior vice President)
Dott. Jürgen Moll

La SOCIETA' Incard S.p.A.
(L'Amministratore Delegato)
Ing. Simone Cavallo

La SOCIETA' Oberthur Card Systems Italia S.r.l.
(L'Amministratore Delegato)
Dott. Angelo Giuseppe Cogliati

La SOCIETA' ORGA Card Systems Italia s.r.l.
(L'Amministratore Delegato)
Dott. Gilberto Tonali

La SOCIETA' SEMA S.p.A.
(per l'Amministratore Delegato)
Ing. Luigi Giacalone

La SOCIETA' Siemens Informatica S.p.A.
(L'Amministratore Delegato)
Sig. Valentino Bravi

Appendice 3

Dati presenti sulla CNS

Vengono definiti i dati presenti sulla CNS, descrivendone il contenuto e la codifica. Vengono descritti i presenti all'emissione. Non viene descritta la parte relativa alla struttura Netlink.
Tali strutture dati e codifiche sono sviluppate in conformità con le specifiche della Carta d'Identità Elettronica (CIE) al fine di garantire l'interoperabilità tra le due carte.

I dati presenti sulla CNS sono:

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 1 - Definizione Dati Personali

Codifica file dati personali

La codifica utilizzata è coerente con quella della CIE.

Ogni dato è codificato con un campo lunghezza (Len) ed un campo valore (Value)

Il campo Len consiste in una stringa di due caratteri ASCII che codifica in esadecimale la lunghezza in byte del campo Value, allineata a destra, con riempimento di zeri a sinistra.

Esempio: la lunghezza di un campo Value di 10 caratteri verrà codificata con la stringa '0A'

Il campo Value viene codificato con una stringa ASCII.

In testa al file è contenuta l'informazione sulla dimensione totale.

La dimensione totale consiste in una stringa di sei caratteri ASCII che codifica in esadecimale la lunghezza in byte dello spazio utilizzato, allineata a destra, con riempimento di zeri a sinistra. Nel calcolo della lunghezza si prendono in conto anche i 6 byte della lunghezza stessa.

I byte rimanenti nel file rispetto all'allocazione massima vengono settati a 00h.

Per compatibilità con l'anagrafica della Tessera Sanitaria, il file Dati Personali presenta delle differenze nella lunghezza massima dei campi Cognome (80) e Nome (86).

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 è 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 è opportuno che coincidano con il numero seriale Netlink..

Le informazioni dettagliate su come costruire il numero seriale sono contenute nel documento NK/4/FNS/T/21/1.0 "Gestione del Serial Number delle Carte Sanitarie" pubblicato sul sito Internet del CNIPA:

http://www.cnipa.gov.it.

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".