Specifiche tecniche del Documento Digitale Unificato

Sommario

Storia del documento

Version	Author	Dates	Nature of Modification
1.0.0	AGID	10/10/2013	First Document Release

Introduzione

Il presente documento contiene le specifiche tecniche della nuova carta di identità elettronica italiana, denominata DDU: Documento Digitale Unificato. Il documento digitale sostituisce anche la tessera sanitaria rilasciata a tutti i cittadini che ne hanno diritto.

Le specifiche tecniche inerenti le caratteristiche e le modalità di colloquio con i microprocessori sono pubblicate, esclusivamente in lingua inglese, con altro documento denominato "**DDU – Documento Digitale Unificato - Functional Specification"**.

Contesto e scelta architetturale

Il Documento Digitale Unificato (DDU) consente di autenticare il cittadino in rete attraverso un certificato X.509 ed una coppia di chiavi crittografiche protette da appositi codici forniti al cittadino. Attraverso detta autenticazione il cittadino potrà fruire dei servizi resi disponibili in rete. Tale caratteristica è peraltro già fornita, attraverso il microprocessore a contatti di cui è dotata, dalla Carta Nazionale dei Servizi (CNS) e carte ad esse conformi quali la nuova Tessera Sanitaria (TS/CNS) e le Carte Regionali Servizi (CRS) che, nell'insieme sono state fornite a diverse decine di milioni di cittadini.

Nell'ambito del progetto CNS, oltre al servizio di autenticazione in rete, è prevista la presenza dei cosiddetti "servizi aggiuntivi", costituiti da dati memorizzati sulla smartcard al fine di consentire l'erogazione di ulteriori servizi applicativi a carattere locale. Generalmente tali servizi sono installati successivamente al rilascio della CNS, in una apposita area denominata "DF2".

Con il progetto DDU si è stabilita l'opportunità di prevedere la presenza di due microprocessori, uno a radiofrequenza (RF) ed uno a contatti. Il chip a RF consente di dare un notevole carattere innovativo al nuovo documento rendendolo conforme agli standard europei. Nel contempo, si è considerato che i numerosi servizi aggiuntivi realizzati dalle pubbliche amministrazioni locali (in specie dalle Regioni) non potrebbero essere direttamente fruibili con tale microprocessore, richiedendo delle modifiche ai servizi web, ma anche e soprattutto la necessità dei cittadini di dotarsi di un nuovo lettore. Per tale ragione si è deciso di dotare il nuovo documento di entrambi i microprocessori. In questo modo i cittadini potranno continuare a fruire dei servizi in essere utilizzando la parte a contatti e le pubbliche amministrazioni disporranno del tempo necessario alle modifiche necessarie per rendere i servizi aggiuntivi fruibili attraverso il microprocessore RF.

Sezione I – Specifiche del chip contactless

1 L'applicazione MRTD

1.1 Sistema operativo

1.1.1 Sistema operativo - Meccanismi di sicurezza

Il sistema operativo del chip deve supportare i meccanismi di sicurezza BAC e Passive Authentication in accordo alle specifiche ICAO Doc 9303, Machine Readable Travel Documents - Part 3 [12] e report supplementari.

Il sistema operativo del chip deve supportare il meccanismo di sicurezza PACE v2 in accordo alle specifiche ICAO Technical Report – Supplemental Access Control for Machine Readable Travel Documents, 2010 [16] e successive versioni.

Il sistema operativo del chip deve supportare il meccanismo di sicurezza EAC in accordo alle specifiche Technical Guideline TR-0311 - Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 e Part 3 v2.10 [18].

1.1.2 Sistema operativo - Algoritmi

1.1.2.1 Sistema operativo - Algoritmi per il protocollo BAC

È richiesto che il sistema operativo supporti per la derivazione delle chiavi di Secure Messaging almeno l'algoritmo di cifratura simmetrica 3DES a 112 bit con meccanismo di hashing SHA-1 secondo quanto riportato nel documento [12].

1.1.2.2 Sistema operativo - Algoritmi per il protocollo PACE

È richiesto che il sistema operativo supporti per la derivazione delle chiavi di Secure Messaging, secondo quanto previsto nel documento [16] almeno i seguenti algoritmi:

1 Algoritmo di cifratura simmetrica AES a 128 bit con meccanismo di hashing SHA-1 e AES a 192 e 256 bit con meccanismo di hashing SHA-256;
2 Algoritmo di cifratura simmetrica 3DES a 112 bit con meccanismo di hashing SHA-1;
3 Algoritmo di condivisione chiavi Diffie Helmann (DH) con dimensione massima dei parametri di dominio della chiave di almeno 1024-bit;
4 Algoritmo di protocollo di condivisione chiavi ECDH con dimensione massima dei parametri di dominio della chiave di almeno 192-bit ;
5 Algoritmo di Generic Mapping dei parametri di dominio;
6 Algoritmo di Integrated Mapping dei parametri di dominio.

1.1.2.3 Sistema operativo - Algoritmi per il protocollo EAC

Chip Authentication

È richiesto che il sistema operativo, secondo quanto previsto nel documento [18], supporti almeno i seguenti algoritmi:

7 Algoritmo di cifratura simmetrica AES a 128 bit con meccanismo di hashing SHA-1 e AES a 192 e 256 bit con meccanismo di hashing SHA-256;
8 Algoritmo di cifratura simmetrica 3DES a 112 bit con meccanismo di hashing SHA-1;
9 Algoritmo di protocollo di condivisione chiavi Diffie Helmann (DH) con dimensione massima dei parametri di dominio della chiave di almeno 1024-bit;
10 Algoritmo di protocollo di condivisione chiavi ECDH con dimensione massima dei parametri di dominio della chiave di almeno 192-bit.

Terminal Authentication

È richiesto che il sistema operativo, secondo quanto previsto nel documento [18], supporti almeno i seguenti algoritmi:

11 Algoritmo di crittografia asimmetrica RSA-v1_5-SHA-1 con dimensione massima di chiave supportata di almeno 2048 bit;
12 Algoritmo di crittografia asimmetrica RSA-v1_5-SHA-256 con dimensione massima di chiave supportata di almeno 2048 bit;
13 Algoritmo di crittografia asimmetrica RSASSA-PSS SHA-1 con dimensione massima di chiave supportata di almeno 2048 bit;
14 Algoritmo di crittografia asimmetrica RSASSA-PSS SHA-256 con dimensione massima di chiave supportata di almeno 2048 bit;
15 Algoritmo di crittografia asimmetrica ECDSA-SHA-1 con dimensione massima di chiave supportata di almeno 192 bit;
16 Algoritmo di crittografia asimmetrica ECDSA-SHA-1 con dimensione massima di chiave supportata di almeno 192 bit.

1.1.3 Sistema operativo - Requisiti operativi

Al termine della fase di personalizzazione, in fase operativa, il sistema operativo deve avere almeno le seguenti caratteristiche.

IDENTIFICATIVO UNICO RANDOMICO: il sistema operativo, a personalizzazione eseguita, deve utilizzare l'identificativo unico (UID o PUPI) randomico, come raccomandato nel documento Supplement to Doc 9303[19].

COMANDI di CHIP AUTHENTICATION: il sistema operativo deve prevedere che la fase di Chip Authentication possa essere implementata sia con il comando MSE AT + GA, che con il comando MSE KAT, in conformità a quanto riportato nelle specifiche [18].

TERMINAL AUTHENTICATION: il sistema operativo deve prevedere per la fase di Terminal Authentication, nel caso di utilizzo del protocollo PACE, l'utilizzo del "dynamic binding" secondo quanto specificato in [18].

TRUST POINT: il sistema operativo deve permettere la memorizzazione e aggiornamento di almeno n.2 Trust Point interni (chiave pubblica della CVCA) in accordo alle specifiche [18].

1.2 Interoperabilità

Deve essere garantita l'interoperabilità con i lettori / scrittori RFid di personalizzazione e verifica delle sedi di rilascio e verifica presenti sul territorio (ISO 14443 Type A e Type B).

2 L'applicazione IAS

2.1 Introduzione

2.1.1 Requisiti

Nella stesura delle specifiche del DDU sono stati definiti dei requisiti da tenere in considerazione nell'implementazione del file system del DDU su sistema operativo conforme alle specifiche IAS.

Di seguito un elenco di tali requisiti:

17 il livello di protezione dei dati presenti nell'applicazione IAS deve essere almeno uguale a quello dei rispettivi dati nell'applicazione ICAO;
18 deve essere presente un Numero Identificativo per i Servizi, univoco del documento, non corrispondente col seriale, a lettura libera (ID Servizi);
19 la comunicazione di tutti i dati personali, nonché del PIN e del PUK deve avvenire tramite un canale sicuro cifrato;
20 i dati personali sono contenuti tutti all'interno del certificato di autenticazione. Non è più usato il file dei dati personali;
21 non è richiesta, l'installazione di servizi aggiuntivi. I servizi aggiuntivi si devono basare esclusivamente sulla lettura del Numero Identificativo per i Servizi;
22 non è richiesta la duplicazione nell'applicazione IAS dei dai biometrici (foto e impronte digitali) già presenti nell'applicazione ICAO.

E' da aggiungere a tali requisiti, dettati da esigenze di protezione dei dati, di privacy e applicativi, l'ulteriore requisito opzionale della non clonabilità del documento. L'esposizione di un file a lettura libera contenente l'ID carta espone con facilità a rischi di clonazione, qualora esso non sia accompagnato a sistemi di verifica di autenticità del documento stesso.

Tali verifiche non devono essere obbligatorie per accedere ai dati contenuti sul chip; è responsabilità dell'applicazione, sulla base della "sensibilità" del servizio offerto, effettuare i test di autenticità del DDU.

In tale ottica, si distinguono due "servizi" che vengono esposti dal DDU e sono disponibili alle applicazioni:

- L'identificazione del documento tramite il Numero Identificativo per i Servizi
- L'identificazione in rete del titolare tramite chiave privata RSA associata ad un certificato di autenticazione client

Entrambi i servizi hanno come scopo l'autenticazione del documento o del titolare per ottenere l'accesso alle applicazioni di un Service Provider.

Il servizio di identificazione tramite Numero Identificativo per i Servizi ha le seguenti caratteristiche:

- Non richiede particolari capacità crittografiche da parte del terminale che dà accesso all'applicazione
- Non richiede l'esplicito consenso del titolare tramite immissione di un PIN
- Non prevede la comunicazione di dati personali del titolare del DDU (nome, cognome, codice fiscale)
- Non prevede la cifratura dei dati sul canale di comunicazione

E' ovvio che, sulla base di tali caratteristiche, questo servizio possa essere utilizzato esclusivamente da applicazioni che richiedono un livello di sicurezza estremamente basso, poiché sistemi più sicuri sarebbero economicamente non giustificati o non applicabili. Inoltre, non essendo comunicato alcun dato personale del titolare, è il documento che viene identificato, piuttosto che titolare stesso.

Il servizio di identificazione in rete tramite certificato di autenticazione client ha le seguenti caratteristiche:

- Richiede che il terminale che dà accesso all'applicazione abbia la capacità di applicare algoritmi crittografici simmetrici (3-DES, AES) e asimmetrici (RSA)
- Richiede l'esplicito consenso del titolare tramite immissione di un PIN
- Prevede la comunicazione di dati personali del titolare del DDU (nome, cognome, codice fiscale)
- Prevede la cifratura dei dati sul canale di comunicazione

Questo servizio è dedicato alle applicazioni più sensibili che necessitano del massimo livello di sicurezza, dell'identificazione certa del titolare e che i dati coinvolti nella transazione non siano intercettati. Per assicurare tutto ciò, il terminale deve avere specifiche capacità crittografiche.

2.1.2 Implementazione

Verrà proposta di seguito un'implementazione del DDU su applicazione IAS che recepisce i requisiti espressi ai paragrafi precedenti.

Requisito	Implementazione
1) Protezione dati IAS almeno uguale a ICAO	I dati personali e il seriale carta sono protetti in lettura tramite secure messaging e richiedono la verifica del PIN utente
2) Presenza di un identificativo a lettura libera	E' presente il file EF_IDServizi, leggibile liberamente e non cifrato, che contiene un codice univoco del documento
3) Canale di comunicazione sicuro per i dati personali	Il canale di comunicazione viene stabilito tramite un protocollo di scambio di chiavi Diffie Hellman

4) Dati personali nel certificato	Non è prevista la presenza del file EF_DatiPersonali, ma solo del certificato CNS
5) Servizi aggiuntivi non richiesti	Il file system IAS proposto è chiuso e non modificabile in nessuna sua parte
6) Duplicazione biometria non richiesta	Non sono presenti file contenenti foto e impronte nell'applicazione IAS

Il primo requisito preso in considerazione nella stesura del file system è il punto 3) espresso nel paragrafo precedente: la necessità di predisporre un canale di comunicazione sicuro. Il sistema IAS recepisce le specifiche ICAO, e mette a disposizione un sistema di scambio di chiavi simile a quello usato durante la fase di Chip Authentication, durante quale viene negoziata una quantità segreta utilizzata per derivare delle chiavi di sessione di secure messaging, che quindi cambiano ad ogni accesso al DDU.

Lo scambio di chiavi Diffie Hellman non richiede alcuna autenticazione preventiva; può essere eseguito da propone chiunque, ma è resistente ad un attacco di eavesdropping (attaccante in ascolto sul canale). Lo scopo è quello di proteggere le comunicazioni, e in particolare l'invio del PIN e del PUK, da attaccanti in ascolto sul canale di comunicazione contactless.

2.1.3 Considerazioni relative alla sicurezza

Il protocollo di scambio di chiavi Diffie Hellman permette di stabilire una comunicazione sicura fra il terminale e il documento e assicura la confidenzialità dei dati scambiati rispetto ad un attaccante in ascolto sul canale (eavesdropping), tuttavia non è resistente ad un attacco di tipo Man-In-The-Middle. Nel MITM l'attaccante si pone come punto intermedio nella comunicazione fra il terminale e il documento, e può stabilire due sessioni di secure messaging con i due end-point tramite le quali intercettare il PIN inserito dall'utente.

Per resistere ad un attacco di questo tipo è necessario l'utilizzo o di una chiave simmetrica condivisa, o di una/due coppie di chiavi asimmetriche possedute dagli endpoint con cui effettuare un'autenticazione interna/esterna.

L'approccio con chiave simmetrica condivisa richiede che essa venga inserita all'interno del middleware software per l'utilizzo del DDU, ma questo approccio è intrinsecamente vulnerabile, poiché si può sempre pensare che un'attaccante sia in grado di ricavare la chiave dalla libreria e utilizzarla per decifrare le comunicazioni. Si preferisce quindi orientarsi all'approccio con chiavi asimmetriche.

Tale approccio può essere utilizzato sia per garantire confidenzialità in modo resistente al MITM, sia per autenticare gli endpoint. In particolare la specifica IAS prevede questa modalità tramite il protocollo di "Device authentication with privacy protection", che richiede l'uso di certificati CV per l'external authentication.

La resistenza all'attacco MITM è assicurata dal fatto che le fasi di internal/external authentication non sono un semplice challenge/response: oltre al challenge viene anche firmata la chiave pubblica usata nello step di scambio di chiavi Diffie Hellman. Poiché il MITM non ha possibilità di conoscere la chiave privata di internal authentication, e poiché questa è certificata dal SOD, il MITM non può generare la response corretta da inviare al terminale.

L'uso di certificati CV in fase di external authentication, con un protocollo del tutto simile alla Terminal Authentication dell'applicazione ICAO, richiede che tali certificati CV siano emessi da una PKI e distribuiti ai terminali che intendono accedere al DDU tramite tale schema di protezione. Tuttavia, mentre tale approccio è pensabile per l'applicazione ICAO, in cui i terminali fanno parte di un dominio circoscritto e ben controllato (Inspection System alle frontiere), non è proponibile per un documento con diffusione capillare e contesti di utilizzo estremamente eterogenei e possibilmente aperti a qualsiasi Service Provider che decida di usare il DDU come mezzo di autenticazione degli utenti. Un ulteriore requisito, quindi, è che non sia necessaria un'infrastruttura PKI e la distribuzione dei certificati CV per i terminali.

Il sistema che si vorrebbe implementare quindi ha le seguenti caratteristiche:

- Resistente all'eavesdropping
- Resistente al MITM
- Non richiede l'uso di una PKI per la gestione delle coppie chiavi di chiavi e relativi certificati dei terminali
- Utilizza il PIN per l'autenticazione del terminale/utente e l'autenticazione interna per l'autenticazione del documento

L'unica differenza fra quanto richiesto e il protocollo di "Device authentication with privacy protection" consiste nell'uso dei certificati CV in fase di external authentication, poiché nel paragrafo 1 abbiamo stabilito che il livello di autenticazione richiesto dalle parti è il PIN (per il terminale/utente) e l'internal authentication (per il documento); questo perché, come già detto, l'infrastruttura della PKI necessaria per gestire le coppie di chiavi dei terminali è onerosa sia in termini di gestione che di distribuzione.

Questo requisito, tuttavia, può essere aggirato generando dei "falsi" certificati CV per il terminale; il terminale, cioè, dovrebbe conoscere la chiave privata corrispondente alla chiave pubblica della CV di root presente sul chip, generare una coppia di chiavi pubblica/privata di sessione e generare contestualmente un certificato CV per tale coppia, firmandolo con la chiave privata della CV di root.

La conoscenza della chiave privata per la generazione del certificato del terminale NON pregiudica la sicurezza del processo, dato che l'autenticazione del terminale non è demandata a questa fase ma alla verifica del PIN. L'external authentication effettuata in questa modalità non contribuisce in alcun modo ad aumentare la sicurezza della transazione, ma è necessario per adattarsi ai meccanismi di autenticazione previsti in IAS.

2.1.4 Protezione dalla clonazione

La protezione dalla clonazione può avvenire con un sistema analogo alla chip authentication dell'applicazione ICAO: l'utilizzo di una chiave asimmetrica di internal authentication, la cui componente pubblica è leggibile liberamente e firmata dall'autorità che emette il documento (Document Signer).

Tale verifica può essere effettuata in modalità differenti a seconda del servizio che il terminale intende utilizzare:

- Identificazione del titolare tramite certificato di autenticazione client

La procedura di Device authentication with privacy protection prevede uno step di Internal authentication. Non è pertanto richiesto alcun passo aggiuntivo rispetto alla procedura già definita, se non la verifica di affidabilità della chiave pubblica utilizzata.

- Identificazione del documento tramite il Numero Identificativo per i Servizi

In questo caso, se l'applicazione richiede la verifica di autenticità del documento, è necessario che il terminale sia in grado di effettuare un'operazione crittografica con chiave asimmetrica per portare a termine un protocollo challenge/response. A tale scopo viene utilizzata una chiave specifica di internal authentication, distinta da quella usata nel protocollo di device authentication, che non richiede preventiva autenticazione né canali di secure messaging.

Parallelamente allo schema ICAO, la firma del document signer viene posta nel file a lettura libera non modificabile EF_SOD, che contiene la firma in formato PKCS#7 degli hash di tutti gli oggetti di cui si vuole assicurare l'integrità; nel DDU l'EF_SOD contiene:

- EF_DH
- EF_Seriale
- EF_IDServizi
- EF_INT_K_{PUB}
- EF_Servizi_INT_K_{PUB}
- EF_CertCNS

2.2 File System

2.2.1 I servizi esposti dal DDU

Il Documento Digitale Unificato prevede l'utilizzo di un chip con interfaccia contactless conforme alle specifiche ECC-IAS. I servizi esposti dal DDU tramite l'interfaccia contactless sono i seguenti:

- L'identificazione del documento tramite il Numero Identificativo per i Servizi
- L'identificazione in rete del titolare tramite chiave privata RSA associata ad un certificato di autenticazione client

Tali servizi devono essere forniti in modalità sicura, con particolare riferimento alle criticità che comporta l'utilizzo dell'interfaccia contactless. In particolare, è richiesto che informazioni come i PIN ed i dati personali scambiati fra il chip contactless e il terminale tramite il quale si accede ai servizi transitino in modalità sicura e non intercettabile.

2.2.2 Meccanismi di protezione

Per ottemperare ai requisiti espressi sopra è necessario utilizzare dei meccanismi di protezione per regolare l'accesso alle quantità contenute all'interno del chip.

Le specifiche DDU offrono varie modalità di protezione, che assicurano vari livelli di sicurezza e richiedono l'utilizzo di determinate infrastrutture (PKI, distribuzione di chiavi e certificati). Poiché i servizi utilizzati hanno requisiti di sicurezza estremamente differenti, verranno usati differenti meccanismi di protezione, corrispondenti a due livelli diversi di sicurezza:

- Identificazione tramite Numero Identificativo per i Servizi: nessuna protezione (opzionale Passive Authentication)
- Identificazione tramite certificato di Client Authentication: Device authentication with privacy protection (opzionale Passive Authentication)

L'accesso ai servizi tramite lettura del Numero Identificativo non richiede l'uso di meccanismi di protezione poiché deve essere utilizzato da terminali che non hanno capacità crittografiche avanzate; il numero identificativo può viaggiare in chiaro poiché non è un dato personale.

Occorre segnalare tuttavia che:

- l'identificazione tramite Numero Identificativo per i Servizi può essere usata esclusivamente in contesti con bassi requisiti di sicurezza, in cui non è richiesta l'implementazione di sistemi di controllo complessi;
- l'utilizzo di un codice univocamente legato alla carta, sempre leggibile senza alcun prerequisito può esporre il titolare ad essere tracciato nei suoi spostamenti, e quindi può

sollevare delle problematiche di privacy. Potrebbe, ad esempio, essere consigliabile l'utilizzo di opportuni schermi.

L'utilizzo del certificato di Client Authentication richiede un elevato livello di protezione, poiché sul canale devono transitare:

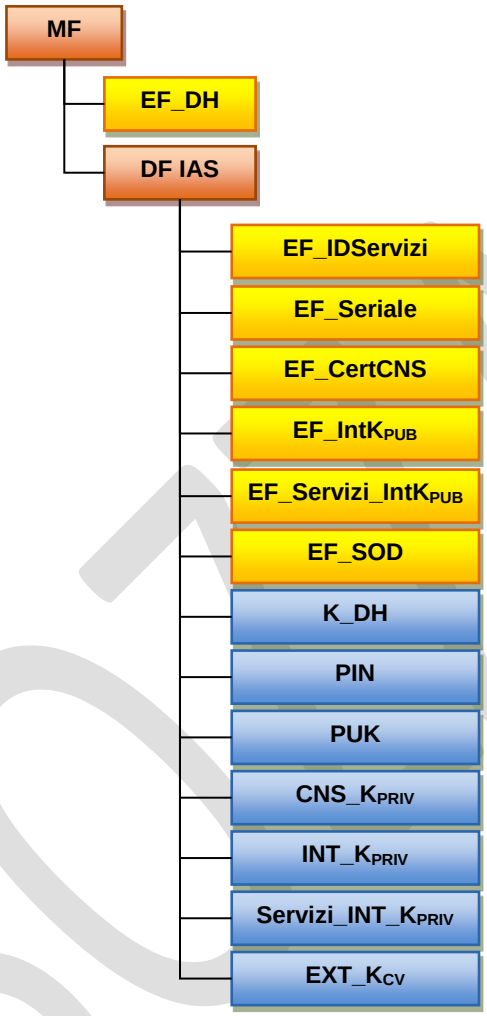
- Il PIN che autorizza l'uso della chiave privata, la lettura del certificato e del seriale carta
- Il certificato di autenticazione contenente nome, cognome e codice fiscale del titolare

Il meccanismo di *Device authentication with privacy protection*, previsto dalla specifica IAS, utilizza un sistema di mutua autenticazione con scambio di chiavi tramite protocollo Diffie Hellman per assicurare la confidenzialità delle informazioni che passano attraverso il canale e la mutua autenticazione degli endpoint.

Per entrambi i servizi il terminale ha la possibilità di verificare l'autenticità del documento (che quindi è protetto dalla clonazione) affiancando Internal Authentication e Passive Authentication, in modo analogo a quanto specificato da ICAO.

2.2.3 Il file system

Di seguito lo schema del file system del DDU:



Gli oggetti presenti nel file system sono i seguenti (laddove non specificato nella colonna Protezione si intende che la condizione di accesso è impostata a Never) :

Nome	Tipo	Condizione d'accesso	Descrizione
EF_DH	EF	Lettura: Always	Parametri di dominio per lo scambio di chiavi Diffie Hellman Il file è firmato in EF_SOD Formato: Struttura ASN1 DomainParameter definita in ANSI X9.42 BER-encoded

K_DH	SDO – DHParam	Uso: Always	Parametri di dominio per lo scambio di chiavi Diffie Hellman
PIN	SDO - UserAuth (PIN)	Uso: Device Auth Sblocco:PUK Cambio:PIN	PIN utente
PUK	SDO - UserAuth (PIN)	Uso: Device Auth Sblocco:Never Cambio:Never	PUK utente
CNS_K_{PRIV}	SDO – AsymKey (Priv)	Uso: PIN	Chiave privata corrispondente al certificato di Client Authentication
INT_K_{PRIV}	SDO – AsymKey (Priv)	Uso: Always	Chiave privata di Internal Authentication (può essere usata solo durante la sequenza di Device Authentication with privacy protection)
Servizi_INT_K_{PRIV}	SDO – AsymKey (Priv)	Uso: Always	Chiave privata di Internal Authentication (può essere usata solo durante la sequenza di Device Authentication with privacy protection)
EXT_K_{CV}	SDO – AsymKey (Pub)	Uso: Always	Chiave pubblica del certificato di root per l'External Authentication (può essere usata solo durante la sequenza di Device Authentication with privacy protection)
EF_IDServizi	EF	Lettura: Always Scrittura: Never	Numero Identificativo per i Servizi Il file è firmato in EF_SOD Formato: Plain ASCII
EF_Seriale	EF	Lettura: PIN	Numero Seriale del documento Il file è firmato in EF_SOD Formato: Plain ASCII
EF_CertCNS	EF	Lettura: PIN	Certificato di Client Authentication Il file è firmato in EF_SOD Formato: Struttura X509Certificate BER-encoded
EF_IntK$_{PUB}$	EF	Lettura: Always	Chiave pubblica di Internal Authentication per l'autenticazione client/server Il file è firmato in EF_SOD Formato: Struttura RSAPublicKey definita in

			PKCS#1 BER-encoded
EF_Servizi_IntK$_{PUB}$	EF	Lettura: Always	Chiave pubblica di Internal Authentication per i servizi Il file è firmato in EF_SOD Formato: Struttura RSAPublicKey definita in PKCS#1 BER-encoded
EF_SOD	EF	Lettura: Always	SOD per la Passive Authentication Formato: Struttura SignedData definita in PKCS#7 BER-encoded

2.2.4 Gli oggetti del file system

L'utilizzo dei servizi esposti dal DDU avviene tramite l'accesso agli oggetti contenuti nel file system; di seguito un dettaglio degli oggetti utilizzati per i servizi offerti dal DDU

- Identificazione del documento tramite Numero Identificativo per i Servizi

Il servizio di identificazione tramite Numero Identificativo per i Servizi richiede richiede la lettura dell' EF_IDServizi a lettura libera. Non è richiesta né autenticazione né secure messaging.

Nel caso sia richiesta la verifica di autenticità del documento, è necessario leggere l'EF_SOD, anch'esso a lettura libera, ed eseguire la Passive Authentication per verificare l'autenticità dell'EF_IDServizi.

E' possibile, se richiesto dall'applicazione, verificare che il documento non sia stato clonato tramite l'internal authentication con la chiave SERVIZI_INT_K$_{PUB}$.

In tal caso è richiesta la lettura del file EF_ SERVIZI_INT_K$_{PUB}$, la verifica dell'autenticità tramite passive authentication e l'esecuzione del protocollo challenge/response.

- Identificazione del titolare tramite certificato di Client Authentication

Il servizio di identificazione tramite Numero Identificativo per i Servizi richiede l'esecuzione di una Device authentication with privacy protection. Gli oggetti coinvolti sono i seguenti:

- Fase di Scambio di chiavi di Diffie Hellman:
- Lettura dell'EF_DH a lettura libera e scambio di chiavi di secure messaging tramite i parametri di dominio K_DH
- Fase di External Authentication:

- Lettura dell'EF_CVCA a lettura libera e presentazione della catena di certificati a partire dalla chiave pubblica EXT_KCV
- Fase di Internal Authentication:
- Lettura dell'EF_INT_KPUB e scambio di challenge/response tramite la chiave privata INT_KPRIV

Una volta terminato il Device authentication with privacy protection i comandi successivi sono sempre inviati in secure messaging con le chiavi scambiate durante la fase di Scambio di chiavi di Diffie Hellman.

Il terminale effettua la verifica del PIN utente, legge gli EF_Seriale e EF_CertCNS e utilizza la chiave privata CNS_K_{PRIV} per effettuare l'autenticazione SSL.

Anche in questo caso può essere effettuata la verifica di autenticità, leggendo l'EF_SOD e verificando l'autenticità di:

- EF_DH
- EF_Seriale
- EF_IDServizi
- EF_INT_K_{PUB}
- EF_CertCNS

2.3 Procedure

2.3.1 Mutua autenticazione

Il servizio di autenticazione tramite il certificato di Client Authentication esposto dal DDU richiede una particolare attenzione al controllo all'accesso ai dati personali del titolare e alla chiave privata corrispondente al certificato SSL.

I requisiti di sicurezza del DDU, infatti, impongono che i dati che transitano fra il terminale e il chip siano protetti da eventuali attaccanti in ascolto sul canale di trasmissione, oltre che da attacchi di tipo Man-In-The-Middle, in cui l'attaccante si pone come tramite fra i due endpoint.

La procedura di mutua autenticazione ha lo scopo di stabilire un canale di comunicazione sicuro fra gli endpoint, tramite la negoziazione di una chiave simmetrica di secure messaging e l'autenticazione delle due entità coinvolte.

L'autenticazione degli endpoint avviene tramite un protocollo di challenge/response basato su chiavi asimmetriche. In linea di principio, affinché tali chiavi siano affidabili deve esistere una PKI che emetta dei certificati che assicurino la credibilità delle chiavi; nel DDU, tuttavia, questo vincolo viene rilassato per non avere l'onere di gestire la distribuzione dei certificati sui terminali che intendono utilizzare il servizio di identificazione tramite tramite certificato di Client Authentication. Come verrà esposto in seguito, il livello di sicurezza ottenuto rimane adeguato ai requisiti applicativi.

La procedura di mutual authentication consta di tre fasi:

- Scambio di chiavi di secure messaging tramite algoritmo Diffie Hellman
- External authentication del terminale
- Internal authentication del chip

2.3.1.1 Scambio di chiavi Diffie Hellman

La prima fase del protocollo di mutua autenticazione richiede la negoziazione di chiavi simmetriche che verranno usate per proteggere tutte le comuncazioni successive (sia le altre fasi del protocollo di mutua autenticazione che le operazioni sugli altri oggetti).

L'algoritmo di Diffie Hellman richiede che gli attori condividano dei parametri di dominio pubblici, e che ognuno di essi generi una coppia di chiavi pubblica/privata basata su tali parametri di dominio.

Il primo step, quindi, consiste nella lettura da parte del terminale di tali parametri di dominio. Queste informazioni si trovano nel file a lettura libera EF_DH, presente nel Master File.

Il terminale genera una coppia di chiavi sulla base dei parametri di dominio e trasmette la propria chiave pubblica al chip. Il chip a sua volta genera una coppia di chiavi e trasmette la propria chiave pubblica al terminale.

A questo punto entrambi gli endpoint possono calcolare il token di autenticazione, usando la proprio chiave privata e la chiave pubblica dell'altra parte, e derivare la stessa chiave di sessione.

	Terminale	DDU

1	• Lettura file *EF_DH* (**READ BINARY**)
	  ○ g (generatore)
	  ○ p (numero primo)
	  ○ q (ordine del gruppo)	

2	• Generazione di PrK.IFD (random) • Calcolo di PuK.IFD: PuK.IFD = $g^{PrK.IFD}$ mod p	
3	• Selezione dei parametri di dominio (*K_DH*) e invio di PuK.IFD al chip (**MSE Set KAT**)	
4		• Generazione di PrK.ICC (random) • Calcolo di PuK.ICC: PuK.ICC = $g^{PrK.ICC}$ mod p
5	• Lettura di PuK.ICC (**GET DATA K.ICC**)	

6	• Calcolo del token: ZZ = PuK.ICC * PrK.IFD = $PuK.ICC^{PrK.IFD}$ mod p	• Calcolo del token: ZZ = PuK.IFD * PrK.ICC = $PuK.IFD^{PrK.ICC}$ mod p

A partire dal token ZZ gli endpoint calcolano la chiave di sessione 3DES.

Lo scambio di chiavi di Diffie Hellman è resistente ad attachi di eavesdropping, poichè sul canale passano in chiaro esclusivamente le chiavi pubbliche, mentre le chiavi private sono necessarie per portare a termine lo scambio di chiavi.

E' tuttavia soggetto ad attacchi MITM, poichè né il terminale né il chip sono in grado di verificare l'identità dell'altra parte. Gli step successivi risolvono questo problema.

2.3.1.2 External authentication

Nella fase di External authentication il terminale deve autenticarsi verso il chip dimostrando di possedere una coppia di chiavi pubblica/privata considerata affidabile. A questo scopo, il terminale deve presentare al chip una catena di certificati in cui la chiave pubblica del certificato di root corrisponde a quella memorizzata nel chip nel BSO EXT_K_{CV}.

Tuttavia, come anticipato precedentemente, non è prevista una infrastruttura PKI per la generazione di tali certificati, a causa degli alti oneri di gestione e per l'eccessiva complessità nella distribuzione di certificati e chiavi ai terminali che utilizzano il DDU.

La chiave pubblica contenuta in EXT_K_{CV} e la relativa chiave privata (PuK.CV e PrK.CV) sono rese pubbliche e note al terminale, che quindi è in grado di generare una coppia di chiavi (PuK.TS e PrK.TS) e un certificato (Cert.TS, firmato con PrK.CV) riconosciuto come credibile dal chip. La chiave privata PrK.TS viene utilizzata per ultimare il protocollo challenge/response e completare l'External authentication.

L'utilizzo di un certificato così generato **non** innalza in alcun modo il livello di sicurezza ottenuto. Qualsiasi attaccante, infatti, sarebbe in grado di generare tale certificato. L'autenticazione del terminale verrà demandata in fase successiva alla verifica del PIN utente.

Lo step di External authentication è necessario la specifica IAS, ma nel contesto del DDU non ha rilevanza dal punto di vista della sicurezza.

Di seguito il dettaglio delle operazioni:

	Terminale	DDU
1	• Selezione chiave pubblica EXT_K_{CV} contenente PuK.CV (**MSE SET CRT DST**)	
2	• Invio certificato Cert.TS (**PSO - VERIFY**	• Verifica validità del certificato in

	CERTIFICATE)	tramite la chiave pubblica PuK.CV
3	• Selezione chiave pubblica PuK.TS (**MSE SET AT**)	
4	• Richiesta del challenge (**GET CHALLENGE**)	• Generazione Random RND.ICC
5	• Calcolo della Response: Resp = ENC(PrK.TS, 6A | PRND | h (PRND | PuK.IFD | SN.IFD | RND.ICC | PuK.ICC | g | p | q) | BC)	
6	• Invio al chip di SN.IFD | Resp (**EXTERNAL AUTHENTICATE)**	• Verifica della firma e di RND.ICC, SN.IFD, PuK.ICC, PuK.IFD, g, p, q

2.3.1.3 Internal authentication

Nella fase di Internal authentication il chip deve autenticarsi verso il terminale, dimostrando di possedere la chiave privata corrispondente ad una chiave pubblica (PrK.INT, PuK.INT) ritenuta affidabile dal terminale stesso.

Il terminale legge la chiave pubblica PuK.INT dal file *EF_IntK*$_{PUB}$, e ne verifica l'affidabilità tramite il SOD.

Una volta effettuata la verifica, avviene un protocollo challenge/response in cui il chip firma un challenge ottenuto dal terminale tramite PrK.INT.

Di seguito il dettaglio delle operazioni:

	Terminale	DDU
1	• Lettura chiave pubblica PuK.INT dal file *EF_IntK*$_{PUB}$	
2	• Selezione chiave privata *INT_K*$_{PRIV}$ contenente PrK.INT (**MSE SET AT**)	
3	• Generazione Challenge RND.IFD	
4	• Invio del Challenge al chip (**INTERNAL AUTHENTICATE**)	• Calcolo della Response: Resp = ENC(PrK.TS, 6A | PRND | h (PRND | PuK.ICC | SN.ICC | RND.IFD | PuK.IFD | g | p | q) | BC)
5	• Verifica della firma e di RND.IFD, SN.ICC, PuK.IFD, PuK.ICC, g, p, q	

Il terminale deve verificare la correttezza delle quantità firmate nella response per assicurarsi che non sia in atto un attacco di Man In The Middle; in questo caso, infatti, l'attaccante dovrebbe sostituire al PuK.ICC ritornato dal chip quello usato per istaurare la connessione con il terminale e firmare nuovamente il challenge. Tuttavia, non possedendo una chiave privata affidabile la cui componente pubblica è firmata nel SOD, non è in grado di restituire la quantità corretta al terminale.

Una volta effettuata la mutua autenticazione il terminale può verificare il PIN utente, che assicura l'identità dell'utente/terminale al chip; solo a questo punto è possibile avere accesso ai dati personali contenuti nel certificato e alla chiave privata di autenticazione in rete.

2.3.2 Passive Authentication

Per assicurare il terminale che i dati contenuti nel documento sono originali e non falsificati, è previsto un meccanismo di Passive authentication analogo a quello utilizzato in ICAO.

Il file system del DDU prevede il file *EF_SOD*, la cui struttura è quella di un PKCS#7 contenente, nei SignedData, un elenco dei digest dei file contenuti nel DDU stesso.

Il contenuto di tali file è quindi protetto da alterazioni e certificato da parte del DocumentSigner (la PKI dedicata a tale scopo contenuta nell'infrastruttura di emissione del DDU e gestita dal Ministero dell'Interno).

I file firmati nel SOD sono i seguenti:

- EF_DH
- EF_Seriale
- EF_IDServizi
- EF_INT_K_{PUB}
- EF_SERVIZI_INT_K_{PUB}
- EF_CertCNS

Il terminale deve:

- Leggere il contenuto del file *EF_SOD*
- Verificare la firma del PKCS#7
- Verificare l'attendibilità del certificato del Document Signer
- Effettuare, se richiesto, la mutua autenticazione col chip
- Verificare la validità dei digest dei file coinvolti nel servizio in uso da parte del terminale, cioè:
  - identificazione del documento tramite il Numero Identificativo per i Servizi : EF_IDServizi e, se richiesta la verifica della clonazione, EF_SERVIZI_INT_K_{PUB}
  - identificazione del titolare tramite certificato di autenticazione client : EF_DH, EF_Seriale, EF_INT_K_{PUB}, EF_CertCNS

Sezione II – Specifiche del chip contact

1 L'applicazione CNS

L'applicazione CNS presente nel chip a contatto del DDU è conforme alle specifiche CNS v1.1.6 [26].

Le uniche variazioni a tale specifica sono volte ad assicurare l'interoperabilità dei comandi per la generazione della Firma Elettronica Avanzata con chiavi a 2048 bit.

Tali modifiche sono riassunte nei paragrafi seguenti.

1.1 Autenticazione CNS e Firma digitale con chiavi RSA a 2048 bit

1.1.1 Premessa

Considerata la durata decennale del Documento unificato e allo scopo di evitare processi di rinnovo della coppia di chiavi di autenticazione, durante il periodo di validità, è stato deciso di adottare chiavi RSA a 2048 bit.

Chiavi di questa lunghezza saranno adottate sia per i processi di autenticazione sia per la creazione della firma digitale.

L'analisi dei Sistemi Operativi delle smart card, sino ad ora utilizzate per produrre la CNS, ha evidenziato una serie di differenze nella gestione della crittografia RSA a 2048 bit..

Lo scopo di questo breve documento è quello di individuare delle soluzioni che consentano di garantire l'interoperabilità della componente CNS, presente nel chip a contatti del Documento Unificato, senza peraltro imporre vincoli ai sistemi operativi delle carte relativamente alla crittografia RSA a 2048 bit.

I requisiti che il sistema operativo del chip a contatti deve possedere sono:

1. Utilizzo della chiave di autenticazione in formato RSA a 2048 bit;
2. Certificazione di sicurezza per la firma digitale di chiavi RSA a 2048 bit;
3. Installazione ed utilizzo dei servizi aggiuntivi creati dalle Regioni secondo le specifiche attuali della CNS.

Quanto precedentemente esposto vale per la componente a contatti del Documento Unificato che sarà mantenuta per un periodo della sua emissione. Passato tale periodo, che sarà determinato in seguito, il Documento Unificato avrà soltanto il chip contact-less.

1.1.2 Autenticazione – interoperabilità tra le carte

In base all'analisi della documentazione delle smart card e ai risultati di alcuni test si può sostenere che l'interoperabilità tra le carte può essere ragionevolmente ottenuta "annegando" nelle librerie crittografiche

(PKCS#11 e CSP) le differenze tra i comandi applicativi (APDU) se ci si limita alla sola fase di utilizzo della carta e quindi dopo la sua emissione. In questo caso non è necessario considerare le specificità dei comandi APDU del tipo PUT_DATA_OCI e GENERATE KEY PAIR implementati dai vari Sistemi Operativi.

A sostegno di questa tesi si rammenta che le raccomandazioni CEN/TC 224 "European Citizen Card Interoperability using an application interface", mutuate dalla normativa ISO 24727, prevedono la presenza di uno strato software GCAL che converte sequenze di comandi APDU generalizzati in comandi APDU specifici per la singola ICC, secondo il contenuto del descrittore CCD (Card Capability Description).

Da un'analisi approfondita della normativa inerente la European Citizen Card è emerso che le CEN/TS 15480-2 e le specifiche IAS ECC definiscono i "Card Identification Data Object", codificati in TAG, length, value, e che il TAG '47' identifica il "Card Capability Data Object". Si è pertanto deciso di prevedere nel File System, a livello di root, il file elementare "Card Capabilities" che dovrà essere inizializzato in fase di emissione con i "Card Identification Data Object" specifici del fornitore della smart card. La tabella che segue definisce il contenuto del file "Card Capabilities".

TAG	LENGHT	Type	Value	Meaning
'80'	**N.A.**	**Category indicator**	**'00'**	**Indicate format of next historical bytes (compact TLV)**
'43'	**'01'**	**Card service data tag**		**Tag for next byte**
		Card service data byte	'81' '80'	b8=1: Application selection by full DF name b7..b2= 000000 (RFU) b1 = 0: Card with MF b1 = 1: Card without MF
'46'	**'04'**	**Pre-issuing DO**		**Tag for next 4 bytes**
		IC Manufacturer	'XX'	IC Manufacturer according ISO/IEC 7816-6
		Type of the IC	'XX'	defined by the IC or card manufacturer
		OS Version	'XX'	Version of the operating system defined by card manufacturer
		Discretionary data	'XY'	DDU version Encoded as follows: X encodes the major version over the 4 most significant bits

				Y encodes the minor version over the least significant bits Then V1.0.0 = ‘10’
‘47’	**‘0A’**	**Card capabilities tag**		**Tag for next 10 bytes**
		Card capabilities data byte 1 *Selection method*	’90’	**DF selection** b8=1: DF selection full name b5=1: DF selection using file identifier **EF selection** b3=0: file selection using short file identifier is NOTsupported
		Card capabilities data byte 2 *Data coding byte*	‘01’	b4...b1 = 0001: data unit size is 1 byte
		Card capabilities data byte 3 Miscellaneous	‘C0’, ‘80’, ‘D0’, ‘90’, ‘40’, ‘00’, ‘50’, ‘10’	b8=1: command chaining is supported b8=0: command chaining is NOT supported b7=0: Extended Lc and Le fields NOT supported b7=1: Extended Lc and Le fields supported b5, b4=00 : no logical channel supported b5, b4=10 : channel number assignment by the card Maximum number of channels supported :4
		Card capabilities data byte 4 Secure messaging TLV coding		b8 = 1 Secure Messaging TLV coding is BER-TLV b7 = 1 Secure Messaging TLV coding is Compact-TLV

‘E0’	’36’	Miscellaneous	‘XX…XX’	12 concatenated data objects with tag ‘02’ (Universal class). ‘02’ L .xx .xx. = DO maximum length of **command** APDU **without** secure messaging ‘02’ L .xx .xx. = DO maximum length of **command** APDU **with** secure messaging ‘02’ L .xx .xx. = DO maximum length of **response** APDU **without** secure messaging ‘02’ L .xx .xx. = DO maximum length of **response** APDU **with** secure messaging. ‘02’ L .xx .xx. = FID of Elementary file used for reading/writing data, used by APDU command, that exceeds 256 bytes **without** secure messaging. Such Elementary File is used only by cards without extended length or command chaining capabilities.If such feature is not implemented then FID is 0000. ‘02’ L .xx .xx. = FID of Elementary file used for reading/writing data, used by APDU command, that exceeds 256 bytes **with** secure messaging. Such Elementary File is used only by cards without extended length or command chaining capabilities. If such feature is not implemented then FID is 0000. ‘02’ L .xx .xx.xx. = Class, Option and Algorithm byte for RSA2 EXP-ENCRYPT/DECRYPT 02’ L .xx .xx.xx. = Class, Option and Algorithm byte for RSA2 MOD-ENCRYPT/DECRYPT 02’ L .xx .xx.xx. = Class, Option and Algorithm byte for RSA2 EXP-SIGN 02’ L .xx .xx.xx. = Class, Option and Algorithm byte for

				RSA2 MOD-SIGN 02' L .xx .xx.xx. = Class, Option and Algorithm byte for RSA2 EXP-EXTERNAL_AUTH 02' L .xx .xx.xx. = Class, Option and Algorithm byte for RSA2 MOD-EXTERNAL_AUTH
'82'	**'02'**	**Status indicator**		**Tag for next 2 bytes**
	Status Word	'9000'	SW1+ SW2	

L'interoperabilità tra le carte, nel processo di autenticazione, sarà ottenuta a livello di **libreria crittografica** che, leggendo il **contenuto** del file "*Card Capabilities*", sarà in grado di sottomettere alla smartcard i comandi applicativi di Autenticazione compatibili con il sistema operativo della carta. Con questa soluzione non è necessario riconoscere la carta tramite il messaggio ATR.

Si osserva che il contenuto del file elementare "*Card Capabilities*", non si limita a all'autenticazione ma normalizza tutti gli aspetti inerenti la crittografia a RSA a 2048 bit.

La libreria di autenticazione specifica per ogni ambiente operativo (MS Windows, Linux e MAC-OS), sarà esposta sul sito di AgID e liberamente scaricabile dai cittadini.

1.1.3 Utilizzo della carta tramite i comandi APDU

Si fa notare l'impossibilità di poter modificare l'attuale documento che descrive la struttura dei comandi APDU della CNS (CNS – Carta Nazionale dei Servizi Functional Specification) a causa delle differenze che esistono tra le diverse implementazioni dei comandi relativi all'utilizzo delle chiavi RSA a 2048 bit.

In assenza di tale uniformità si **sconsiglia** l'utilizzo della chiave privata del certificato di autenticazione tramite i comandi APDU.

Qualora una Pubblica Amministrazione intendesse comunque realizzare un processo di Strong Authentication, per esempio in modalità Challenge/Response (CH/R), utilizzando la chiave privata direttamente tramite comandi APDU, è necessario che venga riconosciuto il chip tramite l'analisi dell'ATR. In questo modo è possibile identificare il fornitore e la versione di sistema operativo e selezionare il comando opportuno. A questo proposito dovranno essere resi pubblici i comandi APDU a 2048 bit di ciascun fornitore necessari a realizzare i processi di autenticazione.

Richiesto un parere alle Regioni sull'effettiva necessità di utilizzare la chiave di autenticazione direttamente tramite comandi APDU, si è riscontrato solo in un progetto, ancora in fase di

realizzazione, che coinvolgerebbe un potenziale di circa 2500 utenti, che utilizza il comando PSO DEC con la chiave privata di autenticazione.

Per il resto, sia i dati personali del titolare che il suo certificato di autenticazione possono continuare ad essere utilizzati senza nessun accorgimento aggiuntivo.

1.1.4 Firma digitale

Rispetto a quanto visto a proposito dell'autenticazione, un modulo software in grado di consentire l'interoperabilità tra le carte, nel caso sia presente la firma digitale, è di difficile realizzazione anche se si considera solamente la fase di utilizzo della smart card per apporre la firma, in quanto le librerie crittografiche attuano la comunicazione con la carta in modalità "secure messaging" e quindi custodiscono apposite chiavi crittografiche specifiche di ogni fornitore. Tale comportamento è reso necessario dal profilo di certificazione di sicurezza richiesto per i dispositivi di creazione della firma digitale. In particolare, per soddisfare il profilo di certificazione di sicurezza, le chiavi RSA dedicate alla firma digitale vengono create con un attributo che le vincola a questo preciso scopo e vengono inviati, in "secure messaging", i seguenti comandi: "VERIFY PIN" e "PSO CDS".

Dato il numero limitato di utenti che necessitano di firma digitale rispetto alla totalità dei cittadini e la loro specificità (p.e. dipendenti della PA), sono vantaggiose tecniche di wrapping di librerie ed è quindi fondamentale che la libreria fornita dal produttore del chip abbia **nome** e procedura d'installazione diversi da quelli che ufficialmente distribuisce in proprio. Ciò al fine di evitare, dopo la fase di upgrade della libreria, la sovrascrittura degli oggetti sulla la stazione di lavoro utilizzata e rischiare di renderla inoperabile per le funzionalità d'utilizzo del certificato d'autenticazione e/o firma digitale. Il wrapper sarà fornito contestualmente alla gara di selezione dei fornitori.

Le librerie crittografiche PKCS#11 saranno fornite per gli ambienti MS Windows, Linux e MAC-OS. Per l'ambiente MS Windows sarà fornita anche le libreria CSP.

Le librerie crittografiche, oltre a consentire l'apposizione della firma digitale dovranno anche consentire i processi di autenticazione previsti dalla Carta Nazionale dei Servizi.

1.1.5 Requisiti minimi del modulo software di tipo PKCS#11

Il modulo software, rilasciato dal singolo fornitore, deve implementare tutte le funzioni definite nello standard PKCS#11 ed in particolare quelle in grado di effettuare le seguenti operazioni:

- Generazione coppia di chiavi RSA sia a 1024 che 2048 bit (C_generateKeyPair)
- Importazione del certificato (C_CreateObject)
- Firma (C_SignInit, C_SignUpdate e C_SignFinal)
- Decifratura (C_DecryptInit, C_DecryptUpdate e C_DecryptFinal)

L'oggetto chiave privata di autenticazione così come il certificato d'autenticazione a cui si riferisce devono essere referenziati tramite l'attributo CKA_ID valorizzato a "CNS0" (o anche "CIE0").

L'oggetto chiave privata di firma digitale così come il certificato di firma a cui si riferisce devono essere referenziati tramite l'attributo CKA_ID valorizzato a "DS0".
Se è possibile creare più coppie di chiavi di firma digitale allora i valori dell'attributo CKA_ID che assumerà la seconda chiave ed il relativo certificato sarà "DS1" e così via per le successive chiavi di firma digitale.

1.1.6 Ulteriori requisiti

La libreria crittografica per la firma digitale deve gestire anche la chiave privata di autenticazione ed il relativo certificato e deve prevedere la funzionalità di sincronizzazione del PIN di sblocco della chiave di firma digitale con il PIN di sblocco della chiave di autenticazione.

2 Profilo dei certificati

2.1 Servizi della pubblica amministrazione

Le pubbliche amministrazione, in specie regionali, da tempo forniscono sul territorio servizi in rete. Detti servizi sono acceduti con le modalità di autenticazione client/server basate sull'utilizzo del certificato di autenticazione che richiede l'inserimento del PIN da parte del cittadino. Tali servizi continueranno ad essere fruibili attraverso il certificato di autenticazione presente sia sul chip a contatti che sul chip contactless.

Altra rilevante tipologia di servizi è riconducibile a servizi sul territorio, volti all'accesso dei cittadini autorizzati attraverso la libera lettura del certificato di autenticazione presente sulle carte a contatto (vedi par. per esempi di servizi senza autenticazione).

In considerazione che in linea teorica dati non protetti presenti sul chip contactless sono leggibili anche ad una certa distanza, sebbene illegalmente, al fine di proteggere i dati personali del cittadino contenuti nel certificato di autenticazione la lettura di quest'ultimo è soggetto alla protezione attraverso il PIN.

Questa misura a protezione dei dati personali implica l'impossibilità di continuare a fornire servizi che prevedono un semplice controllo accessi (ad es. l'accesso alle discariche). Al fine di ovviare a tale inconveniente, si introduce un numero univoco, denominato "**numero identificativo per i servizi**", accessibile liberamente sul chip contactless e riportato all'interno del certificato di autenticazione. Tale "numero identificativo per i servizi" non è un numero parlante (come il codice fiscale) ed è assegnato con un algoritmo di generazione numerica casuale.

Il Ministero dell'Interno rende disponibile alle pubbliche amministrazioni interessate, un servizio applicativo su SPC che ricevendo il "numero identificativo per i servizi" risponde con il codice fiscale corrispondente, a condizione che il DDU cui afferisce non sia scaduto o revocato.

Al fine di rendere fruibili i varchi di accesso non connessi alla rete, tale servizio consente anche l'interrogazione opposta: dato il codice fiscale restituisce il "*numero identificativo per i servizi*".

In questo modo le pubbliche amministrazioni potranno continuare a fornire i servizi attuali senza alcun disagio per i cittadini.

2.2 Certificato di autenticazione del DDU

Il profilo del certificato di autenticazione è basato sugli standard IETF RFC 3739 [8] e RFC 5280 [7], ETSI TS 102280 e ETSI EN 319412-2.

Per la sottoscrizione dei certificati di autenticazione è utilizzato l'algoritmo definito nella norma ISO/IEC 10118-3:2004: *dedicated hash-function* 4, corrispondente alla funzione SHA-256.

La valorizzazione di ulteriori elementi nel certificato, non prevista dalle presenti specifiche, *DEVE* essere eseguita in conformità allo RFC 5280 [7], previa autorizzazione del comitato tecnico di cui all'art. 8 del DM[11].

2.2.1 Informazioni contenute nel certificato

	Campo	Valore contenuto	Codifica
	version	"2" *per indicare il V3*	Integer
	serialNumber	*numero seriale univoco nella CA*	Integer
	signature	*sha256WithRSAEncryption (1.2.840.113549.1.1.11)*	
	validity	*"notBefore" e "notAfter"*	UTCTime
estensioni	*subjectKeyIdentifier(2.5.29.14)*	*"keyIdentifier"*	Octet string
	auhotityKeyIdentifier (2.5.29.35)	*"keyIdentifier"*	Octet string
	keyUsage (2.5.29.15)	digitalsignature	Bit string
	extKeyUsage (2.5.29.37)	id-kp-clientAuth (id-kp 2)	Bit string
	certificatePolicies (2.5.29.32)	1. *policyIdentifier* l'object identifier (OID) della Certificate Policy 2. CPS Pointer Qualifier	IA5String
	crlDistributionaPoints (2.5.29.31)	*distributionPoint*	Octet string
	authorityInfoAccess (1.3.6.1.5.5.7.1.1)	*accessMethod + accessLocation*	Octet string
issuer	*organizationName*	Valori corrispondenti del campo *subject* del certificato di certificazione	UTF8String
	organizationalUnitName		UTF8String
	commonName		UTF8String
	countryname		PrintableString
subject	*serialNumber*	Vedi par. 5.3	PrintableString
	surname		UTF8String
	givenname		UTF8String
	commonName		UTF8String
	countryname		PrintableString

Il contenuto del campo "validity" è codificato in UTCTime se contiene date fino all'anno 2049, in GeneralizedTime se contiene una data successiva (dall'anno 2050 in poi). Il campo riporta il periodo di validità del documento.
I certificati sono codificati in DER.

L'unica estensione marcata critica è il *keyUsage* (Object ID: 2.5.29.15).

2.2.2 Informazioni contenute nelle estensioni

L'estensione *subjectKeyIdentifier(2.5.29.14)* contiene il *keyIdentifier* composto, conformemente al RFC 5280 [7], dai 160-bit prodotti dall'applicazione dell'algoritmo di hash SHA-1 sul valore bit string del *subjectPublicKey* (esclusi tag, lunghezza, e numero di bit inutilizzati).

L'estensione *auhotityKeyIdentifier (2.5.29.35)* contiene il *keyIdentifier* con il medesimo valore contenuto nel *keyIdentifier* del *subjectKeyIdentifier* presente nel certificato di certificazione contenente la chiave pubblica utile per la verifica del certificato di autenticazione.

L'estensione *keyUsage* (Object ID: 2.5.29.15) che *DEVE* avere attivato il bit digitalSignature (bit 0) ed è l'unica estensione che *DEVE* essere marcata critica. L'estensione, conformemente al profilo di tipo C dello standard ETSI TS 102280, non deve contenere altri bit attivi corrispondenti ad altri key usage.

L'estensione e*xtKeyUsage* (Object ID: 2.5.29.37), che *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), *NON DEVE* essere marcata critica. L'estensione, conformemente a quanto indicato in RFC 5280 [7], non deve contenere altri valori che indicano altri scopi.

L'estensione *certificatePolicies (2.5.29.32)* DEVE contenere le *PolicyInformation* costituite da un *policyIdentifier* e un *policyQualifiers*.

Il *policyIdentifier* contiene quale *CertPolicyId* l'object identifier "1.3.X.X.X" della Certificate Policy (CP).

Il *policyQualifiers* contiene il *PolicyQualifierID* costituito da *id-qt-cps* e *id-qt-unotice*.

L'*id-qt-cps* è costituito dal *CPS pointer qualifier* (1.3.6.1.5.5.7.2.1) con valorizzata l'URI (IA5String) che punta al Certificate Practice Statement (CPS) nel rispetto del quale è stato emesso il certificato, redatto in lingua italiana e inglese.

L'*id-qt-unotice* contiene uno *UserNotice (2.5.29.49)* contenente un *explicitText* codificato UTF8String.

L'*explicitText* contiene il seguente testo: "Identifies X.509 authentication certificates issued by the Ministry of Interior for the Italian electronic identification card project in accordance with the national regulation.".

L'estensione *crlDistributionPoints (2.5.29.31)* DEVE contenere l'*uniformResourceIdentifier* (URI) del *distribution Point.* Il protocollo utilizzato è HTTP. L'URI punta ad una sola CRL codificata DER in conformità con la RFC2585.

L'estensione *authorityInfoAccess (1.3.6.1.5.5.7.1.1)* DEVE contenere almeno un *AccessDescription* contenente l'indicazione dell'*accessMethod* OID id-ad-ocsp (1.3.6.1.5.5.7.48.1) e la *accessLocation* l'URI dell'OCSP responder. L'accesso all'OCSP Responder deve essere libero ed accettare richieste non firmate e non vincolate da autenticazione.

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 [5]. Detto RFC è stato reso obsoleto e sostituito dal RFC 6960 [6] nel giugno 2013. In considerazione che gran parte dei prodotti disponibili ancora non gestiscono le

modifiche introdotte dal nuovo RFC, in prima istanza, si garantisce la conformità con il precedente, in seguito sarà resa nota la data dalla quale le nuove funzioni saranno disponibili.

Nel caso siano valorizzati più di un AccessDescription per l'estensione, tali indicazioni debbono configurare diversi percorsi alternativi per ottenere lo stesso risultato.

2.2.3 Informazioni contenute nel campo subject

Le informazioni relative al titolare del certificato *DEVONO* essere inserite nel campo Subject (Subject DN).

Conformemente alle specifiche tecniche ETSI EN 319412-2 il campo ***Subject*** contiene i seguenti attributi:

1. *serialNumber*(Object ID: 2.5.4.5), valorizzato con il seguente valore:
   a) i tre caratteri iniziali "**IDC**"
   b) la codifica del codice nazione ISO 3166 "IT"
   c) il carattere separatore "-" (codifica ASCII 0x2D, UTF-8 U+002D)
   d) il numero del documento (corrisponde a quanto riportato nella Zona 2 della carta)

   Esempio: **IDCIT-***12345678901*

2. *surname (Object ID: 2.5.4.42):* contenente il cognome del titolare
3. *givenname(Object ID: 2.5.4.4):* contenente il nome del titolare
4. *commonName (Object ID: 2.5.4.3):* contenente il codice fiscale seguito dal numero identificativo per i servizi. Il codice fiscale e il numero identificativo per i servizi sono separati dal carattere "/" (slash, ASCII 0x2F)
5. *countryName (2.5.4.6):* contiene il codice ISO 3166 della nazione di cittadinanza del titolare (corrisponde a quanto riportato nella Zona 2 sul fronte della carta)

2.2.4 Informazioni contenute nel campo issuer

Il campo issuer contiene i medesimi valori contenuti nel campo *subject* del corrispondente certificato di certificazione.

La codifica utilizzata DEVE essere la stessa utilizzata nel certificato di certificazione.

2.2.5 Esempi servizi senza autenticazione

Si citano, a titolo di esempio, alcuni servizi attualmente in uso in Regione Lombardia e che si basano essenzialmente sulla lettura delle informazioni contenute nel file EF-Dati personali o del numero seriale della CNS. In generale l'accesso a questi servizi è effettuato tramite postazioni o terminali POS messi a disposizione degli utenti dall'erogatore del servizio.

Questa tipologia di servizi ben si presta all'erogazione in modalità contact less in quanto i terminali POS, in ottemperanza alle direttive SEPA, adotteranno a breve l'interfaccia contact less e, per quanto riguarda postazioni basate su personal computer, la connessione di un semplice lettore c-less non costituisce un particolare problema.

Carta Sconto benzina

Questo servizio si basa sull'accesso ad una Base Dati regionale contenente i codici fiscali/targhe automobilistiche degli aventi diritto allo sconto sui carburanti. La Base Dati è precostituita in funzione delle informazioni possedute da Regione Lombardia. Ai cittadini è richiesto di presentarsi presso apposite sedi solamente nel caso si debba associare più codici fiscali alla medesima targa.

In sintesi il servizio opera nel modo seguente:

- Presso le stazioni di servizio del territorio in cui è concesso lo sconto è installato un terminale POS connesso al servizio centralizzato gestito da Regione Lombardia;
- Il cittadino introduce la propria TS-CNS e digita il codice PIN; se la verifica del PIN ha esito positivo viene letto il codice fiscale ed inviato al servizio Carta Sconto Benzina;
- Se il codice fiscale è presente nella base dati del servizio e se non è stata raggiunta la soglia di carburante prevista è concesso lo sconto.

Progetto Nuova Celiachia

Si ritiene interessante illustrare in sintesi il "progetto celiachia" in quanto si presta ad essere erogato tramite DDU a causa dei requisiti di privacy che prevedano l'anonimato dell'utenza e quindi impediscono la propagazione di dati anagrafici.

Questo progetto ha la finalità di consentire diffusione più capillare dei prodotti per celiaci e piena apertura al libero mercato grazie al coinvolgimento della Grande Distribuzione Organizzata (GDO) e la completa dematerializzazione del processo di gestione.

L'erogazione del servizio è condizionata da un codice personale di riconoscimento rilasciato al cittadino dall'ASL di pertinenza.

Il cittadino, con la propria TS-CNS ed il codice personale fornito dalle ASL con il nuovo applicativo informatico, può recarsi a fare la spesa, in un supermercato della GDO, e "**pagare" i prodotti per celiaci alla cassa con la TS-CNS**. In cassa viene verificata la compatibilità del valore dell'acquisto con il budget a disposizione tramite collegamento diretto con il sistema centrale, effettuato attraverso la rete di processor bancari. Superati i controlli, viene contestualmente decurtato l'importo dal budget.

Ulteriore specificità del sistema è quella di verificare in tempo reale l'identità del cittadino senza alcuno scambio di dati sensibili in rete (lettura del solo numero seriale della CNS) e verificare la presenza dell'esenzione attraverso la consultazione dell'anagrafe regionale centrale. Il codice personale, digitato sul terminale POS e trasmesso congiuntamente al seriale della CNS, ha lo scopo

di dimostrare che la transazione è attivata dall'utente beneficiario dell'esenzione. In questo modo il nuovo sistema, permette alle Asl di **disporre in tempo reale della situazione esatta della spesa** riferita a ciascun assistito.

Per poter erogare tramite DDU questo servizio è necessario creare la corrispondenza tra *quantità* e dati anagrafici. I nuovi aventi diritto possono essere censiti presso gli sportelli delle ASL mentre per i cittadini già censiti nel servizio può essere utilizzata una delle modalità descritte nel paragrafo che segue.

Dote Scuola

Il funzionamento è analogo a quello dei servizi analizzati precedentemente. I codici fiscali degli aventi diritto sono contenuti in una base dati regionale precostituita ed abbinati ai relativi seriali CNS. Il servizio è erogato presso le cartolerie e le librerie del territorio regionale.

Tramite il terminale POS o il Personal Computer dell'esercente viene letto il numero seriale, presente nella CNS del cittadino, e viene quindi trasmesso alla base dati regionale per determinare il diritto al buono scuola.

Cassette H_2O

Servizio rilasciato da alcuni comuni che distribuiscono acqua microfiltrata, refrigerata e in alcuni casi gassata tramite appositi erogatori (Cassette H_2O).

Le informazioni sugli aventi diritto, i cittadini residenti nel comune che eroga il servizio, sono contenute in una base dati precostituita con le informazioni detenute dal Comune.

L'accesso alla cassetta è tramite lettura del codice fiscale del cittadino, contenuto nella CNS, e si verificano il diritto ed il limite di prelievo.

Accesso alle isole ecologiche

L'accesso a queste aree avviene tramite la lettura del codice fiscale, presente sulla CNS, che è verificato nella base dati degli aventi diritto.

La base dati è costruita con le informazioni possedute dal comune.

Riferimenti

[1] RFC 3494, “Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status”, IETF, March 2003.

[2] RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”, IETF, March 1997.

[3] RFC 2246, “The Transport Layer Security (TLS) Protocol Version 1.1”, IETF, April 2006.

[4] RFC 4516, “Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator”, IETF, June 2006.

[5] RFC 2560, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”, IETF, June 1999

[6] RFC 6960, “X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP”, IETF, June 2013.

[7] RFC 5280, “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile”, IETF, May 2008.

[8] RFC 3739, “Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”, IETF, March 2004

[9] Decreto XXXXXX.

[10] DDU: il documento digitale unificato e la carta di identità elettronica di cui al decreto[9]

[11] DM: il Decreto interministeriale XXXXXXX recante “Modalità tecniche di emissione della Carta d’identità elettronica e del Documento digitale unificato nonché definizione del piano per il graduale rilascio, in attuazione dell’art. 10, commi 2 e 3, del decreto-legge 13 maggio 2011, n. 70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106, e successive modificazioni”

[12] ICAO 9303 - Machine Readable Travel Documents, Doc 9303, Part 3, sesta edizione.

[13] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards .

[14] ISO/IEC 7816-4:2005, Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange.

[15] ISO/IEC 7816-8:2004, Identifications cards – Integrated circuit cards – Part 8: Commands for security operations.

[16] ICAO Technical Report – Supplemental Access Control for Machine Travel Documents 2010.

[17] ICAO Technical Report – Development of a logical data structure -LDS for optional capacity expansion technologies. Rev. 1.7.

[18] BSI:TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Part 1, Part 3, Version 2.10, 2012.

[19] Supplement TO ICAO 9303 – Release 11 , November 17, 2011.

[20] Decisione della Commissione C (2009) 3770 del 20.5.2009.

[21] Decisione della Commissione C (2011) 5478 del 4.8.2011.

[22] ICAO Technical Report – Development of a logical data structure -LDS for optional capacity expansion technologies. Rev. 1.7.ICAO NTWG, RF Protocol and Application Test Standard for E-Passport; Parts 2&3.

[23] BSI, AFNOR, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC) - Tests for Security Implementation, 2007.
[24] ICAO NTWG, RF Protocol and Application Test Standard for E-Passport; Part2&3
[25] ISO/IEC 10373-6: Identification cards -- Test methods -- Part 6: Proximity cards.

[26] CNS – Carta Nazionale dei Servizi - Functional Specification - v1.1.6 del 2/04/2011

[27] IAS ECC - Identification Authentication Signature. Technical Specifications Revision: 1.0.1