Carta d’Identità Elettronica
CIE 3.0 – Specifiche Chip

Document History

Versione	Data	Modifica
1.0	19/11/2015	

Sommario

1 Definizioni ed acronimi

BAC	Basic Access Control
Certificato di autenticazione Certificato di client authentication	Certificato utilizzato per verificare l'identità di un soggetto durante il processo di autenticazione
Certificato di certificazione	Certificato utilizzato per verificare i certificati di autenticazione
CIE	Carta d' Identità Elettronica
CIE3	La Carta d'Identità Elettronica descritta in queste specifiche
ICAO	International Civil Aviation Organization
MRTD	Machine Readable Travel Document
NFC	Near Field Communication
PKI	Public Key Infrastructure, infrastruttura a chiave pubblica. L'insieme delle risorse necessarie alla creazione ed alla verifica dei certificati digitali

2 Funzionalità del chip

Il chip presente sulla CIE3 svolge due funzioni:

- dispositivo di verifica dell' **identità personale**, in linea con i più moderni documenti elettronici europei ed internazionali
- strumento di accesso ai **servizi online**, come richiesto dal Codice dell'Amministrazione Digitale

Le due funzioni vengono implementate da due distinte applicazioni presenti sul chip:

- Applicazione MRTD per la verifica dell'identità personale
- Applicazione IAS ECC per l'accesso ai servizi

Le applicazioni vengono definite in dettaglio nel seguito del documento.

I dati di un'applicazione non sono accessibili dall'altra applicazione. Il sistema operativo della carta deve garantire la separazione dei dati delle due applicazioni.

3 Protocolli di comunicazione

Il chip comunica esclusivamente mediante un'interfaccia contactless, conforme alle ISO 14443 [10].

Per tutte le applicazioni la CIE3 utilizza i bit rate 106, 212, 424, 848 bps.

La CIE3 è compatibile con gli standard NFC applicabili.

4 Interoperabilità

La CIE30 può essere utilizzata con lettori compatibili con ISO 14443 Type A e Type B e con gli smartphone che implementano l'interfaccia NFC.

5 Applicazione MRTD per la verifica dell'identità personale

L'applicazione MRTD consente la verifica dell'identità personale in conformità con quanto previsto per il passaporto elettronico ed il permesso di soggiorno elettronico. Si applicano quindi le stesse specifiche tecniche internazionali.

L'applicazione prevede quindi la memorizzazione sul chip dei dati personali, della fotografia e delle impronte digitali, opportunamente protette. Nel seguito si specificano i meccanismi di sicurezza, gli algoritmi e alcuni requisiti che le specifiche internazionali lasciano alla decisione dei singoli stati ed alle singole implementazioni.

5.1 Meccanismi di sicurezza

La CIE3 supporta i meccanismi di sicurezza BAC e Passive Authentication in accordo alle specifiche ICAO Doc 9303, Machine Readable Travel Documents - Part 3 [9] e report supplementari.

La CIE3 supporta il meccanismo di sicurezza PACE v2 in accordo alle specifiche ICAO Technical Report – Supplemental Access Control for Machine Readable Travel Documents, 2010 [13] e successive versioni.

La CIE3 supporta il meccanismo di sicurezza EAC in accordo alle specifiche Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 e Part 3 v2.10 [15].

5.2 Algoritmi per il protocollo BAC

L'unico algoritmo per la derivazione delle chiavi di Secure Messaging è l'algoritmo di cifratura simmetrica 3DES a 112 bit con funzione di hashing SHA-1 secondo quanto riportato nel documento [9].

5.3 Algoritmi per il protocollo PACE

Possono essere utilizzati i seguenti algoritmi:

Algoritmi di cifratura simmetrica

1. Algoritmo di cifratura simmetrica AES a 192 oppure 256 bit con funzione di hashing SHA-256;
2. Algoritmo di cifratura simmetrica 3DES a 112 bit con funzione di hashing SHA-1.

Algoritmi di condivisione di chiave

1. Algoritmo di condivisione chiavi Diffie Helmann (DH) con dimensione dei parametri di dominio della chiave di almeno 2048-bit;
2. Algoritmo di protocollo di condivisione chiavi ECDH con dimensione dei parametri di dominio della chiave di almeno 192-bit .

Algoritmi di mapping

La CIE3 utilizza il Generic Mapping dei parametri di dominio.

5.4 Algoritmi per il protocollo EAC – Chip Authentication

Secondo quanto previsto nel documento [15], possono essere utilizzati i seguenti algoritmi:

Algoritmi di cifratura simmetrica

1 Algoritmo di cifratura simmetrica AES a 192 o 256 bit con funzione di hash SHA-256;
2 Algoritmo di cifratura simmetrica 3DES a 112 bit con funzione di hash SHA-1.

Algoritmi di condivisione di chiave

1 Algoritmo di protocollo di condivisione chiavi Diffie Helmann (DH) con dimensione dei parametri di dominio della chiave di almeno 2048-bit;
2. Algoritmo di protocollo di condivisione chiavi ECDH con dimensione dei parametri di dominio della chiave di almeno 192-bit.

5.5 Algoritmi per il protocollo EAC – Terminal Authentication

Secondo quanto previsto nel documento [15], possono essere utilizzati i seguenti algoritmi:

1 Algoritmo di crittografia asimmetrica RSA-v1_5-SHA-256 con dimensione di chiave supportata di almeno 2048 bit;
2 Algoritmo di crittografia asimmetrica RSASSA-PSS SHA-256 con dimensione di chiave supportata di almeno 2048 bit;
3 Algoritmo di crittografia asimmetrica ECDSA-SHA-256 con dimensione di chiave supportata di almeno 192 bit.

Nel caso si utilizzi il protocollo PACE, durante la fase di Terminal Authentication la CIE3 utilizza il “dynamic binding”, come definito in [15].

5.6 Altri requisiti

Identificativo Unico Randomico: la CIE3 presenta un identificativo unico (UID o PUPI) randomico, come raccomandato nel documento Supplement to Doc 9303[16].

Comandi di Chip Authentication: la CIE3 prevede 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 [15]. Entrambi i comandi devono essere supportati.

Trust Point: la CIE3 permette la memorizzazione e l'aggiornamento di almeno 2 Trust Point interni in accordo alle specifiche [15].

6 Applicazione IAS per l'accesso ai servizi

6.1 Introduzione

L'accesso ai servizi viene implementato da un'applicazione i cui comandi sono conformi alle specifiche IAS ECC [23]. I protocolli applicativi sono stati adattati all'uso su un'interfaccia contactless.

6.2 Requisiti

La CIE3 tiene conto dei requisiti applicativi definiti dal "Tavolo di lavoro per l'attuazione delle norme in materia di identità digitale", definito con il DM del Ministero dell'interno del 25/3/2013:

1. il livello di protezione dei dati presenti nell'applicazione IAS deve essere almeno uguale a quello dei rispettivi dati nell'applicazione ICAO;
2. deve essere presente un Numero Identificativo per i Servizi, univoco del documento, non corrispondente col seriale, a lettura libera (ID Servizi), per una rapida identificazione del documento;
3. la comunicazione di tutti i dati personali, nonché del PIN e del PUK deve avvenire tramite un canale sicuro cifrato;
4. i dati personali sono contenuti tutti all'interno del certificato di autenticazione. Non è più usato il file dei dati personali;
5. non è prevista l'installazione di servizi aggiuntivi come definiti per le precedenti CIE a contatti. I servizi aggiuntivi si basano esclusivamente sulla lettura del Numero Identificativo per i Servizi e sul certificato di autenticazione;
6. i dati biometrici (foto e impronte digitali) sono presenti solo nell'applicazione ICAO;
7. non deve essere necessaria una PKI di Terminal Authentication.

6.3 Servizi di autenticazione disponibili

In linea con i requisiti su esposti, si distinguono due servizi di autenticazione che vengono resi disponibili dalla CIE3 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 documento (nome, cognome, codice fiscale)
- Non prevede la cifratura dei dati sul canale di comunicazione

Ovviamente, sulla base di tali caratteristiche, questo servizio può essere utilizzato esclusivamente da applicazioni che richiedono un livello di sicurezza estremamente basso, e quando sistemi più sicuri sarebbero economicamente non giustificati o non applicabili. Inoltre, non essendo comunicato alcun dato personale del titolare, e non venendo richiesto un PIN, l'utilizzo del Numero Identificativo per i Servizi identifica solo il documento, non il titolare.

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) e asimmetrici (RSA)
- Richiede l'esplicito consenso del titolare tramite immissione di un PIN
- Prevede la comunicazione di dati personali del titolare della CIE3 (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 o deve consentire la connessione con un sistema dotato di capacità crittografiche.

6.4 Implementazione

I requisiti espressi vengono mappati su un'applicazione IAS come illustrato in tabella:

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.ID_Servizi, 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 di un file con i dati personali, ma solo del certificato di autenticazione
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 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 alla CIE3.

Lo scambio di chiavi Diffie Hellman non richiede alcuna autenticazione preventiva; può essere eseguito da 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.

6.5 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.

La CIE3 implementa l'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 simile alla Terminal Authentication dell'applicazione ICAO, richiede che tali certificati CV siano emessi da una PKI e distribuiti ai terminali che intendono accedere alla CIE3 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 la CIE3 come mezzo di autenticazione degli utenti.

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 è stato stabilito che il livello di autenticazione richiesto dalle parti è il PIN (per il terminale/utente) e l'internal authentication (per il documento); questo per evitare l'infrastruttura PKI necessaria per gestire le coppie di chiavi dei terminali, ritenuta onerosa sia in termini di gestione che di distribuzione.

Si generano quindi 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.

6.6 Protezione dalla clonazione

La protezione dalla clonazione può avvenire con un sistema analogo alla Chip Authentication dell'applicazione MRTD: 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; nella CIE3 l'EF.SOD contiene:

- EF.DH
- EF.Seriale
- EF.ID_Servizi
- EF.INT.K_{PUB}

- EF.Servizi_INT.K_{PUB}
- EF.Cert_CIE

6.7 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 CIE3 offrono varie modalità di protezione, che assicurano diversi 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 ai due livelli diversi di sicurezza associati ai servizi di identificazione:

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

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 realizzabile l'implementazione di sistemi di controllo complessi;
- il codice univocamente legato alla carta è sempre leggibile senza alcun prerequisito. 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.

6.8 Il file system

Il file system della CIE3 è organizzato su due DF (DF.ICAO e DF.CIE), contenenti i dati necessari per le applicazioni MRTD e IAS. Sotto l'MF si trovano quindi tali DF più gli EF previsti dalle specifiche ICAO e IAS (EF.DH, EF.ATR, EF.SN.ICC).

Gli oggetti presenti nel file system, al di fuori di quelli previsti dall'applicazione MRTD, sono descritti nella "Tabella File System" nell'allegato A.

6.9 Gli oggetti del file system

L'utilizzo dei servizi esposti dalla CIE3 avviene tramite l'accesso agli oggetti contenuti nel file system; di seguito un dettaglio degli oggetti utilizzati per i servizi offerti dalla CIE3.

Identificazione del documento tramite Numero Identificativo per i Servizi

Il servizio di identificazione tramite Numero Identificativo per i Servizi richiede la lettura dell' EF.ID_Servizi 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.ID_Servizi.

E' possibile, se richiesto dall'applicazione, verificare che il documento non sia stato clonato tramite l'internal authentication con la chiave SERVIZI_INT.K_{PRIV}.

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 certificato di Client Authentication 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:
  Presentazione della catena di certificati a partire dalla chiave pubblica ExtCV.K_{pub}
- Fase di Internal Authentication:
  Lettura dell'EF.INT.K_{pub} 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.Cert_CIE e utilizza la chiave privata CIE_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.ID_Servizi
- EF.INT.K_{PUB}
- EF.Cert_CIE

6.10 Procedure

6.10.1 Mutua autenticazione

Il servizio di autenticazione tramite il certificato di Client Authentication esposto dalla CIE3 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 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; nella CIE3 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 certificato di Client Authentication. 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

6.10.2 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 comunicazioni 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	CIE3

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 attacchi di eavesdropping, poiché 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, poiché né il terminale né il chip sono in grado di verificare l'identità dell'altra parte. Gli step successivi risolvono questo problema.

6.10.3 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 *ExtCV_*K_{PUB}.

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 documento.

La chiave pubblica contenuta in *ExtCV.*K_{PUB} 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 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 per la specifica IAS, ma nel contesto della CIE3 non ha rilevanza dal punto di vista della sicurezza.

Di seguito il dettaglio delle operazioni:

	Terminale	CIE3
1	• Selezione chiave pubblica *ExtCV_*K_{PUB} contenente PuK.CV (**MSE SET CRT DST**)	
2	• Invio certificato Cert.TS (**PSO – VERIFY CERTIFICATE)**	• Verifica validità del certificato in 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

6.10.4 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 (INT.PrK, INT.PuK) ritenuta affidabile dal terminale stesso.

Il terminale legge la chiave pubblica INT.PuK dal file *EF.Int.*K_{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 INT.PrK.

Di seguito il dettaglio delle operazioni:

	Terminale	CIE3
1	• Lettura chiave pubblica INT.PuK dal file *EF.Int.K_{PUB}*	
2	• Selezione chiave privata *INT.K_{PRIV}* contenente INT.PrK (**MSE SET AT**)	
3	• Generazione Challenge RND.IFD	
4	• Invio del Challenge al chip (**INTERNAL AUTHENTICATE**)	• Calcolo della Response: Resp = ENC(INT.PrK, 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.

6.10.5 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 nell'applicazione MRTD.

Il file system della CIE3 prevede il file *EF.SOD*, la cui struttura è quella di un PKCS#7 contenente, nei SignedData, un elenco dei digest dei file contenuti nella CIE3 stessa.

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 della CIE3 e gestita dal Ministero dell'Interno).

I file firmati nel SOD sono i seguenti:

- EF.DH
- EF.Seriale
- EF.ID_Servizi
- EF.INT.K_{PUB}
- EF.SERVIZI_INT.K_{PUB}
- EF.CertCIE

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.ID_Servizi 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.Cert_CIE

6.11 Utilizzo del Numero Identificativo per i Servizi

In considerazione che in linea teorica dati non protetti presenti sul chip contactless sono leggibili illegalmente anche ad una certa distanza, 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 una verifica rapida senza inserimento del PIN. 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 ed è assegnato con un algoritmo di generazione numerica casuale.

Deve essere reso 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 la CIE3 cui afferisce non sia scaduta o revocata. Al fine di rendere fruibili i servizi non connessi alla rete, tale servizio consente anche l'interrogazione opposta: dato il codice fiscale restituisce il "*numero identificativo per i servizi*".

6.12 Certificato di autenticazione della CIE3

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].

6.12.1 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
	authorityKeyIdentifier (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. 6.12.3	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).

6.12.2 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 *authorityKeyIdentifier (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 definito nella Certificate Policy (CP) e registrato a cura del Ministero dell'Interno.

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: "X.509 authentication certificate issued by the Italian Ministry of Interior for the Electronic Identity Card".

L'estensione *crlDistributionPoints (2.5.29.31)* DEVE contenere l'*uniformResourceIdentifie*r (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.

6.12.3 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)

6.12.4 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.

7 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] ICAO 9303, Part 3, Vol. 2

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

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

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

[13] Technical Report – Supplemental Access Control for Machine Travel Documents 2010

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

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

[16] Supplement to ICAO 9303 – Release 11 , November 17, 2011

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

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

[19] 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
[20] BSI, AFNOR, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC) - Tests for Security Implementation, 2007
[21] ICAO NTWG, RF Protocol and Application Test Standard for E-Passport; Part2&3
[22] ISO/IEC 10373-6: Identification cards - Test methods - Part 6: Proximity cards
[23] GIXEL - IAS ECC - Identification Authentication Signature. Technical Specifications Revision: 1.0.1

8 Allegato A: Tabella File System

Nota: l'AID (Application IDentifier) del DF CIE deve essere registrato a cura del Ministero dell'Interno.

Applica -zione	Oggetto	ID	Condizioni d'accesso	Protezione	Commenti	SDO DCOP	SDO DOUP
MF		DFID=3F00	Delete	NEVER			
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Create EF	NEVER			
ROOT	EF.DH	EFID=D004 SFI=1B	Delete	NEVER	DH parameters Encoding: BER-Encoded ASN1 DomainParameter structure		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	ALWAYS			
	EF.ATR	EFID=2F01 SFI=1D	Delete	NEVER	IAS EF.ATR File		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	ALWAYS			
	EF.SN.ICC	EFID=D003	Delete	NEVER	Card Serial number		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	ALWAYS			

Applica-zione	Oggetto	ID	Condizioni d'accesso	Protezione	Commenti	SDO DCOP	SDO DOUP
DF		DFID= AID=	Delete	NEVER			
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Create EF	NEVER			
DF_CIE	EF.ID_Servizi	EFID=1001 SFI=01	Delete	NEVER	Card Identifier for low-security services (PAN number in EF.SN.ICC)		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	ALWAYS			
	EF.Seriale	EFID=1002 SFI=02	Delete	NEVER	CIE Card serial number		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	SM and PIN (SE PIN)			
	EF.Cert_CIE	EFID=1003 SFI=03	Delete	NEVER	CIE auth Certificate Encoding: BER-encoded X509 certificate structure		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	SM and PIN (SE PIN)			
	EF.Int.Kpub	EFID=1004 SFI=04	Delete	NEVER	Public Key for Internal auth in Device auth with Privacy Protection Encoding: BER-encoded RSAPublicKey structure defined in PKCS#1		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	ALWAYS			

Applica-zione	Oggetto	ID	Condizioni d'accesso	Protezione	Commenti	SDO DCOP	SDO DOUP
DF_CIE	EF.Servizi_Int.Kpub	EFID=1005 SFI=05	Delete	NEVER	Public Key for anti-cloning Internal auth protection Encoding: BER-encoded RSAPublicKey structure defined in PKCS#1		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	ALWAYS			
	EF.SOD	EFID=1006 SFI=06	Delete	NEVER	SOD for Passive auth Encoding: BER-encoded SignedData structure defined in PKCS#7		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	ALWAYS			
	EF.CIE.Kpub	EFID=1007 SFI=07	Delete	NEVER	Public Key for CIE auth Certificate Encoding: BER-encoded RSAPublicKey structure defined in PKCS#1 Only present if the key is generated onboard		
			Terminate	NEVER			
			Activate	NEVER			
			Deactivate	NEVER			
			Update Binary	NEVER			
			Read Binary	SM and PIN (SE PIN)			
	SDO ExtCV.Kpub	SDO ID=BFA004	Verify Certificate	ALWAYS	Public CV Key for External auth in Device auth with Privacy Protecion	(84h) Data Object Name = "ExtAu.PuK" (80h) Object len = 256 (0x0100)	(80h) Algorithm = 41h (5F20h) CHR = 00h 00h 00h 00h 'ITCIE' 10h 01h 15h (5F4Ch) CHA=6MSB of AID || 00h
			External Authenticate	NEVER			
			Generate Key	NEVER			
			Put Data	NEVER			
			Get Data	ALWAYS			
	SDO Servizi_Int.Kpriv	SDO ID=BF9003	Compute Digital Signature	NEVER	Private Key for anti-cloning Internal auth protection	(84h) Data Object Name= "SrvInt.PrK" (9Eh) Non-repudiation flag = 0 (80h) Object len = 256 (0x0100)	(80h) Algorithm = 02h
			Internal Authenticate	ALWAYS			
			Decipher	NEVER			
			Generate Key	NEVER			
			Put Data	NEVER			
			Get Data	NEVER			

Applica-zione	Oggetto	ID	Condizioni d'accesso	Protezione	Commenti	SDO DCOP	SDO DOUP
DF_CIE	SDO PIN	SDO ID=BF8101	Change Reference Data	SM and PIN (SE PIN)	User PIN	(84h) Data Object Name= "PIN" (9Ah) Maximum number of tries = 3 (80h) Object len = 8 (0x0008)	(80h) maximum size = 8 (81h) minimum size = 8
			Verify	SM and Ext Auth (SE DAPP)			
			Reset Retry Counter	SM and PIN (SE PUK)			
			Put Data	NEVER			
			Get Data	SM and Ext Auth (SE DAPP)			
	SDO PUK	SDO ID=BF8102	Change Reference Data	NEVER	User PUK	(84h) Data Object Name= "PUK" (9Ah) Maximum number of tries = 10 (80h) Object len = 8 (0x0008)	((80h) maximum size = 8 (81h) minimum size = 8
			Verify	SM and Ext Auth (SE DAPP)			
			Reset Retry Counter	NEVER			
			Put Data	NEVER			
			Get Data	SM and Ext Auth (SE DAPP)			
	SDO Cert_CIE.Kpriv	SDO ID=BF9001	Compute Digital Signature	NEVER	Private Key of CIE auth Certificate	(84h) Data Object Name= "CIE.PrK" (9Eh) Non-repudiation flag = 0 (80h) Object len = 256 (0x0100)	(80h) Algorithm = 02h
			Internal Authenticate	SM and PIN (SE PIN)			
			Decipher	NEVER			
			Generate Key	NEVER			
			Put Data	NEVER			
			Get Data	NEVER			
	SDO Int.Kpriv	SDO ID=BF9002	Compute Digital Signature	NEVER	Private Key for Internal auth in Device auth with Privacy Protection	(84h) Data Object Name= "IntAu.PrK" (9Eh) Non-repudiation flag = 0 (80h) Object len = 256 (0x0100)	(80h) Algorithm = 9Bh
			Internal Authenticate	ALWAYS			
			Decipher	NEVER			
			Generate Key	NEVER			
			Put Data	NEVER			
			Get Data	NEVER			
	SDO K_DH	SDO ID=BFA101	Put Data	NEVER	DH Private Key	(84h) Data Object Name= "DH.PrK" (80h) Object len = 256 (0x0100)	(80h) Algorithm = 9Bh
			Get Data	ALWAYS			

Applica-zione	Oggetto	ID	Condizioni d'accesso	Protezione	Commenti	SDO DCOP	SDO DOUP
DF_CIE	SE KEY	SDO ID=BFFB01	MSE Restore	NEVER	Default Security Environment - Cert_CIE.Kpriv	(84h) Data Object Name= "SE.Sign" (80h) Object len = 1	(A4h) AT (80h) Algorithm = 2 (84h) PrK ref = 81h (local PrK 1)
			Get Data	ALWAYS			
	SE PIN	SDO ID=BFFB02	MSE Restore	NEVER	SSE Security Environment - PIN verified	(84h) Data Object Name= "SE.PIN" (80h) Object len = 3	(A4h) AT (80h) Algorithm = 0 (83h) PIN ref = 81h (local PIN 1) (95h) UQB = 8 (User auth) (B8h) CT (80h) Algorithm = 9Bh (84h) PrK ref = 82h (local PrK 2) (95h) UQB = 30h (Sec. Mess.) (B4h) CCT (80h) Algorithm = 9Bh (84h) PrK ref = 82h (local PrK 2) (95h) UQB = 30h (Sec. Mess.)
			Get Data	NEVER			
	SE PUK	SDO ID=BFFB03	MSE Restore	NEVER	SSE Security Environment - PUK verified	(84h) Data Object Name= "SE.PUK"	(A4h) AT (80h) Algorithm = 0 (83h) PIN ref = 82h ((local PIN 2) (95h) UQB = 08h (User auth) (B8h) CT (80h) Algorithm = 9Bh (84h) PrK ref = 82h (local PrK 2) (95h) UQB = 30h (Sec. Mess.) (B4h) CCT (80h) Algorithm = 9Bh (84h) PrK ref = 82h (local PrK 2) (95h) UQB = 30h (Sec. Mess.)
			Get Data	NEVER			
	SE DAPP	SDO ID=BFFB04	MSE Restore	NEVER	SSE Security Environment - Device auth with Privacy Protection protocol performed	(84h) Data Object Name= "SE.DAPP"	(A4h) AT (80h) Algorithm = 9Bh (84h) PrK ref = 82h (local PrK 2) (95h) UQB = 40h (Internal auth) (B8h) CT (80h) Algorithm = 9Bh (84h) PrK ref = 82h (local PrK 2) (95h) UQB = 30h (Sec. Mess.) (B4h) CCT (80h) Algorithm = 9Bh (84h) PrK ref = 82h (local PrK 2) (95h) UQB = 30h (Sec. Mess.)
			Get Data	NEVER			