Requisiti SPID per identificazione digitale basata su Remote Secure Element

SOMMARIO

Document Control

Date	Note	Version	Authors
18/02/2015	Draft	1.0	Mauro Antonelli Enrico Pavoni
04/03/2015	Draft	1.1	Mauro Antonelli Enrico Pavoni
20/05/2015	Draft	1.2	Mauro Antonelli Enrico Pavoni

Scopo

Lo scopo del documento è definire i requisiti di certificazione dell'architettura implementata da un Gestore d'Identità SPID per soddisfare i requisiti del terzo livello (LoA4) in assenza di un Secure Element hardware. Non è oggetto del presente documento definire le procedure di identificazione richieste per il rilascio delle credenziali SPID o per il rilascio di credenziali preesistenti da cui ottenere credenziali SPID.
Il documento è da intendersi come BOZZA di discussione, non vincolante.

Definizioni

Utente: entità utilizzatrice del servizio di autenticazione SPID basato su Secure Element Remoto
Dispositivo Mobile: dispositivo mobile (ad esempio Smartphone) in grado di scaricare e installare un'applicazione da uno Store standard specifico per la piattaforma, come ad esempio Google Play.
Applicazione Mobile (AM): applicazione installata sul Dispositivo Mobile dell'Utente in grado di supportare l'autenticazione dello stesso verso il suo gestore di identità digitale SPID.
Sistema Gestione Credenziali (SGC): Componente server che ha responsabilità di gestire il ciclo di vita dell'Applicazione Mobile e di validare i crittogrammi generati dall'AM durante il processo di identificazione dell'Utente

Riferimenti esterni

Di seguito è riportata una lista di riferimenti a documenti esterni citati nel presente documento.

Identificativo documento	Nome Documento
[OT-SPIDRSEGLO]	Glossario tecnico per SPID RSE
[OT-SPIDRSECRY]	Requisiti crittografici per la gestione di identita SPID tramite RSE

Introduzione

A differenza degli scenari in cui l'identificazione digitale è basata sulla presenza di un Secure Element hardware locale, la soluzione basata su *Secure Element Remoto* permette di utilizzare un'Applicazione Mobile eseguita su un dispositivo mobile per gestire un'identità digitale conforme con il livello di sicurezza 3 di SPID.
Poiché un dispositivo mobile non fornisce le stesse garanzie di un Secure Element hardware riguardo la memorizzazione dei dati e l'esecuzione delle applicazioni, le chiavi private utilizzate nel processo di identificazione non sono memorizzate sul dispositivo, ma sono accessibili on-line, ed è necessario soddisfare specifici requisiti nella gestione del ciclo di vita delle credenziali, secondo quanto proposto nel presente documento.

Componenti

Il modello di funzionamento basato su *Secure Element Remoto* fa leva su due entità:

- Sistema di Gestione Credenziali
- Applicazione Mobile

Il Sistema di Gestione Credenziali o SGC è il componente server responsabile per:

- il mantenimento delle chiavi asimmetriche associate alle Identità Digitali gestite,
- la gestione del ciclo di vita delle istanze di Applicazioni Mobile specifiche per ogni Identità Digitale gestita,
- la verifica, tramite tecniche crittografiche basate su cifratura simmetrica e asimmetrica dell'identità dell'Utente che ha accesso alla specifica istanza di Applicazione Mobile
- la gestione del rischio associato all'eventuale compromissione di istanze dell'Applicazione Mobile

L'Applicazione Mobile è la componente software installata sul Dispositivo Mobile dell'utente responsabile per:

- garantire all'Utente un accesso efficace alla propria Identità Digitale tramite interfaccia utente grafica e meccanismi che ne abilitano o semplificano l'utilizzo in scenari d'uso specifici.
- agire, una volta registrata e inizializzata, come fattore di identificazione dell'Utente che ne ha accesso.

Ciclo di vita dell'Applicazione Mobile

Registrazione

Validazione identità

Non è scopo di questo documento definire la procedura di validazione dell'identità dell'entità

richiedente il rilascio dell'Identità Digitale, tale procedura deve essere conforme al DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014 (SPID) ed a quanto indicato da Agid in merito all'utilizzo delle Identità Pregresse, ad esempio in merito alla possibilità di utilizzo delle disposizioni attuative di Adeguata Verifica formalizzate da Banca d'Italia in riferimento alla normativa antiriciclaggio (D.Lgs. 21 novembre 2007, n. 231).

Registrazione

L'utente effettua l'installazione dell'applicazione mobile da uno Store come ad esempio Google Play o Apple AppStore. Quando l'applicazione è avviata per la prima volta viene eseguita dall'SGC una verifica di elegibilità per valutare se l'AM ed il dispositivo mobile siano effettivamente in grado di supportare il processo di identificazione basato su Secure Element Remoto. Se la verifica va a buon fine il processo continua con l'identificazione dell'utente, tale identificazione deve essere eseguita con una procedura definita dal gestore dell'identità digitale, conforme con quanto indicato nel capitolo validazione identità. Una volta identificato l'utente verrà chiesto allo stesso di scegliere il PIN che verrà utilizzato per accedere alla propria identità tramite l'applicazione mobile[1]. Al termine di questa fase il SGC invia all'AM un codice di attivazione (AMSGC_ACTV) ed un identificativo del processo di attivazione (ATT_ID), entrambi i codici vengono memorizzati in modo trasparente per l'utente, questi codici saranno utilizzati nella fase successiva di inizializzazione per identificare il relativo processo di registrazione.

Inizializzazione

Nella fase di inizializzazione l'AM invia al SGC i codici AMSGC_ACTV e ATT_ID, utilizzando questi codici il SCG correla il processo di inizializzazione appena aperto con il processo di registrazione già eseguito.
Sia il SGC che l'AM creano un Mobile Device Fingerprint (AM_FGP). Tale fingerprint è uno dei fattori dell' Authentication Code (AMSGC_AUTH) utilizzato dall'AM nelle fasi successive di gestione per identificarsi verso il SGC.
E' inoltre necessario che l'AM si registri al sistema di Remote Notification specifico per la piattaforma, tale registrazione è obbligatoria ed è preferibile che venga eseguita in modo trasparente per l'utente, il risultato della registrazione sarà un codice (RNSAM_ID) che verrà utilizzato dal SGC nella fase di gestione per indirizzare notifiche push al Dispositivo Mobile e dunque all'Apllicazione Mobile.
In questa fase viene inoltre inizializzato dall'AM il Database Cifrato Locale (DBCRITT), ovvero lo strumento che verrà utilizzato dall'AM per memorizzare i dati sensibili ricevuti dal SGC.
La fase di inizializzazione viene chiusa da una serie di attività eseguite dal SGC:

- Consegna delle Mobile Keys (MK) all'AM, queste chiavi verranno utilizzate per gestire la

[1] Modalità alternative di identificazione sono possibili (ad es. Touch ID, utilizzato in modalità encrypt del Keychain), ma non sono dettagliate in questa versione del documento

sicurezza nelle comunicazioni trà AM e SGC nella fase di gestione. Gestire la sicurezza implica:
    - Garantire la sicurezza dei messaggi pèush inviati all'AM allo scopo di aprire una sessione di gestione
    - Garantire la sicurezza (oltre il livello SSL/TLS) del canale di comunicazione aperto a fini di gestione trà il SGC e l'AM.
- Consegna di un identificativo (AMSGC_ID) all'AM, tale identificativo è uno dei fattori che compongono il AMSGC_AUTH utilizzato dalla AM quando stabilisce una connessione all'SGC a scopo di gestione.
- Consegna della URL (URL_RM) che verrà utilizzata dalla MA per connettersi al SGC quando lo stesso SGC richiede l'apertura di una sessione di gestione tramite l'invio di notifica push.

Gestione remota

Il SGC è responsabile delle gestione remota dell'Applicazione Mobile. Il protocollo utilizzato nella comunicazione tra le due entità è definito nella tabella seguente:

Funzione	Descrizione
Provisioning (DC_CP)	Utilizzata per effettuare il provisioning dell' profilo di identità (DC_CP) verso l'Applicazione Mobile
Provisioning (DC_CHSOP)	Utilizzata per inviare all'AM almeno un set di chiavi incluse le chiavi a singolo utilizzo
Provisioning (Parameters)	invio di parametri generici all'AM
Management (Mobile Check)	Utilizzata per monitorare lo stato dell'AM, in particolare per verificare: • Informazioni circa il Dispositivo Mobile • informazioni circa l'Applicazione Mobile • Informazioni circa il profilo di identità caricato nell'AM • Informazioni sui set di chiavi associate al profilo di identità
Management (Information Delivery)	Utilizzata per inviare informazioni che devono essere mostrate all'utente
Management (Remote Wipe [DC_CHSOP])	Utilizzata per cancellare tutti i set di chiavi associati al profilo di identità (Utile in caso di cambio PIN)

Management (Remote Wipe [Digitized Identity])	Questa funzione viene utilizzata quando il profilo di identità deve essere rimosso dalla AM.
Management (Reset AM to Installed State)	questa funzione riporta lo stato dell'Applicazione Mobile come se fosse stata appena installata, tutti i dati devono essere cancellati incluso Il DBCRITT. In questo scenario l'utente per utilizzare la AM deve ri eseguire la procedura di registrazione

La fase di inizializzazione è l'unica fase del ciclo di vita dell'Applicazione Mobile in cui questa effettua proattivamente una connessione verso il Sistema di Gestione Credenziali, in tutti gli altri scenari l'applicazione stabilisce una connessione solamente quando richiesto dal Sistema di Gestione Credenziali tramite l'invio di una richiesta asincrona (push notification).
Il Sistema di Gestione Credenziali apre il canale di comunicazione verso l'Apllicazione Mobile utilizzando il sistema di push notification cui la mobile application si è registrata, indirizzandola tramite il RNSAM_ID definito in fase di inizializzazione. La richiesta inviata all'AM via push notification contiene un ID di sessione (protetto con le MK). A questo punto l'Applicazione Mobile si connette al Sistema di Gestione Credenziali (utilizzando la URL URL_RM) instaurando una connessione protetta SSL/TLS con pinning del certificato, si autentica utilizzando un codice di Autenticazione derivato dall' ID di sessione e stabilisce un ulteriore canale cifrato sopra il quello SSL/TLS utilizzando le Chiavi di Sessione Mobile (derivate dall'ID di Sessione e dalle MK). Attraverso questo canale il Sistema di Gestione Credenziali invia all'Applicazione Mobile i comandi di gestione indicati nella tabella sopra.

Utilizzo

In questa fase si considera che l'Utente abbia accesso all'AM installata su di un Dispositivo Mobile e che dunque:

- L'AM sia stata inizializzata
- L'AM contegga il profilo di identità ed almeno un set di chiavi.

Ad ogni richiesta di identificazione l'Utente deve inserire il proprio PIN (definito nella fase di registrazione) nell'interfaccia utente della Mobile Application, quest'ultima utilizzando le MK fornite dal SGC in fase di inizializzazione ed il PIN inserito, prosegue alla generazione dei crittogrammi (UTENTE_DISP e DISP) che sono inviati al SGC e dunque validati al fine di effettuare l'dentificazione dell'Utente. Tali crittogrammi identificano rispettivamente il dispositivo mobile ed il dispositivo mobile in associazione con l'utente.
La validazione dei crittogrammu UTENTE_DISP ed DISP viene sempre effettuata dal SGC, che può dunque indirizzare la gestione di:

- PIN errato in caso di UTENTE_DISP non valido e DISP valido

- Dispositivo compromesso in caso di DISP non valido
- Autenticazione corretta in caso di DISP ed UTENTE_DISP validi

Scenario online

Nello scenario online l'Utente effettua l'autenticazione utilizzando il dispositivo mobile connesso ad Internet. Questo scenario può essere articolato in uno dei seguenti modi:

- identificazione diretta da dispositivo mobile;
- identificazione tramite browser web esterno al dispositivo;
- identificazione tramite browser web esterno al dispositivo già accoppiato all'applicazione mobile.

Scenario offline

Nello scenario offline l'entià effettua l'autenticazione utilizzando il dispositivo mobile non connesso ad Internet. In questo caso il canale di comunicazione verso il SGC è instaurato dal fornitore del servizio che richiede l'identificazione tramite SPID, ad esempio in questo scenario l'entità potrebbe interagire attraverso l'utilizzo di tecnologia NFC con un dispositivo di identificazione collegato al sistema del fornitore del servizio.

Concetti chiave

Codice di attivazione

Il codice di attivazione (AMSGC_ACTV) viene generato e fornito all'Applicazione Mobile nella fase di registrazione, nella successiva fase di inizializzazione è utilizzato per identificare il processo di registrazione già eseguito.

Identificativo Applicazione Mobile

Nella fase di inizializzazione Il Sistema di Gestione Credenziali fornisce all'AM un identificativo (AMSGC_ID)

Codice di autenticazione

L'Applicazione Mobile genera un codice di autenticazione (AMSGC_AUTH) ogni volta che stabilisce una connessione con il Sistema Gestione Credenziali. Le due entità si autenticano a vicenda secondo le seguenti modalità:

- L'AM autentica il SGC a livello di comunicazione SSL/TLS, utilizzando la tecnica del Certificate Pinning
- Il SGC autentica l'AM utilizzando il codice di autenticazione fornito a livello di sessione.

Metodi di autenticazione

Il sistema di autenticazione basato su Secure Element Remoto utilizza due metodi di

autenticazione:

- UTENTE_DISP per l'autenticazione dell'Utente e del Dispositivo Mobile
- DISP per l'autenticazione del Dispositivo Mobile

Identità digitalizzata

Un Identità Digitalizzata è la combinazione del Profilo di Identità e di almeno un set di chiavi, memorizzati nel Dispositivo Mobile (area DBCRITT dell' AM) associato all'Utente titolare della stessa Identità. Un Identità Digitalizzata può essere utilizzata in scenari online (Dispositivo Mobile connesso ad Internet) ed in scenari offline (Dispositivo Mobile non connesso ad Internet), nel secondo scenario è richiesto l'utilizzo di un dispositivo di autenticazione da parte del fornitore del servizio.
Con il termine DC_CP si identifica il contenitore logico del Profilo di Identità, con il termine DC_CHSOP si identifica il contenitore logico delle chiavi simmetriche.

PIN

Il PIN scelto dall'utente in fase di registrazione è utilizzato in ogni operazione di identificazione effettuata tramite l'AM. Al momento dell'utilizzo l'Utente inserisce il PIN tramite l'interfaccia grafica dell'Applicazione Mobile che lo utilizza per la computazione di chiavi e crittogrammi. Il PIN non viene in nessun caso memorizzato dall'Applicazione Mobile.
Occorre tenere presente che:

- la validazione del PIN avviene sempre sul SGC tramite la verifica del crittogrammi UTENTE_DISP e DISP
- l'Utente viene notificato dell'errato inserimento del PIN solamente una volta terminato il processo di validazione dei crittogrammi inviati al SGC.

Chiave di sessione e Chiavi Singolo Uso

La chiave di sessione (CHSESS_xx_DISP) è generata a partire dalla Chiave Master di Identità (CH_M_ID_xx_DISP) utilizzando il CONT_OP (un contatore incrementato ad ogni utilizzo) come diversificatore.
La chiave di sessione (CHSESS_xx_UTENTE_DISP) è generata a partire dalla Chiave Master di Identità (CH_M_ID_xx_UTENTE_DISP) utilizzando il CONT_OP come diversificatore.
La Chiave Singolo Uso (CHSOP_xx_UTENTE_DISP) è ottenuta combinando il PIN con la chiave di sessione CHSESS_xx_UTENTE_DISP.
La parte xx indicata nei nomi delle chiavi va declinata in OnLine in caso di utilizzo in scenari con Dispositivo Mobile connesso ad Internet ed OffLine nello scenario di utilizzo opposto.
La Chiave Singolo Uso (CHSOP_xx_UTENTE_DISP) ottenuta come sopra puo essere combinata con il PIN per ri-ottenere la chiave di sessione CHSESS_xx_UTENTE_DISP. Le chiavi CH_M_ID_xx_yy sono chiavi asimmetriche specifiche dell'Profilo di Identità mantenute dal SGC utilizzando un HSM.
Le chiavi singolo uso sono consumate durante ogni autenticazione effettuata o tentata

dall'Utente, il DC_CHSOP è il buffer locale all'AM che contiene tali chiavi e che consente all'AM di operare anche offline fin tanto che buffer contiene ancora chiavi utilizzabili. Il SGC controlla la quantità di chiavi nel DC_CHSOP ri popolandolo ogni qual volta il numero di chiavi scende sotto la soglia definita. Tale ripopolamento è eseguito aprendo una sessione di gestione remota dell'AM.

Master Slave

Il design della soluzione basata su Secure Element Remoto utilizza un modello in cui l'Applicazione Mobile agisce come slave rispetto al Sistema Gestione Credenziali che agisce come master. E' sempre il SGC a decidere quando aprire una sessione di gestione verso una specifica AM.

Requisiti per L'applicazione Mobile

L'Applicazione Mobile deve essere protetta utilizzando tecniche di:

- string encryption
- class encryption
- asset encryption
- runtime anti tampering

L'Applicazione Mobile deve essere oggetto di assessment di sicurezza da parte di società specializzata.

DBCRITT

L'Applicazione Mobile deve memorizzare informazioni su un database locale (o meccanismo equivalente). Il modello di sicurezza proposto considera che l'AM non può proteggere i dati sensibili o le chiavi crittografiche da attacchi di tipo fisico, logico o da clonazione. L'utilizzo dell' DBCRITT è una delle contromisure inserite nell'approccio di gestione della sicurezza multi livello del sistema di identificazione basato su Secure Element Remoto.
L' DBCRITT deve garantire:

- Utilizzo di meccanismi di protezione forniti a livello OS dalla piattaforma specifica;
- Accesso da parte del'AM senza la richiesta di credenziali all'Utente;
- Accesso ai dati ristretto alle sole componenti logiche che hanno dipendenze funzionali sugli stessi;
- I dati devono essere cifrati utilizzando una chiave crittografica (ST_key) ottenuta combinando tramite hashing (SHA 256) i seguenti componenti:
    - Valore Random (DBCRITT_RND) generato dall'AM e memorizzato all'interno dello spazio di memoria proprio dell'AM ma fuori dalll DBCRITT

- Mobile Device fingerprint (DBCRITT_FGP) ovvero un insieme di dati associati al dispositivo e che non cambiano per tutto il ciclo di vita dell'AM
- Valore definito all'interno del codice dell'AM (DBCRITT_AM).

HSM Certificati

Gli HSM utilizzati a supporto della soluzione devono essere conformi agli standard di sicurezza industriale NIST FIPS 140-2 Level 3 e ISO 13491.
L'accesso agli HSM deve essere controllato tramite meccanismi in grado di garantire che solo entità autorizzate possano utilizzare gli HSM per le attività specifiche per cui sono autorizzate.
Inoltre gli HSM devono essere mantenuti in un ambiente sicuro e oggetto di controlli di accesso rigorosi in conformità con una policy di gestione HSM (ISO 11568).