Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Funzionalità fornite dall'SDK ActivIdentity

L'SDK offre funzionalità per la gestione del ciclo di vita dei dispositivi hardware (o software, come nel caso del "SoftToken") ActivIdentity per la generazione di OTP (One Time Password). Tipicamente, il ciclo di vita di un dispositivo comprende le fasi di seguito elencate.

1) Definizione delle modalità di funzionamento supportate (profilo): definizione dei parametri di configurazione che determinano le funzionalità ed il comportamento di un dispositivo OTP.

Le funzionalità includono:

- autenticazione sincrona dell'utente;
- autenticazione asincrona dell'utente;
- autenticazione asincrona del server;
- autenticazione sincrona dei dati;
- autenticazione asincrona dei dati.

I parametri di definizione del comportamento includono (ma non sono limitati a):

- richiesta del PIN all'accensione del dispositivo;
- lunghezza minima e massima del PIN;
- selezione funzionalità di default (che viene attiviata all'accensione del token);
- messaggi visualizzati dal token.

Al termine della definizione del profilo, esso deve essere compilato, ottenendo una immagine SDB (Secure Data Block) per l'inizializzazione del dispositivo.

2) Inizializzazione: trasferimento della immagine SDB sul dispositivo. L'immagine è costituita da due componenti:

- *device image*: è la parte dell'immagine che viene copiata sul dispositivo durante la sua inizialiazzazione;
- *authentication server image*: è la parte dell'immagine che il server di autenticazione utilizza per verificare la correttezza delle OTP fornite dagli utenti. Tale immagine è una copia di quanto presente sul dispositivo e permette, tramite opportune funzioni dell'SDK, di calcolare la OTP generata da quel dispositivo in un dato istante temporale.

Si noti che l'SDK copre le sole funzionalità di trasferimento della device image. La gestione della authentication server image deve essere sviluppata durante l'integrazione dell'SDK nel sistema target.

Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

3) Utilizzo del dispositivo: generazione di OTP (da parte dell'utente finale) e verifica delle stesse (da parte dell'authentication server). L'authentication server verifica la correttezza di una OTP fornita da un utente mediante funzioni dell'SDK, che ricevono in input la *authentication server image* del dispositivo associato all'utente stesso.
Si noti che l'SDK copre le sole funzionalità di verifica di una OTP data la authentication server image del dispositivo da cui è stata generata. Le componenti per la gestione del repository delle immagini e per l'identificazione dell'immagine da utilizzarsi per ogni particolare utente devono essere sviluppate in fase di integrazione.

4) Gestione delle anomalie: ripristino delle funzionalità di autenticazione OTP in seguito al verificarsi di condizioni anomale, quali

- perdita di sincronia;
- bloccaggio del dispositivo per inserimento ripetuto di PIN errati (solo per i dispositivi che ne richiedono l'utilizzo).

Si noti che l'SDK copre solo le funzionalità di basso livello per riportare la *authentication server image* in uno stato di sincronia con la corrispondente *device image*. Tutte le funzionalità e le interfacce di help desk necessarie per supportare gli utenti il cui dispositivo si trova in condizioni anomale devono essere sviluppate in fase di integrazione.

Integrazione dell'SDK

L'integrazione dell'SDK nell'ambiente target richiede attività di sviluppo per l'interfacciamento delle funzioni offerte con le applicazioni che necessitano delle funzionalità di autenticazione. La tipologia e l'impegno di risorse di tali attività può essere stimato sulla base delle seguenti considerazioni.

1) l'architettura dell'SDK assume che nell'ambiente target sia disponibile un repository per la memorizzazione degli SDB e di informazioni relative al loro stato (inclusa l'associazione agli utenti), ma non offre funzionalità per la realizzazione di un tale repository o per l'accesso a repository di terze parti (ad esempio, database relazionali). Sebbene i metodi di accesso alle principali tipologie di repository (DBMS, directory X.500) siano consolidati e standard, la loro struttura interna è fortemente legata all'organizzazione in cui sono utilizzati. La progettazione del repository per la gestione degli SDB e la logica di accesso ai dati non può quindi essere coperta dall'SDK, e viene lasciata alla fase di integrazione.

2) le funzioni dell'SDK sono concepite con lo scopo di permettere la massima flessibilità nella gestione dei dispositivi. Per tale motivo l'SDK non incapsula la complessità di

Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

funzionamento del dispositivo e ne demanda la gestione completa all'applicazione che utilizza i servizi di autenticazione. L'implementazione di una funzionalità di alto livello (ad esempio "verifica credenziali di autenticazione") comporta la sua scomposizione di basso livello (identificazione del dispositivo associato all'utente, identificazione dell'SDB corrispondente, decifratura dello stesso, calcolo della OTP, confronto della OTP) e, quindi, la necessità di implementare layer di interfacciamento per l'invocazione della corretta sequenza di funzioni dell'SDK.

3) l'utilizzo di OTP per applicazioni con numerosi utenti comporta la necessità di servizi di gestione del repository per l'inserimento la rimozione e l'assegnazione degli SDB, in corrispondenza di nuove emissioni di token o di terminazione di token danneggiati/smarriti. Gli operatori che svolgono queste operazioni devono disporre di funzionalità opportune, che devono essere implementate mediante un layer di interfacciamento per l'invocazione della corretta sequenza di funzioni dell'SDK.

4) l'utilizzo di OTP per applicazioni con numerosi utenti comporta la necessità di servizi help desk per la gestione delle condizioni anomale. Gli operatori di un tale servizio devono disporre di funzionalità di verifica dello stato di un dispositivo e di modifica dello stesso (sblocco, risincronizzazione). Queste funzionalità devono essere implementate mediante un layer di interfacciamento per l'invocazione della corretta sequenza di funzioni dell'SDK.

5) L'SDK è una libreria di funzioni C. Nessuna sua funzionalità è pertanto direttamente disponibile per un utente finale (ad esempio un operatore help desk). L'esposizione di ogni funzione richiede necessariamente lo sviluppo di un programma completo oppure di un layer di interfacciamento con gli ambienti applicativi (per utenti finali o per operatoti help desk) che devono interagire con il meccanismo di autenticazione basato su OTP.

La seguente tabella elenca le attività necessarie per l'integrazione dell'SDK nel sistema di internet banking di Banca Sella. Per ogni fase del ciclo di vita del dispositivo OTP vengono indicate le funzionalità che si dovranno implementare, sia nella fase pilota sia nel deployment in ambiente di produzione.

]HackingTeam[

Hacking Team S.r.l.
Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano
e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

	Ambiente Target	
Fase	***Pilota***	***Produzione***
Definizione profilo	Saranno utilizzati minitoken con profilo di default già compilato fornito da ActivIdentity. Nessuna attività di sviluppo necessaria	ActivIdentity fornirà a Banca Sella minitoken con profilo pre-compilato, da definirsi in base alle esigenze. Nessuna attività di sviluppo necessaria
Inizializzazione	Saranno utilizzati minitoken già inizializzati forniti da ActivIdentity. Le attività che dovranno essere svolte sono: 1) disegno delle tavole del DBMS necessarie per la memorizzazione degli SDB; 2) sviluppo di un tool a linea di comando per l'importazione da file degli SDB	ActivIdentiy fornirà a Banca Sella minitoken pre-inizializzati ed i corrispondenti SDB. Saranno sviluppate funzioni C per: 1) consentire l'utilizzo delle funzioni di importazione da console remota in modalità "user-friendly" 2) assegnare un dispositivo ad un utente 3) rimuovere un dispositivo dal repository
Utilizzo del dispositivo	Sarà sviluppata una funzione C richiamabile da una procedura PL/SQL per la verifica della correttezza di una coppia (username, OTP)	Nessuna modifica rispetto a quanto realizzato in fase pilota
Gestione delle anomalie	Sarà sviluppato un tool a linea di comando per la risincronizzazione dei dispositivi	Saranno sviluppate funzioni per l'interfacciamento con tool di help desk per: 1) ricavare SN (serial number) di un dispositivo dato il corrispondente SDB 2) ricavare tutte le informazioni di stato di un SDB 3) impostare la modalità di risincronizzazione per un SDB 4) risincronizzare in modalità manuale un dispositivo