GT 50 改善

VISIONARY INNOVATORS

Q-ID Platform

Meccanismo di autenticazione integrabile in SPID Livello 2

Q-ID™: the Platform

La piattaforma Q-ID permette l'introduzione di un sistema di autenticazione HOTP (HMAC-Based One-Time Password Algorithm - rfc 4226) e TOTP (Time-Based One-Time Password Algorithm - rfc 6238), tramite utilizzo di App su piattaforma mobile, che operano come token software.

La piattaforma comprende, oltre alle applicazioni per ambienti mobile [Q-ID App], una libreria software [Q-ID™ Controller Library] che espone una serie di interfacce per l'amministrazione e per la gestione dei vari token OTP in uso.

Essendo completamente aderente alle specifiche rfc, la libreria puo' gestire oltre ai token software, anche token hardware che rispettino completamente le specifiche indicare negli rfc sopra indicati.

I prodotti che compongono la Piattaforma, sono forniti gratuitamente:
- Q-ID App puo' essere scaricata senza vincoli, dagli opportuni store on-line;
- Q-ID™ Controller Library viene rilasciata a fronte di una registrazione;

Q-ID™: the sw Library

Q-ID™ Controller Library è quindi un Credential Service Provider per OTP, strutturato in modo da poter essere integrato in un sistema di autenticazione evoluto.

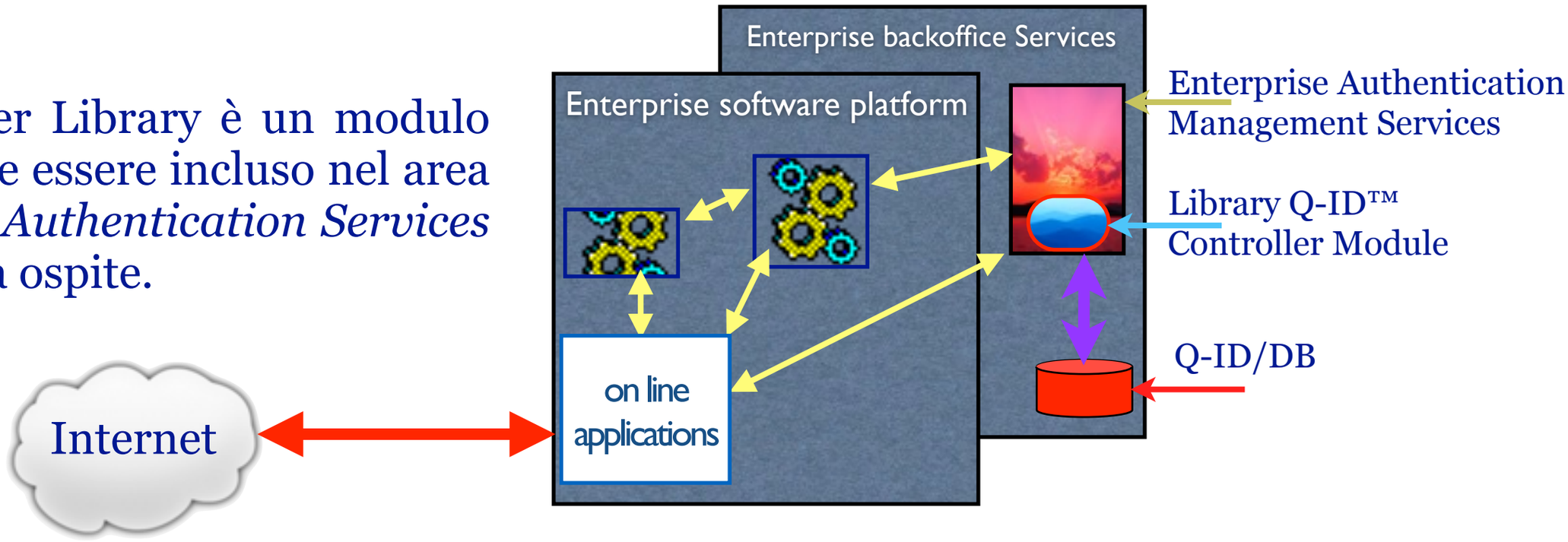
In questo contesto si vuole proporre la piattaforma Q-ID (Q-ID App e Q-ID™ Controller Library), come Meccanismo di Autenticazione Informatica a Livello 2 SPID (LoA3 dello standard ISO/IEC 29115)

Di per se la sola App Q-ID su mobile, comprende una serie di funzioni dedicate alla generazione di password sicure, di lunghezza variabile e di contenuto configurabile. Da questo punto di vista, potrebbe essere considerata un Meccanismo di Sicurezza a Livello 1 SPID (LoA2 dello standard ISO/IEC 29115)

Server Architecture

Oltre l'App Q-ID™, la piattaforma è composta di un modulo software centrale:
Q-ID™ Controller Library

Q-ID™ Controller Library è un modulo software che deve essere incluso nel area degli *Enterprise Authentication Services* della Piattaforma ospite.



Questo modulo fornisce agli sviluppatori di software dell'Azienda, tutte le funzioni (API) per gestire gli elementi di OTP, dalla fase di iscrizione (tramite *SQCode aidSystem*), alle verifiche delle OTP, agli eventi di sincronizzazione, alla gestione di licenze d'uso nel loro ciclo vitale.

Q-ID™ Controller Library: API

Admin Functions:

- ShowLibVersion
- DestroyAll
- DBCheck
- DBUpdate
- LibInit
- AddLicense
- AddLicenseUpdate
- SetupOTPParams
- SetEDesc
- Stats
- GetUsersList

Operating functions :

- GetErrorMessage
- AddUser
- ResetUser
- DelUser
- UserStatus
- GenSQA
- GenSQAU
- GenSQE
- VerOTP
- VerOTPE
- SyncOTP

All'interno della Piattaforma Q-ID, vengono implementati esclusivamente i seguenti algoritmi di sicurezza:

- AES256 (symmetric Encryption);
- SHA256 (cryptographic digest);
- RSA1024 (electronic signature);
- BCrypt (cryptographic digest);

Sono inoltre implementati gli algoritmi descritti in:

- rfc4226: HOTP: An HMAC-Based One-Time Password Algorithm
- rfc6238: TOTP: Time-Based One-Time Password Algorithm

in sviluppo:

- rfc6287: OCRA: OATH Challenge-Response Algorithm
- Electronic Signature: OTP Based

Seed Security: server side

La fase di generazione sicura dei *seed* OTP, fa parte della fase di richiesta di licenze d'uso per i Token OTP, da utilizzare nella Piattaforma Q-ID.

I seed vengono generati all'interno di dispositivi hardware certificati Common Criteria EAL4+; vengono firmati (RSA1024) e l'intero package viene codificato (AES256).
Il tutto viene consegnati nelle mani dell'Amministratore del sistema di Autenticazione: una corretta security policy, deve prevedere che la password sia fornita all'Amministratore tramite un canale alternativo.

Quando i seed vengono acquisiti da *Q-ID™ Controller Library*, vengono ulteriormente trasformati all'interno e sotto il controllo della Applicazione di Autenticazione dell'Azienda che sta utilizzando la Piattaforma Q-ID™.

In questo modo, nessuno all'esterno dell'Azienda -neppure noi che abbiamo generato i seed di base- può avere il controllo o informazioni sulle OTP in esercizio.

Nel sistema ospite, i seed delle OTP, vivono perennemente crittografati tramite AES256; la decodifica viene effettuata esclusivamente per l'elemento che in quel momento è in esercizio.
Al termine di ogni operazione, il software effettua l'azzeramento delle variabili utilizzate.

Q-ID™ Enrolment

Q-ID™ Controller Library permette di implementare la fase di Enrolment di un nuovo utente.

Anche nella fase di enrolment di un nuovo Virtual Token, l'App dell'utente non ha necessità di essere connessa da Internet.

Il messaggio contenente il seed ed i metadati necessari per la generazione del Virtual Token, sono protetti da crittografia simmetrica (AES256); questi dati possono essere acquisiti dall'App, tramite la lettura di uno speciale QrCode o tramite cut&paste di un messaggio.

L'App chiedera' all'utente la password necessaria alla decodifica.

Una corretta security policy, deve prevedere che questa password sia fornita all'utente tramite un canale alternativo.

Seed Security: App side

Oltre a sfruttare i meccanismi di sicurezza propri dell'OS della device, l'App aggiunge un suo sistema di protezione basato fondamentalmente su crittografia simmetrica (AES256)

Prima di poter essere utilizzata l'App, una volta installata, deve essere inizializzata dall'utente.

In particolare è richiesta la creazione di una MasterPassword, la cui chiave derivata serve alla protezione della password di crittografia del DB dove verranno custoditi tutti i segreti dall'utente e naturalmente i vari seed delle OTP che gli verranno assegnate.

Tramite l'interfaccia touch-screen del terminale, viene chiesto all'utente una minima operatività che serve a definire una ulteriore sorgente di dati random.

Da quel momento, tutti i dati riservati dell'utente, compresi i seed della/e OTP a lui assegnate, saranno costantemente crittografati tramite AES256; la decodifica viene effettuata esclusivamente per l'elemento che in quel momento è in esercizio.

Al termine di ogni operazione, il software effettua l'azzeramento delle variabili utilizzate.