Biometrika

PKCS#11 SDK

Soluzione Custom

Fx3000 e Smart Card come un unico token crittografico ad attivazione biometrica

La soluzione **PKCS#11** di Biometrika utilizza lo scanner Fx3000 e una Smart Card come un unico **token crittografico ad attivazione biometrica**.
La libreria PKCS#11 consente totale **interoperabilità applicativa** con minimo sforzo di sviluppo, permettendo inoltre la convivenza di token biometrici e token tradizionali.
La biometria rappresenta la soluzione naturale per tutte le problematiche che richiedono **autenticazione forte**, consentendo di creare token crittografici ad attivazione biometrica: ovvero attivabili previa autenticazione dell'utente tramite impronta digitale.
Mentre la tecnologia Match On Card non risulta ad oggi sufficientemente matura (non esistono test indipendenti sull'accuratezza di questi sistemi) la tecnologia **Match On Board** (detta anche Match On Device), come quella di Fx3000, garantisce prestazioni ad elevata affidabilità e totale sicurezza dei dati biometrici.
PKCS#11 è fortemente dipendente dal tipo di carta utilizzato, pertanto questo SDK va considerato come una soluzione da personalizzare.

Caratteristiche e Vantaggi

Semplicità d'uso

- Nessuna password da ricordare
- Possibilità di gestire password distinte per diversi applicativi
- Nessun dato memorizzato sul PC

Protezione dei dati biometrici

- Tecnonologia Smart Card e algoritmi crittografica allo stato dell'arte garantiscono la sicurezza del dato biometrico

Interoperabilità a livello applicativo

- Minimo sforzo per l'integrazione
- Possibilità di utilizzo contemporaneo di token tradizionali e token biometrici

Interfacciamento e sviluppo

- Interfaccia di programmazione standard che consente massima interoperabilità applicativa
- Compatibile con i principali linguaggi di programmazione (C, C++, VB6, VB.Net, Java,..)
- Sistemi operativi Windows 98/NT/2000/XP

PKCS#11 SDK

Fx3000 e Smart Card come un unico token crittografico ad attivazione biometrica

Problematiche dei token tradizionali

PKCS#11 è uno degli standard più diffusi per l'utilizzo delle funzionalità crittografiche dei token sicuri (Smart Card, chiavi USB ecc). Esso definisce un'interfaccia standard tramite la quale è possibile utilizzare le funzionalità crittografiche di un token.

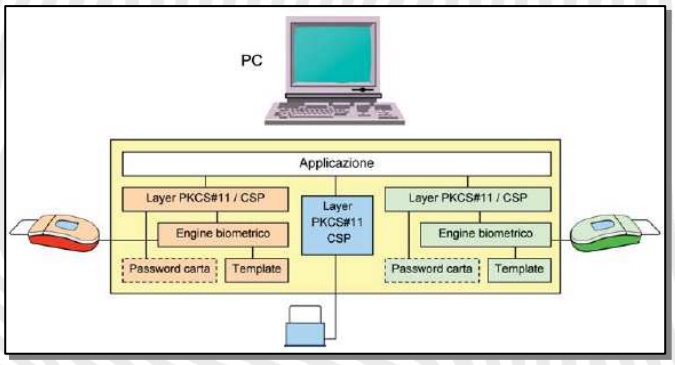
Trattandosi di token crittografici sicuri l'accesso alle funzionalità critiche è subordinato all'autenticazione dell'utente che normalmente avviene attraverso la digitazione di un PIN o di una password. Purtroppo PIN e password possono essere prestati, rubati o indovinati.

Tramite PKCS#11 è possibile utilizzare i token sicuri per tutte le applicazioni che prevedono questo tipo di interfaccia. Alcuni esempi sono: Logon, Firma digitale, Single Sign On, Autenticazione SSL ecc.

In particolare, per quanto riguarda la firma digitale, la legislazione di molti paesi (tra cui l'Italia) garantisce a questo strumento la stessa valenza legale della firma autografa, e pertanto è fondamentale implementare un meccanismo di autenticazione forte che consenta di garantire che solo e soltanto il legittimo proprietario del token lo possa effettivamente utilizzare.

PKCS#11 SDK di Biometrika

PKCS#11 SDK, proposto da Biometrika, prevede di utilizzare lo scanner Fx3000 in combinazione con una SmartCard come un unico token sicuro ad attivazione biometrica.



Il template di impronta viene memorizzato sulla smart card contenente il certificato X.509 e la relativa chiave privata. Quando l'utente deve autenticarsi, il template viene estratto dalla carta e confrontato (all'interno di Fx3000) con l'impronta dell'utente: nessuna informazione di natura biometrica viene inviata al PC. In caso di esito positivo l'utente viene autenticato ed ottiene l'accesso alle funzionalità crittografiche della carta.

Biometrika ha già efficacemente sviluppato diverse soluzioni dimostrative, ma essendo questo tipo di approccio per sua natura dipendente dal tipo di carta utilizzato, PKCS#11 SDK richiede adattamenti derivanti dallo specifico tipo di carta. Per questo motivo PKCS#11 SDK va inteso come un prodotto custom che deve essere adattato alle esigenze dell'applicazione.

Biometrika
Via Monte Santo 21, 47100 Forlì (FC) ITALY
Tel +39 0543 370680 Fax +39 0543 456198
www.biometrika.it