White Paper

Introduzione alla Strong Authetication

Data ultimo aggiornamento: 30 Agosto 2010
Codice white paper: ev 0830-10
v. 1.0

Contatto ICT System: operation@ictsystem.it

INDICE

1 PERIMETRO DI PERTINENZA DEL DOCUMENTO

Nel presente documento si introducono brevemente le soluzioni considerate da ICTsystem per le problematiche di Strong Authentication integrata a livello di:

- Autenticazione Microsoft Windows Domain;
- Autenticazione VPN;
- Autenticazione WEB / Single-Sign-On.

Le soluzioni accennate nel documento sono basate sull'utilizzo di smart-cards o tokens USB integrabili con soluzioni di Identity Management già presenti presso il cliente oppure progettate da ICTsystem.

I nostri consulenti hanno sviluppato soluzioni di controllo accessi multifunzione su clienti nel settore Finanziario ed Industriale, integrando infrastrutture di controllo accessi fisici e rilevazione presenze con le nostre soluzioni di Single-Sign-On e controllo accessi ICT.

1.1 TECNOLOGIE DI RIFERIMENTO

Le soluzioni indicate si possono realizzare su diverse tecnologie per quanto riguarda i dispositivi utilizzati dall'utente finale. Ad esempio possiamo avere Smart-Cards tradizionali in formato credit-card oppure USB Keys e possiamo avere funzioni multiple: Smart-Card, Mag-strip Badge, RFID TAG, Memory Card, One-Time-Password.

Le varie tecnologie di gestione utenti (Identity Management) supportate dai differenti dispositivi sono in linea di massima basate su Microsoft Active Directory o su una directory LDAP.

Naturalmente non tutti i dispositivi sono in grado di assumere tutte le funzioni, in particolare i dispositivi in formato credit-card, che hanno però il vantaggio di essere personalizzabili con foto e scritte relative all'utente assegnatario.

I dispositivi USB-Key sono attualmente disponibili off-the-shelf con una grande versatilità di utilizzo ma purtroppo, per via della loro dimensione, non dispongono della superficie adatta a visualizzare le informazioni Human-Readable come avviene per il formato Credit-Card.

Di seguito vengono quindi descritte le caratteristiche e le funzionalità di massima offerte da diverse soluzioni, con attenzione all'integrabilità con le applicazioni esistenti e/o di mercato.

1.1.1 Credit-Card Tokens

Il formato di questi dispositivi è quello della comune carta di credito, possono essere personalizzati con grafica e testo, tipicamente per il classico badge con foto e dati anagrafici aziendali. Esistono diversi formati, ma in genere la scelta va indirizzata tra la Smart-Card standard e la card a Magnetic-Strip, con l'opzione RFID disponibile per alcuni produttori.

I prezzi sono variabili a seconda delle funzionalità offerte, delle serigrafie richieste e dei volumi ordinati, da pochi Euro a diverse decine di Euro.

Pro:

- Ampia scelta di produttori nelle varie tipologie di dispositivo (card)
- Personalizzazione visuale per l'utilizzo come badge aziendale
- Costi ragionevoli se utilizzata solo come badge a Magnetic-Strip ed eventualmente RFID
- Aderente agli standars internazionali ed italiani per le smart-cards
- Alcuni produttori internazionali ed italiani hanno nel catalogo delle soluzioni che includono almeno due delle funzioni di autenticazione ed un software in grado di gestire il provisioning delle cards.
- Integrabile con Windows Active Directory ed altre tecnologie di Identity Management
- Integrabile con tecnologie di crittografia dei dati

Contro:

- Necessità di un lettore fisico specifico collegato sul PC/Server nel quale verrà utilizzata in funzione Smart-Card, costo da qualche Euro a qualche decina di Euro per un sistema Windows, oltre ai costi di distribuzione, installazione e test del lettore, se non incluso nell'Hardware standard del PC.
- Necessità di una infrastruttura PKI-based per l'autenticazione e la generazione dei certificati digitali

- La disponibilità di funzioni multiple non è disponibile presso molti produttori di Smart-Cards, che in genere lavorano solo in grandi volumi, mentre per i modelli Magnetic-Strip con RFID esiste una buona disponibilità anche in Italia.

- I modelli che non supportano certificati digitali non sono compatibili con le tecnologie di crittografia dei dati (prodotti di mercato, è possibile la presenza di una funzione proprietaria del singolo produttore)

1.1.2 USB Tokens

Il formato di questi dispositivi è quello di una normale USB Key, di varie dimensioni a seconda che possa o meno contenere una serigrafia piuttosto che un Tag RFID, in genere più piccola di una Internet Key attualmente ben conosciuta.

Alcuni dei principali produttori offrono in questi prodotti diverse funzionalità, dalla Smart-Card all'OTP (One-Time-Password) con diverse tecnologie

I prezzi dei singoli dispositivi variano nel campo delle decine di Euro, a seconda delle funzionalità e dei volumi richiesti. È possibile la personalizzazione con logo con un sovrapprezzo.

Tipicamente viene offerto a parte il software di gestione (rilascio, revoca, reporting) dei dispositivi, qualora non vi sia già in essere presso il cliente un sistema di Identity Management in grado di effettuare tale gestione.

Pro:

- Disponibilità di alcuni produttori internazionali con vasta gamma di prodotti off-the-shelf per tutte le funzionalità

- Smart-Card Java-OS certificata per PKI a livello internazionale ed italiano

- One-Time-Password Generator, funzione estendibile eventualmente anche ad un sistema SMS con software aggiuntivo

- Encrypted Storage per la memorizzazione di passwords, private keys di vario genere, dati personali (questi ultimi nella versione con Flash Memory in emulazione USB Flash Memory Key fino a 32 GB o più)

- Integrabile con Windows Active Directory ed altre tecnologie di Identity Management

- Integrabile con tecnologie di crittografia dei dati di terze parti, incluse quelle che implicano una autenticazione BIOS (pre-Boot Authentication), come SafeBoot (McAfee) e Check Point (ex-PointSec Security)

- Disponibilità di software per la gestione del rilascio/revoca/assegnazione provvisoria di un dispositivo, integrato con Windows Active Directory

- Disponibilità di Tokens Software, su MS Windows e su Smart-Phones, sia per l'utilizzo operativo che per la gestione della perdita del token fisico, ovvero disponibilità del Virtual Token per tutti i casi di rilascio di un Token temporaneo

- Disponibilità di Tag RFID Mifare 1K integrato, per l'integrazione con applicazioni di controllo accessi e rilevazione presenze compatibili con lettori Mifare.

Contro:

- Necessità di una infrastruttura PKI-based per l'autenticazione e la generazione dei cetificati digitali, a meno delle applicazioni limitate alla gestione delle passwords sul dispositivo e quelle RFID-Based

- Per una ottimale gestione del dispositivo in tutte le sue funzioni è necessario installare il relativo driver

- La limitata superficie del dispositivo consente solo di apporre un logo aziendale e poco più

1.2 POSSIBILI SCENARI

I diversi scenari che comprendono le soluzioni di Strong Authentication possono essere riassunti in alcuni macro-scenari, non necessariamente esaustivi:

1. Accesso Extranet/Internet verso applicazioni e/o reti da parte di dipendenti e/o collaboratori con diversi gradi di confidenzialità (utenti mobili, home-workers, ecc.);

2. Accesso Extranet/Internet da parte di Partner e/o Clienti (agenti, partners, clienti);

3. Accesso Intranet verso dati e/o applicazioni di particolare criticità;

4. Single Sign-On verso tutte o parte delle applicazioni.

Per tutti questi scenari è necessario definire il livello di rischio accettabile per l'accesso alle varie tipologie di informazioni e le contromisure sufficienti a mitigare il rischio ad un livello accettabile rispetto al costo delle contromisure.

In alcuni casi è sufficiente una infrastruttura One-Time-Password (OTP), ad esempio per gli accessi VPN, per garantire l'adeguatezza a diversi standard di sicurezza; in altri casi è necessario effettuare un'analisi sui requisiti del cliente con riferimento agli standard o alle regolamentazioni correnti, per stabilire quale soluzione sia la più rispondente ai costi ed agli obblighi.

In altri casi è necessario impostare una politica di salvaguardia dei dati critici per mezzo della crittografia a vari livelli: per alcune situazioni è sufficiente impostare la crittografia con il controllo del singolo utente (ma cosa succede se il dipendente si licenzia?), per altre è indispensabile un controllo centralizzato delle chiavi pur mantenendo la riservatezza a livello individuale, per altre è assolutamente necessario mantenere il controllo delle informazioni proprietarie, per esempio utilizzando strumenti che limitano l'accesso alle informazioni aziendali tramite desktop virtuali connessi in VPN (evitando del tutto l'accesso a media removibili e fissi in disponibilità dell'utente). Un esempio di quest'ultimo scenario è implementabile tramite prodotti come Check Point Abra: in una USB Key viene implementato un ambiente desktop con le applicazioni necessarie per la produttività aziendale, isolato dall'ambiente HW/SW in cui viene eseguito. In questo modo il dipendente/consulente può utilizzare il proprio PC personale per connettersi alla rete aziendale senza interazioni tra i due ambienti e senza alterazioni o tracce residue sul PC utilizzato.

La tematica è quindi piuttosto complessa e per lo studio e l'eventuale realizzazione di un progetto di Single Sign-On o di protezione dati con crittografia è quindi opportuno valutare gli impatti sull'attuale infrastruttura ed analizzare le possibili soluzioni integrate con le diverse piattaforme software presenti e/o previste.

E' quindi sempre opportuno confrontarsi con il cliente per definire le migliori soluzioni al minor costo di esercizio.

www.ictsystem.it

operation@ictsystem.it

Tel. 02.699.000.19