

Secure Password Store

La grande diffusione delle applicazioni client/server ha evidenziato la problematica relativa alla memorizzazione e gestione delle password di accesso. Tipicamente le applicazioni client/server che non sono integrate nativamente nell'architettura di dominio (ossia non condividono il database degli utenti del dominio) forniscono una propria procedura di autenticazione che richiede una coppia user - password diversa da quella usata quotidianamente per l'accesso al dominio. Di conseguenza, gli utenti che accedono spesso ad applicazioni di questo tipo sono costretti a ricordare, per ogni applicazione, la specifica coppia user-password.

La situazione è ancora più complessa in quei contesti in cui le policy aziendali costringono a cambiare le password periodicamente. In tali casi l'utente non può scegliere la password in un insieme ristretto di parole mnemoniche ma è tenuto a ricordare password lunghe e complicate, spesso contenenti caratteri speciali.

Nella realtà dei fatti, poiché risulta effettivamente molto difficile ricordare tante password diverse, accade che gli utenti, per semplificare il proprio lavoro, conservano nel cassetto, nell'agenda o, nei casi più eclatanti, sul monitor, un foglio con le triple applicazione-user-password, minando in tal modo la sicurezza dell'intero sistema.

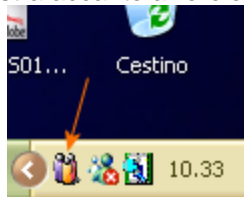
L'architettura di dominio Microsoft già implementa un sistema di Single Sign-On. Difatti, una volta effettuato il login al dominio dalla propria postazione, l'utente è automaticamente autenticato rispetto a tutte le applicazioni che poggiano sul dominio (ossia condividono lo stesso database degli utenti; fra queste si individuano, ad esempio le applicazioni Microsoft IIS, SQLServer, Exchange, Cytrix Metaframe, etc.), e rispetto a tutti i domini per i quali vige una relazione di trust con il primo.

Tuttavia, quando l'ambiente operativo è piuttosto eterogeneo, ossia include applicazioni che non poggiano su architettura Microsoft (servizi web, applicazioni client-server proprietarie, applicazioni *legacy*, ecc.) il meccanismo di Single Sign-On offerto dall'architettura Microsoft non è più sufficiente.

Il *Secure Password Store* unitamente alla smart card offre una possibile soluzione a tale problematica.

Il foglio contenente le credenziali associate alle varie applicazioni, che tipicamente l'utente conserva nell'agenda, può essere considerato a tutti gli effetti una tabella composta da tre colonne: applicazione, username, password. Tale tabella è conservata sulla smart card protetta da PIN o da Impronta digitale.

Il *Secure Password Store* consiste di un insieme di strumenti per la gestione e visualizzazione delle credenziali utente conservate nella tabella sulla smart card. Più specificamente il modulo si presenta come un servizio di Windows 2000 (NT/XP) il cui menù degli strumenti è richiamabile con un click sull'icona nella barra di sistema di windows (in basso a destra accanto all'orologio).



Il paradigma di funzionamento prevede due fasi:

- una fase di registrazione centralizzata in cui le applicazioni da porre sotto il controllo di Secure Password Store vengono registrate centralmente in una tabella che sarà poi spedita al client che ne fa richiesta e copiata sulla smart card dell'utente insieme alla coppia user-password;
- una fase di utilizzo in cui l'agente software viene attivato in seguito alla richiesta di autenticazione di un'applicazione registrata, accede in lettura alla tabella sulla smart card e invia all'applicazione le credenziali associate.

Secure Password Store è integrato in:

- Internet Explorer per completare i campi user-password nelle form di login;
- Applicazioni che richiedono l'autenticazione mediante finestra di dialogo. Ad esempio la finestra di autenticazione di Outlook;
- Applicazioni con interfaccia a carattere che richiedono l'autenticazione mediante il prompt (ad esempio applicazioni 3270)