digital Aim Consulting

Le chiavi della sicurezza

La AIM Consulting progetta e realizza, per importanti aziende del Canton Ticino, infrastrutture informatiche nell'ambito dei sistemi e servizi di rete su piattaforme Microsoft, avvalendosi della pluriennale esperienza dei suoi collaboratori.

Sicurezza. Parlarne è facile, ma tradurla in pratica non è semplice. «Notevoli passi sulla strada della standardizzazione sono ormai stati compiuti», spiega Giuliano De Marco, senior consultant della Aim Consulting di Lugano, riferendosi in particolare ai certificati digitali. Di cosa si tratta?

Il certificato è un documento pubblico (e quindi accessibile attraverso un web server, una cartella condivisa, o meglio ancora Active Directory) che consente di effettuare operazioni di crittografia, e la cui autenticità è garantita da un ente certificatore. «Nella sua forma più semplice», continua De Marco, «il certificato contiene le informazioni anagrafiche relative al titolare (nome, cognome, indirizzo di mail, ecc...), e una chiave digitale, denominata pubblica. Mediante questa chiave, un generico utente può cifrare un documento in modo che solo il titolare del certificato possa poi leggerlo. Con la stessa chiave l'utente in questione può verificare la firma digitale apposta ad un documento dal titolare del certificato, sia per garantirne l'integrità, sia per certificarne la provenienza».

La firma digitale è, difatti, una funzione crittografica che permette di assicurare che un insieme di dati non sia stato alterato, e che l'identità del redattore sia certa: questo è il motivo per cui un certificato digitale è firmato dall'ente che lo ha rilasciato, cioè garantisce le informazioni in esso contenute.

La cifratura e la firma sono applicabili in numerosi contesti come ad esempio la firma di documenti Office Xp, la cifratura e firma della posta elettronica, o l'autenticazione in rete tramite SmartCard (scheda dotata di un processore e avente le dimensioni di una carta di credito).

I certificati sono rilasciati da enti certificatori (Ca - Certification Authority), cioè sistemi costituiti da uomini e macchine che hanno il compito di redigere certificati digitali e garantire, tramite una firma digitale, i dati in essi contenuti. «Pertanto le Ca sono dei garanti d'identità per sistemi informatici, e quindi un supporto essenziale per la sicurezza di una rete», nota Danilo Giorgetti, direttore della Aim Consulting Sa.

La struttura dei servizi di certificazione viene denominata Public Key Infrastructure (Pki). Windows 2000 consente di realizzare strutture gerarchiche di questo tipo, sia permettendo di creare una nuova Pki in cui l'intera struttura di certificazione,

A destra, Danilo Giorgetti, direttore della Aim Consulting di Lugano, con il collaboratore Giuliano De Marco.

«Nella sua forma più semplice il certificato contiene le informazioni anagrafiche relative al titolare (nome, cognome, indirizzo di mail, ecc...), e una chiave digitale, denominata pubblica. Mediante questa chiave, un generico utente può cifrare un documento in modo che solo il titolare del certificato possa poi leggerlo»

GIULIANO DE MARCO,
SENIOR CONSULTANT
AIM CONSULTING DI LUGANO

compresa la Root Ca (radice dell'albero gerarchico), appartiene all'azienda, sia innestando una struttura Pki subordinata ad un ente di certificazioni pubblico, come ad esempio VeriSign, Thawte, ecc...

Gli strumenti per costruire sicurezza utilizzando certificati digitali sono presenti nei normali sistemi operativi di Microsoft. Windows 2000, infatti, permette di realizzare infrastrutture complesse Pki, alle quali fanno riferimento molti prodotti della casa di Seattle e di terze parti.

Tra le applicazioni che fanno riferimento all'uso dei certificati digitali, De Marco sottolinea la Strong Authentication, cioè l'autenticazione forte ottenuta mediante la verifica di almeno due fattori di identificazione, che «rappresenta un importante impiego della Pki. Windows 2000/XP permette infatti di autenticarsi alla rete aziendale mediante la presentazione di un certificato digitale custodito in una SmartCard. Questo è reso possibile grazie all'integrazione dei certificati nel protocollo d'autenticazione Windows 2000, basato sullo standard Kerberos«, continua De Marco. L'autenticazione viene eseguita inserendo la SmartCard nell'apposito lettore, ed inserendo un Pin, o password. La stessa soluzione è ottenibile con altri supporti che memorizzano il certificato, come ad esempio le UsbKey, cioè un dispositivo dalle dimensioni contenute inseribile in un'interfaccia Usb presente su tutti i computer attuali.

Mediante i certificati digitali è inoltre possibile proteggere le informazioni ritenute confidenziali in modo da garantirne la riservatezza e la sicurezza. I sistemi e gli ambiti sono diversi: l'Encryption File System (il più semplice) risulta idoneo alla protezione dei documenti confidenziali di un utente; mentre il Key Management Service, integrato nel server di posta elettronica Exchange 2000, permette di aggiungere le funzioni di cifratura e firma delle mail in una rete aziendale. Parlando di protezione dei documenti «esistono però sul mercato soluzioni più complesse dell'Encryption File System, anch'esse integrate con la Pki di Windows 2000, ma che permettono una maggiore flessibilità nella condivisione dei dati confidenziali tra gruppi di utenti», conclude De Marco.

Per informazioni:
AIM Consulting Sa
Via Monte Brè, 8 - 6900 Lugano
Tel. 091/9249590 - Fax 091/9249591
e-mail: admin@aimconsulting.ch
Web: www.aimconsulting.com