PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 8 - numero 1460 di venerdì 14 aprile 2006

ARRIVA MOC, LA FIRMA CON IL POLLICE A PROVA DI FALSARIO

Niente più password. Sarà l'impronta digitale a rendere sicura e affidabile l'identificazione personale e a confermare l'autenticità di una firma digitale. Con una semplice smart card a prova di falsificatore di impronte digitali.

Pubblicità

Una "smart card", piccola come una carta bancomat, con la nostra firma e la prova inconfutabile della nostra identità. È questa la nuova sfida della sicurezza informatica che promette di liberare l'utente dalla necessità di memorizzare decine di password, sostituendole con l'impronta del dito.

La firma digitale, già usata, è il risultato finale di un complesso algoritmo matematico, che permette di autenticare e identificare un documento a livello informatico, dandogli la stessa validità di una firma autografa. Il titolare possiede una chiave segreta, custodita su una smart card e protetta da un codice di accesso (pin), e una chiave pubblica, garantita dall'Ente Certificatore, usata per la verifica.

L'Istituto di informatica e telematica (Iit) del Consiglio nazionale delle ricerche di Pisa ha realizzato un'applicazione che consente di evitare l'uso del codice, trasportando in una tessera portatile il riconoscimento biometrico del possessore. L'Istituto ha progettato un sistema che consente di verificare l'identità del titolare attraverso la sua impronta digitale, confrontandola con quella "memorizzata" nella smart card. Sia i dati (l'impronta di un polpastrello) sia l'algoritmo di verifica si trovano all'interno della carta ed è quindi impossibile manometterli per violarne la sicurezza. Essi, inoltre, non lasciano mai il supporto, non attraversano alcun canale di comunicazione, impedendo l'intercettazione da parte di un possibile "pirata".

"Questa tecnologia, prende il nome di Match-on-Card (Moc), è in grado di fornire una maggiore sicurezza e privacy", dice l'ingegner Anna Vaccarelli, responsabile del settore sicurezza informatica dell'Iit-Cnr di Pisa. "Attualmente viene usata una tecnologia più semplice, la Toc (Template-on-Card), nella quale il supporto smart card offre sì la possibilità di memorizzazione dei dati ma lasciando al pc quella di verifica mediante la digitazione del pin".

"La tecnologia realizzata dall'Iit-Cnr", sottolinea ancora Vaccarelli, "consente invece di firmare digitalmente un documento solo dopo un'autenticazione biometrica positiva con il riconoscimento dell'impronta, sostituendo così i codici che possono essere sottratti e copiati. Al momento della consegna della smart card, l'impronta dell'utente (template) viene codificata e memorizzata all'interno della carta (processo di enrollment), all'atto dell'apposizione della firma, il template memorizzato nella smart card sarà confrontato con quello scansionato in tempo reale". In sostanza, un lettore di impronta collegato al computer digitalizza l'immagine e la confronta con un modello preacquisito per verificarne la corrispondenza.

"Sul prototipo realizzato sono state rilevate prestazioni di affidabilità e velocità molto interessanti", conclude l'ingegner Vaccarelli, "per ottenere la verifica biometrica, infatti, sono necessari pochi secondi e la percentuale di falsi positivi è inferiore allo 0,1 per cento".

Cattive notizie per i malintenzionati: con questo sistema è impossibile usare impronte ricostruite artificialmente o addirittura utilizzare dita asportate alla vittima..... Le contromisure previste dai lettori di impronta digitale consentono infatti di rilevare l'autenticità attraverso le proprietà elettriche o fisiche legate alla vitalità dell'individuo, i segnali involontari come il battito o la pressione sanguigna, l'elasticità naturale della pelle, umidità e temperatura, che polpastrelli artificiali o di cadaveri non hanno.