

Le tecnologie biometriche per la sicurezza

In pochi anni, l'impiego di tecnologie biometriche si è diffuso anche in ambito civile dopo un lungo periodo di uso esclusivo in ambito criminale. Le soluzioni basate sulla biometria sono in grado di fornire una risposta alle necessità emergenti nel campo delle transazioni finanziarie e confidenziali, nella gestione della privacy e dei dati personali.

La necessità di soluzioni biometriche si va sempre più diffondendo a livello mondiale, negli Stati e nei governi locali, nella difesa e nelle applicazioni commerciali; è sentita a livello di infrastrutture di sicurezza per la rete delle imprese, per le applicazioni governative, per proteggere le transazioni finanziarie nel settore bancario, per le vendite al dettaglio, per ottemperare alle disposizioni di legge, per la sanità e i servizi sociali. Sono tutti campi di applicazione che traggono beneficio dall'utilizzo di queste tecnologie.

Le metodologie di riconoscimento biometrico sono molteplici: il riconoscimento facciale, quello dell'iride o della retina, le varie modalità di riconoscimento della mano o vocale sono solo alcuni esempi. La tecnologia che però è al momento più diffusa, di più agevole utilizzo e più attendibile è quella delle impronte digitali, che è senza ombra di dubbio quella che ha una storia più lunga e una comprovata efficacia nell'ambito criminale.

Le metodologie di autenticazione basate su tecnologie di riconoscimento delle impronte digitali sono applicabili a stazioni di lavoro, "networks", domini d'accesso, "single sign-on", accesso applicativo, protezione dei dati, accesso a risorse remote, sicurezza nelle transazioni e sicurezza nei Web.

La fiducia nella esercibilità delle transazioni elettroniche è essenziale per una sana crescita dell'economia a livello mondiale. Utilizzate da sole o integrate con altre tecnologie come le smart-card, le chiavi di crittografia e la firma elettronica, le applicazioni biometriche sono destinate a pervadere quasi tutti gli aspetti dell'economia e della nostra vita quotidiana. Questa diffusione ha portato alla presenza in commercio di una moltitudine di dispositivi e software che cercano di garantire un'autenticazione certa dell'individuo che compie un'azione. La scelta di un sistema per il riconoscimento biometrico tramite impronte digitali è quindi impegnativa. Le considerazioni da fare sono molteplici. Prima di tutto deve essere valutato il livello di accuratezza della verifica.

Esistono molti dispositivi in commercio, alcuni dei quali particolarmente economici, ma non tutti possono garantire un livello di sicurezza elevato. Sicuramente l'utilizzo di componenti hardware e algoritmi di riconoscimento derivati dall'uso in campo criminale fa sì che si possa essere confidenti in una prestazione di livello superiore.

L'analisi dell'impronta deve essere effettuata sull'intera superficie disponibile e quindi la dimensione del sensore è fondamentale. L'utilizzo di zone circoscritte della superficie dell'impronta può, infatti, non essere sufficiente a garantire un livello di riconoscimento adeguato alle nostre esigenze.

Molte persone continuano a percepire la verifica biometrica come una forma di controllo, associandola esclusivamente alla vecchia immagine di tali tecnologie applicate alle indagini criminali. L'impiego delle nostre peculiari caratteristiche fisiche deve invece trasformarsi in una garanzia per noi stessi, in una protezione da possibili attacchi alla nostra identità e in una comodità da utilizzare quotidianamente.

Dobbiamo trasformare i meccanismi attraverso cui dimostriamo la titolarità di un diritto, passando da una situazione in cui la garanzia sia dovuta a qualcosa che "abbiamo" (documento, carta di credito, ecc.) o che "conosciamo" (PIN, password, ecc.), anche combinate tra di loro, a qualcosa che invece "siamo" (impronte digitali, riconoscimento dell'iride, riconoscimento facciale, ecc.).

Al momento della rilevazione del dato biometrico, le informazioni ricavate dal dispositivo vengono trasformate in un dato informatico, generalmente detto "template", dal quale non è possibile risalire all'informazione originaria dell'immagine dell'impronta digitale. Proprio per l'importanza dell'unicità di queste informazioni che portiamo con noi, dobbiamo, ogni volta che ci apprestiamo all'utilizzo delle stesse, cercare di proteggerle. Dobbiamo riuscire a fare sì che le nostre informazioni non possano essere in qualche maniera trafugate e indebitamente utilizzate.

In Italia il Garante per la privacy sta incominciando ad occuparsi della questione. Il compito di chi progetta sistemi (e non solo dispositivi) per l'autenticazione biometrica è anche quello di far sì che i dati non siano riproducibili, intercettabili e utilizzabili da nessuno.

All'interno di Elsag, Italdata ingegneria dell'idea aveva intuito già da tempo che le soluzioni informatiche basate sulla biometria sarebbero diventate strategiche sia nel settore della sicurezza professionale che in quello consumer. Dall'analisi delle prime tecnologie che il mercato rendeva disponibili, Italdata aveva anche compreso quanto fosse alto il rischio di "screditare" il settore, avvalorando soluzioni di dubbia validità al solo scopo di sviluppare un rapido business. Grazie ad un'analisi attenta, si è percepito quanto fosse importante sperimentare, valutare nuovi materiali, studiare l'evoluzione degli algoritmi matematici, analizzare i diversi contesti operativi per capire esattamente quali caratteristiche fossero, di volta in volta, fondamentali e necessarie. La collaborazione con le forze di sicurezza nazionali e internazionali è stata, ed è ancora oggi, il contributo maggiore allo sviluppo delle nostre soluzioni informatiche. La professionalità, necessaria per soddisfare i requisiti che questo settore richiede, è la risorsa fondamentale cui Italdata fa riferimento per la realizzazione dei propri prodotti.