Le Tecnologie Biometriche ed il loro Utilizzo

di * Federico Fumagalli

La tecnologia, i processi
ed i campi di utilizzazione,

Introduzione

Biometria = caratteristiche fisiologiche o comportamentali misurabili che possono essere utilizzate per identificare un individuo o per verificarne l'identità.

Il riconoscimento e l'identificazione delle persone tramite tecnologie basate sulla biometria (= tecnologie biometriche) sono generalmente finalizzati alla realizzazione di sistemi di sicurezza nei quali l'identificazione "immediata e certa" di un individuo è da considerarsi un obbiettivo prioritario.

In questa prospettiva le soluzioni basate sull'impiego della tecnologia biometrica affiancano con caratteristiche uniche le altre soluzioni tradizionali che si basano sull'uso di password, di PIN, di tessere "intelligenti", etc.

Metodo	Esempio	Proprietà
Ciò che si conosce	User ID Password PIN	Può essere condiviso tra più utilizzatori Molte password oggi utilizzate sono facili da indovinare Può essere dimenticato
Ciò che si possiede	Tessera Badge Chiave elettronica	Può essere condiviso tra più utilizzatori Può essere duplicato Si può smarrire o può essere rubato
Ciò che si conosce e che si possiede	Tessere ATM + PIN	Può essere condiviso tra più utilizzatori Il PIN è il punto debole e può essere dimenticato
Ciò che è unico e specifico dell'individuo	Impronta digitale Iride Viso Etc.	È utilizzabile solo dal proprietario Difficilmente falsificabile Non può essere smarrito, rubato, o dimenticato

Rispetto alle altre soluzioni tuttavia, la tecnologia biometrica, in quanto si basa su caratteristiche fisiologiche o comportamentali ben definite e di solito facilmente misurabili, garanti-

sce in modo univoco il riconoscimento di un individuo. Per queste ragioni, questa tecnologia permette di realizzare un livello di sicurezza molto efficiente in tutti i casi in cui è essenziale ottenere un'identificazione certa, anche in condizioni ambientali poco favorevoli (si pensi alla necessità di implementare sistemi in cui il riconoscimento di un individuo deve essere effettuato senza dovere coinvolgere attivamente l'individuo stesso).

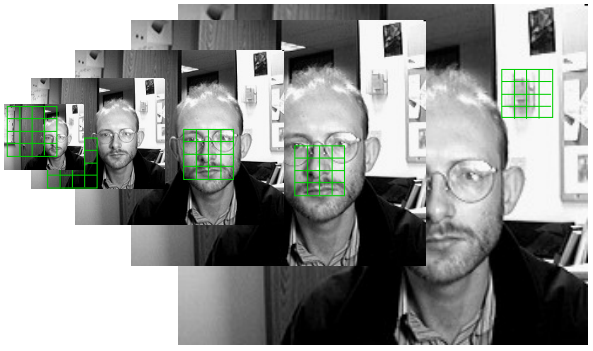
È interessante notare che le caratteristiche fisiche individuali utilizzate in un sistema basato sulla biometria non possono essere copiate, falsificate, rubate, o ... dimenticate, in quanto esse sono proprietà intrinseche dell'individuo. È altresì vero che alcune di esse possono essere "perse" in seguito a gravi traumi, ma ciò non è argomento di questo documento.

In questo documento si descrivono le principali tecnologie biometriche ed il loro utilizzo. In particolare si descrive:

- Un possibile approccio tecnologico
- I processi necessari all'utilizzo di queste tecnologie
- Le caratteristiche di sicurezza delle diverse tecnologie
- Le applicazioni

L'Approccio Tecnologico

L'implementazione di una soluzione biometrica richiede che siano definiti i valori da assegnare alle soglie di riconoscimento. Infatti, a causa di fattori diversi (fisici, ambientali, etc.), il risultato di un processo di riconoscimento biometrico non è mai preciso. Esso è costituito da un valore approssimato che indica quanto l'impronta biometrica utilizzata corrisponde al modello di riferimento. Valori estremi, zero o 100%, sono alquanto improbabili.

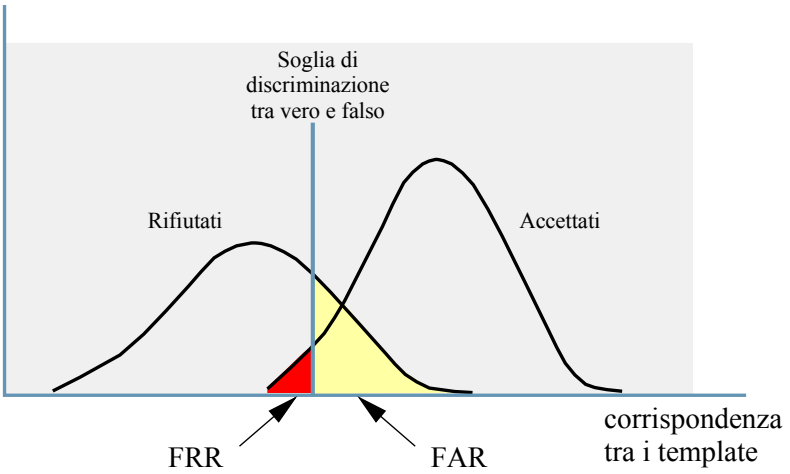


La definizione della soglia di riconoscimento stabilisce il confine tra l'accettazione o il rifiuto della richiesta. In tale modo è quindi possibile impostare il livello di sicurezza del sistema.

Questa definizione serve anche a stabilire l'influenza che due effetti contrastanti hanno sulle caratteristiche e sul livello di sicurezza e di prestazione del sistema:

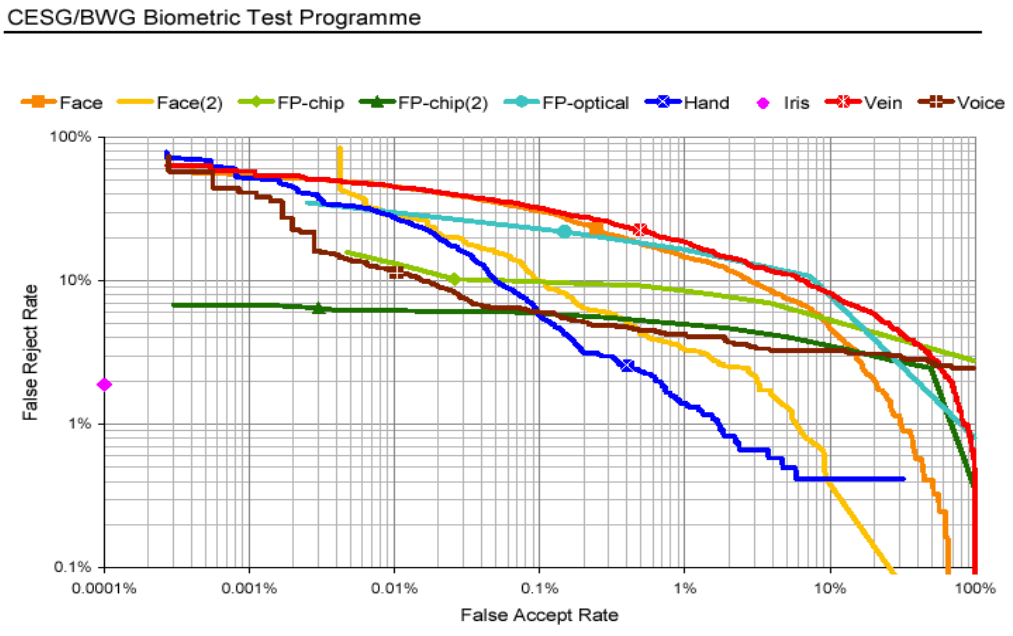
- False Reject Rate (FRR) – definisce, in percentuale, il numero di volte in cui il sistema considera invalida (non riconosce) un'impronta valida.
- False Accept Rate (FAR) – definisce, in percentuale, il numero di volte in cui il sistema considera valida un'impronta invalida.

In base alle definizioni, i due fattori (FRR e FAR) possono essere considerati come errori dei processi biometrici. Il loro verificarsi statistico è descritto nel grafico che segue:



Considerando l'andamento delle due curve risulta ovvio che, scelto il tipo di soluzione biometrica da utilizzare, l'ottenimento di alte percentuali di sicurezza (FAR minimo) comporta lo spostamento della soglia di discriminazione verso destra. Ciò rende il sistema più selettivo (sicuro) poiché il riconoscimento richiede un maggior numero di punti di corrispondenza tra i template. Tuttavia, ciò comporta un aumento dei casi di False Reject (FRR). Analogamente lo spostamento della soglia verso sinistra favorisce il riconoscimento in casi ambigui, ma comporta anche statisticamente l'accettazione di impronte invalide (FAR) con valori che non sempre possono essere accettabili.

L'andamento dei due parametri (FAR e FRR) per ciascuna tecnologia biometrica è stato misurato mediante prove sperimentali. I risultati sono tracciati nel grafico che segue:



Detection error trade-off: FAR vs FRR

Le tecnologie biometriche

Come detto, le tecnologie biometriche si basano sull'utilizzo di alcune caratteristiche individuali per permettere, in modo sicuro, il riconoscimento o l'identificazione di una persona. Esse si suddividono in due aree:

- Le caratteristiche Fisiologiche (uniche e invarianti) – che comprendono la geometria della mano e l'impronta del palmo, l'impronta digitale, l'immagine della retina o dell'iride, le caratteristiche (geometriche) del volto.
- Le caratteristiche Comportamentali (uniche ma variabili) – che comprendono la firma, il modo di camminare, la voce (quest'ultima appartiene anche al gruppo precedente), il modo con cui si scrive su una tastiera.

Esistono invero altre "impronte" biometriche, quali il DNA, la forma del padiglione auricolare, il battito cardiaco, etc. Esse non saranno prese in considerazione in questo documento o perché ancora in una fase iniziale di ricerca/sviluppo, o perché il loro campo di applicabilità si limita a soluzioni estremamente specializzate e generalmente molto costose.

Le tecnologie oggi più comunemente utilizzate sono:

Impronta digitale – consiste nel confrontare una data impronta, acquisita al momento della richiesta di accesso con una di riferimento, ottenuta in modo controllato e sicuro. Il confronto avviene con tecnologie simili a quelle usate per l'elaborazione delle immagini, principalmente tramite la verifica di corrispondenza di una serie di "minutie" ricavate dalle due impronte che sono oggetto del confronto. È una tecnologia che richiede bassi costi di implementazione ed è facilmente integrabile in diversi sistemi di sicurezza.

Geometria e impronta della mano – consiste nel confrontare alcune misure della mano (dita, forma del palmo, etc.), ricavate in 3D, con analoghe misure di riferimento acquisite in modo controllato. Gli elementi oggetto della misura sono quelli che mantengono dei rapporti geometrici costanti durante tutta la vita.

Caratteristiche della voce – consiste nel paragonare alcuni elementi identificativi della voce dell'individuo che sono caratteristici indipendentemente dalle parole pronunciate.

Scansione della retina – consiste nella lettura ottica della dimensione e del disegno formato dai vasi sanguigni che coprono la retina. La lettura avviene mediante una sorgente di luce a bassa intensità.

Scansione dell'iride – consiste nella lettura e nella successiva interpretazione delle caratteristiche dell'iride acquisite mediante una fotocamera o una videocamera tradizionale.

Verifica della firma – consiste nella "lettura" di alcuni parametri dinamici (velocità, pressione, accelerazione, etc.) rilevati mediante opportuni dispositivi durante la firma.

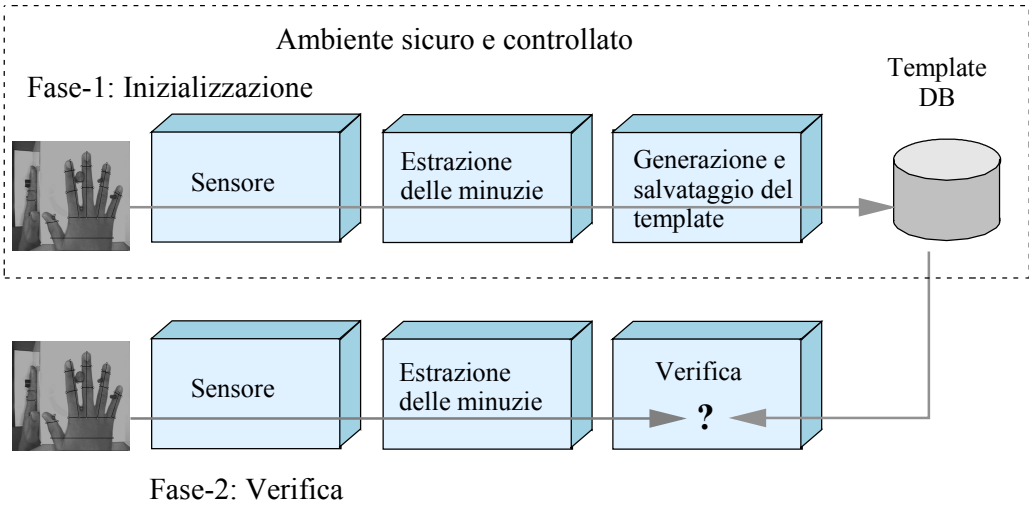
Geometria del volto – consiste nel confrontare alcune caratteristiche dei tratti del viso con il corrispondente modello di identificazione acquisito in modo sicuro. Il confronto avviene tramite immagini acquisite, da fermo ed in movimento, con dispositivi ottici (generalmente telecamere).

Il processo di identificazione biometrica

Il processo di identificazione o verifica tramite un'impronta biometria è generalmente comune a tutte le tecnologie biometriche. Esso consiste in alcuni processi basilari, quali:

- Acquisizione dell'impronta biometrica di riferimento e sua trasformazione in un template binario di riferimento
- Acquisizione di una nuova impronta al momento dell'identificazione, elaborazione del template e confronto con quello di riferimento
- Se c'è sufficiente corrispondenza tra i due template l'identificazione è valida

Questa sequenza di operazioni può presentare delle differenze in funzione del tipo di impronta biometrica utilizzata, in base alle caratteristiche dei dispositivi utilizzati, ed in base alle caratteristiche ambientali in cui viene effettuata la verifica.



Fase-2: Verifica

La figura mostra le due fasi di implementazione di una soluzione basata sulla biometria. La prima fase, di Inizializzazione (Enrollment), serve ad acquisire un'immagine di riferimento e da questa costruire un template utilizzabile come modello per le successive verifiche. Questo processo viene eseguito in un ambiente controllato atto a garantire in modo sicuro l'origine e la proprietà dell'impronta biometrica.

La seconda fase, di Verifica (Matching), viene attivata ogni volta che si debba eseguire un'azione di verifica della stessa impronta acquisita localmente. Quest'operazione può essere eseguita per due scopi diversi:

- AUTENTICAZIONE o VERIFICA – viene effettuata mediante confronto dell'impronta acquisita con un template di riferimento. Serve per garantire l'identità dichiarata.
- IDENTIFICAZIONE o RICONOSCIMENTO – viene effettuata mediante ricerca di un template compatibile all'interno di un archivio. Serve quindi a identificare una persona di cui non si conosce necessariamente a priori l'identità.

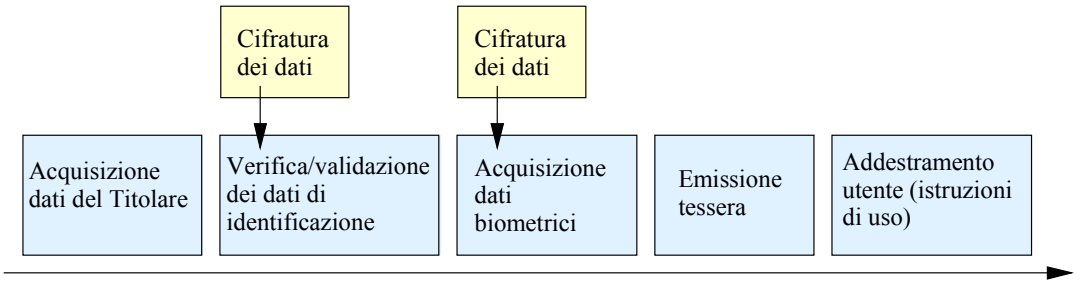
Le tecnologie biometriche e le smartcard

Le smartcard, sia quelle dotate di un processore, sia quelle in cui il chip elettronico è semplicemente costituito da una memoria cablata, costituiscono una valida alternativa alle banche dati usate per la memorizzazione di massa dei template biometrici. In questo caso la smartcard si caratterizza come dispositivo sicuro per l'identificazione del titolare. Inoltre, essa è in grado di ospitare tutte le strutture di dati necessarie all'accesso a servizi diversi.

La tecnologia più diffusa si basa su dispositivi con caratteristiche attive (smartcard a processore), così mediante l'inserimento della smartcard in un apposito lettore da potere fornire in modo indipendente solo le informazioni richieste da uno specifico servizio associato al dispositivo di accesso.

Generalmente, il supporto biometrico è associato alle smartcard utilizzate come documenti di identificazione del titolare. Ciò avviene mediante l'inserimento della smartcard in un apposito lettore in grado di comunicare con il processore presente sulla smartcard e, in alcuni casi, di attivare dei processi elaborativi nello stesso processore.

Qui di seguito viene riportato, per blocchi, il processo di registrazione e di emissione di una tessera di identificazione i cui dati sono protetti tramite un dispositivo di verifica biometrica.

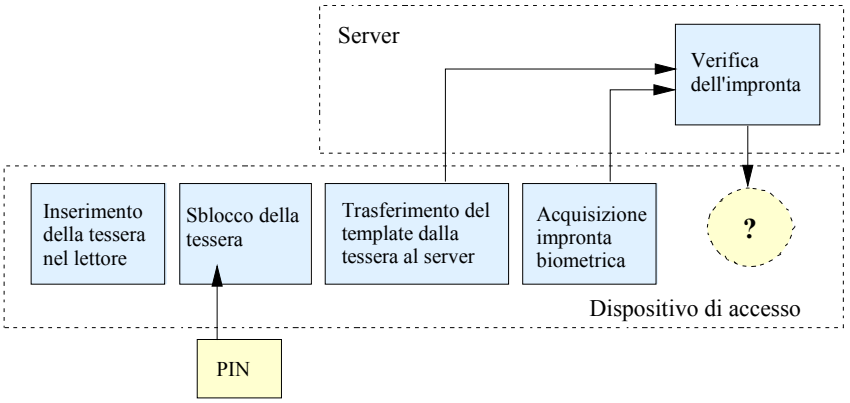


La memorizzazione di un template biometrico su smartcard avviene tramite un processo crittografico (encrypted hash) che ne protegge il contenuto. Il template viene "firmato" in modo digitale e "sigillato" nella memoria della smartcard dall'Autorità responsabile di garantirne la sicurezza e l'integrità. In questo modo la smartcard stessa è in grado di impedire qualunque tipo di accesso non autorizzato alla memoria in cui è stato salvato il template, e quindi al template stesso.

L'identificazione del titolare della smartcard così prodotta tramite i dati biometrici in essa memorizzati, può ora essere effettuata in due modi diversi:

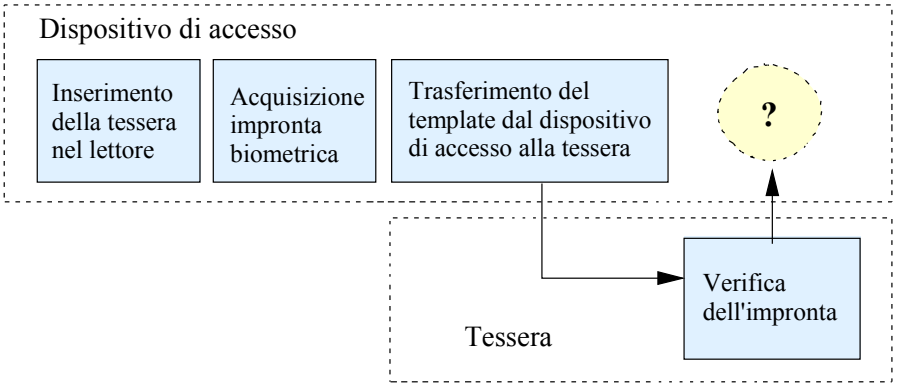
- Verifica esterna alla tessera
- Verifica interna

Nel primo caso il processo è il seguente:

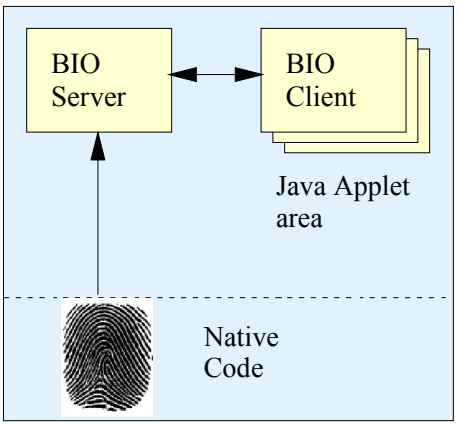


La verifica dell'impronta biometrica avviene esternamente alla tessera su un servente a cui è collegato il dispositivo di accesso. In questa caso la tessera è utilizzata solo per il salvataggio (sicuro) dei dati del titolare e del template di riferimento.

Nel secondo caso il processo è il seguente:



In questo caso la verifica della validità dell'impronta biometrica avviene mediante la comparazione con il template di riferimento effettuato dal processore della tessera. Il template di riferimento rimane nella memoria della tessera. La tessera stessa assume un ruolo attivo, garantendo la massima sicurezza dei dati utilizzati per questo processo.



Nel caso di una smartcard Java, questo processo si basa su una struttura interna simile a quella mostrata nella figura a lato. Il template di riferimento è salvato in modo sicuro nella memoria base della carta, e viene elaborato nella memoria dinamica da un Applet opportunamente predisposto. L'Applet può essere residente sulla tessera, oppure essere trasferito dinamicamente in questa al momento dell'esecuzione della transazione di verifica.

Quando si usano smartcard non –Java, il processo di verifica eseguito nella memoria della smartcard comporta la predisposizione di opportuni "comandi" nel sistema operativo della smartcard stessa.

I due modi possono essere utilizzati indifferentemente con la stessa tessera. La scelta tra il primo ed il secondo è funzione del dispositivo di accesso utilizzato e delle caratteristiche della soluzione.

L'utilizzo delle smartcard per la memorizzazione dei template biometrici in alternativa alla memorizzazione centrale su database di tali dati, garantisce inoltre i requisiti di privacy delle informazioni.

L'Uso della Biometria

L'applicazione delle tecnologie biometriche ai fini della sicurezza consiste principalmente in:

Un applicativo che misura alcune caratteristiche uniche di un individuo e le confronta con analoghe caratteristiche precedentemente acquisite e salvate.

I campi di applicabilità

Il mercato chiede soluzioni in cui la tecnologia biometrica garantisce il "sicuro" riconoscimento dell'individuo, in settori diversi. Più frequentemente le soluzioni richieste riguardano:

- Controllo (fisico) degli accessi – edifici, parcheggi, uffici, ospedali, prigioni, ed, in genere, tutte le aree chiuse in cui è importante riconoscere chi entra ed esce.
- Controllo (logico) degli accessi – personal computer, reti informatiche (intranet), telefoni cellulari, posta elettronica, dati riservati (es. cartelle sanitarie), servizi bancari.
- Sorveglianza – eventi sportivi, centri commerciali, concerti, edifici, musei.

La scelta della tecnologia da utilizzare è generalmente dettata dal tipo di soluzione richiesto e dall'ambiente in cui essa va implementata. Fattori da non trascurare sono anche quelli associati al livello di accettazione da parte dell'utenza finale, e le caratteristiche di funzionamento di ciascuna tecnologia in relazione al livello di sicurezza richiesto.

La tabella che segue riassume e quantifica alcuni dei valori caratterizzanti le tecnologie qui discusse.

Tecnica	Valore indicativo FRR (%)	Valore indicativo FAR (%)	Costo dispositivi	Dimensioni template di riferimento (Bytes)	Accettazione da parte degli utenti
Impronta digitale	3-7	0.0001-0.001	Medio	300-1200	Media
Geometria della mano	1-10	1	Medio	< 10	Media
Caratteristiche della voce	10-20	2-5	Basso	1500	Alta

Tecnica	Valore indicativo FRR (%)	Valore indicativo FAR (%)	Costo dispositivi	Dimensioni template di riferimento (Bytes)	Accettazione da parte degli utenti
Scansione della retina	1	0.01	Molto alto		Bassa
Scansione dell'iride	1-10	~ 0	Alto	512	Alta
Verifica della firma	3-10	1	Medio		Media
Geometria del volto (verifica identità)	10-20	0.001-1	Medio	Pochi bytes	Alta

Il problema della tutela della privacy

Come accennato precedentemente, l'uso di smartcard per la memorizzazione dei template biometrici di riferimento, oltre a garantire buone prestazioni nelle operazioni di identificazione del titolare, costituisce una valida alternativa alla creazione di banche dati (centrali o distribuite) in cui memorizzare tali template.

È infatti noto che servizi che richiedono l'identificazione di coloro che accedono al servizio stesso possono avere dei potenziali impatti sulle norme che tutelano la privacy quando il sistema di identificazione si basa sulla creazione di banche dati di riferimento.

Quando si utilizzano le smartcard per la memorizzazione dei dati personali di riferimento (il template biometrico è uno di essi), l'informazione privata e personale rimane in possesso del titolare e viene utilizzata solo quando necessario per accedere a servizi ben identificati, e solo nel momento in cui la smartcard viene acceduta tramite il dispositivo di lettura associato al servizio stesso.

*Federico Fumagalli

IBM Technical Solutions