Integrazione di Sistemi Biometrici

Andrea Patrignani
patrignani@biometrika.it

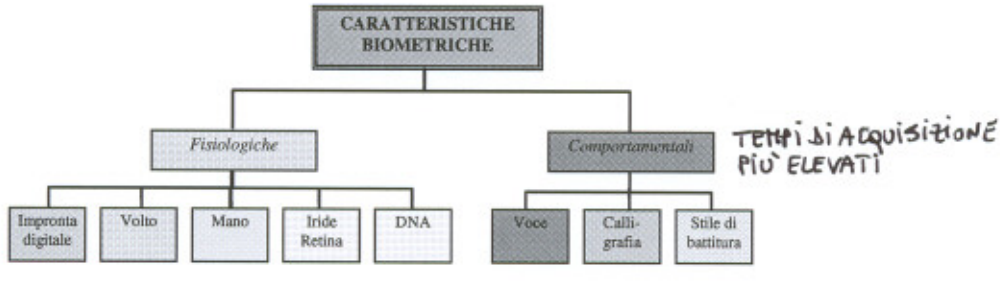
CLUSIT EDUCATION

Introduzione ai sistemi Biometrici
Aspetti Implementativi

- **Sistemi biometrici**

  Utilizzano caratteristiche fisiologica o comportamentali per il riconoscimento automatico di individui
  - Che obbiettivi ci si pone?
  - Quale caratteristica utilizzare?

- **Principali caratteristiche biometriche**



Parametri di confronto fra le diverse caratteristiche biometriche

Sicurezza
- Prestazioni (FAR, FRR ...)
- Resistenza a contraffazioni (Vivezza, Mimica)
- Resistenza a manomissioni
- Unicità

Robustezza
- Accuratezza dell'acquisizione
- Universalità
- Stabilità (tempo e ambiente)

VIVEZZA PER LE CARATTERISTICHE FISIOLOGICHE

MIMICA PER LE CARATTERISTICHE COMPORTAMENTALI

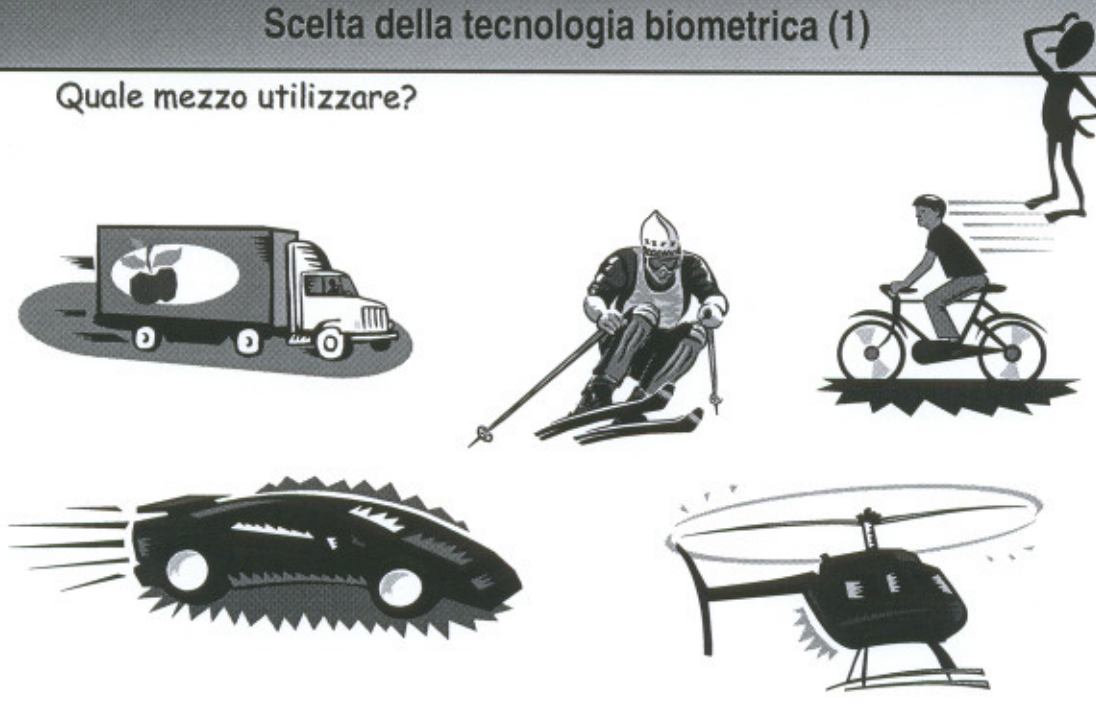
Usabilità
- Semplicità, praticità e invasività
- Difficoltà nell'enrollment e nell'acquisizione
- Training, supervisione, manutenzione
- Tempi di enrollment e riconoscimento

Accettabilità
- Della caratteristica biometrica
- Delle operazioni di enroll e riconoscimento (aspetti medici)
- Del trattamento dei dati

Altro
- Costo e ingombro
- Dimensioni del template
- Aderenza a standard

Scelta della tecnologia biometrica (1)

Quale mezzo utilizzare?



Scelta della tecnologia biometrica (2)

- Per poter sviluppare in modo efficace una soluzione biometrica, è necessario analizzare la specifica applicazione sotto molteplici aspetti.

Alcuni esempi:

- È possibile operare in verifica o è necessario operare in identificazione?
- È un caso di riconoscimento positivo o negativo?
- Qual è il rischio nel caso di errore di false-match? e di false-rejection?
- L'utente è interessato/motivato a cooperare?
- In quale ambiente deve operare il sistema (luci, rumori, ...)?
- Il processo di riconoscimento è supervisionato?
- Con quale frequenza gli utenti utilizzano il sistema?
- Quali sono i rischi per la privacy?
- ...

Scelta della tecnologia biometrica (3)

Caratteristiche	**SICUREZZA** unicità, prestazioni, contraffazioni	**ROBUSTEZZA** universalità, stabilità	**ACCET-TABILITA'**	**USABILITA'** Semplicità, praticità, invasività	**ACCES-SIBILITA'** Costi, dimensioni
Impronta digitale	4/5	4/5	4	4/5	5
Mano	4	4	4	4/5	4
Volto	3	2	5	5	3
Iride	5	4/5	3	4	3
Retina	5	4/5	2/3	4	2/3
Firma	2	2	5	5	5
Voce	2	2/3	5	5	5
DNA	5-	5+	1	1	1

Classificazione delle applicazioni

Cosa si vuole proteggere?

Gli utenti sono a conoscenza dell'identificazione biometrica a cui sono sottoposti?
Si tratta di utenti abituati ad interagire con un sistema biometrico? Qual è il loro "livello tecnologico"?

E' necessaria o prevista la supervisione nella fase di enroll e di riconoscimento?

L'ambiente in cui opera il SB è un ambiente che garantisce condizioni standard? E' un ambiente controllato?

Quale il grado di interoperabilità del SB? I dati vengono esportati verso altre applicazioni?

Il soggetto che gestisce il SB è privato o pubblico?

Sicurezza logica	Sicurezza fisica
Manifesta	Non Manifesta
Utenti Abituati	Utenti non abituati
Supervisionata	Non supervisionata
Ambiente Standard	Ambiente non Standard
Aperta	Chiusa
Governativa	Privata

Fattibilità: esistono esperienze precedenti ?

- *Come in tutti i settori, molto si può imparare dalle esperienze (positive/negative) di altri che hanno tentato di percorrere la stessa strada.*
  - Difficilmente si potranno trovare esperienze precedenti in Italia.
  - All'estero (principalmente negli USA ma anche in altri paesi europei esperienze significative. Principali fonti di informazione:
    - Sito web del Biometric Consortium (http://www.biometrics.org) e relativa mailing list cui si può aderire su richiesta.
    - Sito web del Dipartimento di Servizi Sociali del Connecticut (http://www.dss.state.ct.us/digital.htm) che pubblica bimestralmente un newsletter BHSUG che include una panoramica dei principali progetti governativi (e non) in corso...
    - Diverse riviste market-oriented (non free) tra cui: *Biometric Market Intelligence* (BMI), *Biometric Digest*, *Biometric Technology Today*.

Implementazione graduale

- *Consente di ridurre il rischio e permette di maturare e far maturare la giusta cultura.*
  - Progetto pilota (coinvolgendo uno o più fornitori).
  - Introduzione prudente della tecnologia senza abbandonare bruscamente le vecchie procedure (laddove possibile).
    - *Un caso dove la biometria è l'unico metodo possibile è quello della cosiddetta "identificazione negativa", ovvero stabilire se l'affermazione di un individuo che sostiene di non far parte di una certo gruppo è vera (es: welfare benefit).*
  - E' necessario che tutti gli attori coinvolti (utenti, amministratori, dirigenti), anche quelli inizialmente scettici si convincano dei reali vantaggi.
  - La sicurezza è importante e apprezzata (specie in momenti storici caratterizzati dalla paura del Terrorismo internazionale), ma l'utente comune apprezza maggiormente quelle tecnologie che gli semplificano la vita.

MATCHING

IDENTIFICAZIONE DI UNA PERSONA DOPO IL MATCHING CON TUTTE LE IMPRONTE DI UN DB

Aspetti Tecnologici: verifica o identificazione ?

- Evitare assolutamente *di utilizzare un sistema biometrico per identificazione (riconoscimento 1:N su database di utenti) quando ciò non è strettamente necessario (esempio identificazione negativa).*
  - Vengono percepiti solo i vincoli di capacità di memorizzazione e di tempo di esecuzione, ma viene ignorato il problema principale: l'accuratezza.
  - Certo l'inserimento di un PIN può essere scomodo ma:
    - Il PIN non è segreto
    - Il PIN potrebbe essere anche non univoco (ad esempio l'utilizzo del giorno di nascita permette di ridurre di circa 1/30 la dimensione del DB).
    - Il PIN può essere memorizzato su Smart Card (magari Contactless).
    - Il sistema può ricordare l'ultimo utente che ha avuto accesso e riproporre il PIN corrispondente.

Aspetti tecnologici: lo zoo biometrico

Per diverse caratteristiche biometriche (impronte, voce, firma, ecc.) *è stato sperimentalmente dimostrato che alcuni utenti si discostano dalla media circa la capacità di fornire buone rappresentazioni delle loro caratterista biometrica:*

- **GOAT** (capre): questi utenti non riescono a fornire rappresentazioni di buona qualità. Questo può essere dovuto a bassa qualità intrinseca della caratteristica o difficoltà di interazione con il dispositivo.
- **SHEEP** (pecore): la caratteristica biometrica di questi utenti è priva o comunque povera di segni distintivi e quindi è poco discriminante e si presta bene a essere imitata.
- **WOLF** (lupo): colui che dimostra particolari abilità nel produrre caratteristiche biometriche (comportamentali o volto) che imitano quelle di altri utenti (sheep).

Queste famiglie di utenti non possono essere trascurate quando si progetta un sistema biometrico "large-scale".

Un esempio: GOAT e impronte digitali

Perché scarsa qualità intrinseca ?

- Spessore ridotto delle ridge line (lavoratori manuali, anziani, donne asiatiche).
- Dita molto secche o molto umide
- Errata interazione con lo scanner (es. pressione o posizione inadeguate)

La sicurezza dell'intero sistema

- *E' noto che il livello di sicurezza di un sistema è dato dal livello di sicurezza del sottosistema meno sicuro (in OR) che questo include*:
  - E' inutile prevedere meccanismi biometrici complessi e costosi se poi rimangono aperti "buchi di sicurezza" clamorosi in altre parti del sistema.
  - La sicurezza non è solo una questione tecnologica ma spesso legata alle procedure e all'organizzazione.
  - E' spesso più semplice corrompere un funzionario che conosce una chiave che decriptare un file cifrato con tale chiave.
- **Esempi negativi**:
  - Il varco biometrico non supervisionato privo di "tornello" o "sensori di chiusura".
  - L'accesso biometrico a locali dei quali sono comunque diffuse diverse copie di chiavi a utenti comuni …

Dal punto di vista organizzativo ...

- **Comodità d'uso**: l'implementazione del sistema biometrico è **efficace quando arreca agli utenti/amministratori reali vantaggi** in termini di operatività quotidiana:
  - *Dover ricordare molte password è irritante.*
  - *Se queste sono lunghe e difficili la loro digitazione causa frequenti "falsi rifiuti"*
  - *Portare con se le chiavi di diversi uffici è scomodo*
  - *L'amministratore (o il responsabile della sicurezza) che debba abilitare o meno l'accesso fisico a un ambiente deve gestire duplicazioni di chiavi, modifica delle serrature, …*
- In ogni caso è bene **non obbligare** mai gli utenti all'uso della soluzione biometrica (anche per privacy e compatibilità sindacale); semplicemente questi devono apprezzare i vantaggi di questa soluzione rispetto a quella tradizionale.

Amministrazione del sistema

- Ogni sistema con numero elevato di utenti deve essere gestito da un amministratore competente. L'**amministratore** deve occuparsi (tra l'altro) di:
  - Gestire la fase di **enrollment** degli utenti.
  - **Istruire** gli utenti sull'impiego di hardware e software.
  - **Verificare il funzionamento** del sistema e **ottimizzarne** i parametri
  - **Gestire modalità di accesso alternative** per "goat" e utenti riluttanti all'uso della tecnologia.
  - Gestire i **rapporti con il fornitore** della tecnologia, e caricare patch/aggiornamenti quando questi sono disponibili

Start-up e Monitoring

- A seguito della **messa in opera del sistema**, l'amministratore deve inoltre, con l'ausilio dei log di accesso e di colloqui diretti con gli utenti:
  - Verificare che gli utenti riescano ad **accedere regolarmente** al sistema.
  - **Supervisionare i tempi di accesso**, per evitare che alcuni utenti interagendo in modo errato con i dispositivi siano costretti a più tentativi.
  - **Personalizzare i parametri di sicurezza** per utenti diversi.
  - **Rilevare accessi "strani"** sintomatici di false accettazioni.

Le impronte digitali

I sistemi biometrici basati su impronte digitali sono quelli con il mercato più ampio (48%). I principali fattori a favore di questa tecnologia:

- Alto grado di accuratezza e stabilità
- Adatta alle esigenze di sicurezza della maggior parte delle applicazioni (sicurezza logica e fisica)
- Tecnologia matura affidabile e universalmente accettata come valida
- Costi contenuti e dimensioni ridotte
- Semplicità d'uso e crescente grado di accettabilità (11 settembre !)

Fattori di difficoltà:

- Alcuni soggetti possono incontrare difficoltà a causa di intrinseca cattiva qualità dell'impronta
- Non idonea ad alcuni ambienti ostili (polverosi o molto umidi)
- Diffidenza di alcuni utenti per fattori psicologici

Sistemi di acquisizione

- I più comuni dispositivi di acquisizione di caratteristiche biometriche
  - Lettori di impronta connessi ad hardware proprietario o ad una porta del PC (seriale, parallela, USB). Dispositivi integrati in mouse o tastiere.
  - Videocamere, macchine fotografiche o scanner fotografici per il riconoscimento del viso
  - Videocamere sensibili alla luce visibile e all'infrarosso dotate di led emettitori di luce infrarossa per l'acquisizione dell'immagine dell'iride
  - Dispositivi proprietari per la geometria della mano
  - Microfoni o apparecchi telefonici per la voce
  - Tavolette o penne elettroniche per il riconoscimento della firma
- Il sistema di acquisizione è la base di ogni sistema biometrico: basse prestazioni del sistema di acquisizione danno inevitabilmente luogo a basse prestazioni dell'intero SB

Esempio: lettori di impronte

STESSA IMPRONTA ACQUISITA CON DIVERSI PRODOTTI

Valutazione di un lettore
- Risoluzione e area sensibile
- Sicurezza nella comunicazione
- Interfaccia e frame rate

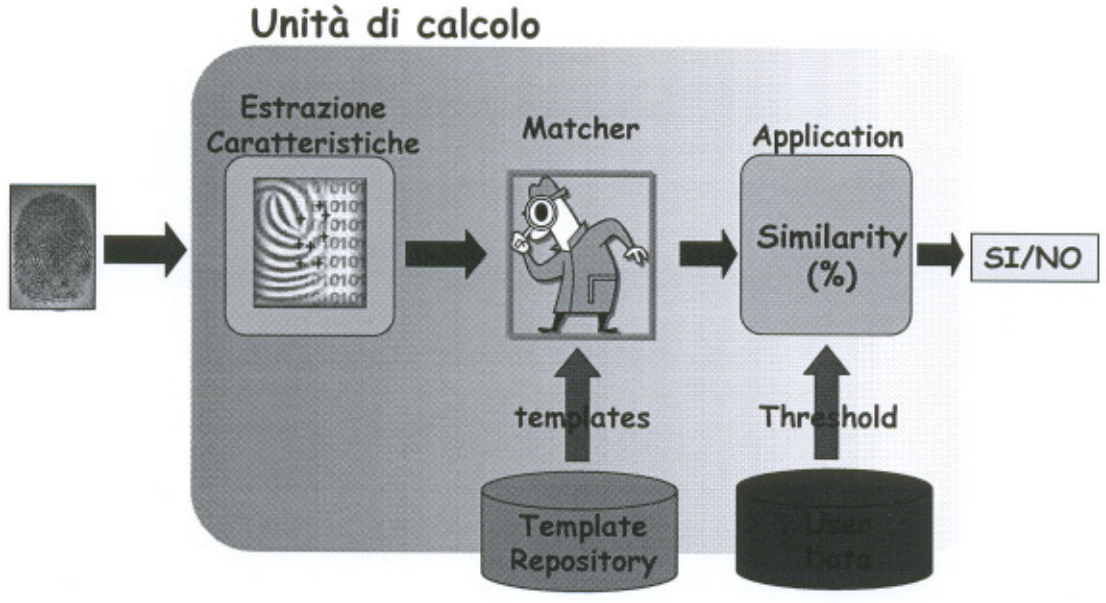
Fonti per valutare un sistema biometrico
- Brochure tecniche (FAR e FRR !)
- Recensioni su riviste IT
- Test eseguiti da organizzazioni accademiche o industriali

Un esempio: lettori ottici e capacitivi
(costi, dimensioni, area sensibile, manutenzione)

La sicurezza di sistemi basati su impronte

- Quando le tecniche biometriche verranno largamente impiegate per la protezione di dati strategici o di transazioni economiche, i tentativi di attacchi contro HW e SW biometrici si moltiplicheranno (hacker, virus, ...).
- Per applicazioni dove la sicurezza e la protezione dei dati biometrici è importante, diffidare ad esempio di:
  - Scanner di impronte che trasmettono "in chiaro", o con banali tecniche di crittografia, le immagini acquisite al PC di controllo.
  - Sistemi di controllo di accesso che pilotano il comando di sblocco di un varco con un semplice impulso elettrico.
- Quali soluzioni adottare:
  - Qualora sia necessario trasferire immagini o template, utilizzare crittografia con chiavi non ripetibili.
  - Tendenza futura sarà quella di realizzare sistemi stand-alone nei quali il "template" non fuoriesce (ancora poco diffusi per motivi di costo).

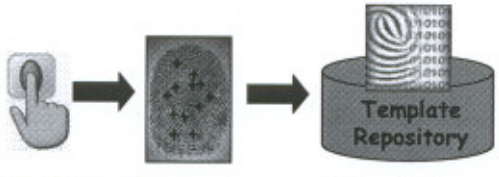
Schema generale di un Sistema Biometrico



La fase di Enroll (1)

- In ogni sistema biometrico ogni utente deve depositare un campione della sua caratteristica biometrica (Enroll)

- Il campione che viene depositato consiste in un template (modello o più in generale "identificativo biometrico") della caratteristica biometrica



- Si tratta di una fase critica: un modello di bassa qualità può degradare drasticamente le prestazioni del sistema (non necessariamente rispetto al singolo utente)

- Viene così creato un Template Repository, che costituisce la base del confronto nella fase di Riconoscimento (1:1 o 1:N)

Template

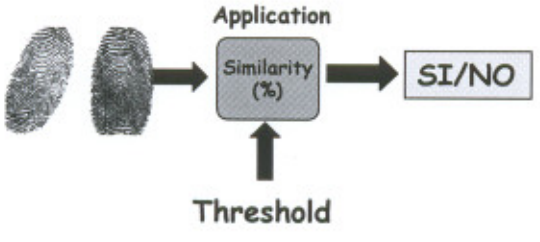
- Il template è generalmente un dato di tipo binario (blob) che contiene le informazioni necessarie al riconoscimento della caratteristica biometrica e quindi dell'utente
- A livello commerciale si ha a che fare con formati proprietari, che difficilmente consentono un'indicizzazione di questo tipo di dato.
- Si parla di template quando vengono estratti dati di tipo numerico dal dato grezzo. In genere dal template non è possibile risalire al dato originale (es. immagine dell'impronta o dell'iride)
- Dimensione del template:
  - E' apprezzabile una dimensione ridotta (riconoscimento e memorizzazione)
  - Al di sotto di determinate dimensioni (variabili per ogni tecnologia) si perde di accuratezza (Es. per le impronte sotto i 2-3 KB)

Impronta digitale	800 - 3000 byte
Mano	10 byte
Volto	1000-2000 byte
Iride	512 byte
Firma	1500 byte
Voce	2000-10000 byte

La soglia di riconoscimento (1)

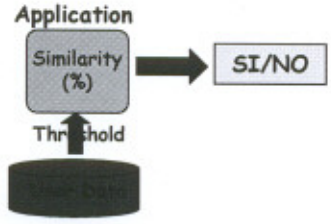
- L'output del motore di riconoscimento è una percentuale di similarità (fase di riconoscimento)

- E' l'applicazione che sovrintende al sistema che deve decidere se la similarità ottenuta dall'utente è sufficiente per considerarlo riconosciuto: soglia di riconoscimento

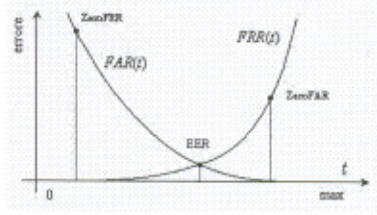


La soglia di riconoscimento (2)

- E' sconsigliato utilizzare un'unica soglia per tutti gli utenti: è opportuno utilizzare una soglia calibrabile per ogni singolo utente



- Considerando le prestazioni del sistema si può scegliere una soglia di default da assegnare ad un utente standard (nel caso di riconoscimento positivo ad esempio zero FAR)



La fase di enroll (2)

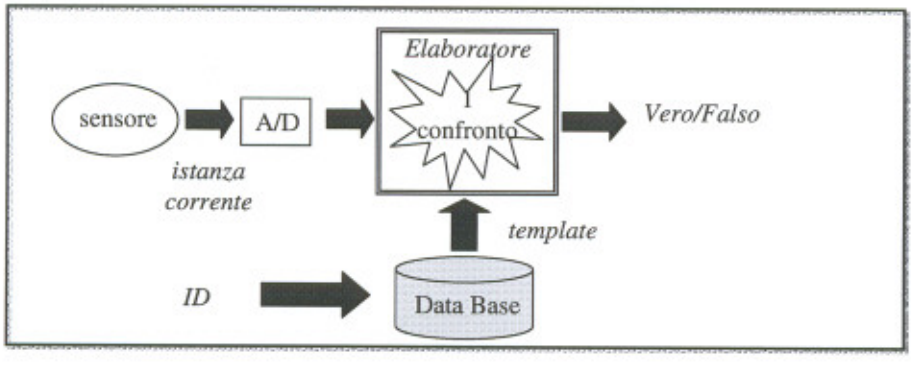
- E' opportuno che la fase di enroll sia supervisionata:
  - Nel caso in cui non sia possibile la supervisione?
  - Quale feedback fornisce il sistema? Esiste un parametro di qualità?
  - E' opportuno verificare immediatamente la similarità ottenuta dall'utente
- Nel caso di impronte di bassa qualità:
  - E' opportuno catturare più copie della stessa impronta
  - Se il sistema lo consente utilizzare i modelli multipli
- Valutare l'opportunità di addestrare gli utenti in fase di primo approccio al sistema
- La fase di enroll è critica. Assicurarsi che il dispositivo venga utilizzato correttamente (almeno in questa fase)

La fase di riconoscimento

- L'output del motore di riconoscimento è una percentuale di similarità:
  - Verifica (1:1) quanto l'impronta è simile a quella del modello registrato dal sistema
  - Identificazione (1:N) quanto l'impronta è simile al modello più simile registrato
- Se l'utente supera la soglia di riconoscimento associata è considerato riconosciuto (SOLITAMENTE L'ALGORITMO ESCE ALL'IDENTIFICAZIONE DEL PRIMO MATCHING TROVATO - PER DIMINUIRE I TEMPI) ⇒ MEGLIO LA VERIFICA!
- La soglia da utilizzare dipende anche dal tipo di utenti e dall'ambiente in cui il sistema opera
  - Utenti con caratteristiche di bassa qualità
  - Possono sussistere fattori che possono degradare le prestazioni del sistema di acquisizione
  - Fattori ambientali. L'ambiente è controllato?

Verifica

- Il sistema verifica se l'utente è chi dice di essere (1:1)
- L'utente specifica la propria identità prima del riconoscimento (Username, PIN, SmartCard)



Verifica (2)

- **L'algoritmo di verifica 1:1 in pseudo codice**

```
Boolean VerifyUser(userId)
Begin
        MODEL userModel;
        NUMBER userTh, similarity;

            userModel = GetUserModel(userId)
            userTh = GetUserThreshold(userId)
            Bio_LoadUserModel(userModel)
            Bio_Acquire ( )
            similarity = Bio_Matching()
            if (similarity > userTh)
              return TRUE
            else
              return FALSE
End
```

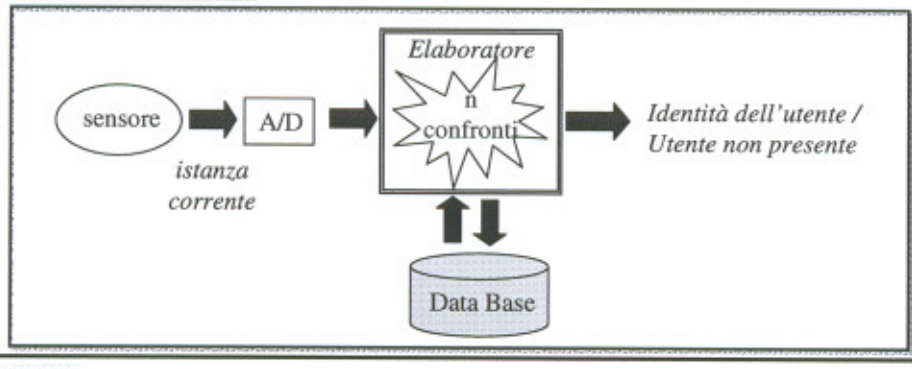
Acquisizione: accesso al dispositivo

Caricamento del modello

Motore di riconoscimento

Identificazione (1)

- Il sistema verifica che l'utente faccia parte di una insieme di utenti (white/black list): 1:N
- L'utente non specifica la propria identità, il template non è memorizzato su un token mnemonico. L'utente fornisce solamente la propria caratteristica biometrica per il riconoscimento.
- L'utente è identificato se supera la soglia del modello più simile alla caratteristica fornita



Identificazione (2)

- In caso di un numero di utenti elevato è fortemente sconsigliato utilizzare l'identificazione (1:N). Indipendentemente delle capacità di memoria e del tempo computazionale vi è un problema di sicurezza.

- La probabilità di false accettazioni cresce linearmente con il numero di utenti

$$FAR_{1:N} = 1-(1-FAR_{1:1})^N \approx N \cdot FAR_{1:1}$$

- Supponiamo un sistema calibrato per avere un $FAR_{1:1} = 0{,}001\ \%$. Operando in identificazione su un bacino di 10.000 utenti si avrebbe:

$$FAR_{1:N} = 0{,}1 = 10\%$$

Una volta su dieci si ha una falsa accettazione!!!

Identificazione (2)

```
Boolen IdentifyUser(out USERID uid, out  NUMBER sim)
Begin
        MODEL userModel;
        NUMBER userTh, similarity, maxSim, maxTh;
        USERID maxUid;

        Bio_Acquire ( )
        userId = GetFirstUser();
        While (userId <> NULL)
            userModel = GetUserModel(userId)
            userTh = GetUserThreshold(userId)
            Bio_LoadUserModel(userModel)
            similarity = Bio_Matching()
            if (similarity > maxSim)
               maxSim = similarity
               maxUid = userId
            endif
            if (similarity > userTh)
               uid = userId
               sim = similarity
               return TRUE
            End If
            userId = GetNextUser()
        End While

        Uid=maxUid
        Sm=maxSim
        return FALSE
End
```

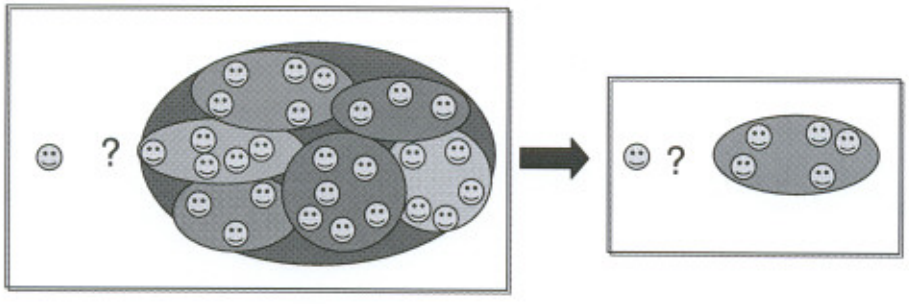
- L'utente viene identificato se esiste un modello sufficientemente simile a superare la soglia associata

- Se nessun modello supera la soglia associata l'utente NON viene riconosciuto ma viene restituito l'utente più simile trovato

- L'identità dell'utente è considerata quella del PRIMO trovato modello che consente di superare la soglia

Dettagli implementativi

- Utilizzando un identificativo non necessariamente univoco si può operare una identificazione 1:N con N piccolo (empiricamente < 100).



- Si elimina in questo caso il problema di false accettazioni o di scambi di identità

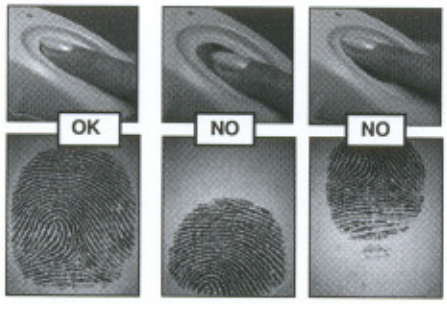
Ex: MESE di NASCITA => N/12 // la ricerca è più performante
DATA di NASCITA => N/30

Gestione del dispositivo

- Per evitare di sprecare risorse dell'host alcuni dispositivi sono in grado di operare in modalità di rilevazione automatica

- Ogni dispositivo ha un tempo di vita limitato. Per aumentare tale tempo di vita è opportuno evitare un utilizzo in acquisizione continua, ma limitarne l'uso ai soli casi di probabile necessità.

- Assicurarsi che il dispositivo venga utilizzato correttamente



Mancanza di standard

La maggior parte dei S.B. oggi utilizzano **tecniche proprietarie** relativamente a:

- Estrazione delle feature
- Metodo di confronto (match)
- Lunghezza e contenuto dei modelli (Header, Metodo di encryption)
- Modalità di memorizzazione dei modelli
- Comunicazione fra software, dispositivi biometrici e applicazioni

Conseguenze:

- Applicazioni che integrano funzionalità biometriche sono strettamente legate ad una particolare tecnologia
- Il passaggio a una diversa tecnologia biometrica richiede uno sforzo implementativo analogo a quello già fatto in precedenza
- Quando l'interoperabilità è fondamentale (es. recente pronunciamento della Commissione Europea in materia di immigrazione), si utilizza **l'immagine della caratteristica invece del modello**...

Standard per sistemi biometrici

Cosa standardizzare?

- È improbabile che **gli algoritmi** con cui vengono estratte e confrontate le feature biometriche possano diventare "aperti" e "intercambiabili", dato che sono alla base della **proprietà intellettuale** della maggior parte delle aziende del settore
- Inoltre definire a priori un set statico di feature da utilizzare è un freno per la ricerca (che potrebbe trovare nuove soluzioni con feature diverse)
- Gli sforzi attuali di standardizzazione riguardano principalmente:
  - API (Application Program Interface)
  - Requisiti in termini di sicurezza (crittografia nei dati memorizzati, nelle comunicazioni)
  - Formato di memorizzazione dei modelli

Gli Standard (1)

- SC37 (ISO/IEC JTC1 SC37)
  - Comitato formato dall'ISO (giugno 2002) che prevede diversi gruppi di lavoro (WG) per la standardizzazione della biometria. Elemento di novità è il un gruppo di lavoro "non tecnico" (WG6) che si occupa degli aspetti giuridici e sociali.
- BioAPI (BioAPI Consortium, 1998)
  - Insieme di API per la comunicazione fra applicazione e dispositivi biometrici
  - Offre funzionalità di enrollment, verifica, identificazione, acquisizione
  - Biometric-indipendent e OS-indipendent
  - I template restano però in formato proprietario, quindi non intercambiabili
- CBEFF (Common Biometric Exchange File Format)
  - Definisce un formato standard per i template
  - Header con campi obbligatori
  - Lo standard non fornisce interoperabilità a livello di dispositivi o di match, ma consente lo scambio di informazioni biometriche fra componenti dello stesso sistema o sistemi diversi

Gli Standard (2)

- ANSI X9.84 (2001)
  - X9 è l'organizzazione responsabile per lo sviluppo di standard tecnici per le aziende operanti nel settore finanziario
  - standard relativo a sicurezza e crittografia per dati biometrici e SB (Trasmissione di dati, Sicurezza HW, Autenticazione dipendenti e clienti)
  - Si noti che IBIA (International Biometric Industries Association) è l'interlocutore ufficiale per il coordinamento con BioApi e CBEFF.
- ICAO (International Civil Aviation Organization)
  - Attiva fin dal '80 per la standardizzazione dei passaporti
- ISO 7816-11 (sviluppato da ISO/IEC JTC1/SC177WG4)
  - Utilizzo di ISO/IEC 7816-4 ai fini del match on card in riferimento ai dati individuati da CBEFF (e problematiche di sicurezza)
- ANSI/NIST-ITL 2000
  - Definisce il contenuto, il formato e le unità di misura per lo scambio di impronte digitali, impronte del palmo, foto segnaletiche, tatuaggi e cicatrici

Controllo accesso a dati

- Sviluppo di uno strumenti che consente di proteggere dati critici mediante riconoscimento biometrico
  - Archivi
  - Applicazioni che trattano dati riservati
- Esempio: FxSecure
  - Paradigma grafico analogo a WinZip
  - Oltre alla password l'archivio è protetto da un multi-modello che contiene fino a un massimo di 3 impronte
  - Si può quindi creare un contenitore sicuro con cui scambiarsi i dati

- Considerazioni
  - In caso di reverse engineering la sicurezza è analoga a quella offerta da una classica protezione con password. Dal modello in nessun modo si può risalire all'impronta.
  - Evita agli utenti di dover ricordare numerose password spesso facili da indovinare (o da dimenticare).

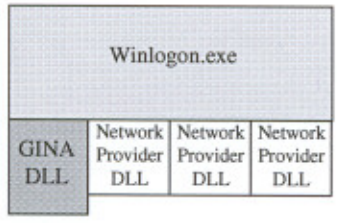
Logon a sistemi

- Una delle più comuni applicazioni della biometria nell'ambito della sicurezza logica è il logon a sistemi. Oltre al classico accesso mediante username e password si affianca l'accesso mediante username e caratteristica biometrica
- Si tratta di una verifica 1:1. Con il suo username l'utente specifica la propria identità. Il sistema verifica l'identità dell'utente confrontando l'impronta fornita "on-line" con quella registrata
- Per garantire a tutti gli utenti (anche ai GOAT) l'accessibilità al sistema è opportuno consentire l'utilizzo alternativo di una password. Le password devono essere lunghe e complicate ed essere modificate con una certa frequenza per non lasciare clamorosi buchi di sicurezza.
- E' inoltre fondamentale garantire la protezione dei template.
  - Sia per quanto riguarda la loro registrazione
  - Sia per eventuali transiti in rete

Logon a Windows

■ Accesso locale a sistemi Windows NT/2000/XP. Winlogon.exe è un componente di Windows NT/2000/XP che fornisce il supporto per un logon interattivo. Il modello su cui è progettato consiste di tre componenti:

- L'eseguibile Winlogon.exe
- Una interfaccia grafica di autenticazione (Graphical Identification and Authentication dynamic-link library) GINA.DLL
- Uno o più Network provider



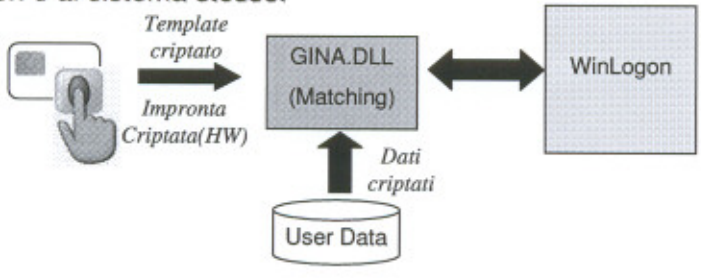
■ GINA è sostituibile. Questa DLL implementa la politica di autenticazione e si occupa di interagire con l'utente per tutte le operazioni di identificazione. Sostituendo tale modulo è possibile implementare un accesso biometrico a Windows

Esempio: FxLogon

■ Tramite il programma di gestione (UserManager), accessibile ai soli utenti amministratori, è possibile gestire i permessi di accesso degli utenti previsti da Windows. I tipi di accesso sono:

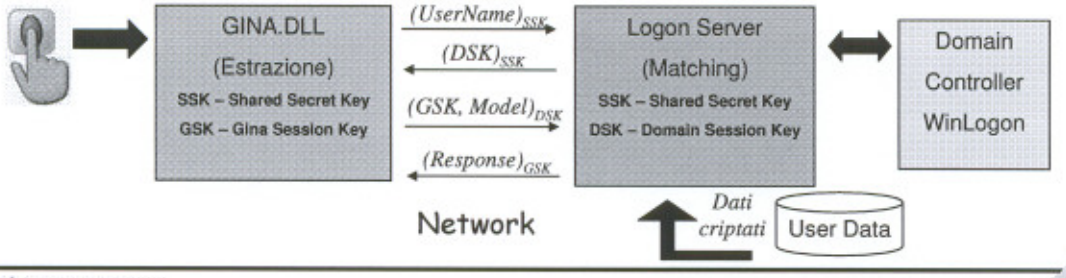
- Password
- Impronta memorizzata su PC locale
- Impronta memorizzata su SmartCard (BioCard)
- mediante SmartCard (AccessCard)

■ I dati relativi agli utenti (permessi, template(*), ecc) vengono criptati e memorizzati in una particolare directory di sistema, accessibile solo agli amministratori e al sistema stesso.



Logon a domini

- In questo caso è necessario un componente aggiuntivo che si occupa di gestire l'autenticazione sul Domain Controller: logon Server
- Poiché i dati dell'utente transitano in rete è necessario adottare le precauzioni necessarie a garantire la sicurezza dei dati. Ad esempio chiavi di sessione, challenge-response, crittografia asimmetrica, certificati e firma digitale
- Considerazioni:
  - L'enroll è eseguito centralmente su Logon Server
  - Il database dei modelli è centralizzato
  - Il riconoscimento è effettuato in remoto da Logon Server
- Esempio: FxLogon Server



Accesso/Riconoscimento remoto

- Applicazioni client/server che consentono di fornire credenziali agli utenti remoti che si collegano al sistema
- La presenza fisica dell'utente è comunque necessaria nella fase di enroll
- Dove è registrato il template
  - Lato server (DB centralizzato) – E' necessario adottare tutti gli strumenti per garantire la sicurezza dei template in transito (SSL, mutua autenticazione, crittografia forte)
  - Token sicuro (Es. SmartCard) – Sono comunque necessari tutte le precauzioni ma non vi è il rischio di furto del template (che a differenza della password non è revocabile)
- In questo caso la fase di enroll ha un costo più elevato. E' perciò necessario eseguirlo correttamente e prevedere metodi di accesso alternativi
- Esempio: ActiveX con template su SmartCard

Quadro normativo sulla Biometria (1)

- L' "elemento biometrico" come identificativo della soggettività fisica non è ad oggi regolato dall'ordinamento italiano. Uniche eccezioni
  - protezione dei dati personali (d.l.vo 196/2003)
  - alcuni principi giuridici applicabili per alcuni aspetti (inviolabilità della libertà personale, responsabilità civile e penale per l'utilizzo di tali tecnologie per scopi illeciti, colposi o dolosi)

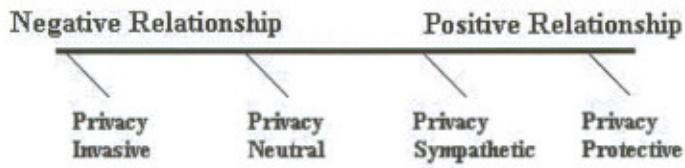
- L' elemento biometrico è comunque citato in diversi corpi normativi emanati dal 2000 in poi
  - Art. 36 dPR 443/2000 (Carta d'Identità elettronica – CIE –)
  - d.l.vo 196/2003 (protezione dei dati personali)
  - d.l.vo 117/2004 (Carta nazionale dei servizi – CNS –)

Quadro normativo sulla Biometria (2)

- Alcune indicazioni sono state fornite da organizzazioni ed enti sovranazionali con il carattere di linee guida e proposte:
  - Work Party art.29 (WP 29 - direttiva 46/95 - Gruppo dei Garanti Europei): pone attenzione sulla natura delicata di alcuni dati biometrici.
  - Nell'agosto del 2004, WP 29, rilascia un documento in cui viene analizzata la proposta di includere dati biometrici nei passaporti dell UE mettendo in luce alcune preoccupazioni: non eccedenza delle finalità, accesso di terzi, sicurezza dell'enrollment, adozione DB centralizzati
  - Consiglio Europeo ("Draft guiding principles for protection of personal data with regard to smart cards", 2003). Incentrato sull'utilizzo delle SC ma coinvolge in molti casi la biometria
  - OECD (Organization for Economic and development) e ICAO (International Civil Aviation Organization)

Sistemi Biometrici e Privacy

- I S.B. sono basati sulla misurazione di caratteristiche fisiche o comportamentali delle persone
  - Quali sono le problematiche relativamente alla privacy?
- Possibile relazione S.B. ↔ Privacy



Sistemi Biometrici e Privacy (2)

- È possibile ricostruire a partire dal modello alla caratteristica biometrica da cui è stato ottenuto?
  - Per molti tipi di modelli (es. minutiae, IrisCode) non è possibile → maggiori garanzie in fatto di privacy
  - In generale dipende dalle feature usate per il modello: in alcuni casi è possibile!

Considerazioni sulla privacy

- L' elemento biometrico come pericolo della privacy:
  - Function creep: i dati vengono utilizzati per scopi diversi de quelli dichiarati
  - Tracciamento o dati raccolti senza il consenso

Oltre alla diffidenza verso "l'invasività" di alcune tecnologie biometriche, tali elementi rappresentano il principale motivo del basso grado di accettazione di certi utenti verso la biometria

- L' elemento biometrico come protezione della privacy:
  - Limita i furti di identità
  - Limita l'accesso ai dati personali

Si tratta di principi riconosciuti dal codice sulla privacy, che pone però fortemente il problema della protezione dei dati biometrici, che se "rubati" non possono essere sostituiti

Nel progettare un sistema biometrico è necessario tenere sempre in alta considerazione l'elemento umano da cui spesso dipende il successo dell'implementazione

Considerazioni sulla privacy (2)

- Codice di protezione dei dati personali (D.Lgs. 196/2003)
  - Il dato biometrico (anche il template) è un dato personale in quanto relativo ad una persona fisica *"identificata o identificabile"*
  - Si considera invece un dato sensibile un dato personale idoneo a rilevare l'origine razziale, etnica, convinzioni religiose, opinioni politiche o orientamento sessuale (il volto è un dato sensibile)
  - L'applicabilità della norma è più probabile in quei sistemi che trattano dati grezzi anziché modelli (da cui in genere non si risale al dato grezzo)
- I principi espressi relativamente al trattamento biometrico (TB):
  - Liceità
    - Soggetti pubblici: funzioni istituzionali
    - Soggetti privati: previo consenso e adempimenti di legge
  - Necessità - il TB non è applicabile se la finalità può essere raggiunta utilizzando dati anonimi o codici identificativi
  - Proporzionalità – solo se l'identificazione deve essere certa. Non ci deve essere sproporzione fra finalità e mezzo utilizzato
  - Finalità – scopi determinati, espliciti e legittimi (informativa all'utente)
- Adempimenti: notifica al Garante, informativa e consenso, documento programmatico per la sicurezza

Caso di studio: Super Bowl

- Il Super Bowl 2001
  - Fu un fallimento non tanto dal punto di vista delle prestazioni della tecnologia biometrica adottata, quanto da quello delle reazioni dei cittadini

> "The public relations disaster for biometrics [in 2001] was the surreptitious use of automatic facial recognition at the most popular sporting event in the U.S."
>
> Dr. James Wayman

  - Benché le telecamere fossero visibili, non era stato chiarito che sarebbe stato usato un sistema automatico di riconoscimento
  - Non era stato chiarita la finalità delle raccolta delle immagini (eliminate al termine dell'evento o mantenute?)
  - Non erano state chiarite le modalità con cui il sistema avrebbe deciso quali persone segnalare alle forze dell'ordine

Caso di studio: accesso fisico alle banche

In molti casi il riconoscimento biometrico è utilizzato solo come deterrente.

La caratteristica biometrica viene acquisita e memorizzata (non avviene autenticazione della persona).

In caso di necessità l'immagine viene messa a disposizione dell'autorità giudiziaria.

- Una possibile soluzione
  - I dispositivi di acquisizione utilizzati trasferiscono al PC di controllo solo immagini criptate con crittografia simmetrica chiavi 128-bit.
  - L'istituto bancario non dispone delle chiavi di decifrazione delle immagini, che sono invece a disposizione dell'autorità giudiziaria.

Caso di studio: accesso fisico alle banche (2)

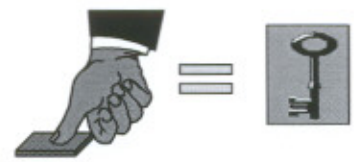
Provvedimento del Garante per la Privacy (Ottobre 2001)

- L'utilizzazione dei sistemi di rilevazione cifrata delle impronte digitali deve essere riferita a situazioni di rischio, valutate dall'istituto bancario anche sulla base di concordanti valutazioni da parte dei locali organi competenti per l'ordine e la sicurezza pubblica.
- La rilevazione delle impronte non può dar luogo ad alcuna "schedatura" da parte degli istituti di credito che, quindi, non potranno costituire alcuna banca dati con le informazioni raccolte. L'accesso agli sportelli deve avvenire solo su base volontaria e consensuale: in caso di indisponibilità dell'utente a sottoporsi alla rilevazione criptata, dovrà essere lasciata ai responsabili delle filiali la valutazione di far accedere comunque l'utente all'istituto bancario con eventuali ragionevoli cautele, astenendosi da qualsiasi comportamento vessatorio nei suoi confronti.
- Le informazioni relative alle impronte devono essere rigorosamente protette da sistemi di cifratura automatica sin dal momento della loro acquisizione. Non saranno quindi immediatamente riconducibili a persone e l'eventuale associazione alle immagini, rilevate con telecamere, potrà avvenire solo dopo la decrittazione.
- Soltanto l'autorità giudiziaria o di polizia, e solo nell'ambito di indagini connesse alla commissione di reati, potrà decifrare ed avere accesso alle informazioni. Il personale della banca non potrà avere in alcun modo accesso "in chiaro" alle informazioni cifrate.
- I dati cifrati devono essere integralmente cancellati dopo una settimana.
- Gli istituti di credito devono fornire all'ingresso indicazioni chiare che avvertano gli utenti della presenza dei sistemi di rilevazione e della possibilità di accedere in modo diverso ai locali.
- Non è consentito alcun sistema di indicizzazione dei dati o di riconoscimento facciale.

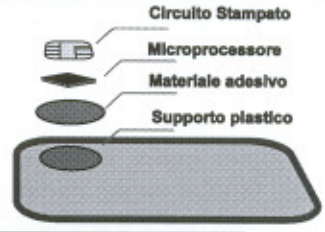
Sicurezza e privacy: biometric hashing

Utilizzare l'impronta come chiave per cifrare un messaggio senza dover memorizzare il modello dell'utente:

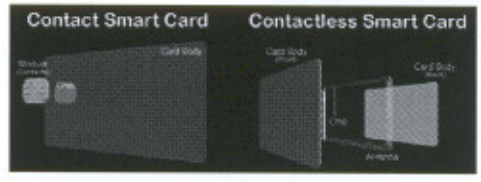
- A tal fine viene utilizzata una funzione hash non invertibile "guidata" dalle informazioni biometriche.
  - In pratica ciò è quanto accade nei sistemi operativi dove le password degli utenti non vengono memorizzate "in chiaro", ma viene memorizzato solo un loro hash
  - Nella biometria la cosa è molto più complessa, perché la chiave non è "costante" (come una password) ma *varia ogni volta* che viene acquisita
- La ricerca in questa direzione è piuttosto attiva; oggi non esistono ancora sistemi sufficientemente robusti (ovvero con accettabili frequenze di falsi rifiuti).



La tecnologia Smart Card



- Dispositivo sicuro:
  - Dal punto di vista fisico ("spoliazione")
  - Dal punto di vista logico (accesso controllato)
  - Funzionalità crittografiche
- Tipo di carte:
  - Memory card e chip card
  - Contact e contactless



- Standard:
  - ISO 7816 1/2/3/4
  - PC/SC
  - PKCS
  - Non vi è standardizzazione a livello di COS (SISTEMA OPERATIVO)

Smart Card e Biometria

- Alla luce dei problemi di privacy e di accettabilità, grazie alla sicurezza e funzionalità offerte dalle SC, appare naturale la combinazione di tali dispositivi con la tecnologia biometrica:
  - innalzamento della sicurezza: SC è un supporto sicuro(aspetto sicurezza)
  - Il dato biometrico è nella esclusiva disponibilità dell'utente (aspetto privacy)
  - Maggiore interoperabilità con costi minori e minore ridondanza dei dati
- La biometria non implica necessariamente maggiore sicurezza: è necessario proteggere l'identificativo biometrico (Smart Card e crittografia)
- Considerazioni sulla memorizzazione dell'identificativo biometrico
  - E' opportuno memorizzare il template (dimensioni e non reversibilità del template)
  - Considerare la possibilità di cifrare il template
  - Attenzione ai tempi di estrazione del template dalla carta (dimensioni e crittografia)
  - Un elemento critico è costituito dal PIN per l'accesso al dato biometrico (soliti problemi delle password). E' possibile utilizzare il dato biometrico per accedere alla carta (in alternativa al PIN)?

Match on Card

■ Tecnologia innovativa che consente di utilizzare la potenza di calcolo delle Smart Card per eseguire l'operazione di matching direttamente sul chip della carta

■ Caratteristiche
- Massima sicurezza del template che non può essere "rubato" (Se non in fase di enroll)
- L'estrazione delle caratteristiche è eseguita o dal computer o dal device (es. lettore di impronta), ma non dalla carta
- Il template è di dimensioni generalmente ridotte

■ Problematiche
- La limitata potenza di calcolo delle chip card porta ad una semplificazione degli algoritmi di riconoscimento
- Tale semplificazione porta a problemi di affidabilità dovuti a falsi rifiuti

Match on Device

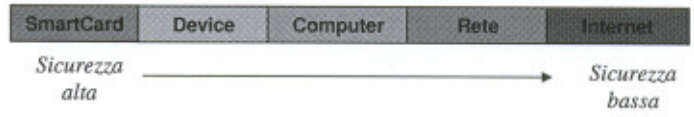
■ Alcuni dispositivi di acquisizione hanno la potenza di calcolo necessaria ad eseguire le operazioni di estrazione delle caratteristiche e le operazioni di matching. Tali dispositivi prendo il nome di "Stand-Alone"

■ Caratteristiche
- Tali dispositivi sono generalmente integrati con un lettore di Smart Card
- Il template che si trova sulla carta non deve essere inviato al computer per il matching.
- Se il dispositivo ha sufficiente potenza di calcolo, non sono necessarie semplificazione all'algoritmo di riconoscimento. In questo caso le prestazioni sono identiche a quelle del classico *match on computer*

■ Problematiche
- Il template deve comunque essere recuperato dalla carta, per cui in teoria è possibile la sua intercettazione (anche in questo caso dovranno essere utilizzate tecniche crittografiche per la comunicazione con la carta)

Smart Card: dove avviene il matching

■ Sicurezza degli ambienti.



■ **Match on computer.**

- La carta è solo un supporto di memoria sicuro. Il confronto avviene sul sistema di elaborazione
- Il template è esposto a virus o cavalli di troia che possono intercettarlo e sostituirlo per il riconoscimento
- Utilizzando la crittografia si è esposti al caso di reverse engineering dell'applicazione che si occupa di decifrare il template

■ **Match on device.**

- La carta è solo un supporto di memoria sicuro. Il confronto avviene sul dispositivo di acquisizione Stand-Alone
- Remota possibilità di intercettazione del template in caso di reverse engineering del firmware che si occupa di recuperalo e decifrarlo (si suppone criptato)

■ **Match on card.**

- La carta è una vera e propria unità di calcolo che sovrintende al matching. Il template non esce dalla carta
- Supponendo gli stessi pericoli del caso precedente, il template corrente può essere sostituito per il riconoscimento.

La firma digitale: quadro generale

■ Definizioni (Direttiva 1999/93/CE e DPCM 08/02/1999 e 13/01/2004)

- Firma elettronica (FE): insieme dei dati elettronici utilizzati come metodo di autenticazione informatica di documenti elettronici
- Firma elettronica avanzata (FEA): FE che garantisce la connessione univoca al firmatario e la sua univoca identificazione, che consente di rilevare se i dati firmati siano stati modificati.
- Firma elettronica qualificata (FEQ): FEA basata su un certificato qualificato, e creata mediante un dispositivo sicuro.
- Firma digitale (FD): FEQ con particolari caratteristiche di attendibilità derivanti dal certificatore (certificatore accreditato)

■ La firma digitale ("firma forte") è giuridicamente equivalente alla firma autografa. Le sue caratteristiche sono:

- Certificato basata su una coppia di chiavi asimmetriche generate con particolari modalità (all. I Direttiva)
- Riconducibile a un certificatore accreditato (all. II Direttiva)
- Generata mediante un dispositivo sicuro (all. III Direttiva)

■ Anche alle "firme deboli" è garantita dignità giuridica ma con grado probatorio valutabile in sede di giudizio

La firma digitale con Smart Card

- Il kit di firma:
  - Smart Card rilasciata dal un Certificatore accreditato (ad oggi sono 14 i certificatori a cui potersi rivolgere) contenente il certificato di firma (chiave pubblica/chiave privata)
  - Lettore di Smart Card.
  - Il software in grado di interagire con la carta.

Il programma di firma interagisce con la carta mediante interfaccia definita da PKI (Public Key Infrastructure). L'interfaccia PKI viene implementata sfruttando interfacce standard delle carte che danno accesso alle loro funzionalità crittografiche: PKCS#11 e CSP

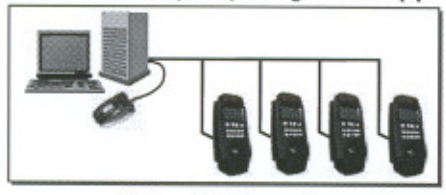
- La procedura di firma:
  - Mediante il software di firma si seleziona il documento da firmare
  - Digitando il PIN di accesso alla carta viene avviata la procedura di firma
  - La carta verifica il PIN e avvia la procedura di firma.
  - Il documento firmato può essere salvato (.p7m)

La firma digitale ad attivazione biometrica

- La firma digitale basata su Smart Card fonda la sua sicurezza sulla segretezza del PIN. La verifica d'identità del firmatario è basata su "qualcosa che il firmatario conosce"
  - Nel caso di PIN rubato (o come spesso accade prestato) uno strumento potente (a livello legale) come la firma digitale può avere conseguenze molto gravi
- La tecnologia Match on Card non è ad oggi sufficientemente matura per consentire il grado di affidabilità che l' applicazione "Firma Digitale" richiede.
- Sfruttando la tecnologia Match on Device si può costruire un'interfaccia PKI che combini sicurezza della carta e affidabilità del riconoscimento biometrico senza rischio per il template
  - In questo modo si potrebbe attivare la procedura di firma mediante verifica (1:1) biometrica
  - Il template è al sicuro all'interno della carta
  - La verifica biometrica garantisce che il firmatario, e nessun altro, abbia effettivamente firmato il documento

Cenni sulla sicurezza fisica

■Controllo accessi: sistema per il controllo dell'accesso fisico degli utenti a determinati locali o ambienti (aeroporti, laboratori, CED, uffici, abitazioni, auto). Prevede l'utilizzo di attuatori (relè) da gestire opportunamente.



■Controllo presenze (Time&Attendance): applicazioni il cui scopo è attribuire un orario certo alla presenza degli utenti (es. dei dipendenti sul luogo di lavoro).

- Indubbi vantaggi offerti dalla biometria.
- Possibilità di utilizzo di sistemi multibiometrici

■Sistemi antirapina: sistemi che mirano a garantire l'acquisizione di una caratteristica biometrica a scopo cautelativo e preventivo (Banche)

- Filosofia diversa rispetto ai SB. Non è previsto alcun riconoscimento
- Sistemi multibiometrici
- Stretti vincoli dovuti alla legge sulla privacy

Un Esempio: FX3 SDK (1)

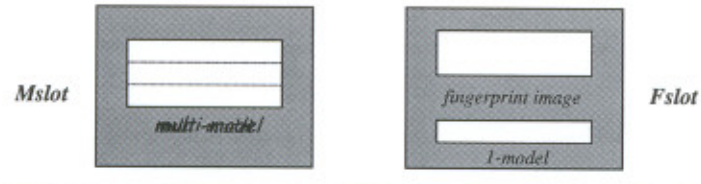
■ FX3 SDK è il software di sviluppo dello scanner ottico di impronte FX2000 (Biometrika). Le funzionalità si suddividono in due gruppi:

- Gestione dello scanner Fx2000
- Motore di riconoscimento

■ Il motore di riconoscimento prevede l'utilizzo di modelli singoli o multipli. In nessun modo dal modello è possibile risalire all'immagine dell'impronta. Il modello racchiude informazioni relative a :

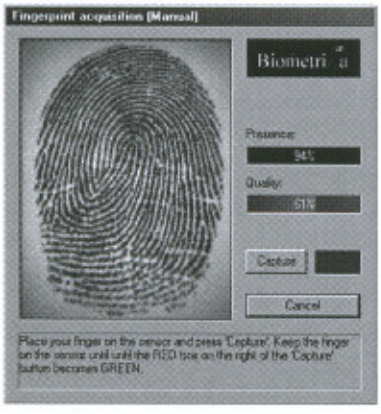
- Minuzie
- Orientamento delle creste epidermiche
- Densità delle creste epidermiche
- Lunghezza delle creste epidermiche

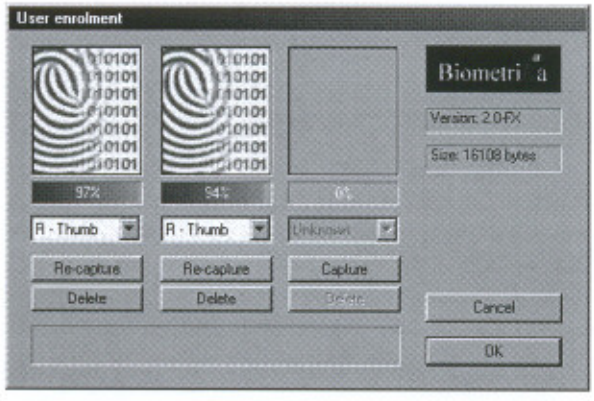
■ Strutture dati:



Un Esempio: FX3 SDK (2)

- Interfacce utente:
  - AGI (Acquisition Graphical Interface)
  - EGI (Enrollment Graphical Interface)





Un Esempio: FX3 SDK (3)

- Funzionalità di Acquisizione (Slot F)

ACQUISITION	**FX3_AcquireFingerprintOffLine**	**I** : HWND hwnd **I** : int x **I** : int y **O**: float* q	Load image into F	Opens AGI and capture a new fingerprint image. Acquisition is supervised (user must press a button to confirm).
	FX3_AcquireFingerprintOnLine	**I** : HWND hwnd **I** : int x **I** : int y **O** : float* q **I** : int det_th **I** : float timeout **I** : float delay	Load image into F	Opens AGI and capture a new fingerprint image. Acquisition is unsupervised (fingerprint presence is auto-detected).

Un Esempio: FX3 SDK (4)

■ Autodetection e selezione scanner attivo

SCANNER	**FX3_FX_EnterAutoDetection**	-	-	Enters AutoDetection mode
	FX3_FX_Presence	**O**: BYTE* Presence	-	Gets finger presence
	FX3_FX_ExitAutoDetection	-	-	Leaves AutoDetection mode
	FX3_FX_SetActiveScanner	**I**: int* ID	-	Sets as active scanner that identified by ID
	FX3_FX_GetActiveScanner	**O**: int* ID	-	Gets the ID of the active scanner

Un Esempio: FX3 SDK (5)

■ Enroll (Slot M)

ENROLL	**FX3_CreateModel**		Enrolls the image in F and stores the corresponding 1-model in F. Image in F is destroyed.	Performs enrollment of a fingerprint image. The image in F is altered and cannot be re-used after enrollment
	FX3ENR_Enrollment	**I** : int enrol_mode **I** : char* Fpathname **I** : BYTE* Mmodel **O**: int* Msize **I** : int det_type **I** : int det_th **I** : float delay **I** : float timeout **I** : int x **I** : int y	Destroys F contents.	Performs enrollment though EGI graphical interface.

Un Esempio: FX3 SDK (6)

- I/O (Slot M e F)

I / O	**FX3_LoadFingerprintFromFile**	**I** : char* pathname **O**: float* q	Loads image into F	
	FX3_SaveFingerprintToFile	**I** : char* pathname	Stores the image from F	Stores a fingerprint image to file (native format).
	FX3_SaveFingerprintFullImageToFile	**I** : char* pathname	Stores the image from F after normalization	
	FX3_LoadFingerprintFromModelOnFile	**I** : char* pathname	Loads a 1-model in F	Loads a 1-model from file in F.
	FX3_LoadModelFromFile	**I** : char* pathname	Loads a model in M	Loads a model from file in M.
	FX3_SaveModelToFile	**I** : char* pathname **I** : int mode **O**: int* num	Stores the 1-model enrolled in F	Stores to file the 1-model enrolled in F by FX3_CreateModel

Un Esempio: FX3 SDK (7)

- Matching (Slot M e F)

MATCH	**FX3_Matching**	**I** : float mins **O**: float* similarity	Alters the image in F, which cannot be saved after matching.	Matches the model in M against the fingerprint image or 1-model in F.