La sicurezza dei dati

Il codice della privacy /1

- Entra in vigore il 1 gennaio 2004 il decreto legislativo n. 196 del 30 giugno 2003, denominato *"Codice in materia di protezione dei dati personali"*
- compone in maniera organica le innumerevoli disposizioni relative, anche in via indiretta, alla privacy, riunisce in unico contesto la legge 675/1996 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti in questi anni, e contiene anche importanti innovazioni tenendo conto della "giurisprudenza" del Garante e della direttiva Ue 2000/58 **sulla riservatezza nelle comunicazioni elettroniche**.

Il codice della privacy /2

- **Spamming**
  L'invio di messaggi attraverso sistemi automatizzati (*Sms*, *Mms*, fax, posta elettronica) richiede il consenso degli interessati. Il cliente deve essere informato della possibilità di opporsi a "messaggi indesiderati".
- **Internet,** videosorveglianza, direct marketing, "centrali rischi" private
  Per settori così delicati il codice conferma la previsione di appositi codici deontologici che fissano regole specifiche

I dati

- **Dato personale**
  Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- **Dato identificativo**
  Dato personale che permette la diretta identificazione dell'interessato

I dati

- **Dati sensibili**
  Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale
- **Dati giudiziari**
  Dati personali idonei a rivelare i provvedimenti di cui al casellario giudiziario,anagrafe sanzioni amministrative dipendenti da reato, carichi pendenti (art. 3 ....) e qualità di imputato o di indagato

I ruoli

- **Titolare**
  la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
- **Responsabile**
  la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- **Incaricato**
  le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- **Interessato**
  la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Il "trattamento" dei dati

- ..si intende per "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati

Principio di necessità

- **Art. 3. Principio di necessità nel trattamento dei dati**

  I **sistemi informativi** e i **programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali** e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Titolo V – Capo I – Misure di Sicurezza

- **Art. 31. Obblighi di sicurezza**
  I dati personali oggetto di trattamento sono custoditi e controllati, **anche in relazione alle conoscenze acquisite in base al progresso tecnico**, alla natura dei dati e alle specifiche caratteristiche del trattamento, **in modo da ridurre al minimo**, mediante l'adozione di idonee e preventive misure di sicurezza, **i rischi di distruzione o perdita**, anche accidentale, dei dati stessi, **di accesso non autorizzato** o di **trattamento non consentito o non conforme alle finalità della raccolta**.

Misure minime di sicurezza

- **Quando il trattamento avviene con strumenti elettronici…**
  - **Sistema di autenticazione e autorizzazione**
  - **Protezione da intrusioni nel sistema**
  - **Aggiornamento periodico e correzione dei difetti**
  - **Salvataggio e ripristino dei dati**
  - **Cifratura dei dati sensibili**

Il DPS

- Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
  - l'elenco dei trattamenti di dati personali;
  - la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
  - l'analisi dei rischi che incombono sui dati;
  - le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché
  - la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
  - descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
  - la previsione di interventi formativi degli incaricati del trattamento, per renderli
  - edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire

Il DPS /2

- eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Sicurezza Informatica

IT Security

Il tema della Sicurezza informatica: prospettive

- **IT security**
  - **Sicurezza delle informazioni "gestite" da calcolatori**
    - "Gestite" → "memorizzate" nei calcolatori
    - "Gestite" → "trasmesse" da un calcolatore a un altro

vs

- **IT for security**
  - **Sistemi IT per garantire la sicurezza di cose / persone (dove inf… a cose/persone)**
    - Persone → Sistemi biometrici
    - Cose (in futuro: persone?) → Sistemi RFId

Misure minime di sicurezza

- **Quando il trattamento avviene con strumenti elettronici…**
  - Sistema di autenticazione e autorizzazione

Sistemi di autenticazione

- **Utilizzo di credenziali**
  - **Codice identificativo**
  - **Parola chiave**
    - Almeno 8 caratteri
    - Da modificare ogni 6 mesi
  - **Se non utilizzate disattivate dopo 6 mesi**
  - **Custodite garantendo segretezza**

Misure minime di sicurezza

- **Quando il trattamento avviene con strumenti elettronici…**
  - Sistema di autenticazione e autorizzazione
  - Protezione da intrusioni nel sistema

Intrusioni nel sistema: classi di attacco

- **Social engineering**
  - **Identity theft**
  - **Phishing**
  - **Pharming**
- **Spyware**
- **Troyan Horses**
- **Virus e minacce software**

Social engineering

= l'uso di inganni psicologici verso gli utenti legittimi di un sistema di computer da parte di un hacker intenzionato ad ottenere le informazioni necessarie per accedere al sistema

- Es. soluzioni a disposizione degli utenti
  - Non rivelare a nessuno la propria password.
  - Mettere alla prova l'organizzazione, chiedendo di rivelarci per telefono la nostra password

Identity theft

= furto di informazioni personali di un utente allo scopo di utilizzarle per commettere azioni fraudolente

- Soluzioni a disposizione degli utenti
  - Non usare le e-mail per invio e ricezione di documenti finanziari.
  - Consultare settimanalmente il proprio conto.
  - Evitare tutti quei comportamenti che la banche classificano come pericolosi.
  - Non pubblicare informazioni personali sul web.
- Soluzioni offerte dal mercato
  - Sistemi per la difesa della privacy ("McAfee Wireless Home Network Security"; "Identity Defense Kit")

Phishing

= attacco via e-mail, apparentemente inviata dal responsabile o da un collaboratore di un sito a cui siamo iscritti, che ci invita a collegarci a tale sito effettuando l'operazione di login, cioè inserendo il nostro username e la nostra password

- Soluzioni a disposizione degli utenti
  - Non fidarsi delle e-mail che richiedono di collegarci urgentemente ad un sito.
  - Prestare attenzione al sito che compare nella barra degli indirizzi.
  - Cambiare spesso password.
- Soluzioni offerte dal mercato
  - Token e smart card per l'assegnazione di password nuove ad ogni login.
  - Software anti-phishing.
  - Filtri contro lo spam

Pharming

= modificare la richiesta dell'utente per aprire un determinato sito web in modo tale che al posto della pagina legittima compaia sullo schermo del suo pc un sito Internet fraudolento, all'interno del quale gli artefici della pagina, chiamati "pharmer", possono venire a conoscenza di informazioni personali relative alle loro vittime

- Soluzioni a disposizione degli utenti
  - Verificare che un sito usi un sistema per criptare le informazioni sensibili.
  - Controllare che il certificato SSL di un sito sia ancora valido e non presenti caratteristiche sospette
  - Cambiare la propria password in caso di presunto pharming.
- Soluzioni offerte dal mercato
  - Token e smart card per l'assegnazione di password nuove ad ogni login.
  - Software anti-pharming (es.: "Anti-pharming 1.00", "Identity Defender", Anti-pharming solution")
  - Anti-virus; Anti-spyware.
  - Firewall
  - Software per la protezione del DNS

Spyware

= programmi informatici di due tipi

- che rilevano le abitudini di navigazione degli utenti allo scopo di inviare loro, in un momento successivo, pubblicità mirata.
- in grado di ricavare informazioni che vengono in seguito utilizzate per perpetrare furti di identità e crimini di tipo finanziario

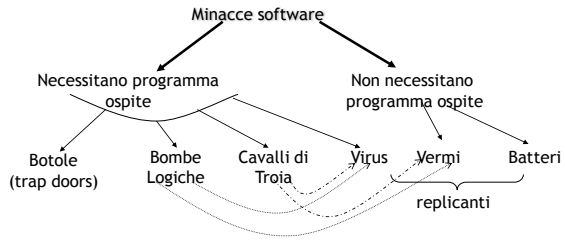
- Soluzioni a disposizione degli utenti
  - Prestare attenzione al funzionamento del computer
  - Istallare anti-spyware e studiarne il funzionamento
- Soluzioni offerte dal mercato
  - Software anti-spyware ("SpywareBlaster"; "Ad-Aware"; "Spybot-Search & Destroy"; "Windows Antispyware Beta")
  - Software anti-virus.

Trojan horse

= programma non autorizzato (spesso contenuto all'interno di un programma legittimo) che agisce all'insaputa dell'utente

- Soluzioni a disposizione degli utenti
  - Usare anti-virus e anti-trojan e aggiornarli periodicamente.
  - Non aprire file sospetti.
- Soluzioni offerte dal mercato
  - Software anti-trojan ("TDS-3"; "Lock Down2000"; "Trojan Remover"; "Pc Door Guard"; "Panda Platinum Internet Security")

Virus e minacce software



Virus e minacce software: fasi

- fase silente: virus inattivo, attivato da qualche evento
- fase di propagazione: si duplica in altri programmi che vanno in esecuzione; si mette in aree particolari del disco
- fase di attivazione: si attiva per compiere le azioni programmate. Può essere attivato da un evento esterno
- fase di esecuzione: compie le funzioni di danneggiamento e/o disturbo
- sono spesso progettati per un particolare s.o. o piattaforma hw

Virus e minacce software: tipi

- parassita: si attacca ad un eseguibile e si replica;
- residente in memoria: si carica in memoria come parte di un programma residente;
- settore di boot: infetta boot record;
- furtivo (stealth): nato per nascondersi dagli antivirus (tecnica più che un tipo)
- polimorfico (mutante): cambia ad ogni infezione anche attraverso tecniche criptografiche
- macro virus: sono la tipologia in più rapido sviluppo (due terzi dei virus), indipendenti dalla piattaforma, infettano documenti non eseguibili, si diffondono facilmente, si basano sulle macro di Word (Excel, ...)

Le protezioni dalle intrusioni

Firewall

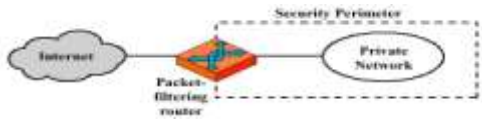
- componente situato fra due reti che gode delle seguenti proprietà:
  - tutto il traffico dall'esterno verso l'interno e viceversa deve passare attraverso il firewall
  - solo al traffico autorizzato, definito dalle politiche di sicurezza locali, è consentito il transito
  - il firewall stesso è immune dalle penetrazioni

Firewall: tipologie di controllo

- controllo del servizio: determina tipi di servizio Internet accessibili dall'interno e dall'esterno filtrando il traffico sulla base degli indirizzi e delle porte
- controllo direzione: dei flussi di dati
- controllo utente: accesso al servizio da parte di utenti interni ed esterni
- controllo comportamento: come sono usati i servizi

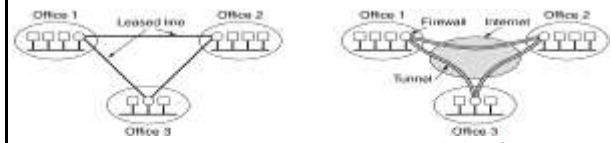
- limiti:
  - non può impedire l'aggiramento ad esempio attraverso un modem
  - non può impedire attacchi dall'interno
  - non può proteggere dal trasferimento di programmi o file infetti da virus

Firewall: filtri di pacchetto



- Selezione basata su pacchetti IP
- semplici e poco costosi
- non sempre molto efficaci
- primo livello di sicurezza
- facilmente realizzabile con i router

Virtual Private Networks



A leased-line private network

A virtual private network

VPN

- Le Virtual Private Network, specialmente se basate su protocollo SSL si stanno imponendo come soluzioni per la creazione di extranet.
- Hanno buone prestazioni di sicurezza.
- Non richiedono l'installazione di software lato client.
- Possono essere usate in quasi tutte le situazioni. Supportano un ristretto numero di protocolli basati su TCP e UDP.

Come si protegge una azienda ?

- Controllare le informazioni pubblicamente disponibili
- Identificare una naming convention non troppo esplicativa per i sistemi/reti/servizi esposti all'esterno
- Controllare periodicamente le informazioni che escono dall'azienda e finiscono sui motori di ricerca
- Verificare la presenza di informazioni sensibili in newsgroup o forum
- Mantenersi in contatto con le comunità di hacker e con i siti dedicati alla sicurezza. www.securiteam.com, www.zone-h.org, www.securityfocus.com, www.packetstormsecurity.org, www.k-otik.com

Come mi proteggo io ?

- Personal firewall (quello di XP va benissimo)
- Antivirus (Norton o avg)
- Antispyware (ADAware, SpyBot)
- Service pack e patch sempre aggiornati
- Blocco dei servizi e dei device non necessari.

La cifratura dei dati

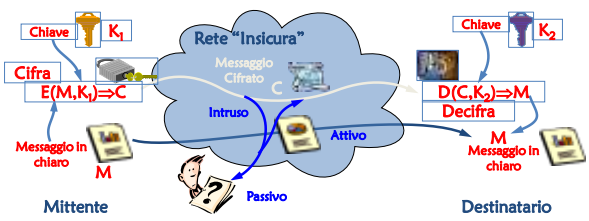
Misure minime di sicurezza

- Quando il trattamento avviene con strumenti elettronici…
  - Sistema di autenticazione e autorizzazione
  - Protezione da intrusioni nel sistema
  - Aggiornamento periodico e correzione dei difetti
  - Salvataggio e ripristino dei dati
  - Cifratura dei dati sensibili

Sicurezza di un messaggio: requisiti base

- Confidenzialità del messaggio (segretezza):
  evitare eventuali intercettazioni dei dati in transito.
- Autenticazione del mittente:
  garantire l'identità di chi invia il messaggio e/o accede alle risorse.
- Integrità del messaggio:
  evitare eventuali contraffazioni dei dati in transito.
- Non-repudiation:
  evitare che sia possibile rinnegare di aver accettato e/o proposto una transazione.

Crittografia: il contesto



Sicurezza Informatica e organizzazioni

Sicurezza informatica
=
problema degli "informatici" ???

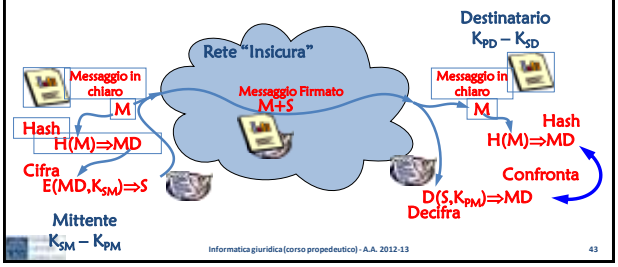
Come funziona la cifratura?

- La sicurezza offerta si basa sulla pratica impossibilità di decifrare il testo inviato.
  - In realtà è possibile, generando tutte le chiavi possibili, riuscire a decodificare un messaggio inviato usando la crittografia asimmetrica.
  - Il problema è che questo approccio richiede un tempo enorme di calcolo da parte di un computer.
  - Collegando però tra di loro più computer il tempo si riduce.

Aumentare la robustezza

- Per aumentare la robustezza si utilizzano chiavi con un numero maggiore di bit.
  - Nel 1995 con 8 giorni di lavoro 120 computer hanno decifrato un messaggio cifrato con una chiave lunga 40 bit.
  - Per generare le chiavi, RSA di solito utilizza 2048 bit. Con chiavi di questa lunghezza il tempo stimato per decifrare un messaggio, con i metodi attuali, è di alcune decine di migliaia di anni.

Firma Digitale



Autenticazione e Non-repudiation

- Nella Firma digitale ciascun utente possiede una coppia di chiavi
- Problemi:
  - Come si può verificare che il proprietario di una coppia di chiavi sia effettivamente colui che dichiara di essere?
  - Se cambia coppia di chiavi, come si può dimostrare che ha partecipato ad una transazione?
- Serve un'autorità superiore che
  - certifichi l'identità del proprietario di una coppia di chiavi;
  - tenga traccia di quali chiavi vengono usate in quali periodi.

Firma digitale e ordinamento

- La firma digitale è basata sulla tecnologia della crittografia a chiave pubblica o PKI. Dal punto di vista informatico essa rappresenta un sistema di autenticazione di documenti digitali tale da garantire il c.d. *non ripudio*.
- Nell'ordinamento giuridico italiano il termine firma digitale sta ad indicare un tipo di firma elettronica qualificata, basato su crittografia asimmetrica, alla quale si attribuisce piena efficacia probatoria, tale da potersi equiparare, sul piano sostanziale, alla firma autografa

Codice dell'amministrazione digitale

- Decreto Legislativo 7 marzo 2005, n. 82, così come modificato dal D.Lgs. 4 aprile 2006, n. 159). Il Codice, all'articolo 1, distingue i concetti di "firma elettronica", "firma elettronica qualificata" e "firma digitale".
- a) Per "**firma elettronica**" la legge intende l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
- b) La "**firma elettronica qualificata**" è definita come la firma elettronica basata su una procedura che permetta di identificare in modo univoco il titolare, attraverso mezzi di cui il firmatario deve detenere il controllo esclusivo, e la cui titolarità è certificata da un certificato qualificato. È inoltre richiesto l'uso del dispositivo di firma sicuro, capace cioè di proteggere efficacemente la segretezza della chiave privata. Inoltre, la firma stessa deve essere in grado di rilevare qualsiasi alterazione del documento avvenuta dopo l'apposizione della firma stessa. Qualunque tecnologia che permetta tale identificazione univoca, rientra nel concetto di "firma elettronica qualificata".
- c) La "**firma digitale**", è considerata dalla legge come una particolare specie di "firma elettronica qualificata", basata sulla tecnologia della crittografia a chiavi asimmetriche.

I certificatori in Italia

- La titolarità della firma digitale è garantita dai "certificatori " (disciplinati dagli articoli 26-32): si tratta di soggetti con particolari requisiti di onorabilità, che possono essere accreditati presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) (in tal caso vengono chiamati certificatori accreditati), che tengono registri delle chiavi pubbliche, presso i quali è possibile verificare la titolarità del firmatario di un documento elettronico.

Posta elettronica certificata

- La posta elettronica certificata (PEC) è uno strumento che permette di dare ad un messaggio di posta elettronica, lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale. La PEC può aggiungere inoltre la certificazione del contenuto del messaggio solo se in combinazione con un certificato digitale. La PEC non certifica l'identità del mittente, né trasforma il messaggio in "documento informatico", se il mittente omette di usare la propria firma digitale

Autorità di Certificazione

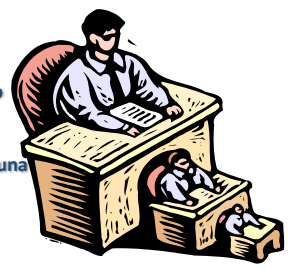
- Rilascia i Certificati Digitali che garantiscono l'identità del proprietario di una chiave pubblica
- I certificati digitali possono essere di diverso livello:
  - Livello 1: garantisce l'esistenza un utente e un indirizzo di e-mail registrato
  - …
  - Livello N: l'identità è certificata dopo un incontro personale con un addetto dell'AC

Certificato Digitale

- AC
- Periodo di validità
- Obiettivo
- Chiave pubblica
- Informazioni aggiuntive
- … …

Quis custodiet ipsos custodes?

- Le stesse autorità di certificazione debbono a loro volta essere certificate da autorità di livello superiore
- La struttura è organizzata in una gerarchia di autorità di certificazione



Il tema della Sicurezza informatica: prospettive

- IT security
  - Sicurezza delle informazioni "gestite" da calcolatori
    - "Gestite" → "memorizzate" nei calcolatori
    - "Gestite" → "trasmesse" da un calcolatore a un altro

vs

- IT for security
  - Sistemi IT per garantire la sicurezza di cose / persone (delle informazioni relative a cose/persone)
    - Persone → Sistemi biometrici
    - Cose (in futuro: persone?) → Sistemi RFId

IT for security

La biometria

Accesso Fisico e Logico

- In biometria due termini ricorrenti sono:
- accesso fisico (controllo biometrico dell')
  - procedura di accertamento della titolarità del soggetto all'ingresso in un locale, edificio, comprensorio o area;
- accesso logico (controllo biometrico dell')
  - procedura di accertamento della titolarità del soggetto ad usufruire di una risorsa informatica.

L' accesso ai sistemi informatici

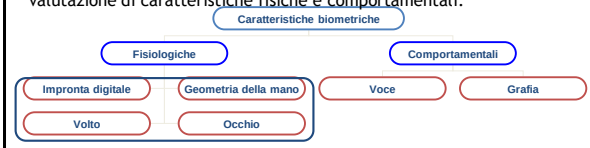
I controlli per l'accesso logico
- devono verificare l'accesso
  - alle risorse di sistema
  - ed ai dati
- al fine di garantire il controllo
  - delle informazioni che gli utenti possono utilizzare,
  - dei programmi che possono eseguire e
  - delle modifiche che possono apportare.

- è strettamente legato all'autenticazione (= processo attraverso cui un utente dimostra l'autenticità dell'identificativo dichiarato nel tentativo di accesso)

La Biometria e i Sistemi Biometrici

La **biometria** è la tecnologia che sfrutta le caratteristiche fisiche e comportamentali uniche di un individuo per autenticare gli accessi a risorse critiche.

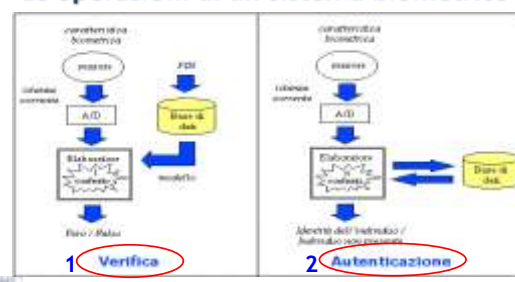
I **sistemi biometrici** sono dispositivi automatici per identificare e/o verificare in modo automatico l'identità di un individuo attraverso la valutazione di caratteristiche fisiche e comportamentali.



I Sistemi Biometrici /2

- Il controllo impone sempre una fase iniziale:
  0. Registrazione *(enrollment)*
     - acquisizione della caratteristica biometrica
     - creazione del modello
     - registrazione del modello
- L'attuazione del controllo avviene secondo due modalità alternative:
  1. Verifica
     - acquisizione della caratteristica biometrica
     - acquisizione di un dato da parte dell'utente
     - creazione del modello
     - confronto tra il modello acquisito e quelli archiviati
  2. Identificazione
     - acquisizione della caratteristica biometrica
     - creazione del modello
     - confronto tra il modello acquisito e quelli archiviati

Le operazioni di un sistema biometrico



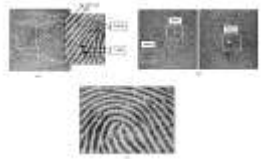
I Sistemi Biometrici /3

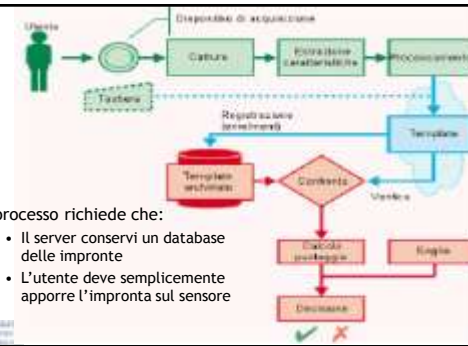
- Struttura:
  - Acquisizione ed elaborazione
    - scanner
    - preprocessore
    - feature extractor
    - generatore di template
  - Archiviazione
    - dispositivi locali
    - token portabile
    - database remoto
  - Pattern matching

L'impronta digitale

L'impronta digitale

Un'impronta digitale è la riproduzione dell'epidermide del polpastrello di una delle dita della mano ottenuta quando il dito è premuto contro una superficie levigata.





Il processo richiede che:

- Il server conservi un database delle impronte
- L'utente deve semplicemente apporre l'impronta sul sensore

Controllo dell'impronta con supporto Smart-card

- Generalmente si procede immagazzinando il template dell'impronta all'interno della smart-card, in particolare l'hashed fingerprint viene inserita all'interno di un certificato di attributo
- All'interno della smart-card viene inserito anche un certificato X.510 per la firma digitale.
- Per rendere valida l'impronta immagazzinata sono aggiunte due informazioni al certificato di attributo:
  - Il numero seriale della smart card (in modo che quel template possa essere utilizzato solo con quella smart-card).
  - Il numero seriale del certificato X.510.
- In questo modo il possessore della carta è libero di autenticarsi o a mezzo della sola smart-card (con l'utilizzo di un apposito PIN), o con la sola impronta digitale oppure utilizzando una combinazione delle due tecniche

Rilevazione dell'Impronta: vantaggi e svantaggi

- **Pro**
  - Tecnologia consolidata
  - Elevata accuratezza
  - Dispositivi di acquisizione di piccole dimensioni
  - Costi ridotti
- **Contro**
  - Alcuni soggetti possono incontrare difficoltà a causa dello spessore ridotto delle creste epidermiche
  - Non idoneo in alcuni ambienti (umidi o polverosi)
  - Diffidenza di alcuni soggetti per fattori psicologici

Campi di applicazione

- I sistemi biometrici basati su impronte digitali trovano applicazione in molteplici settori:
  - AFIS (Automated Fingerprint Identification System) in ambienti di polizia per l'identificazione dei criminali;
  - AFIS in ambito civile (ad esempio in diversi stati americani vengono utilizzati per impedire che un soggetto riceva più volte benefici assistenziali sotto identità diverse);
  - documenti elettronici (passaporto, visti, carta identità): per il controllo sicuro dell'identità presso frontiere e aeroporti; per l'identificazione di immigrati clandestini; per gli ordinari controlli eseguiti da organi di polizia;
  - accesso a servizi: particolare rilievo riveste l'applicabilità di tale tecnologia per l'erogazione di servizi sulla base di carte contenenti dati biometrici;
  - accesso logico a risorse (PC singoli, reti informatiche, singoli applicativi);
  - firma digitale con autenticazione dell'utente che appone la firma;
  - accesso fisico ad ambienti (locali protetti, laboratori, uffici, ecc.);
  - accesso in ambito bancario;
  - controllo delle presenze del personale.

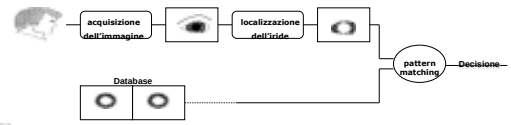
L'iride

L'iride umana

- Iride è una parola che deriva dal greco "ἶρίζ" significa "arcobaleno" ed è una membrana, situata tra la cornea e il cristallino preposta al controllo della quantità di luce che entra nell'occhio

Il riconoscimento dell'iride

- Un sistema automatico per il riconoscimento dell'iride è suddiviso in tre parti:
  - acquisizione dell'immagine
  - localizzazione dell'iride
  - pattern matching (feature encoding e metriche di confronto)



Rilevazione dell'iride: vantaggi e svantaggi

- **Pro**
  - Tecnologia senza contatto fisico
  - Elevata accuratezza
  - Velocità di ricerca in un archivio
- **Contro**
  - Necessità di una fase di apprendimento
  - Costo medio-alto
  - Non funziona in caso di forte illuminazione solare

Campi di applicazione

- I campi di applicazione del riconoscimento dell'iride sono specializzati verso l'alta sicurezza e si vanno orientando verso il controllo dell' accesso ad aree ristrette e ai controlli di frontiera.
- Per ciò che attiene alle frontiere, numerosi scali aeroportuali hanno in esercizio applicazioni per l'espletamento automatizzato delle procedure come ad esempio l'Automated Border Crossing di Schipol (Olanda).
- Altre applicazioni riguardano l'accesso ad aree ristrette come sale server, o ambienti ospedalieri. Altre applicazioni concernono l'accesso logico a dati medici sensibili.

Il volto

Il riconoscimento biometrico del volto

- Indipendentemente dalla modalità statica o dinamica del processo, il riconoscimento biometrico del volto si articola in varie fasi:
  - individuazione del volto (face detection);
  - segmentazione (segmentation);
  - estrazione delle caratteristiche (feature extraction);
  - riconoscimento (recognition).

Rilevazione del volto: vantaggi e svantaggi

- **Pro**
  - Bassa invasività (nessun contatto fisico)
  - Possibilità di acquisizione a distanza
- **Contro**
  - Bassa stabilità della caratteristica biometrica nel tempo
  - Prestazioni inferiori
  - Sensibilità alle variazioni di illuminazione
  - Dimensioni del template prodotto rispetto ad altre tecnologie (da 1 a 5 KB per 2D fino a 10KB per 3D)

Campi di applicazione

- Il riconoscimento biometrico del volto può essere utilizzato per varie applicazioni di cui alcune comuni ad altre tecniche come il controllo dell'accesso fisico e logico, altre specifiche come:
  - sorveglianza (surveillance);
  - controllo di documenti;
  - ricerca dei duplicati (interessante applicazione che prevede la comparazione su base biometrica delle immagini all'interno di un archivio alla ricerca di potenziali soggetti lecui fotografie, pur appartenendo allo stesso soggetto, sono dichiarate sotto più identità. In occasione di elezioni politiche in un paese del centro America il metodo sembra abbia permesso di scoprire numerosi duplicati e quindi potenziali brogli elettorali).

La mano

La geometria della mano

- A differenza delle impronte digitali o dell'iride, le caratteristiche della mano di un individuo non sono descrittive al punto da risultare uniche, quindi non possono essere utilizzate per l'identificazione di una persona, ma, allo stesso tempo, sono sufficientemente descrittive per essere impiegate ai fini della verifica di identità

Rilevazione della mano: vantaggi e svantaggi

- **Pro**
  - Tecnologia consolidata
  - Sensore robusto
  - Dimensioni del template molto ridotte
- **Contro**
  - Costo
  - Dimensioni e peso notevoli
  - Sensibilità a forte luce diurna

Campi di applicazione

- I sensori per la geometria della mano vengono attualmente utilizzati in vari contesti e si sono rivelati particolarmente efficaci per applicazioni del tipo "time and attendance" cioè per il controllo delle presenze sui luoghi di lavoro.
- Dal 1991, un sistema biometrico basato sulla geometria della mano è in funzione all'aeroporto di San Francisco mentre in Canada e negli Stati Uniti, il riconoscimento della geometria della mano è usato in numerosi impianti nucleari.
- Andrebbe inoltre ricordato che per anni i lettori per la geometria della mano sono stati usati per espletare rapidamente le procedure di immigrazione negli Stati Uniti in conseguenza del programma "InsPass".
- Nel 1996, durante i giochi olimpici di Atlanta, il riconoscimento della geometria della mano è stato usato per identificare 150.000 tra atleti, staff e partecipanti. Il sistema è inoltre in funzione all'aeroporto di Tel Aviv per i cosiddetti "frequent travellers".

La voce

Il riconoscimento biometrico della voce

- E' considerato tecnicamente un ibrido tra biometria fisiologica e comportamentale, dal momento che l'emissione è determinata non solo dalla conformazione della gola e della laringe, ma anche da aspetti comportamentali dell'utente, quali ad esempio il proprio tono umorale.

Rilevazione della voce: vantaggi e svantaggi

- **Pro**
  - Tecnologia basata su hardware di grande diffusione
- **Contro**
  - Lunghi tempi di enrollment
  - Dimensioni del template
  - Sensibilità a rumori di fondo

Le applicazioni

- Al di là delle applicazioni investigative, l'uso più indicato per i sistemi di riconoscimento vocale è l'autenticazione degli utenti in applicazioni di medio/bassa sicurezza. Sono in fase prototipale applicazioni nelle quali il riconoscimento della voce è accoppiato ad altre tecniche biometriche (ad esempio volto e movimento delle labbra)

La firma

Il riconoscimento biometrico della firma

- La propria firma è ragionevolmente unica per una serie di caratteristiche, quali ad esempio
  - la velocità di scrittura
  - i punti nei quali si esercita più pressione che appartengono alla sfera comportamentale e sono pressoché inimitabili.
- Se la firma non è apposta su un foglio di carta ma con una tavoletta elettronica oppure viene usata una particolare penna, è possibile trasformare in dati gli aspetti comportamentali

Rilevazione della firma: vantaggi e svantaggi

- **Pro**
  - Hardware poco costoso
  - Buona accettabilità da parte degli utenti
- **Contro**
  - Instabilità temporale del campione
  - Dimensioni del template
  - Numero limitato di applicazioni