

The logo for i.consulting features a stylized, pixelated graphic of a person or figure in shades of blue and grey, positioned above the text 'i.consulting'.

i.consulting srl  
20043 Arcore  
Via Foppa 15  
Milano - Italy

# **CONTROLLO ACCESSI**

## **A CURA DI GIANCARLO SOLA**

# Indice

- Nozioni Base
- Controllo Accessi fisici
- Tecnologie di Lettura
- Protocolli
- Sistemi STAND ALONE, ON LINE
- Nuove Tendenze
- Sistemi Integrati
- RFID nuove tendenze ed applicazioni

# Cosa è il Controllo Accessi

- La tecnologia della sicurezza che applica il controllo di beni e persone, nell'ambito di transiti attraverso varchi liberi oppure chiusi. Questo si realizza con l'ausilio l'uso di opportuni Hardware e Software.
- E' quindi un sistema di sicurezza che serve a:
  - - Controllare l'accesso ai Siti
  - - Proteggere beni e persone all'interno di siti o aree
  - - Evitare il trafugamento di persone o cose
  - - Percorsi definiti per ogni tipologia di persona o cosa
- Fornire dei sistemi di identificazione

# Principi fondamentali

- CHI SIETE ?
  - DOVE ANDATE ?
  - Siete Abilitati
  - Report e transazioni dei passaggi.
- 
- IDENTIFICAZIONE
  - PERCORSO PERMESSO
  - LOG DEI PASSAGGI
  - STAMPA DEI TRANSITI



# Controllo accessi fisici tornelli a tripode



MONO E BIDIREZIONALI

FUNZIONE ANTISCAVALCAMENTO



# Tornelli a tutta altezza



MONO E BIDIREZIONALI TUTTA ALTEZZA  
ADATTI PER APPLICAZIONI DA STADIO  
INGRESSO PRIGIONI

# Varco Ottico



MONO E BIDIREZIONALE ADATTO PER INSTALLAZIONI IN  
AMBIENTI ELEGANTI  
BUONO PER ABBINARE A LETTORI RFID MANI LIBERE

# IL Concetto dell'Identificazione

- Controllare le persone nell'ambito di un sito, è una necessità naturale che si perde nella notte dei tempi.
- Effettuato manualmente da persona preposta. Una volta c'erano molte guardie, anche armate.
- Tramite il possesso individuale di uno Badge o attributo biometrico, oppure altro.....
- ***CONTROLLO ACCESSI*** *identifica una persona o bene tramite lettori e Tessere. Esso è in grado di decifrare degli strumenti di riconoscimento. Il sistema Stand Alone è in grado da solo di aprire il varco. Nei sistemi ON Line i dati e le informazioni vengono gestite da un Software, e l'autorizzazione all'apertura del varco viene data da un Controller oppure da un software.*



# Perché il sistema C.A.

- Economia di esercizio e utilizzo razionale della sorveglianza
- Identificazione delle persone e beni in transito
- Sicurezza a impianto di allarme disinserito con controllo di aree ad alto flusso di transito
- Sicurezza organizzativa a livello gerarchico per aree di importanza.
- Possibilità di Integrazione con impianti di sorveglianza esistenti e con sistemi di allarme ed antincendio.

# Lettori STAND-ALONE

- Sistema composto per lo più da un lettore, tutto quanto concerne la gestione del varco è ubicato all'interno del lettore
- Basso numero di utenti, eventi stampabili localmente ove possibile
- Non è possibile gestire da remoto il varco e le segnalazioni di allarme rimangono locali.
- Sistema molto semplice, di basso costo e sicurezza non elevata.



# Sistemi ON-LINE

- Banca dati molto estesa, possibilità di archiviazione e ricerca storici.
- Il sistema è controllato da un PC.
- Controllo di più siti distanti tra loro
- Valore aggiunto dato da servizi facilmente estraibili dai report del C.A.

# IL Software di Gestione

Consente agli operatori di monitorare immediatamente gli eventi di un sito

Settare i Livelli di Accesso-  
Le Anagrafiche Le fasce Orarie.

Importare planimetria in formato jpg o bmp.

Posizionare porte e telecamere sulla planimetria



# Sistemi ON-LINE INTEGRATI

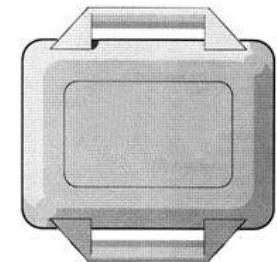
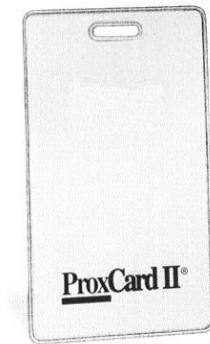
- Continua espansione dei sistemi con necessità di avere sistemi a ***intelligenza distribuita***.
- Interfacciamento tramite protocolli a sistemi di sicurezza (TVCC, INTINTRUSIONE)
- Una sola interfaccia software



## Esempi Badges, tessere oppure Tags di identificazione

- ***Principali strumenti di identificazione:***

- Tessera una carta o badge
- TAG
- Possesso di un PIN
- Riconoscimento Biometrico



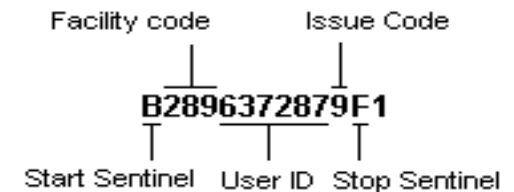
# Percorso

- Individuare un tragitto una meta verso la quale è diretta la persona o il bene.
- *CONTROLLO ACCESSI tramite dei lettori in grado di riconoscere gli strumenti identificativi controlla il percorso e abilita il passaggio o meno in aree controllate.*
- I lettori utilizzati dipendono dalla tecnologia degli strumenti identificativi



# Credenziali per Controllo Accessi

- Le credenziali di accesso sono alla base di ogni tecnologia di identificazione utilizzata nel Controllo Accessi, sono dei **Campi di Dati** utilizzati per riconoscere una persona o una cosa.
- **Facility Code** di solito composto da 3-9 digits determina un gruppo di utilizzatori legati a un sistema.(non sempre usato)
- **User-Id** di solito composto da 4-16 digits è l'identificativo dell'utilizzatore
- **Issue Code** composto da 1-2 digits utilizzato per indicare l'emissione della carta



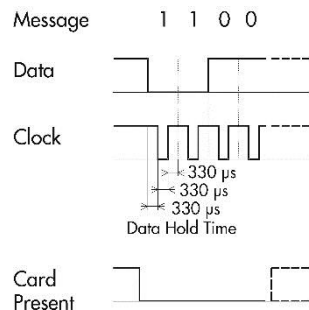
**10 Bit Standard**



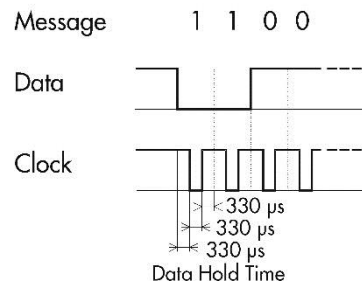
# Protocolli di comunicazione

- Le credenziali devono essere rese leggibili al sistema, tramite dei protocolli trasmissivi: I lettori comunicano in questo modo
- CLOCK&DATA
- WIEGAND

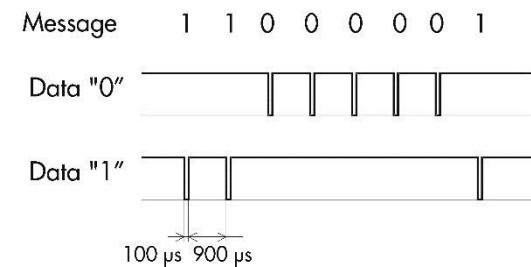
## Magstripe Emulation



## Data/Clock



## Wiegand Standard



# Principali tecnologie di identificazione

- Tessere o Tags Attive
- Tessere o Tags Passivi
- Banda Magnetica
- Prossimità RFID
- (si suddivide in varie tecnologie semplificando :
  - Bassa Frequenza 125Khz. Solo lettura oppure
  - Read Write. 13,56 Mhz. rappresenta la nuova e più sicura tecnologia, criptata e protetta. NON Copiabile).
- Tessere Long Range 2,45 Ghz, attive.
- Presto arriveranno le tessere passive 868Mhz. UHF Long-Range a passive a basso costo
- Biometrica
- Micro Chip

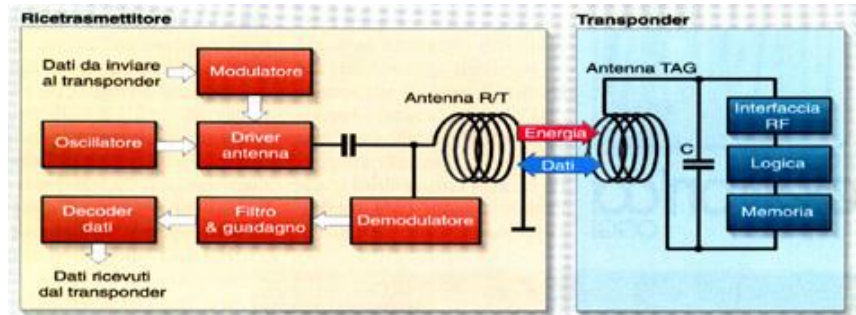
# Banda Magnetica

- Tecnologia più diffusa
- ISO7810 caratteristiche fisiche supporto (85x54) 76/100
- 3 Tracce localizzabili distribuite per parametri fisici ISO ABA 2 75bpi, area divisa per 0,0133 inch
- Bassa-alta coercitività
- Protocollo di base per il controllo accessi
- Basso costo
- Bassa sicurezza, alta riproducibilità, smagnetizzazioni frequenti, soggetto a rotture.



# Prossimità

- Tecnologia in forte espansione
- Alta immunità alla falsificazione
- Alta immunità alla riproduzione
- Assenza di punti di contatto con il lettore
- Basse emissioni elettromagnetiche
- Range di utilizzo da pochi cm. Ad alcuni Mt. freq. 125KHz a 2,45GHz fino a 968 Mhz./901Mhz. UHF Gen.1
- Permette il riconoscimento HAND FREE
- Attenzione alla installazione.

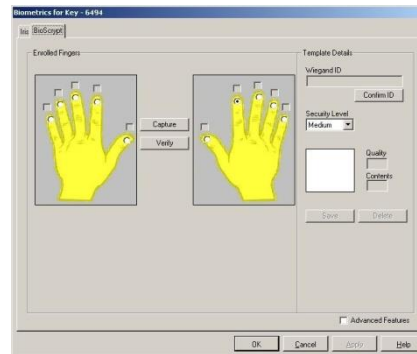
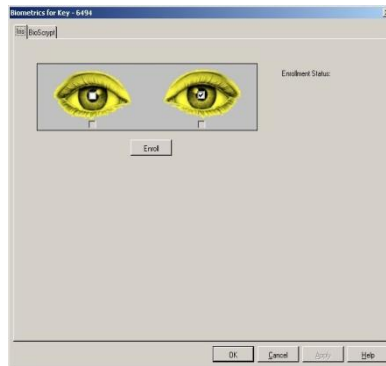


# Biometria

- Tecnologia legata al riconoscimento di particolari somatici propri di ciascun individuo.
- Riconoscimento Impronte, Iride Tratti somatici visto i più utilizzati
- Alta sicurezza
- Libera l'utente da qualsiasi strumento di identificazione
- Concetto di identificazione e autenticazione

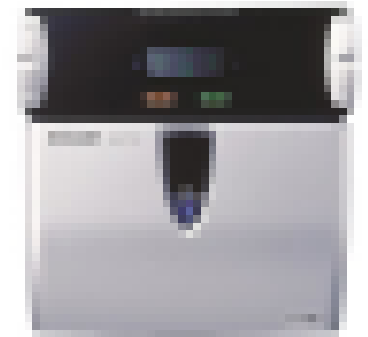


# Biometria del Palmo della mano e lettura dell'Iride



# Iris Recognition

- Semplice utilizzo e sicuro .
- Garantisce le informazioni di identità.
- Nessuna tessera è necessaria per l'identificazione.



**Panasonic**

# Finger Vein Impronta delle vene

- Utilizza il pattern della impronta delle vene.
- Massima sicurezza non si può riprodurre.
- Utilizza una tecnologia a LED's per attivare l'emoglobina e risaltare le vene..
- Facilmente tollerabile , non danneggia la pelle.
- Igienico.
- Non è relazionata all'impronta biometrica delle dita.





# Biometria

- Tecnologie di lettura sempre più affidabili
- Determinante la quantità di memoria utilizzata per la memorizzazione (tempo di risposta)
- Utilizzo in accordo con altre tecnologie per diminuire il tempo di risposta e aumentare l'affidabilità
- L'affidabilità: FAR (False Acceptance Rate), FRR (False Rejection Rate) ERR (Equal Error Rate) Punto di incontro tra FAR e FRR
- In fase di progettazione porre la massima attenzione
- Prezzi ancora alti ma in progressiva diminuzione

# Micro Chip

- Carta formato ISO con grandi capacità di memoria(1-20KB) permette di condensare più tecnologie
- Informazioni per vari settori scrivibili e aggiornabili in linea riscrivibile
- Alta sicurezza
- Tecnologia costosa sia per carte che per lettori
- Lettori e carte con problemi sull'utilizzo estremo causa usura contatti.

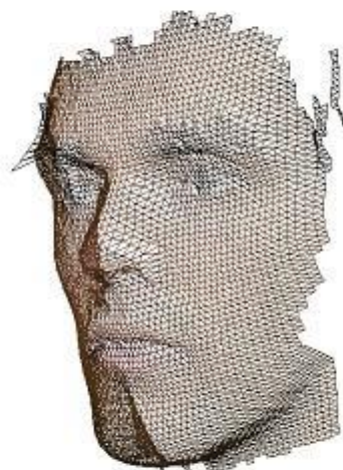


# Mifare-IClass

- Mifare Chip sviluppato da PHILIPS
- Oggi prodotto da NXP ex Philips
- Stà uscendo Mifare Plus per risolvere problemi gravi di sicurezza.
- Unisce i vantaggi della carta Chip con la Prossimità.
- Iclass prodotto da HID.
- Memorie da 1KB o 2KB a 16 settori 32 Bit, MHz13,56, 100mS.
- Molto utilizzata in accoppiata con Lettori Biometrici
- Aggiornamento tramite RF
- Alto costo ma in continua discesa

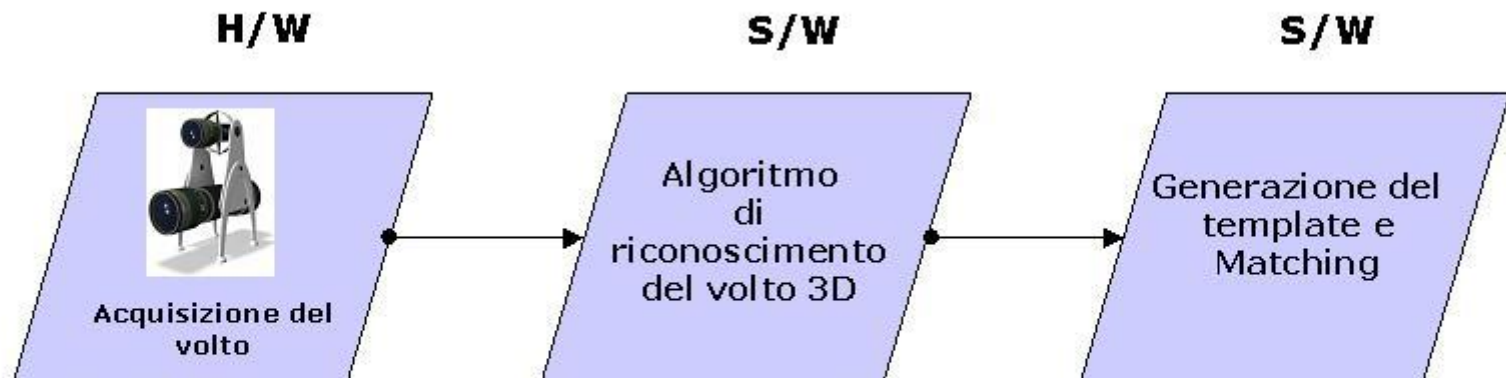


## CONTROLLO ACCESSI CON RICONOSCIMENTO DEL VOLTO

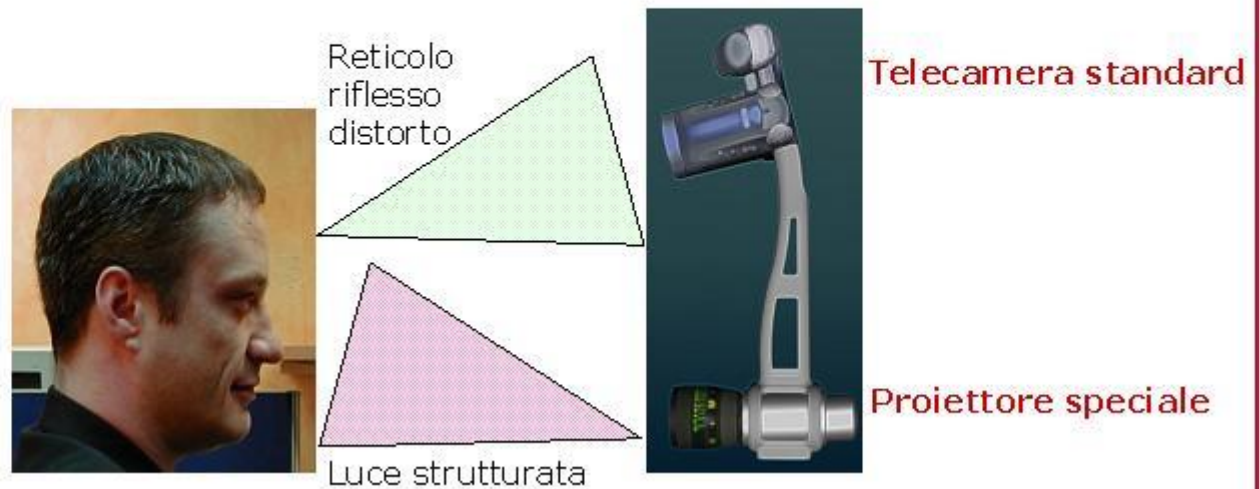
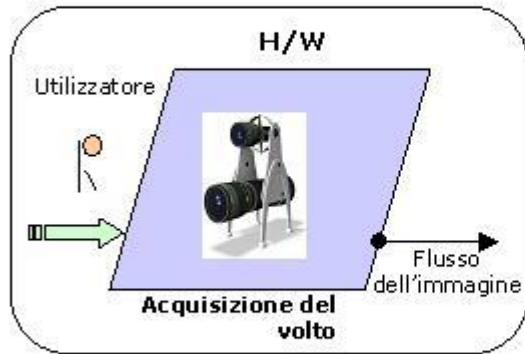


## LA TECNOLOGIA UTILIZZATA

- Rilevamento dell' immagine del volto
- Ricostruzione del volto in 3D con specifico algoritmo
- Estrazione del disegno vettoriale (template) e confronto (matching)



# PROCESSO DI ACQUISIZIONE DEL VOLTO

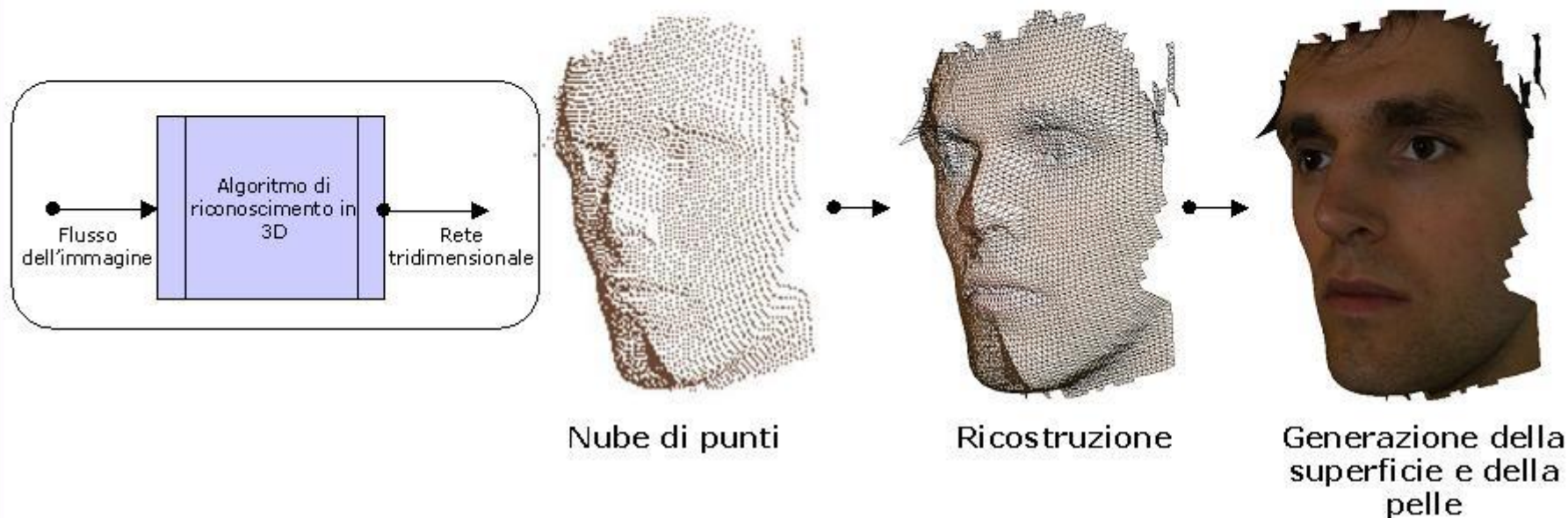


- 1) Il proiettore speciale proietta una luce strutturata sul volto
- 2) Il reticolo regolare di luce viene distorto dalla superficie del volto



- 3) Il sistema registra il volto e le linee riflesse distorte

## RICOSTRUZIONE DEL VOLTO IN 3D



- 1) Estrazione del reticolo distorto dell'immagine reale**
- 2) Calcolo delle tre coordinate di tutti i punti speciali del volto**
- 3) Interpolazione dei punti per generare la superficie tridimensionale del volto**
- 4) Generazione della superficie e sovrapposizione della "pelle" (non necessaria per l'identificazione)**

# DOVE VA' IL MERCATO

- Maggiore richiesta di C.A.
- Crescita culturale di Installatore (Proposta) e Utente (Domanda)
- Sistemi sempre più flessibili e evoluti
- Sistemi Integrati Accessi-TVCC-Allarme-Fire.
- Carte sempre più sicure e meno costose, e soprattutto Read-Write.
- Sistemi Controllo Accessi Multifunzione.
- Accesso Logico a PC, tessere a scalare, gestione mense, gestione utilizzo macchine caffè e fotocopiatrici, etc.etc.