Controllo Accessi Avanzato cenni di RFID

Summary

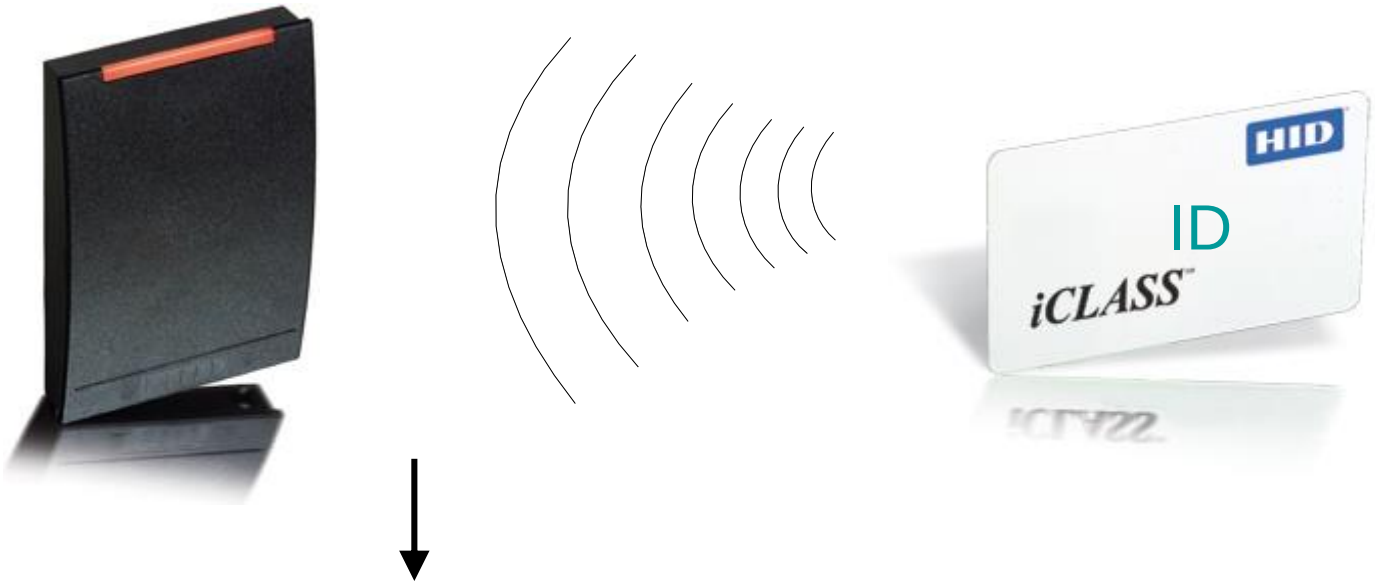
- Che cos'è RFID ?
- L'accoppiamento RFID
- Le Frequenze RFID
- ISO standards
- Smart Cards & EAC
- L'organizzazione delle memorie
- I rischi per la sicurezza
- CSN
- I livelli di sicurezza

Principio di funzionamento

- La lettura avviene quando i tag si trovano all'interno del campo generato dal reader
- In queste condizioni le antenne del tag e del reader trasferiscono le informazioni relative all'identificazione utilizzando i principi delle comunicazioni radio...
- Dopo la lettura, i dati acquisiti diventano disponibili all'intero processo di gestione informatico(SW Access-Control)

www.weblogsinc.com

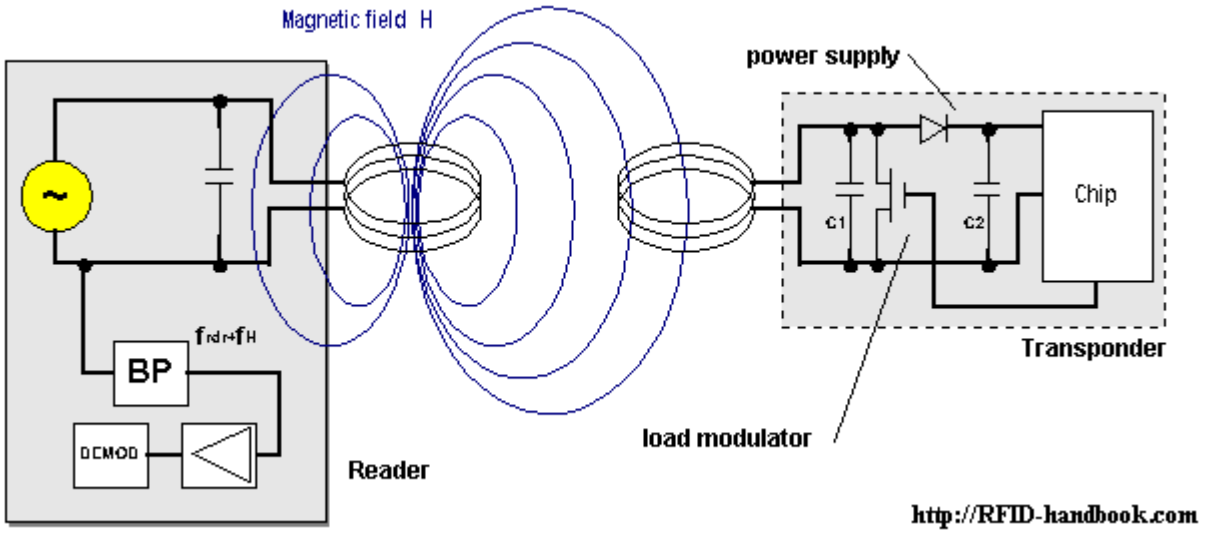
Che Cosa è L'RFID ?



ID:

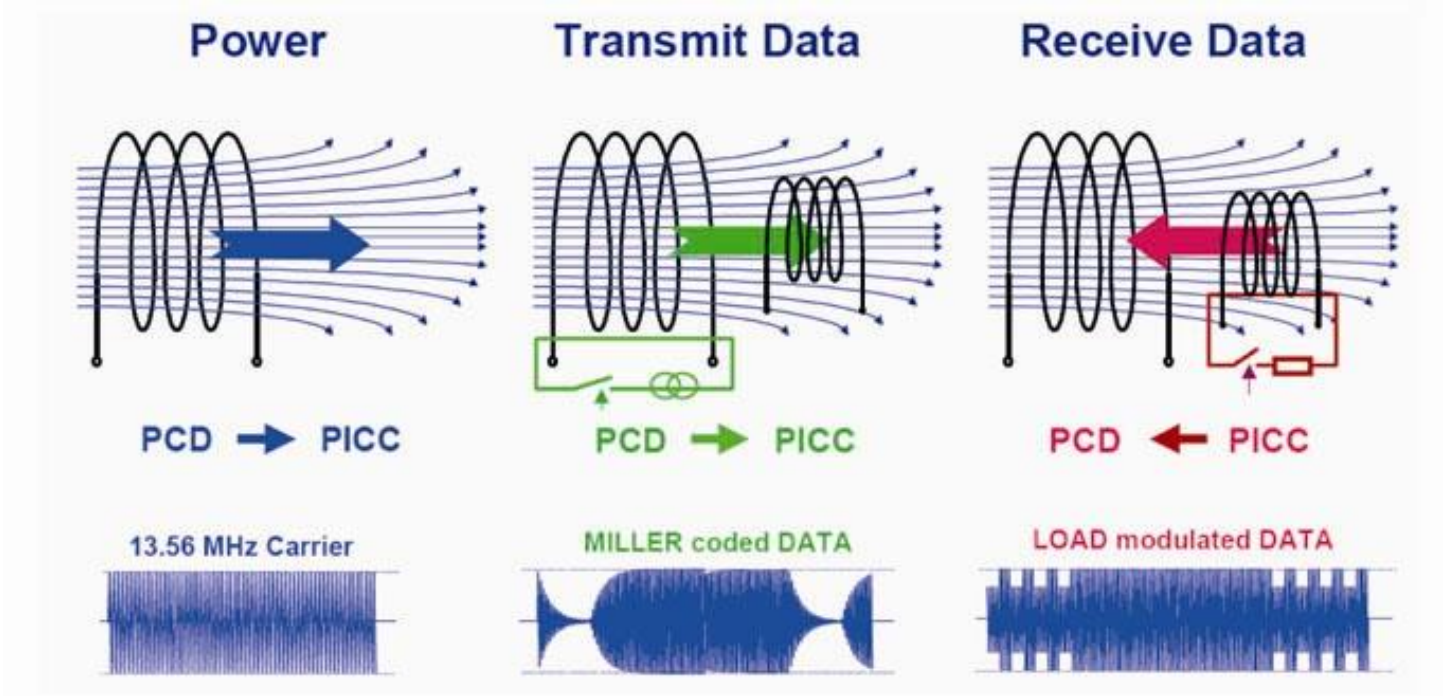
- Codice numerico
- Dati Biometrici
- Accesso corretto
- …

Principio di Funzionamento

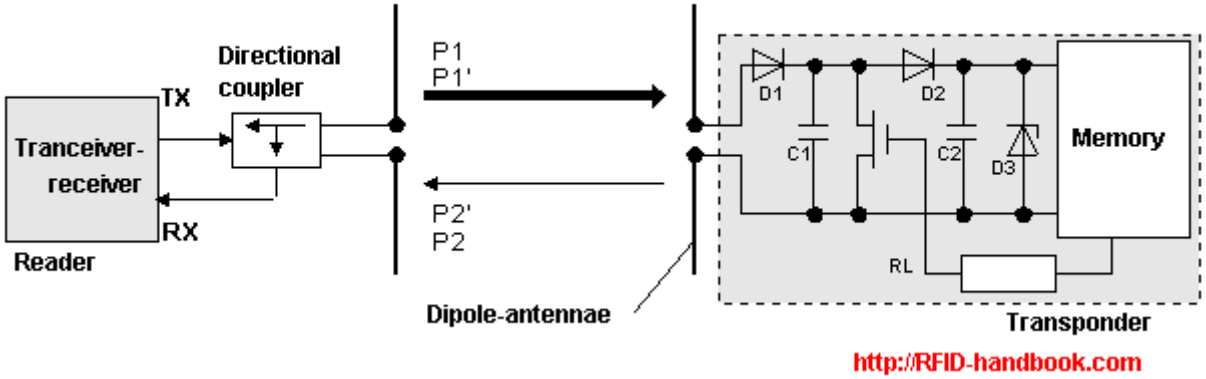


Accoppiamento induttivo
(Tag Passivi)

Accoppiamento RFID



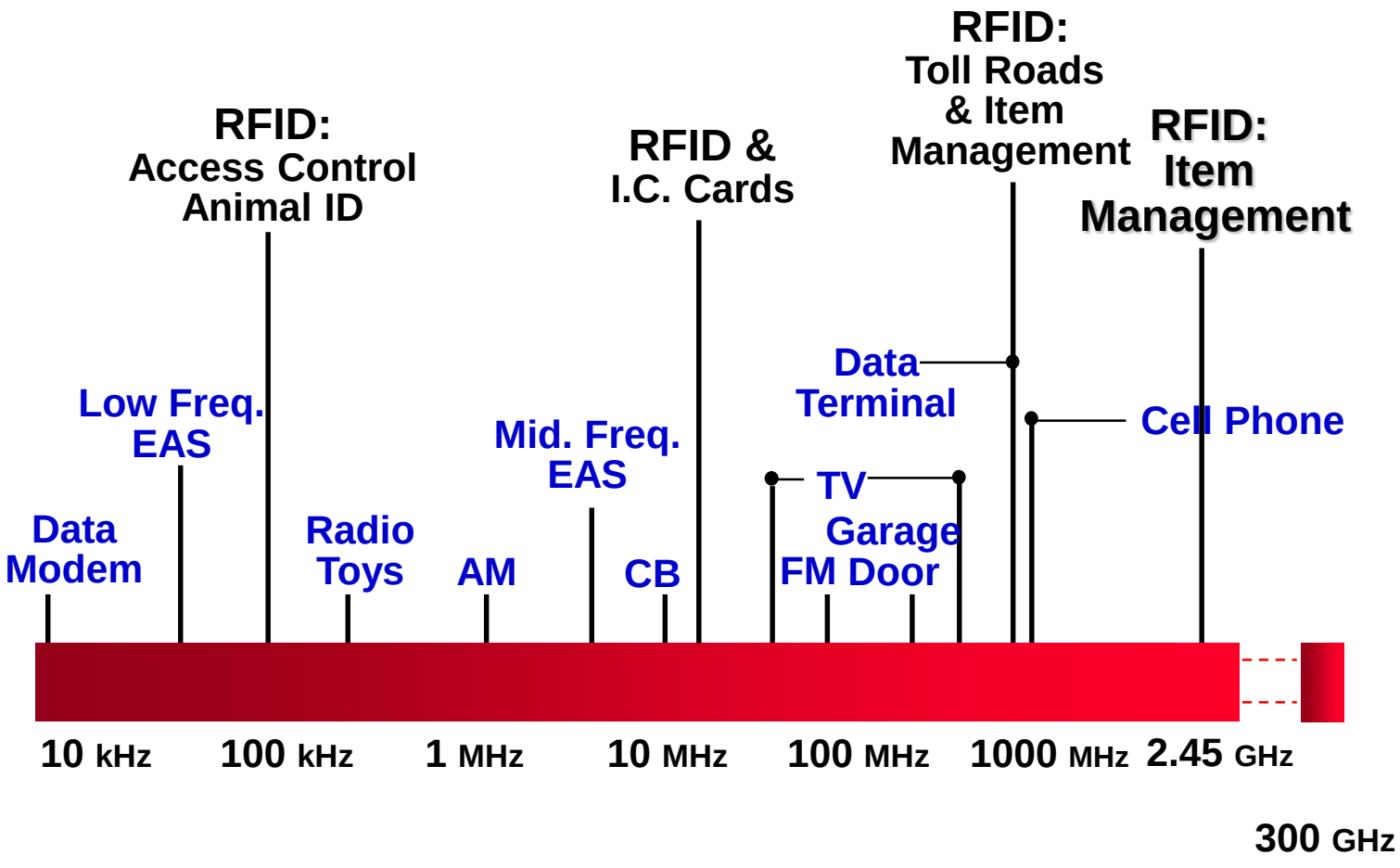
Accopiamento RFID



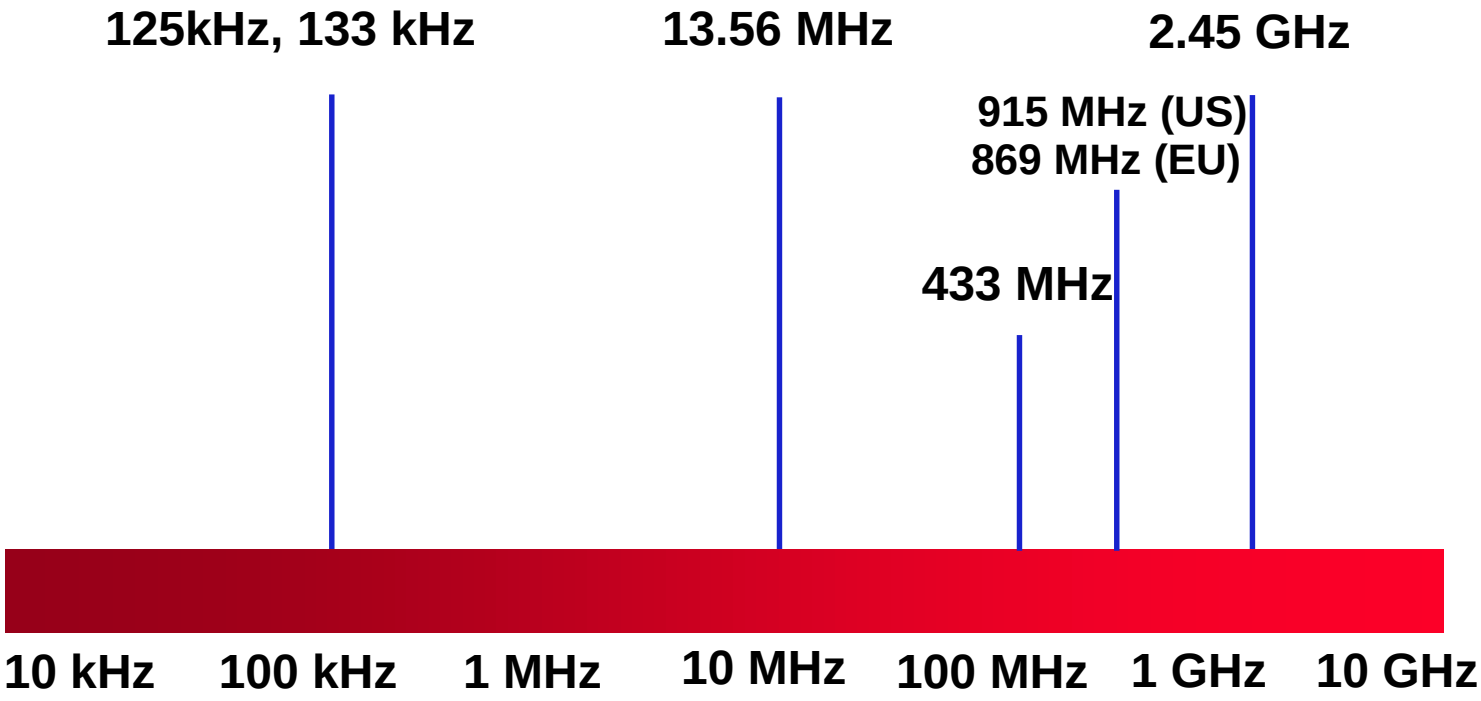
Backscatter Coupling

(Active tags)

Frequenze


RFID:
Access Control
Animal ID
RFID &
I.C. Cards
RFID:
Toll Roads
& Item
Management
RFID:
Item
Management
Low Freq.
EAS
Mid. Freq.
EAS
Data
Terminal
Cell Phone
TV
Garage
Data
Modem
Radio
Toys
AM
CB
FM Door
10 kHz
100 kHz
1 MHz
10 MHz
100 MHz
1000 MHz
2.45 GHz
300 GHz

Frequenze RFID



Livelli massimi :

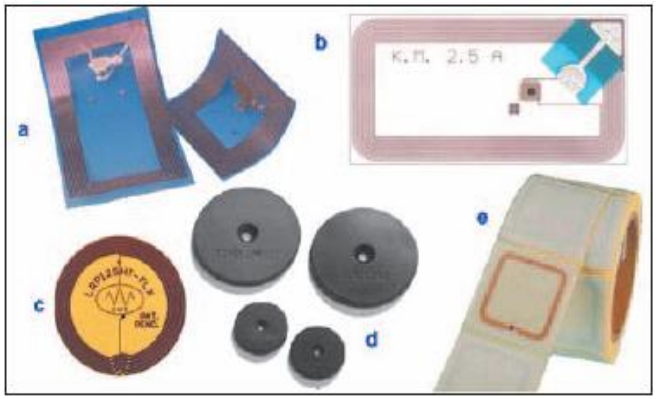
125 KHz : 72dBuA/m
13.56 MHz : 42 dBuA/m
2.45 GHz : 500mW

Tipologie dei Lettori RFID

- Prossimità 125 Khz. EM 4102-4100
- Prossimità HID 125 Prox
- Prossimità HID 13,56 Mhz. Read-Write iClass
- Prossimità 13,56 Mhz. Legic
- Prossimità 13,56 Mhz. Des Fire-
- Longe Range attivi 2,45 Ghz
- Longe Range Passivi 868 Mhz.
- Multitecnologie attivi

I formati costruttivi dei transponder

- Forma a disco e monete (resina, plastica o policarbonato)
- Chiodi per legno
- Capsule di vetro o di plastica
- Chiavette per il caffè, portachiavi (key-fobs) o braccialetti plastici
- Smart labels (etichette stampabili intelligenti)
- Plastica, carta, illays (dry oppure wet)
- Cuciti su stoffa (Textile tag)
- Formato tessera (ISO Card)



TIPOLOGIE DI TESSERE DI PROSSIMITA’

TESSERE PASSIVE 125Khz-
133kHZ. PORTATA 3CM-50CM.

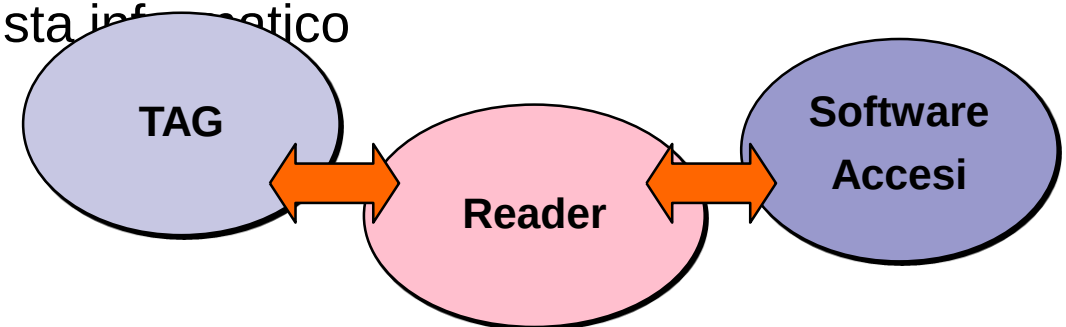
TESSERE DI PROSSIMITA’
Smart card RW
13,56 Mhz.
MULTIFUNZIONE

TESSERE ATTIVE
2,45 Ghz e 125Khz.

PORTATA 1-8 Metri

Elementi dei sistemi Controllo Accessi di prossimità

- Ogni sistema Controllo Accessi è costituito da tre elementi fondamentali
  - **La credenziale-Tessera , transponder** (o TAG), che permette l'identificazione dell'oggetto e della persona che lo porta. Può essere di varie frequenze, case e dimensioni.
  - **L'apparato di lettura** (Reader), che interroga i TAG
  - interagendo con essi . Trasmette le letture al Controllore.
  - **Controllori** Generalmente.hardware di gestione varco
  - **L'applicazione software**, che si interfaccia con uno o più reader e, attingendo a risorse di rete come i database e gli applicativi aziendali, gestisce il processo di controllo, dal punto di vista inf[illegible]tico



Lettori di Prossimità 125 Khz. e 13,56 Mhz.

Lettore di prossimità R10 HID 13,56Mhz.
portata 3-5cm.

Lettore RK 40 HID tessera iClass 13,56
Mhz. più combinazione numerica

Lettori di Prossimità iClass 13,56 Mhz.

Lettore di prossimità R90 HID 13,56Mhz.
Portata22-45 cm.

LE FASI DEL RICONOSCIMENTO BIOMETRICO

- ACQUISIZIONE
  - RILEVAMENTO TRAMITE APPOSITI SENSORI

- PRE ELABORAZIONE DIGITALE DELL' IMMAGINE
  - EQUALIZZAZIONE DELLE DISTORSIONI OTTICHE
  - ELIMINAZIONE DIFETTI
  - RIDUZIONE DEI RUMORI (FILTRAGGIO)
  - ESALTAZIONE DELL' IMPRONTA

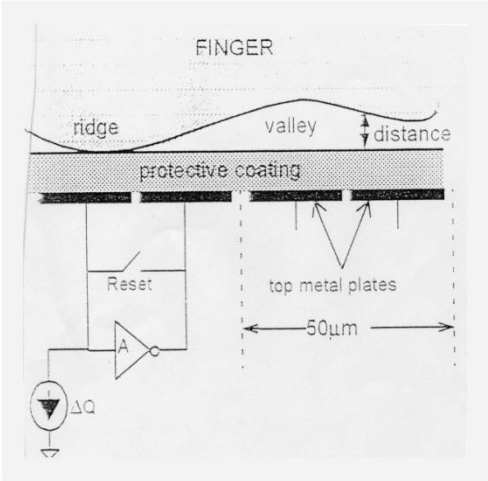
- TRASFORMAZIONE
  - UTILIZZO DI TECNICHE DI TRASFORMAZIONE DI VARIO TIPO
  - COMPRESSIONE DELL' IMMAGINE : RIDUZIONE CON RAPPORTI ANCHE DI 100:1
  - FORMAZIONE DEL "TEMPLATE"

- CONFRONTO PER IL RICONOSCIMENTO (MATCHING)
  - ALGORITMO DI RICONOSCIMENTO

Lettori Biometrici

Lettori Biometrici capacitivi

LETTORE IMPRONTE DIGITALI:
TIPO CAPACITIVO



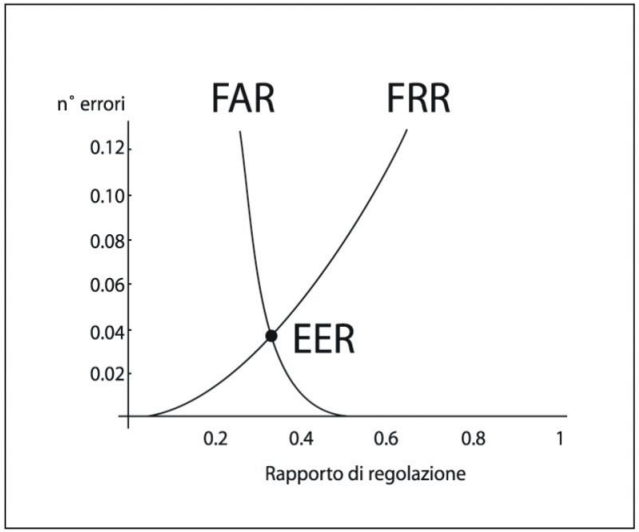
.....ACCURATEZZA

- FAR (False Acceptance Rate)
  Percentuale di utenti non autorizzati erroneamente accettati

- FRR (False Rejection Rate)
  Percentuale di utenti autorizzati erroneamente non riconosciuti e rifiutati

- ERR (Equal Error Rate o Crossover Error Rate)
  Punto di equilibrio fra i due parametri

DIAGRAMMA DELL'ANDAMENTO DEI PARAMETRI



Lettori Biometrici con tessere RW 13,56Mhz.

Lettore Biometrico con memorizzazione impronta del dito nella tessera iClass 16K. Nessun dato rimane nel PC l'apertura del varco avviene per Maching tra la lettura e la verifica dell'impronta residente nella tessera.

Controllo accessi veicolare

➢ Controllare **l'entrata/uscita** dei mezzi

- Impedisce l'accesso o l'uscita ai mezzi non autorizzati
- Generalmente si usano Longe Range 2,45 Ghz. Oppure ultimamente 868 Mhz.UHF
- Memorizza e documenta ogni transito (abbinato al controllo targa)
- Migliora la sicurezza del trasporto dei beni
- Attiva la videoregistrazione
- On-line: colloquia con gli altri sistemi e con il supervisore
- Attenzione all'Installazione

Lettori Longe Range 2,45 Ghz.

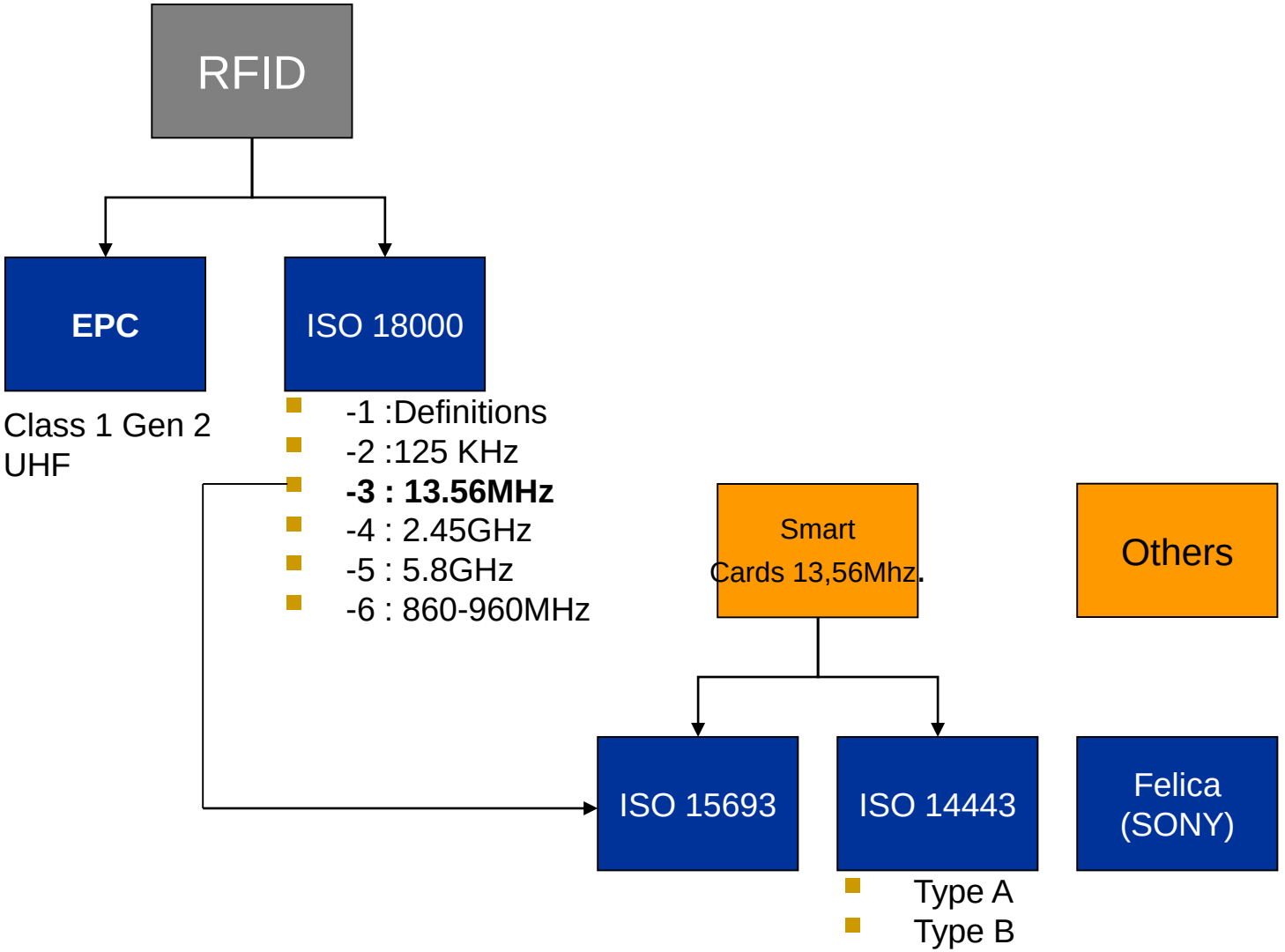
Lettore Longe Range 2,45Ghz. Adatto per uso veicolare, tipo telepass portata 6-8metri. Attenzione all’installazione.

Comparazione tra le Frequenze 125/13,56

125 KHz - 13.56MHz

	Bassa Frequenza 125 KHz	Alta Frequenza 13.56 MHz
Dimensione memoria (1 Byte = 8 bits)	No (UID only) fino a piccole (appx. 64bits)	Grandi fino a 32,000 bits
Velocità di trsmissione dati	4 Kb/sec Non è possibile avere templatesulla tessera	ISO 14443B: Up to 847 Kb/sec (Template nella tessera)
Multiapplicazione	No	SI
Lettura-Scrittura	No	SI
Protezione duplicazioni	No	SI

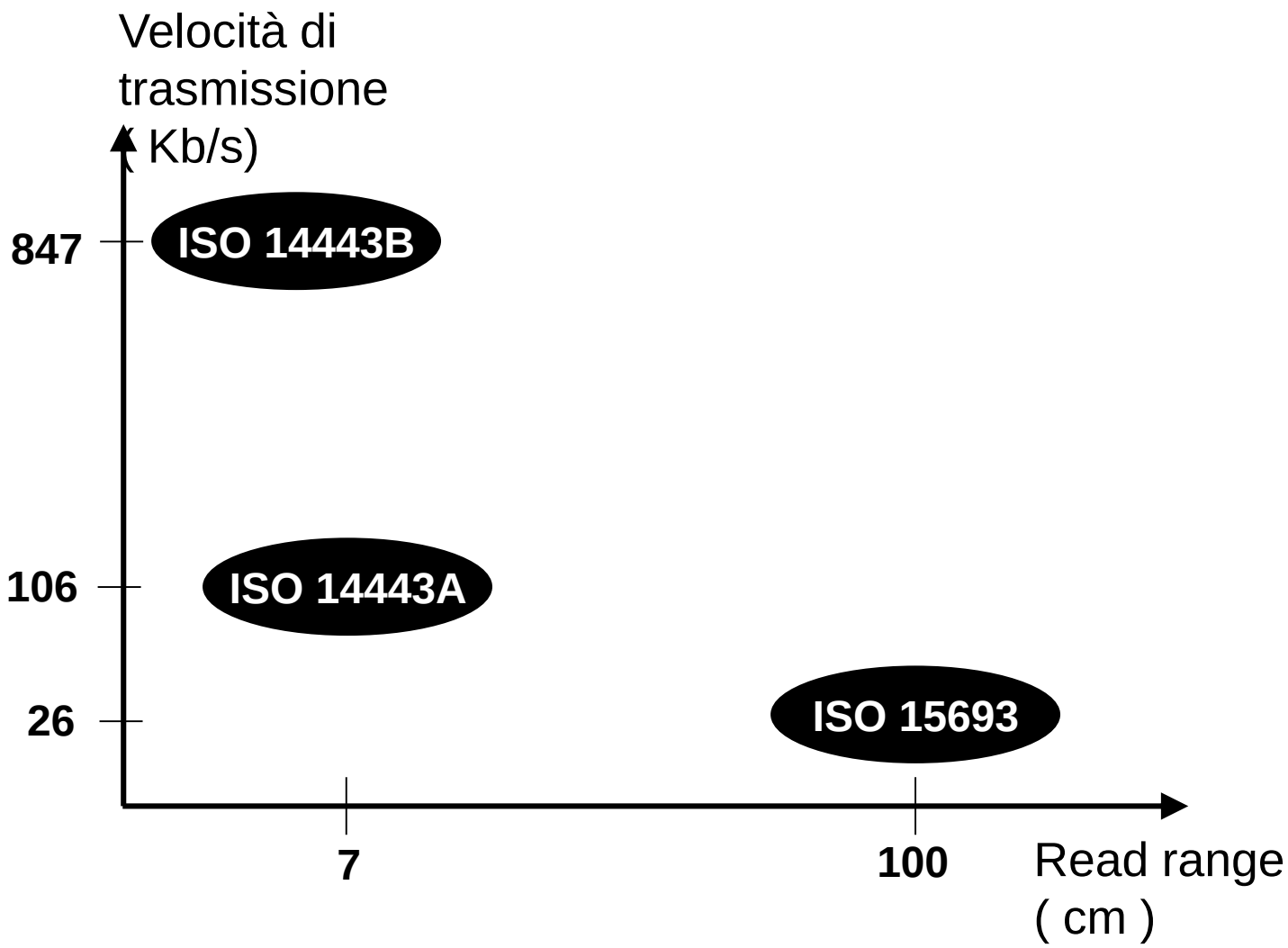
ISO Standards



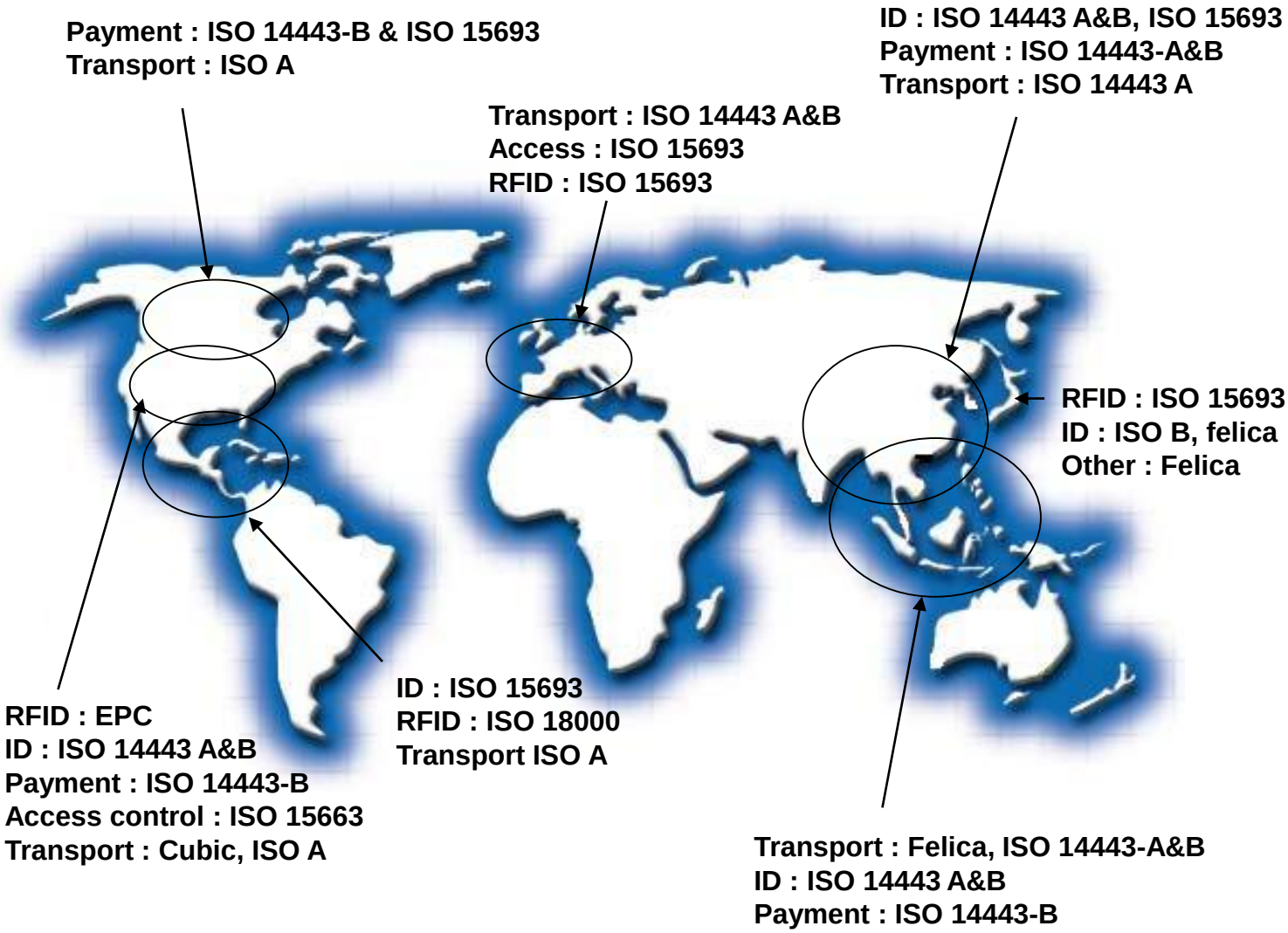
13.56Mhz ISO Standards breve storia

- 1997 : ISO14443A Approvate dal comitato ISO (sviluppate da Mikron , Austria, acquisita da Philips nel 1996)
- 1998 : ISO14443B approvate dal comitato ISO (sviluppate da SGS-Thomson and Motorola)
- 1998 : Philips e Texas presentano ISO15693
- 1999 : Philips and Texas promuovono il nuovo Standard
- 2000 : ISO15693 è approvato dal comitato ISO .

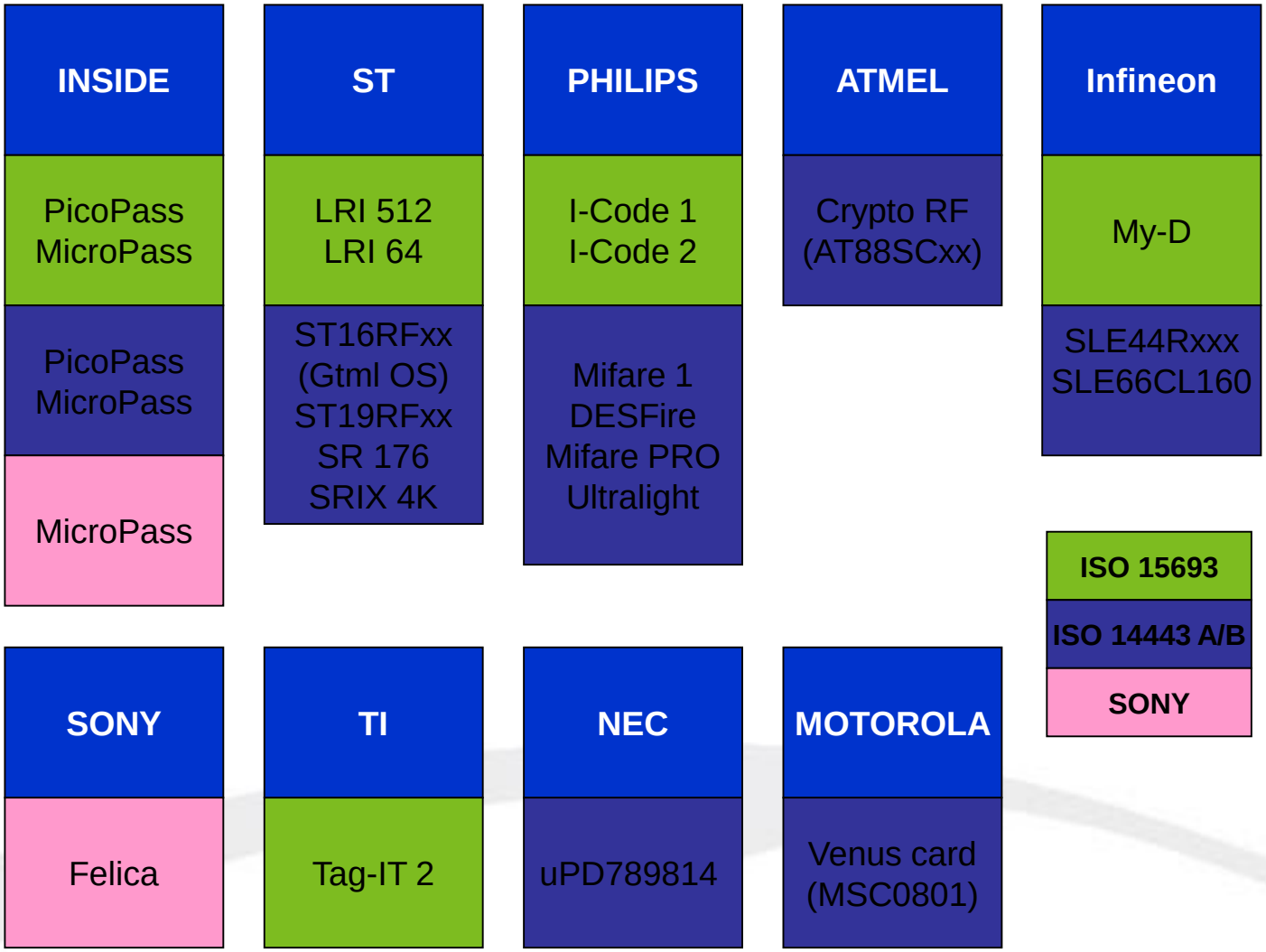
ISO 14443A/B - ISO 15693 Portate di lettura-velocità



Distribuzioni Standard nel mondo

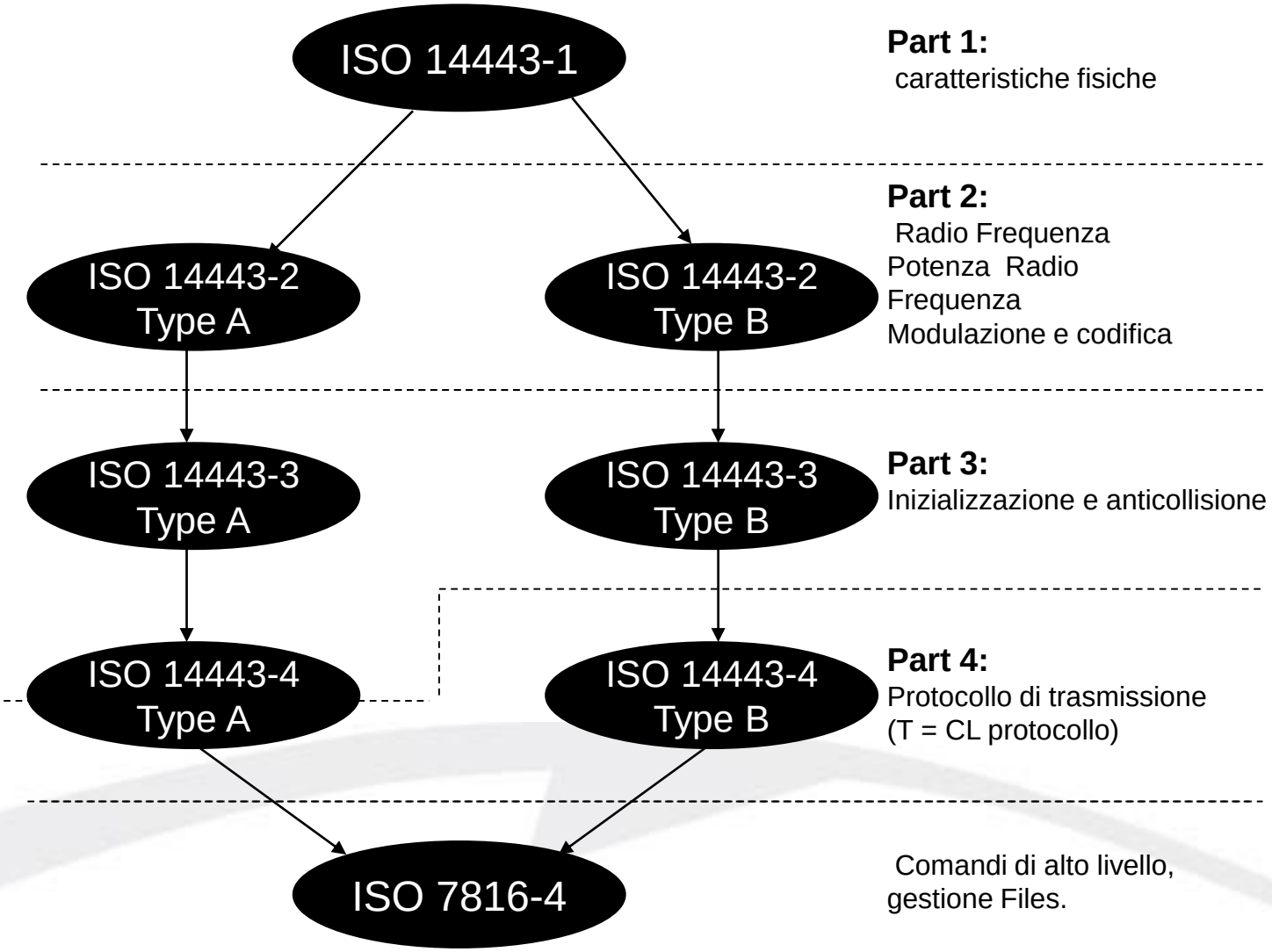


Principali produttori di Smart Cards di prossimità



ISO 14443A/B

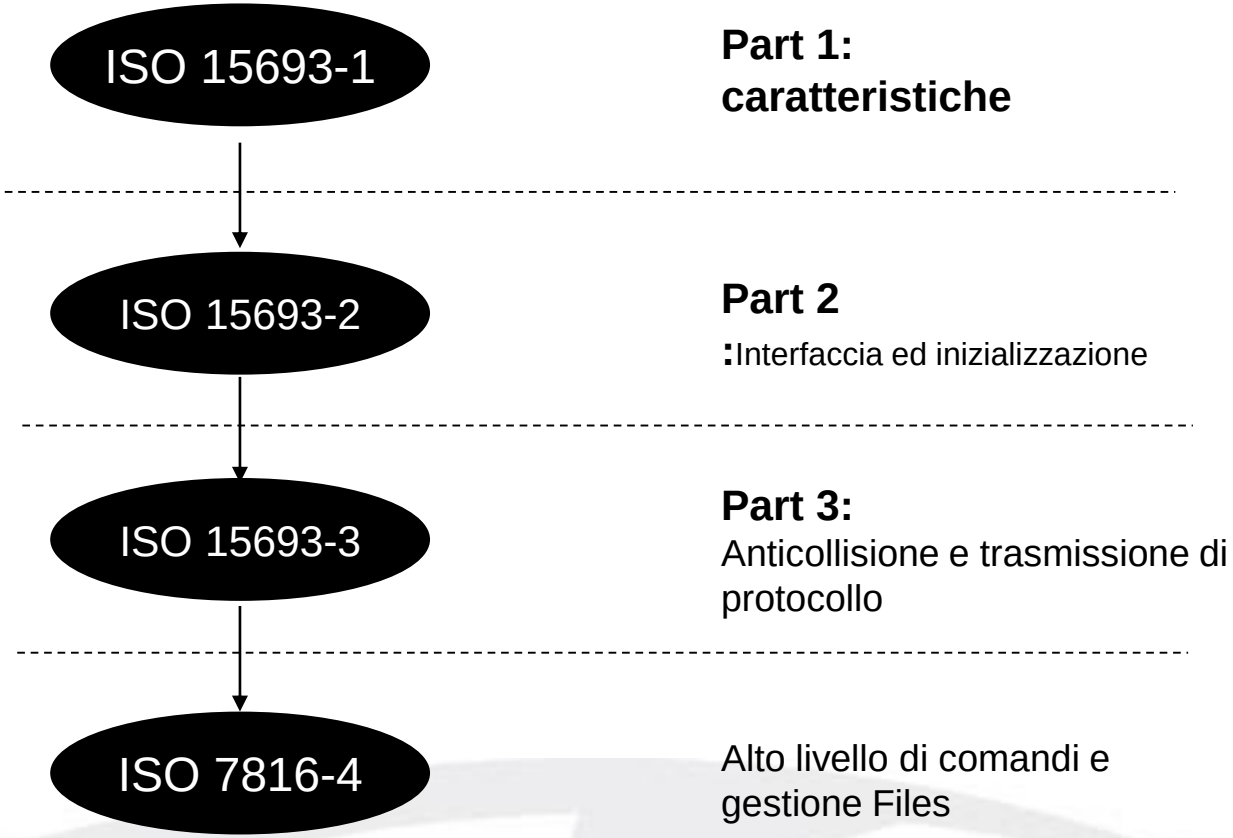
ISO s



ISO 14443 A/B differenze tecniche

	Type A	Type B
Portfolio prodotto	µC and hardwired logic	µC and hardwired logic
Clock	**Portante è interrotta durante la modulazione**	Clock sempre attivato
Realizzazione	Semplice da implementare ad eccetto anticollisione	Semplice da implementare
segnalel/ disturb radio	RD > Card Cards > RD	Alta soggetto a disturbi	Alta-molto alta
Bit Coding	Difficoltà di decodifica	Facilità di codifica-decodifica
Spettro	RD > Card Card > RD	Bassa sensibilità	Migliore sensibilità
Sicurezza	**Possibile violazione della sicurezza**	Alto livello come le Smart card a contatto
Velocità	**106Kbits/s**	**106Kbits ... 847Kbits/s**
Anticollisione-selezione	Complicata	Efficiente

ISO 15693



Smart Cards & EAC

- Sicurezza Elevata

  Le Smart Cards usano gli algoritmi di crittografia,chiavi di accesso segrete, e kla mutua autenticazione per proteggere i dati.

- Maggiore interoperabilità

  ISO Standard (14443A, 14443B, and 15693)

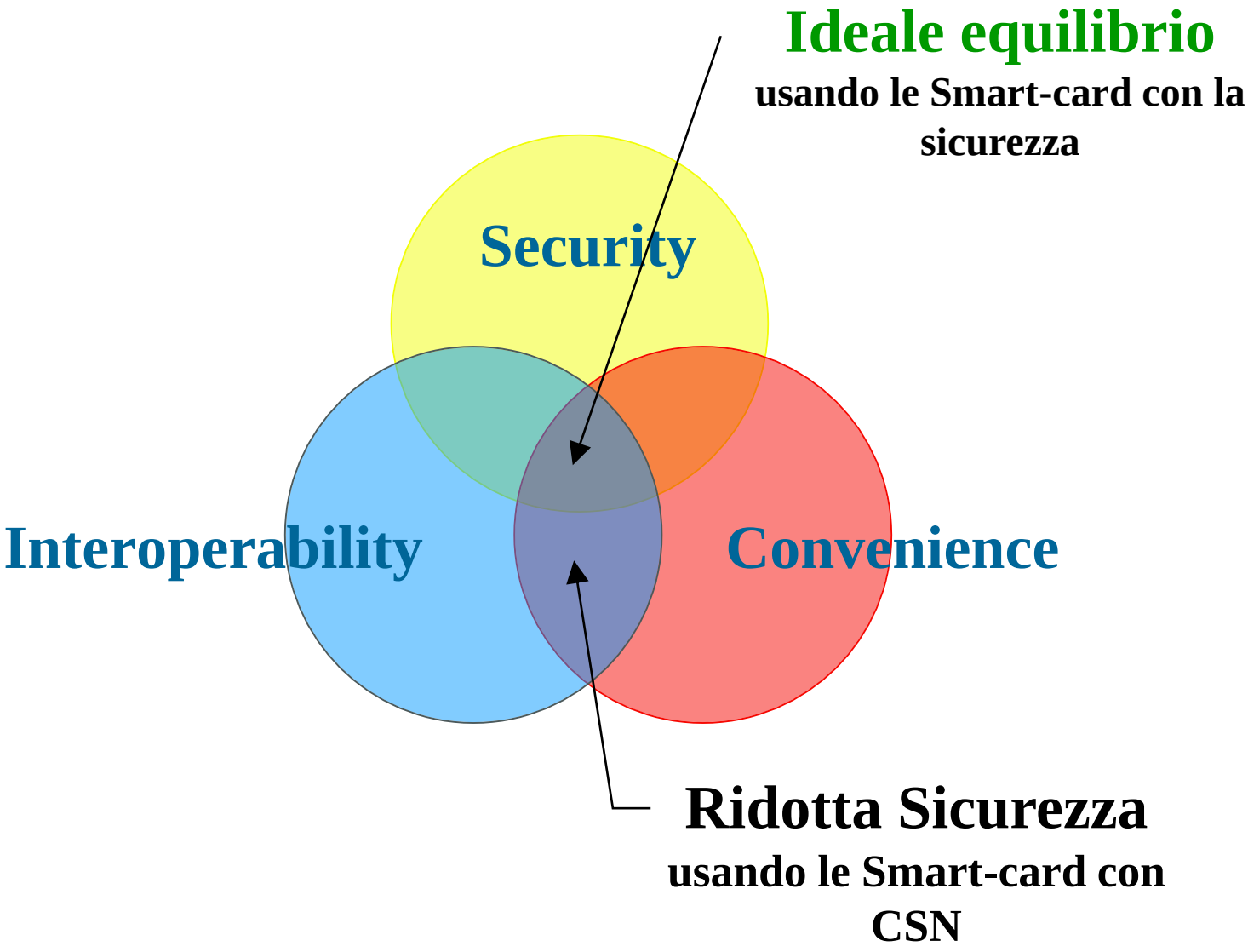
- Maggiore memoria

  Con queste caratteristiche il prodotto matura e si consolida.

- Possibilità di fare multiapplicazioni.

  Con l'incremento della memoria e l'elevata sicurezza, le tessere possono supportare diverse applicazioni, partendo dal controllo accessi, accessi logici, biometria, gestioni pagamenti etc.

Sicurezza-Flessibilità & Convenienza



How smart cards and EAC?

Anticollisione

Mutual autenticatione

Accesso alle memorie

Codici di lettura e conversioni

Definite dagli Standard ISO

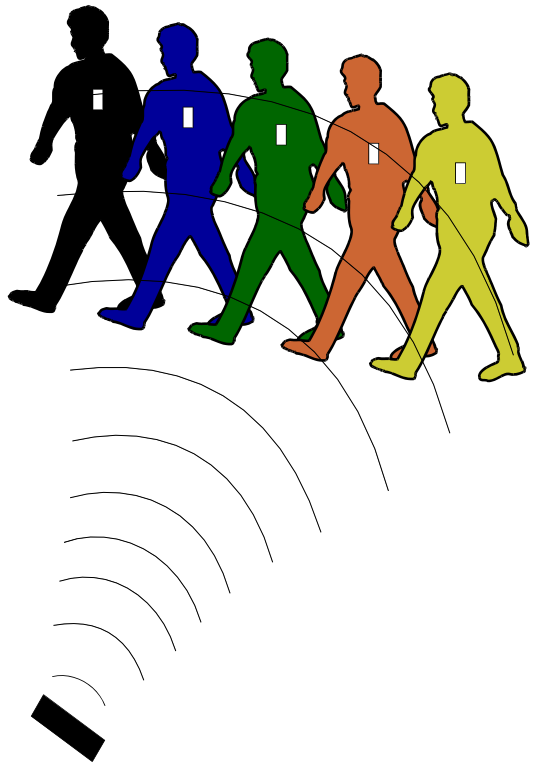
Specifiche delle tecnologie Smart-card

Specifiche del lettore

Wiegand output

Anticollisione

- Possibilità di leggere parecchi trasponders contemporaneamente
- ISO 14443 e15693 rappresentano vari metodi per implementare l'anticcolisione.



Lo scopo delCSN è di essere in grado di indirizzare tessere personali quando sono presenti più di una tessera nel campo RFID nello stesso momento.

CSN Code Serial Number (da fabbrica)

A CSN è come il vostro numero civico dell'abitazione…..Tutti lo possono leggere!

Ma per entrare nella vostra casa……Ti serve la chiave!

Organizzazione Memorie

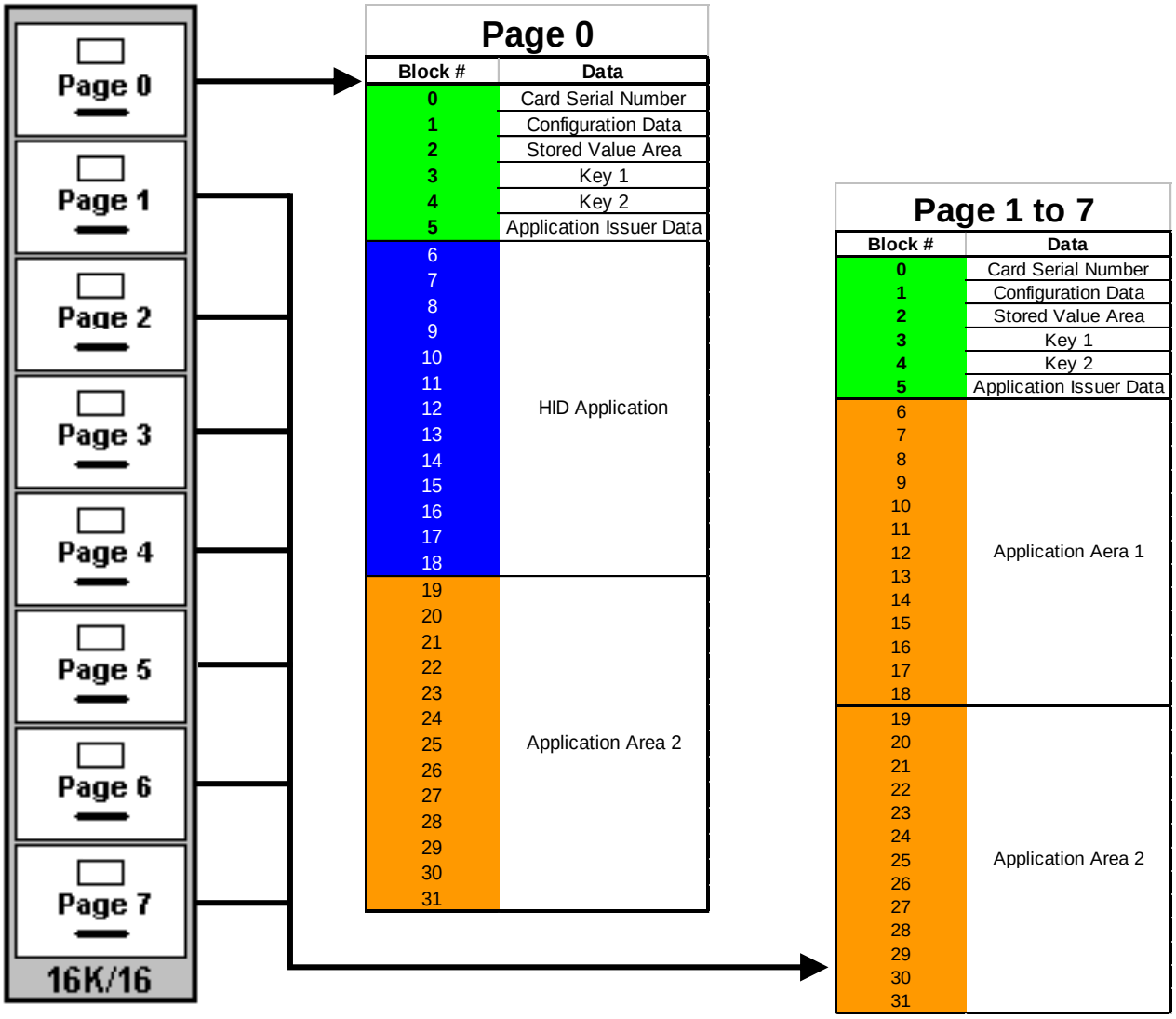
- MIFARE :Settori
- ***iCLASS*** : Libri-Pagine-Aree
- Legic : Applicationi
- *DESFire* : Applicationi - Files

MIFARE

		Bytes															
Sector	**Bloc**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	**Description**
0	0																	Sector trailer
	1																	Data
	2																	Data
	3																	Data
1	0																	Sector trailer
	1																	Data
	2																	Data
	3																	Data
15	0																	Sector trailer
	1																	Data
	2																	Data
	3																	Data

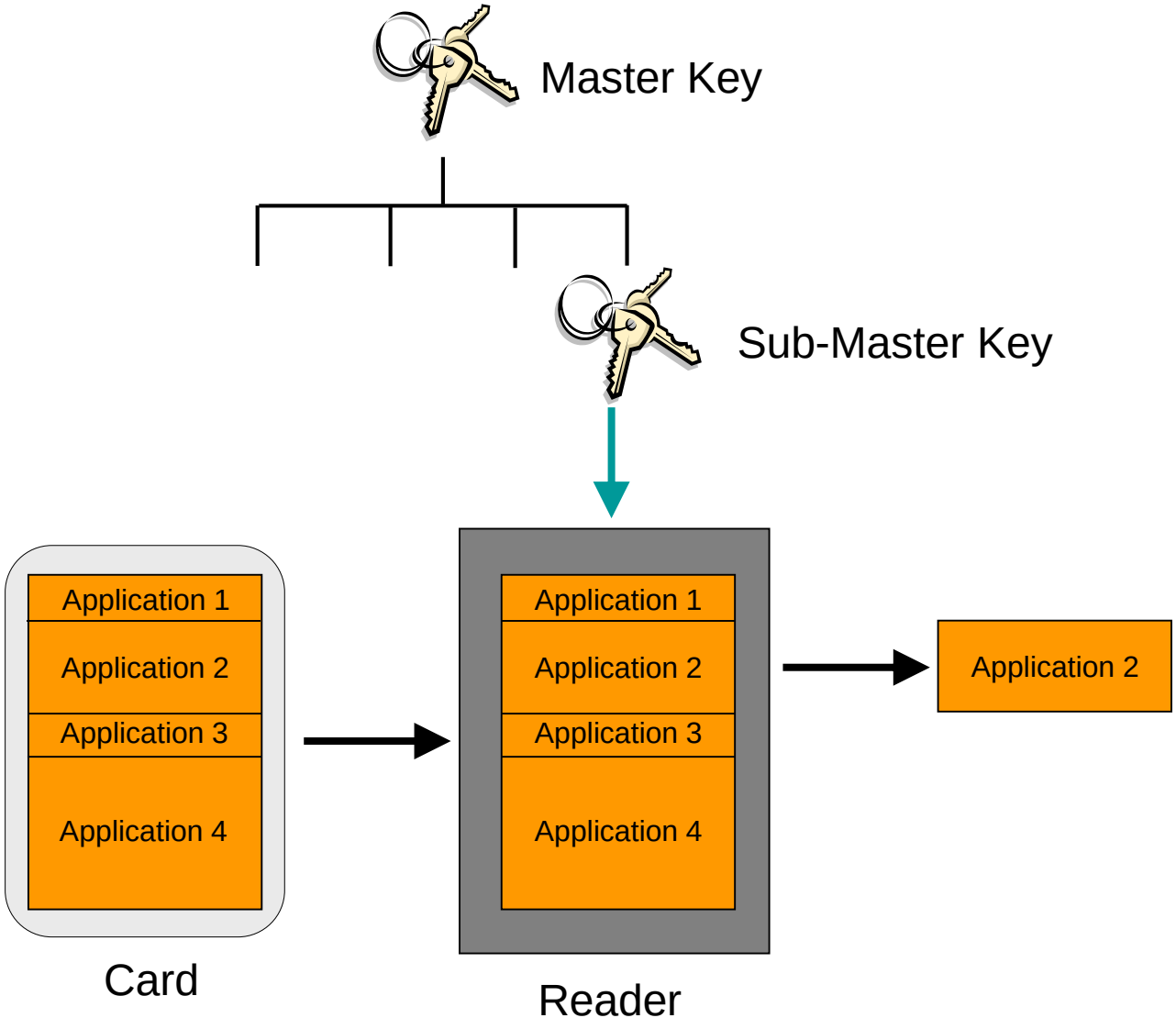
→ Available for applications

iCLASS

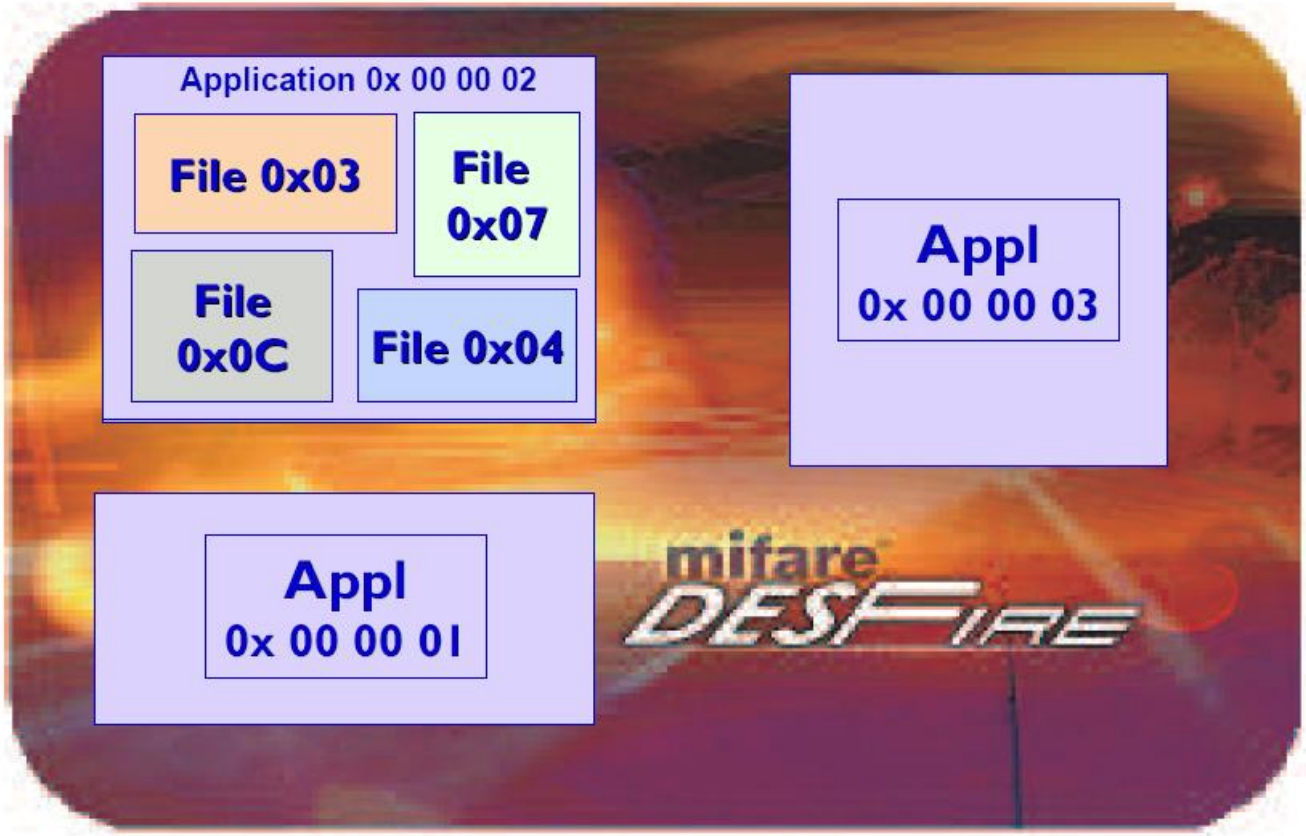

Page 0
Page 1
Page 2
Page 3
Page 4
Page 5
Page 6
Page 7
16K/16
Page 0
Block # | Data
0 | Card Serial Number
1 | Configuration Data
2 | Stored Value Area
3 | Key 1
4 | Key 2
5 | Application Issuer Data
6–18 | HID Application
19–31 | Application Area 2
Page 1 to 7
Block # | Data
0 | Card Serial Number
1 | Configuration Data
2 | Stored Value Area
3 | Key 1
4 | Key 2
5 | Application Issuer Data
6–18 | Application Aera 1
19–31 | Application Area 2

LEGIC

Accesso ai dati di applicazione



DESFIRE

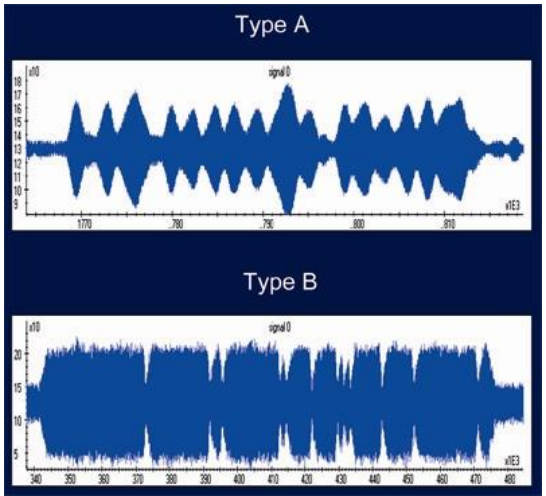

Application 0x 00 00 02
File 0x03
File 0x07
File 0x0C
File 0x04
Appl 0x 00 00 03
Appl 0x 00 00 01
mifare DESFire

Rischi alle applicazioni di tessere di prossimità

- Eavesdropping-Intercettazione
  Intercettazzione della comunicazione tra la tessera di prossimità. ed il lettore
- Replay attack
  Copiare e replicare il segnale intercettato tra la tessera di prossimità ed il lettore.
- Interrogation
  Spedire I dati richiesti alla tessera di prossimità.
- Applicazione /Modifica Dati
  Spedire I dati e scriverli nella memoria.

Rischio: Eavesdropping Clonazione

- Intercettare nella tessera le informazioni personali:
  - Chiavi
  - Codici
  - PIN
  - dati
- L'intercettazione delle informazioni (violazione della privacy)
- Tessera al lettore più di 5 metri.
- Lettore verso la tessera alcune centiinaia di metri.

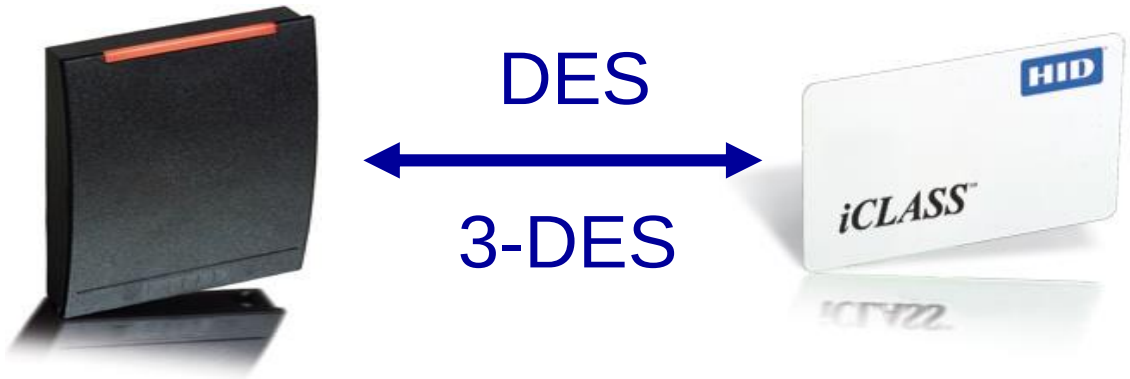


Clonazione nel giusto contesto

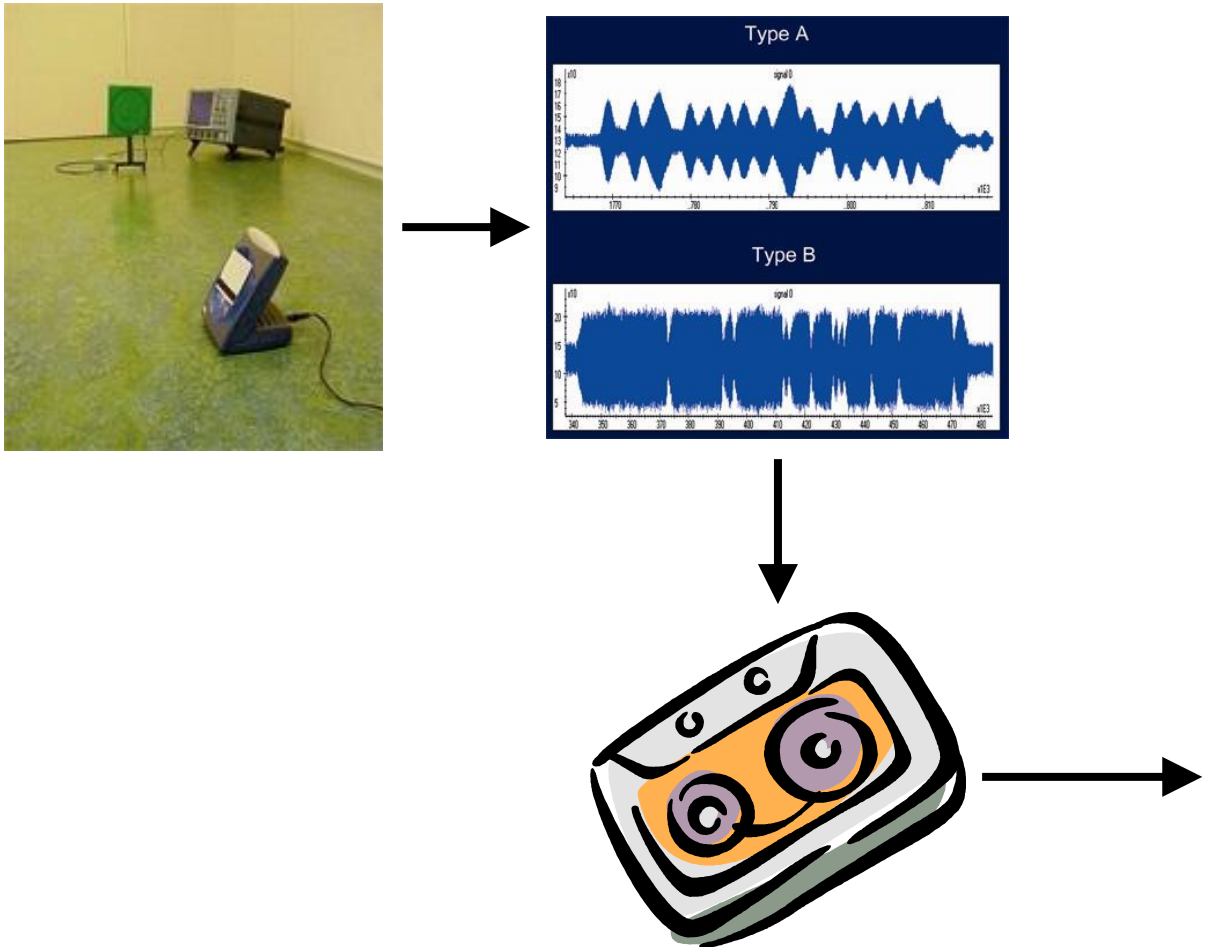
- Cosa è necessario per costruire questo attacco:
  - Knowledgenecessario: essere esperti di Radio Technology, Programmazione Microcontroller , Ingegneri elettronici.
  - Costo : 200 EUR
  - Tempo inizialmente 6 settimane poi 1 giorno.
  - L'attaco si può diffondere via intenet.
- Cosa a volte è successo:
  - Installare falsi lettori in buone posizioni senza avvisare
  - Frodi ATM Bancomat molto diffuse in Italia.Bande organizzate dall'EST .
  - La maggioranza delle grosse frodi non viene dichiarata.
  -

How to counter : Data Encryption

Criptazioni



Rischi clonazioni



How to counter : Mutual authentication

Mutua autenticazione

Richiesta al tag(Excite)

CSN and RND1

RND2 and Challenge

Risposta

Rischio/applicazione:modifica dati interrogazioneThreat

Soluzione:

Protezione con una chiave

Lunghezza chiavi

- 40 bit

  Tag-IT (TI) → già crackata da studenti
  http://rfidanalysis.org

- 48 bit

  MIFARE → già crackata da studenti(caso Amsterdam) e da produttori disonesti.
  www.smartcard.co.uk/mifare.html

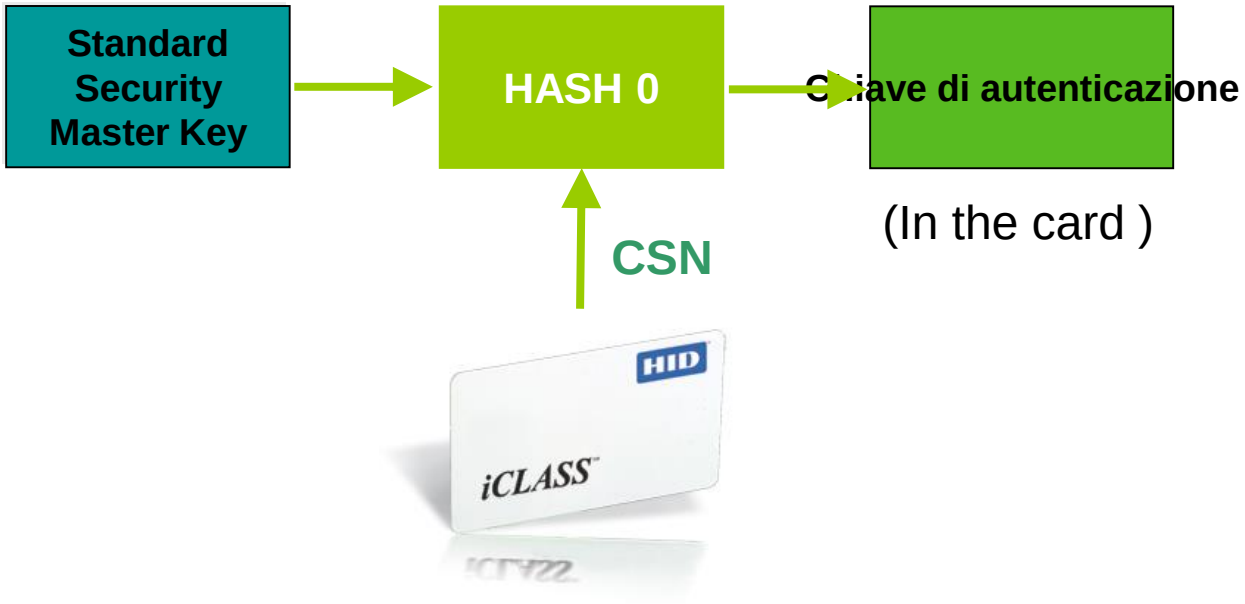
- 64 bit

  iCLASS, LEGIC, My-D, I Code

- 128 bit

  DESFIRE

Protezione Chiavi



La Sicurezza è tutto in una gestione rischi

- Il danno economico ed/o il danno all'immagine, creato dalle copie o clonazioni, e dalle forzature ai relais dipende dal sistema.
  - Il valore dei beni
  - Il tempo, soldi,e l'esperienza richiesti per fare l'attacco.

- L'investimento per forzare e rompere un sistema a volte può essere più alto che il potenziale ritorno economico.
- La clonazione delle tessere Mifare nei sistemi di pagamento dei Trasporti di Amsterdam ha scatenato un putiferio.
- NXP società produttrice dei chip Mifare,ex Phlips, ha studiato subito dopo questa grossa frode economica, MIFARE-PLUS, che avrà un microprocessore a bordo.

(The CSN) IL numero di Codice Seriale

- In armonia con le norme ISO 1443A 1443BAccording to the ISO 14443A, 14443B, and 15693 standard, le tessere di prossimità smart card debbono avere un unico codice seriale.

- Molti termini per definire la stessa cosa :
  - **CSN** ⇨ Card Serial Number
  - **UID** ⇨ Unique ID
  - **CUID** ⇨ Card Unique ID
  - **PUPI** ⇨ Pseudo Unique PICC Identifier
    - » PICC ⇨ Proximity Integrated card Circuit

- **CSN** verrà usato in questa presentazione.

Cosa rappresenta il CSN usato nel Controllo Accessi?

- Fino alla venuta del CSN nella tessera nella tessera era presente un unico numero, I produttori usavano questo per costruire lettori che usavano codice per identificare gli utenti. : Il CSN è un unico numero codice , scritto permanentemente nella memoria non cancellabile della fabbrica di produzione, nella fase di creazione dei Wafer. Non si possono modificare ed è garantito che sono unici.
- L'unicità e la sicurezza di questo è molto discusso dagli esperti del settore.

Programmazione Chips del CSN

- “RFID: Applications, Security, and Privacy” by Simon Garfinkel and Beth Rosenberg:

Tuttavia Anche se il numero di serie può essere bruciato nel chip dal produttore, che è comune anche per i chip da programmare in campo da parte dell'utente finale. Alcuni chip accetterà solo un unico numero di serie, mentre altri chip permettono il numero di serie per essere modificato dopo che è bruciato "

.

Programmable CSN's (cont.)

- ST 13.56 MHz LRI64 data sheet:

  " LRI64 utilizza i primi 8 blocchi (blocchi di 0 a 7) per memorizzare i 64-bit identificatore univoco (UID). L'UID è utilizzato durante la sequenza di anti-collisione (Inventory). E 'scritto, da ST, al momento della fabbricazione, ma parte di esso può essere accessibile al cliente e cliente-scrivibile, su richiesta speciale. "

- ATMEL 13.56 MHz ISO 14443-B CryptoRF data sheet:

"PUPI [CSN] è un numero a 32 bit di serie definite dal cliente nel corso della personalizzazione, la PUPI di solito è unica. ... PUPI può essere impostato su qualsiasi valore ".

→ Usando il CSN non è sicuro

Emulazione CSNC

Molti protocolli si possono emulare in ISO 14443 or 15693 CSN

→ CSN può essere clonato e riprodotto

CSN Security

- David Engberg of Corestreet, Cambridge, MA USA:

  Il numero di serie non ha protezioni crittografiche o a livello di protocollo per impedire a un utente malintenzionato di far valere lo stesso numero seriale di qualsiasi carta reale. Con l'implementazione di ISO 14443 direttamente, un utente malintenzionato può imitare qualsiasi CUID desiderato ".

- Report on “RFID Security” by Prof. Dr. Heiko Knospe and Prof. Dr. Hartmut Pohl of University of Applied Sciences, Cologne, Germany:

  "L'autenticità di un tag è a rischio dato che l'identificatore univoco (UID) di un tag può essere falsificati o manipolati. I tag non sono generalmente resistenti alle manomissioni

→ I ricercatori e gli esperti di crittografia dicono che usare il CSN per l’identificazione non è una buona idea.

Lunghezza ISO 14443A CSN

Le specifiche ISO 14443A dicono che le specifiche della lunghezza può essere 4, 7, or 10 bytes :

- **32 bits** → realmente solo **24 bits** dal primo byte contiene le informazioni.

The ISO 14443A specifiche citano che la CSN possono essere 4, 7, o 10 byte di lunghezza:
:

32 bits → realmente solo **24 bits**dal primo byte contiene informazioni

56 bits → really only **48 bits** dal primo byte contiene informazioni mfr. ID
80 bits → really only **72 bits**dal primo byte contiene informazioni mfr. ID

Per MIFARE standard chip : **24 bits** → **only 16.777.216** CSN values

"Con più di 500 milioni di chip smart card e 5 milioni di lettore componenti venduti, MIFARE è stato selezionato come il più di successo della tecnologia contactless smart card. "
source : www.mifare.net

Chips con CSN Random

- RFID Handbook by Klaus Finkenzeller:

In contrasto con schede di tipo A, il numero di serie di una scheda di tipo B non è necessariamente legata in modo indissolubile al microchip, ma può anche consistere in un numero casuale, che è stato recentemente determinato dopo ogni power-on reset

- ISO 14443 specifications :

  L'UID [CSN] è un numero fisso unico o un numero casuale che viene generata dinamicamente dal PICC [smart card contactless]. “The UID

→ Utilizzo di un CSN per identificare una scheda che utilizza casuale CSN non funzionerà

Problemi Logistici

- Usando solo il CSN non permette l'esistenza di numeri di carte consecutive che rende più difficile:

  - Modificare le credenziali di accesso, specificando una serie di carte, cioè 1-100 Inserisci numeri di carte nel sistema in quanto sono grandi numeri non continua fino a 20 caratteri numerici

- Sarà necessario un lettore per fare l'enrollment.

→ Uso del CSN per il controllo di accesso non conviene

Problemi sulleDistanze di letture CSN

- Perché la lettura del CSN di una smart card contactless richiede meno potenza, distanze di lettura sono spesso maggiori
- Anche se questo può essere considerato un vantaggio, rende di fatto possibile spiare da una distanza più lunga

- Ricorda che non è richiesta nessuna sicurezza per leggere il CSN.
- Inoltre, dà una falsa impressione che le prestazioni di un determinato produttore è maggiore di quanto non sia effettivamente

→Sebbene l'utilizzo della CSN può permettere una carta da leggere ulteriormente, è fatto a rischio la sicurezza è diminuita

→Anche se con il CSN può permettere una carta da leggere ulteriormente, è fatto a rischio la sicurezza è diminuita

Livelli di Sicurezza