26.11.2012

Gianni Becattini

CARTE ELETTRONICHE

Un riepilogo

MASTER CLICKUTILITY NOVEMBRE 2012

AEP Ticketing solutions

Questo sono io

Gianni Becattini
A.D. di AEP Ticketing Solutions

AEP Ticketing solutions

Ultimi incontri

MASTER CLICKUTILITY NOVEMBRE 2012

AEP Ticketing solutions

Introduzione

Il contratto di trasporto

- "il vettore si obbliga, verso corrispettivo, a trasferire persone o cose da un luogo ad un altro... ...e, nel frattempo, a custodirle" (C.C. art. 1678)
- Il passeggero è vincolato alla effettuazione di un pagamento in denaro in cambio del servizio ricevuto.

Titoli di viaggio

- Cartacei tradizionali
- Leggibili per via elettronica
  - magnetici
  - smart card
  - altro

Differenze basilari

TDV	Tradizionali	Elettronici
Lettura	No	Sì, molti bit
Scrittura	Validato/non validato*	Sì, molti bit

** Con le vecchie obliteratrici con taglierina, si arriva a scrivere una decina di bit*

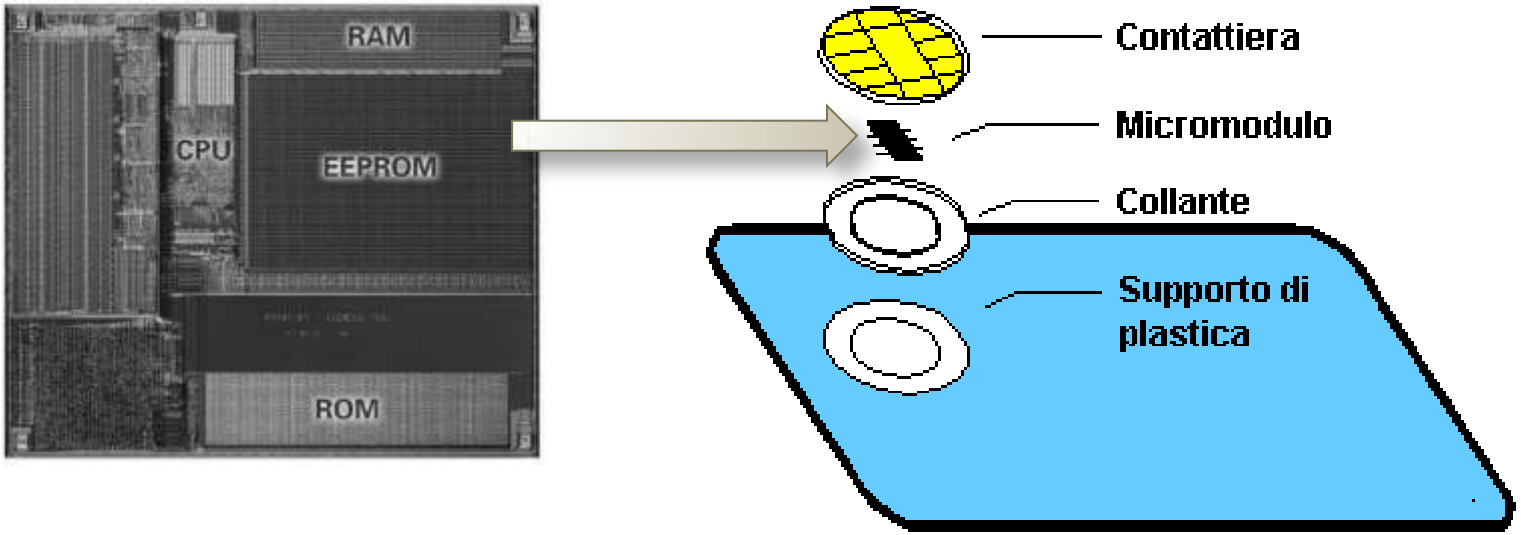
Carte contactless

Carte contactless

- Sono un possibile supporto elettronico per Titoli Di Viaggio
- Allo stato attuale della tecnica sono quelle più largamente utilizzate
- Altri supporti sono possibili (es. NFC)

Struttura fisica

- Dette anche ***chip card*** in quanto hanno un circuito integrato ("chip") a bordo



Classificazione per tipo

- **A memoria,** poco *smart*, sicurezza minore o assente. Es. MIFARE, CTS ecc.
- **A microprocessore,** *smart card*, sicurezza elevata. Es- Calypso, DesFIRE ecc.

Requisiti dei TDVE

- Memorizzare informazioni
- Scriverle o rileggerle in sicurezza

Vantaggi carte contactless

- **Praticità,** comode e rapide da usare
- **Capacità elevata,** fino a parecchi K
- **Sicurezza potenzialmente elevata**
- **Apparati di convalida «a stato solido»**, più semplici, compatti e robusti

Svantaggi

- **Costo,** limite minimo assai maggiore rispetto ai biglietti tradizionali o magnetici
- **Verifica,** necessità di appositi apparati per la verifica a bordo

Classificazione per interfaccia

- **A contatti** (contact)
- **Senza contatti** (contactless)
- **Mista** (contact + contactless) – detta anche *dual interface* o *combo*

Smart card a contatti

- L'energia viene fornita tramite un connettore realizzato sulla superficie stessa della carta.
- Attraverso altri contatti avviene la comunicazione.

Carte a contatti

- Largamente impiegate in campo bancario (POS, ATM...), non sono quasi più in uso come TDV

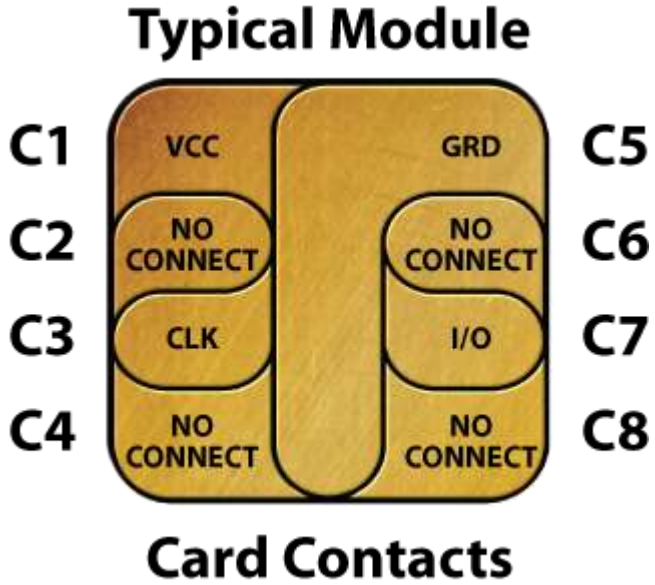


*Image Courtesty of CardLogix

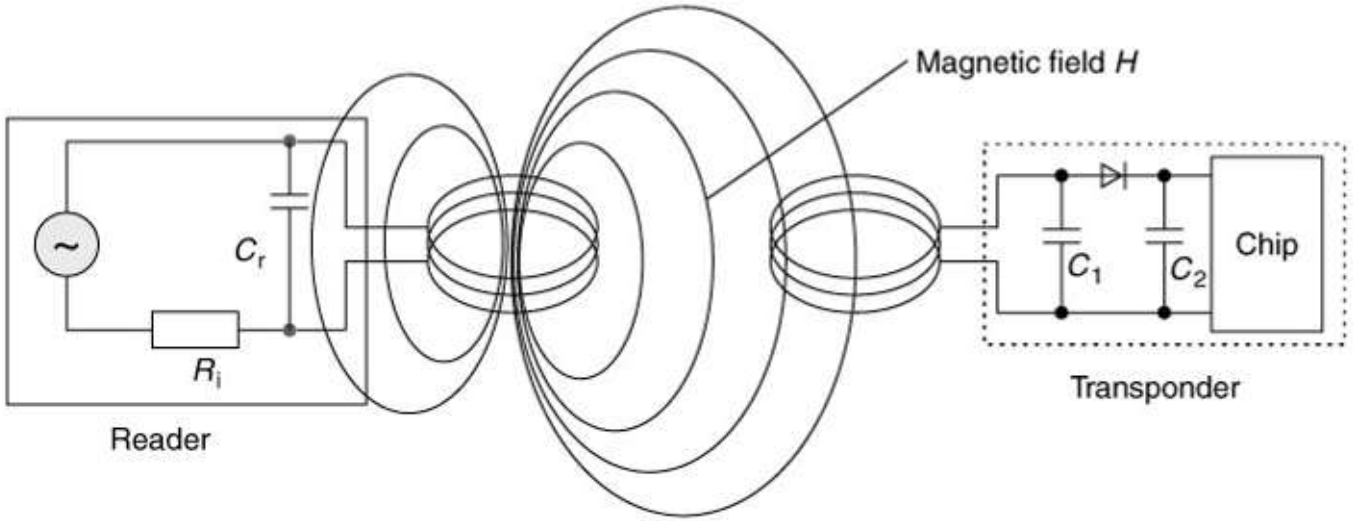
AEP Ticketing solutions

Pillole di tecnica

Come funzionano le smart card contactless?

Smart card contactless

- L'energia alla carta è fornita dal campo magnetico a RF prodotto dal terminale
- La comunicazione avviene tramite lo stesso campo magnetico



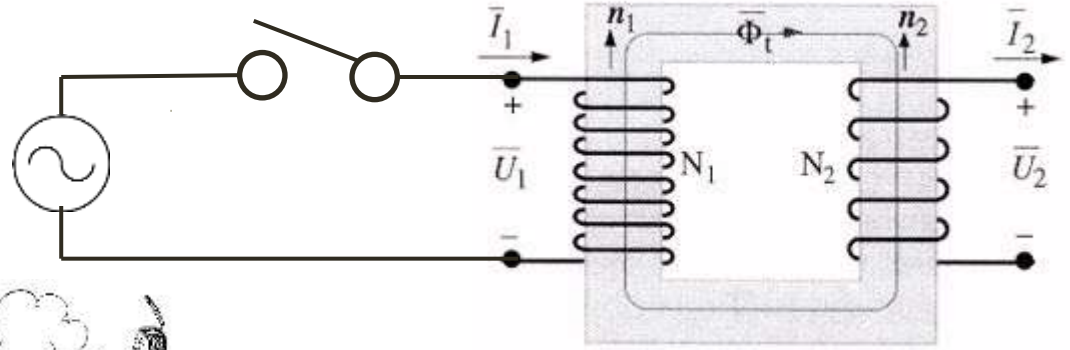
Alfabeto Morse

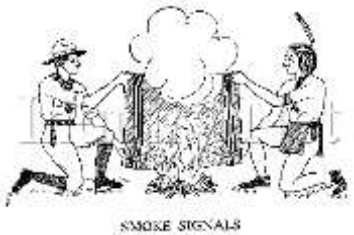
INTERNATIONAL MORSE CODE

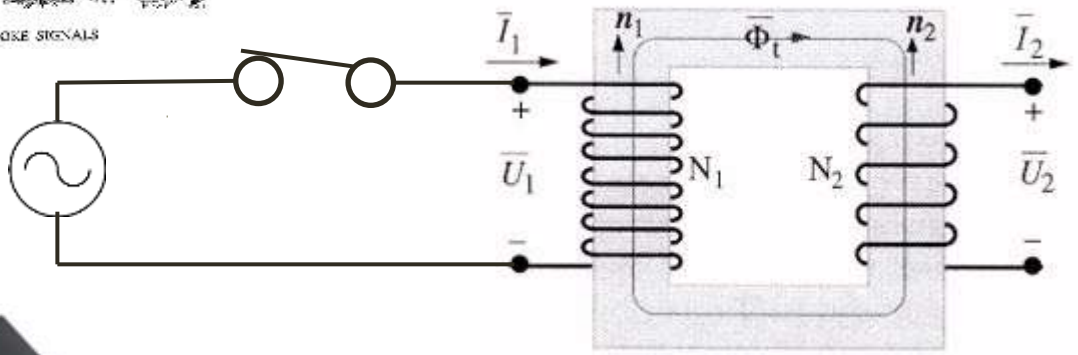
1. A dash is equal to three dots.
2. The space between parts of the same letter is equal to one dot.
3. The space between two letters is equal to three dots.
4. The space between two words is equal to five dots.

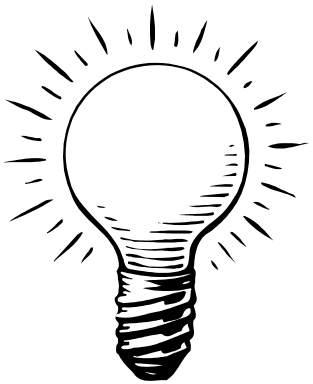
A • —	U • • —
B — • • •	V • • • —
C — • — •	W • — —
D — • •	X — • • —
E •	Y — • — —
F • • — •	Z — — • •
G — — •	
H • • • •	
I • •	
J • — — —	
K — • —	1 • — — — —
L • — • •	2 • • — — —
M — —	3 • • • — —
N — •	4 • • • • —
O — — —	5 • • • • •
P • — — •	6 — • • • •
Q — — • —	7 — — • • •
R • — •	8 — — — • •
S • • •	9 — — — — •
T —	0 — — — — —

Comunicazione → carta

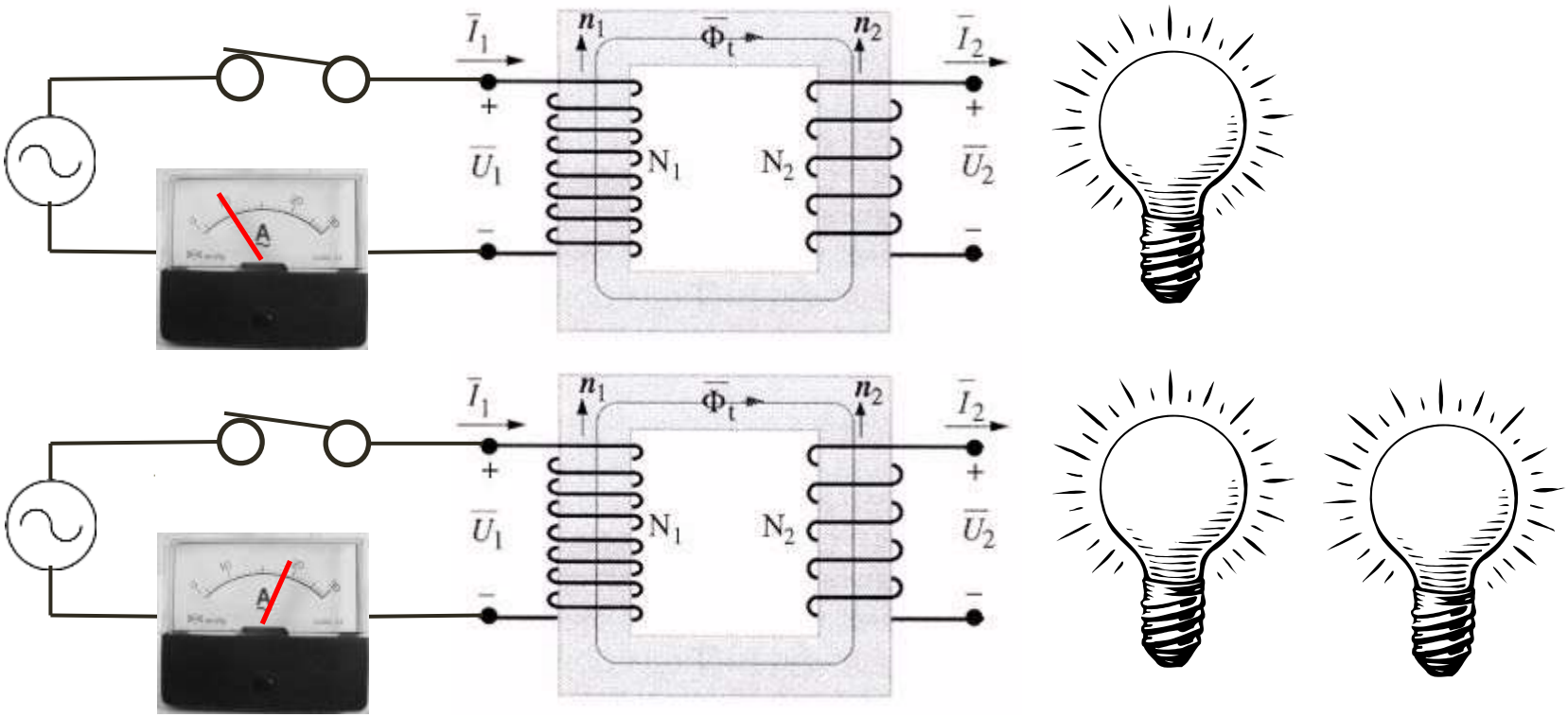






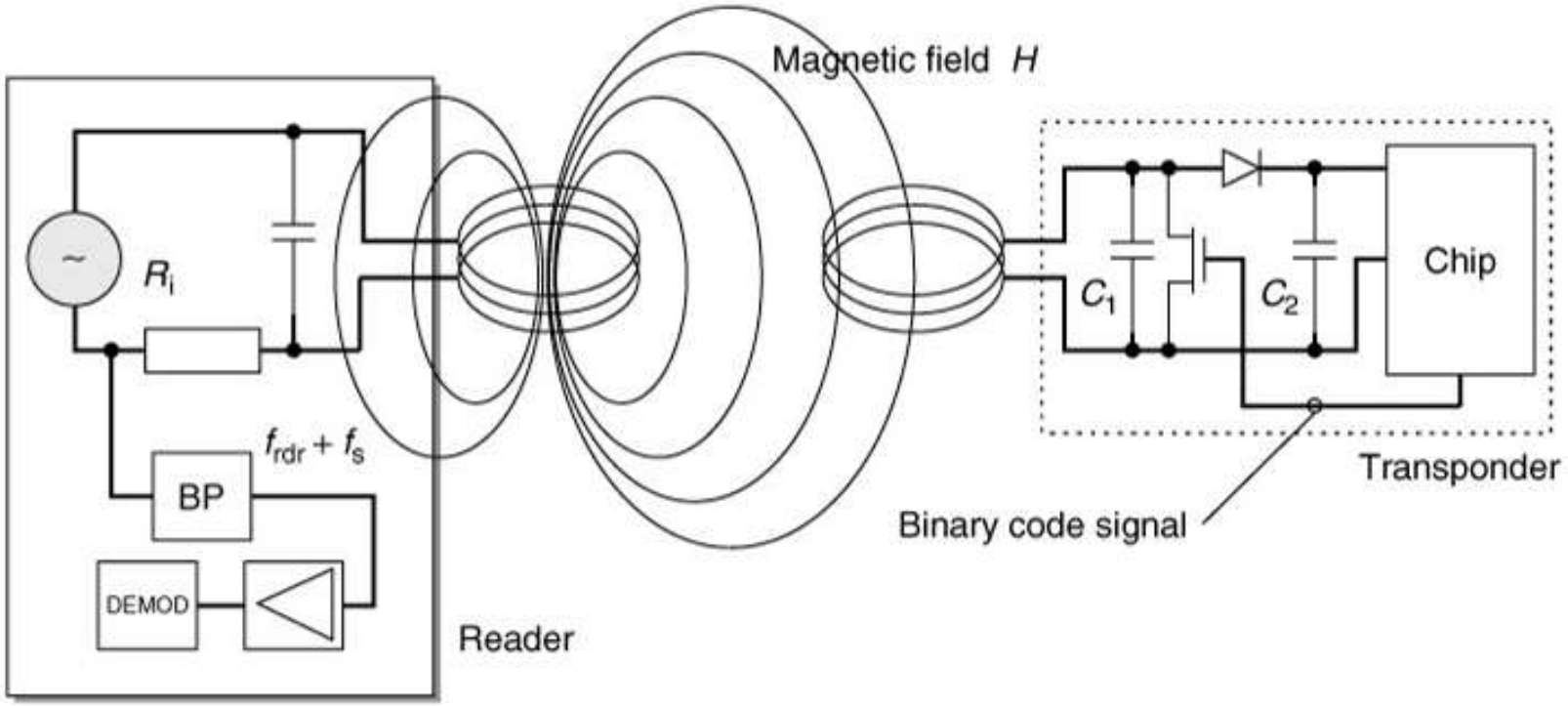


Comunicazione → terminale

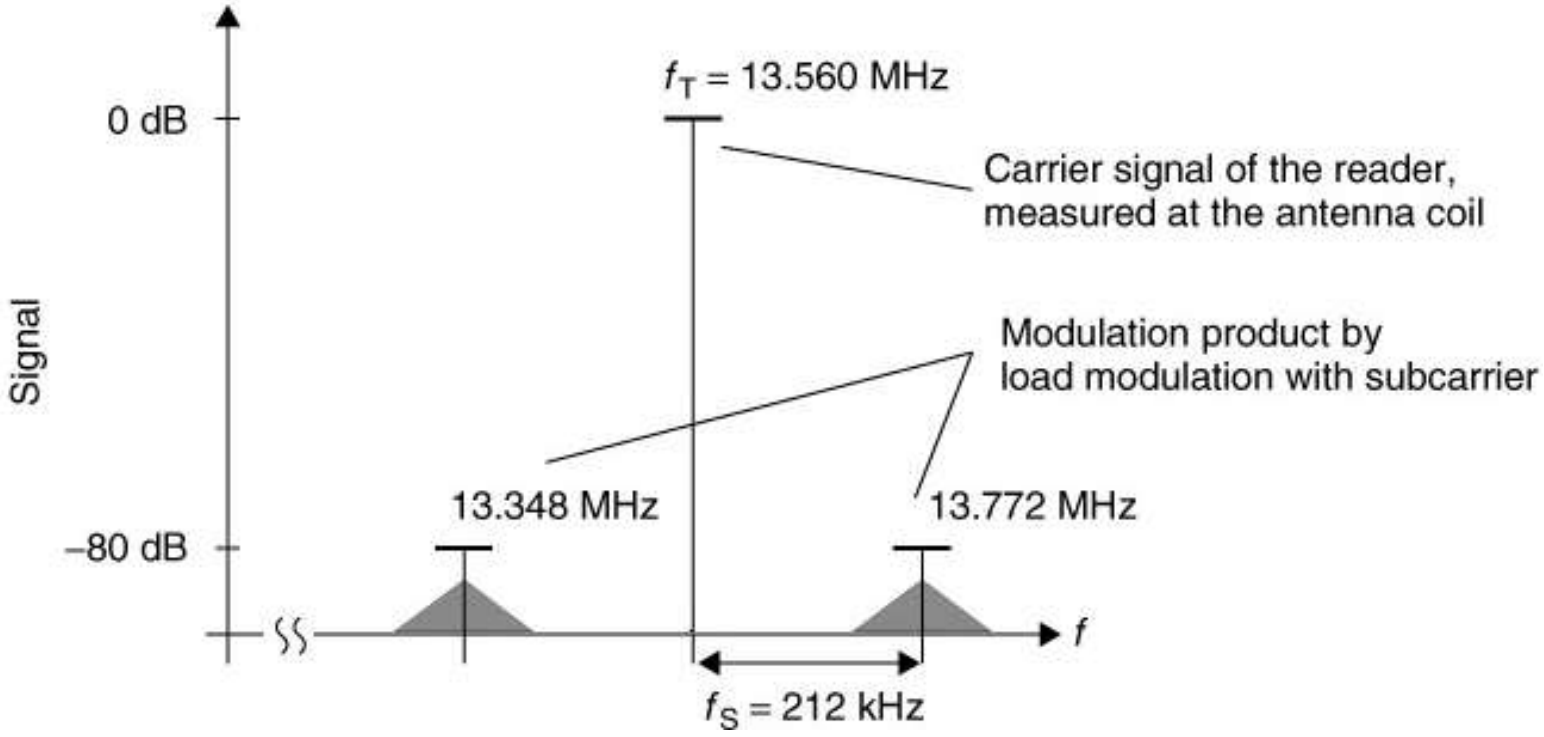


Comunicazione carta/terminale

(modulazione di carico)

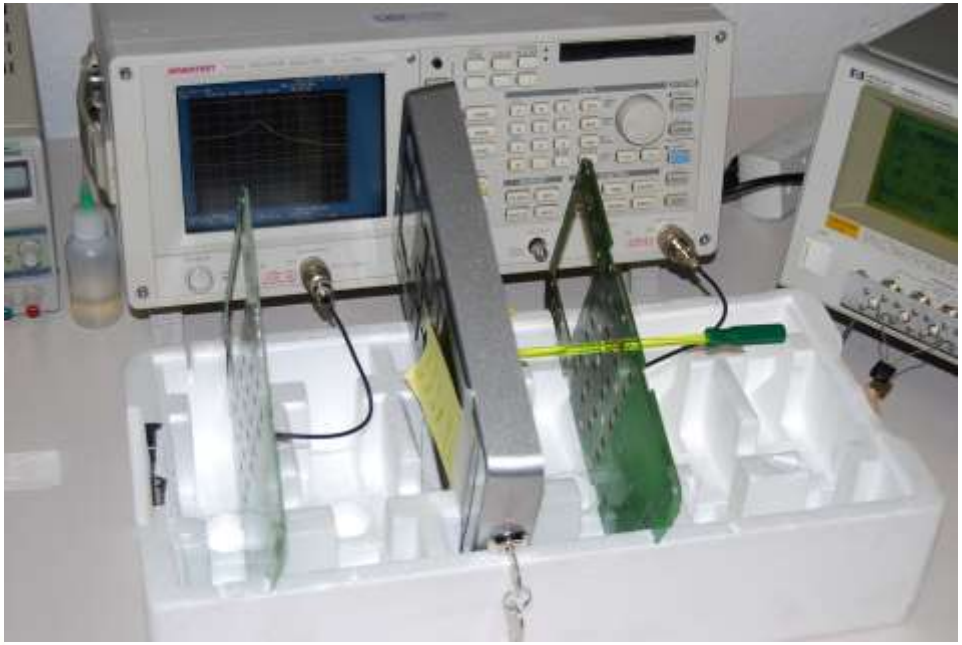


Sottoportanti



Poca energia, molte norme

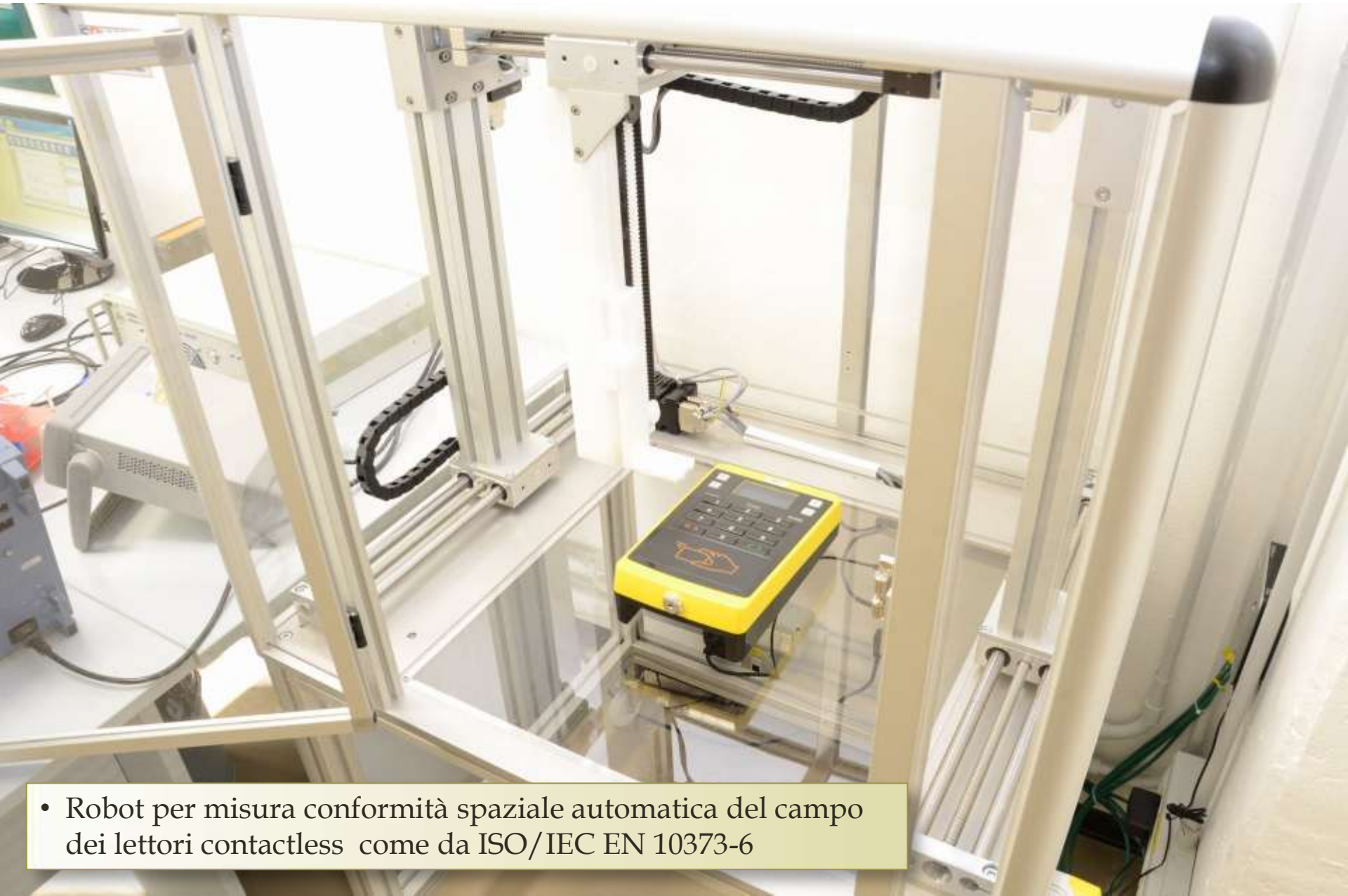
- Quello della comunicazione contactless è un problema di grande complessità, anche dal punto di vista teorico



Laboratorio contactless

- ISO IEC 14443-1, 2, 3 e 4 A & B
- ISO IEC 10373-6

Robot misure contactless



- Robot per misura conformità spaziale automatica del campo dei lettori contactless come da ISO/IEC EN 10373-6

La conferma: primi al mondo

AEP Ticketing solutions

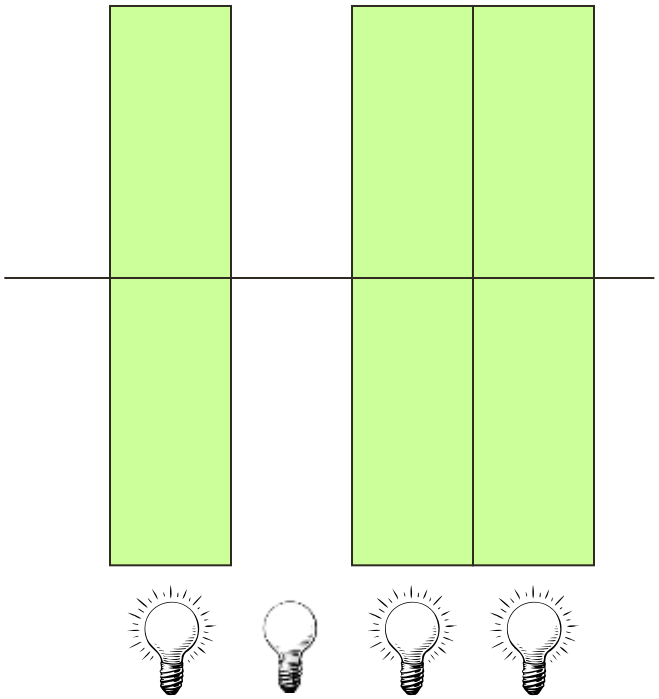
calypso 3

Nov

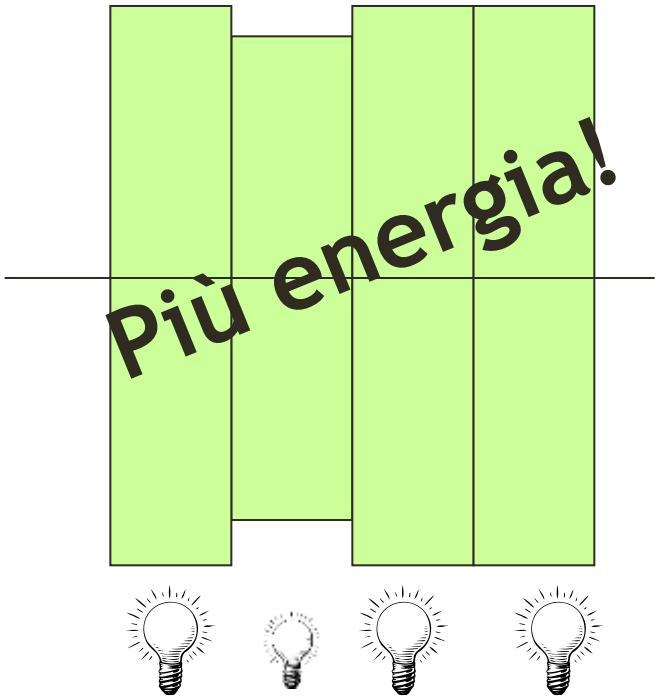
Ticketing solutions

ISO 14443

Tipo A – modulazione 0-100%



Tipo B – modulazione 90-100%



La sicurezza

I numeri scritti nelle smart card sono denaro!

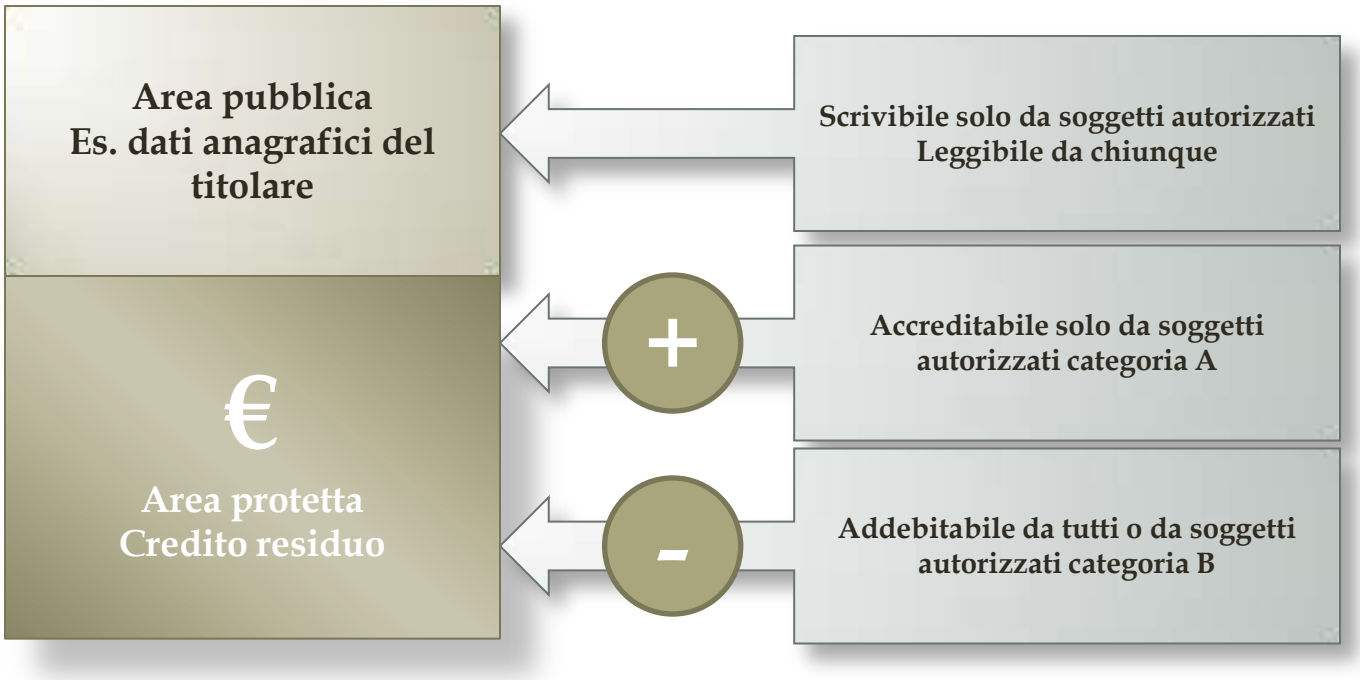
Esigenze generali

- Tutte le operazioni del Sistema di Bigliettazione Elettronica devono avvenire in modo da ridurre al minimo il rischio di frode
- Solo le entità autorizzate devono poter emettere o modificare i TDV
- Deve essere impossibile creare TDV falsi
- Sono auspicabili regole configurabili per i diritti connessi alle possibili operazioni

Non è un optional

- I sistemi di pagamento elettronico del trasporto pubblico finiranno per integrarsi sempre più in sistemi di tipo generale
- La sicurezza è un requisito essenziale in qualunque sistema di pagamento
- La sicurezza del sistema è pari a quella dell'elemento più debole

Esempio: una carta con borsellino



Lo strumento: la crittografia

- Attraverso l'uso delle chiavi e di opportuni algoritmi, è possibile **crittografare** i dati.

Servizi della crittografia

- **Confidenzialità**, solo i destinatari del messaggio possono leggerlo
- **Integrità**, il messaggio crittografato viene trasmesso senza perdita di informazioni
- **Autenticità**, il destinatario è in grado di verificare che il messaggio non sia stato alterato nel corso della trasmissione

Crittografia elementare

M	a	s	t	e	r		C	l	i	c	k	u	t	i	l	i	t	y		2	0	1	2	
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
N	b	t	u	f	s	!	D	m	j	d	l	v	u	j	m	j	u	z	!	3	1	2	3	!

Algoritmo segreto = bassa sicurezza

Principi

- **Principio di Kerkchoff** (1835-1903): la sicurezza di un codifica crittografica deve essere basata su codici segreti detti "chiavi" e non sulla segretezza dell'algoritmo utilizzato.
- **Nessun soggetto** dovrebbe essere fisicamente in possesso delle chiavi.

Sicurezza della transazione

- **Mutua autenticazione** – il terminale sta "parlando" con una carta legittimata e che la carta sta "parlando" con un terminale legittimato;
- **Scambio sicuro** - anche se i dati scambiati sono intercettati, non devono risultare comprensibili;
- **Firme digitali** - garantiscono l'autenticità della registrazione della transazione.

Algoritmi crittografici

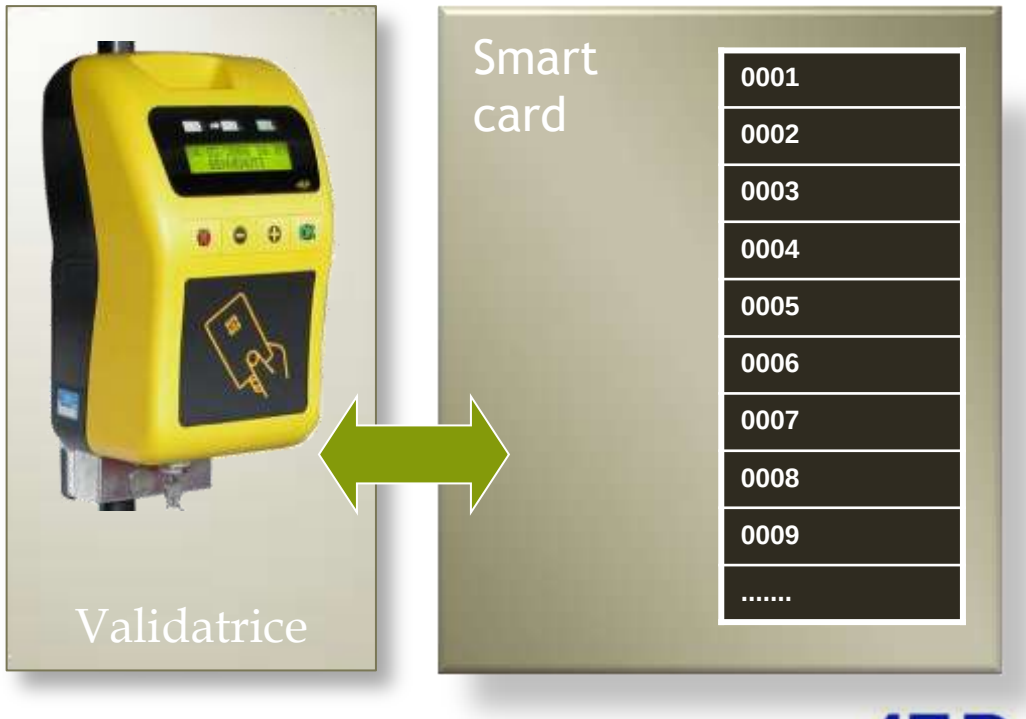
- DES (Data Encryption Standard), introdotto nel 1977 da IBM assieme allo US National Bureau of Standards e definito dalla norma FIPS 46; usa una chiave a 56 bit.
- 3-DES (triplo DES) due chiavi a 56 bit, più sicuro.
- XDES/TDES, sicuri quasi quanto il 3-DES ma più semplici da implementare.
- AES (Advanced Encryption Standard) norma FIPS 197; chiavi a 128, 192 o 256 bit (AES-128, AES-192 or AES-256).

Memoria o microprocessore?

Carte a memoria

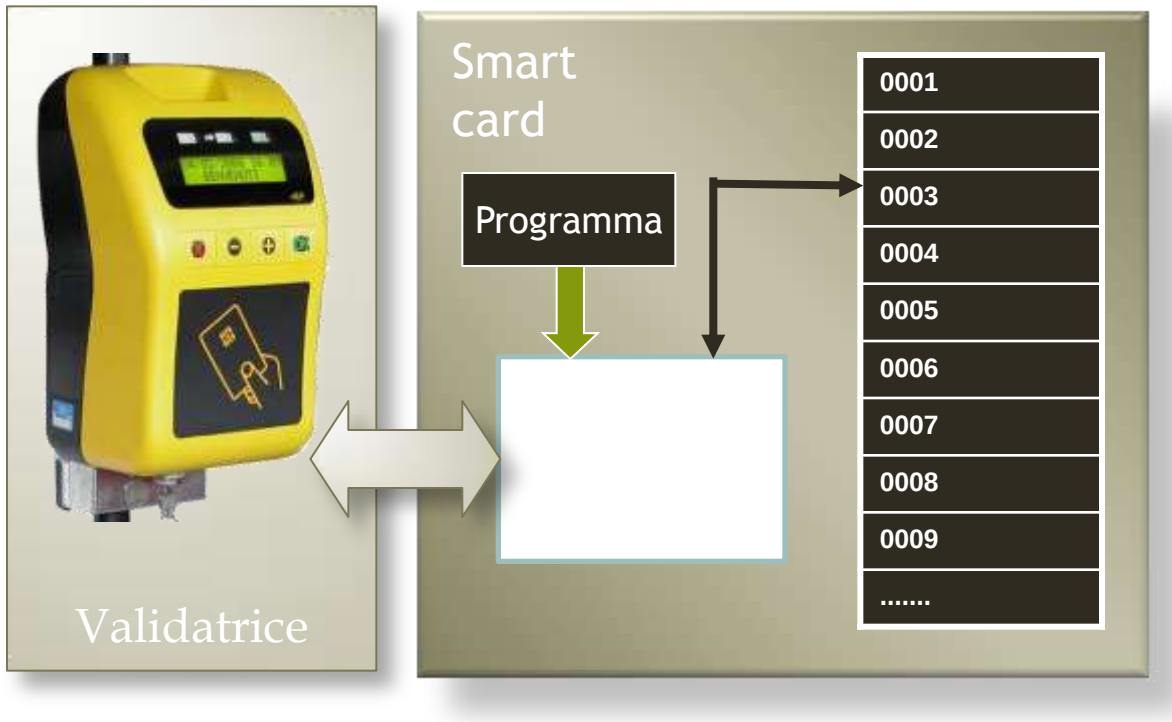
- La carta viene vista come sequenza di locazioni dove è possibile scrivere e leggere dati, spesso con qualche forma di securizzazione (adatta per biglietti)

Scarsa capacità di elaborazione
= bassa sicurezza



Carte a microprocessore

- La carta è vista come un computer con il quale dialogare.
- Il comportamento della carta è determinato da un **programma**.



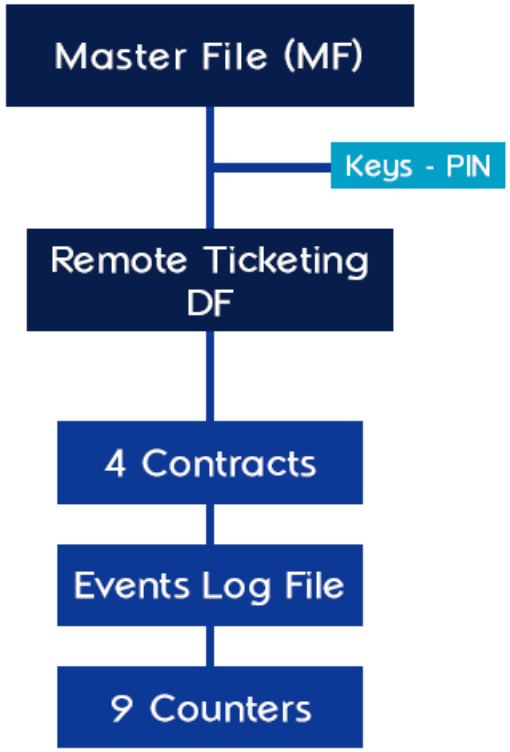
Smart card a µP

- Può eseguire non solo scrittura e lettura ma anche **processo** di informazioni
- Quindi crittografia → sicurezza elevata

La «Maschera»

- Il nome, da evitare, trae origine dalla maschera fotografica delle ROM
- Usata spesso con il significato di "software della smart card"
- Il nome corretto è "firmware" o "Sistema Operativo"
- Da non confondere con il tracciato dei dati
- Caratterizza funzionalmente il comportamento della smart card

Il file system



Prestazioni e costi

*Image Courtesy of CardLogix

Pagamento elettronico del TPL
Uno sguardo sul mondo...

Pagamento TPL

- Carte del mondo trasporti (es. Calypso)
- Carte di credito contactless (es. Paypass)
- Carte emulate da NFC (es. Calypso, Paypass)
- *Altri*

Standardizzazione

- ISO
- Calypso
- EMVco
- NFC
- *Altri*

Gli standard ISO

Tutte le carte contactless condividono oggi la tecnologia di base

ISO 7816

- **ISO 7816 parte prima**: caratteristiche fisiche delle carte a contatti, resistenza a fenomeni fisici quali raggi UV e raggi X, campi elettromagnetici, elettrostatici ecc. Definisce inoltre le caratteristiche meccaniche e di resistenza allo stress
- **ISO 7816 parte seconda**: definisce la posizione e la dimensione dei contatti
- **ISO 7816 parte terza**: definisce segnali e protocolli di comunicazione
- **ISO 7816 parte quarta**: contenuto dei messaggi, comandi e risposte trasmessi dal terminale alle carte e viceversa; struttura dati e file; modo di accesso ai dati ed ai file ecc.

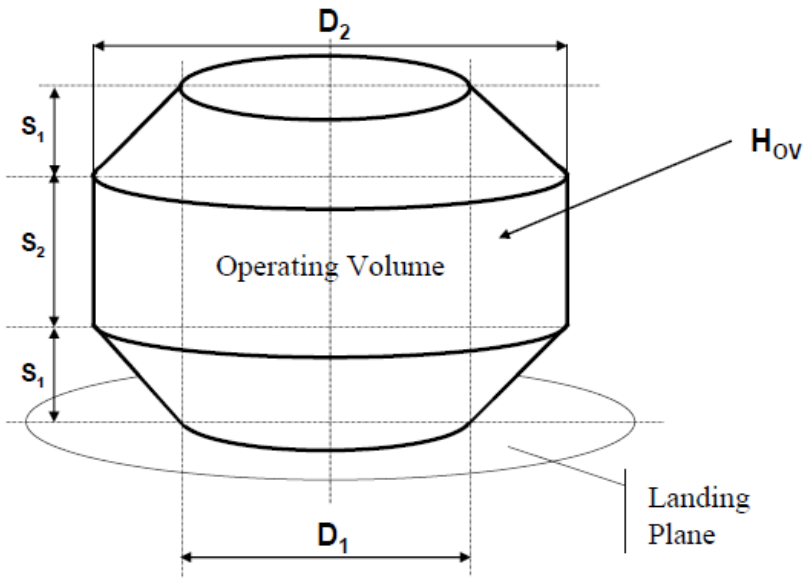
ISO 14443

- **ISO 14443 parte prima**: dimensione delle carte contactless, qualità superficiale per la stampa, resistenza meccanica, resistenza agli UV ed ai raggi X, sensibilità ai campi elettromagnetici. Contiene informazioni molto limitate, rimandando ad altri standard come ad esempio l'ISO 7810 e 7816, stabilendo solo un certo numero di parametri aggiuntivi, come ad esempio i limiti di esposizione ai campi magnetici;
- **ISO 14443 parte seconda**: descrive le caratteristiche del trasferimento di potenza, basato su accoppiamento induttivo, e la comunicazione tra terminale e carta;
- **ISO 14443 parte terza**: descrive i meccanismi di inizializzazione e di anticollisione;
- **ISO 14443 parte quarta**: protocolli di trasmissione

Oltre l'ISO

- EMV e NFC precisano alcune parti di ISO

Figure 2.5: Operating Volume



ISO 10373-6

- Identification cards — Test methods — Part 6: Proximity cards
- Ci dice come capire se una carta rispetta o meno la 14443

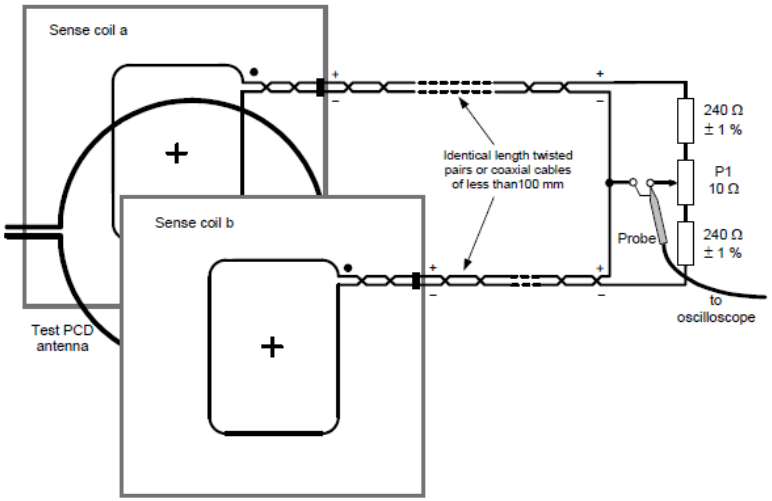


Figure 2 — Test set-up (principle)

ENV-1545

- Definisce le possibili strutture dati dei vari campi possibili nelle applicazioni di trasporto pubblico
- Molto esteso, di solito ne viene usato un sotto assieme
- Molto usato

Lo standard Calypso

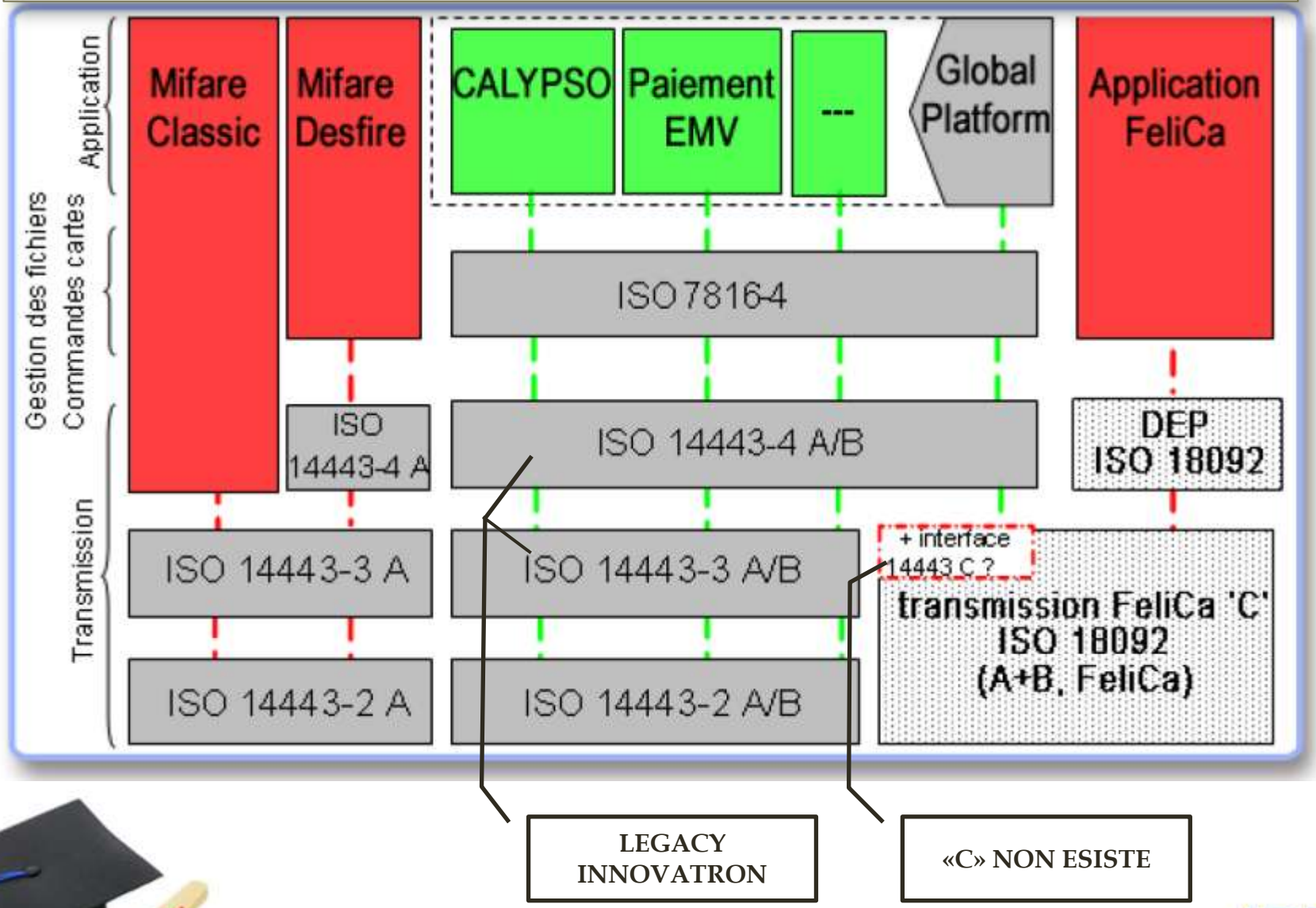
Calypso is a set of technical specifications describing a fast and secure contactless transaction between a terminal and a portable device.

Calypso

- Va oltre gli standard ISO con l'obiettivo di completarli e rendere più facile l'integrazione e l'intercambiabilità degli apparati e delle carte.
- Ad esempio definisce i meccanismi di sicurezza della transazione basati su moduli SAM
- Implica pagamento di licenze per i moduli SAM di conseguenza un (piccolo) aumento di costo per gli acquirenti
- Le specifiche Calypso sono prodotte, manutenute e continuamente evolute ad opera della Calypso Network Association

	Layer	Standard internazionali	Calypso
7	Gestione Sicurezza e architettura		Calypso Security Architecture
6	Software del terminale		Calypso API
5	Modello dati		Calypso Data Model
4	Meccanismi di sicurezza della carta e della SAM		Calypso Card Application
3	Struttura dati della carta	CEN ENV 1545	
2	S.o. della carta, comandi e struttura file	ISO 7816-4	
1	Interfaccia contact e contactless	ISO 7816 1-3 ISO 14443 B 1-4	

APPLICAZIONI



Calypso portable object

- Una tradizionale smart card contactless a µP
- Una smart card JAVA contactless
- Un telefono NFC
- Una chiavetta USB con interfaccia contactless
- altro

Esempio (Calypso)

?

Chiavi e SAM

Il sistema di sicurezza Calypso mutuato poi da altri

MASTER CLICKUTILITY NOVEMBRE 2012

AEP Ticketing solutions

Le chiavi crittografiche

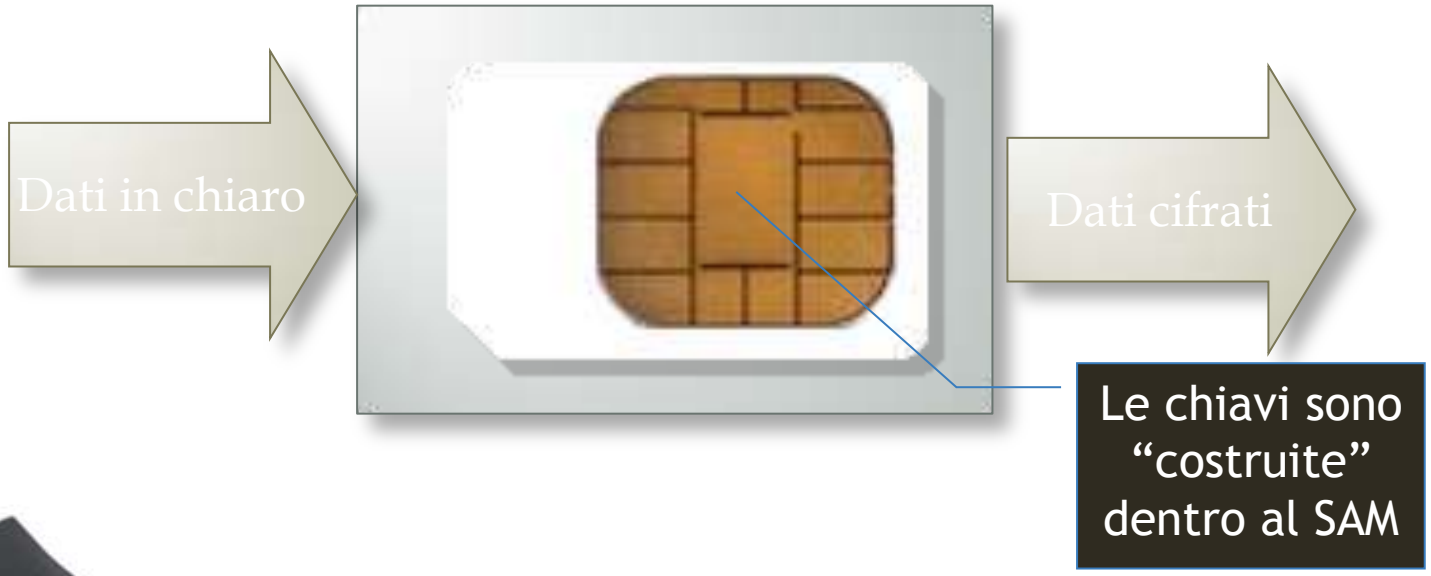
- Sono la base della sicurezza e della relativa crittografia
- Nessuno deve possederle in chiaro
- Possono essere generate da due **semichiavi**, in possesso di soggetti diversi, attraverso procedimenti ragionevolmente sicuri.
- Possono essere conservate all'interno di una speciale smart card detta ***SAM master***

Chiavi negli apparati?

- Introdurre le chiavi in chiaro all'interno degli apparati contraddice il principio per cui nessuno deve conoscere le chiavi.
- Se un apparato contenesse le chiavi in chiaro, un programmatore infedele potrebbe accedervi facilmente.
- Come introdurre e conservare, allora, le chiavi nelle validatrici?

I moduli SAM

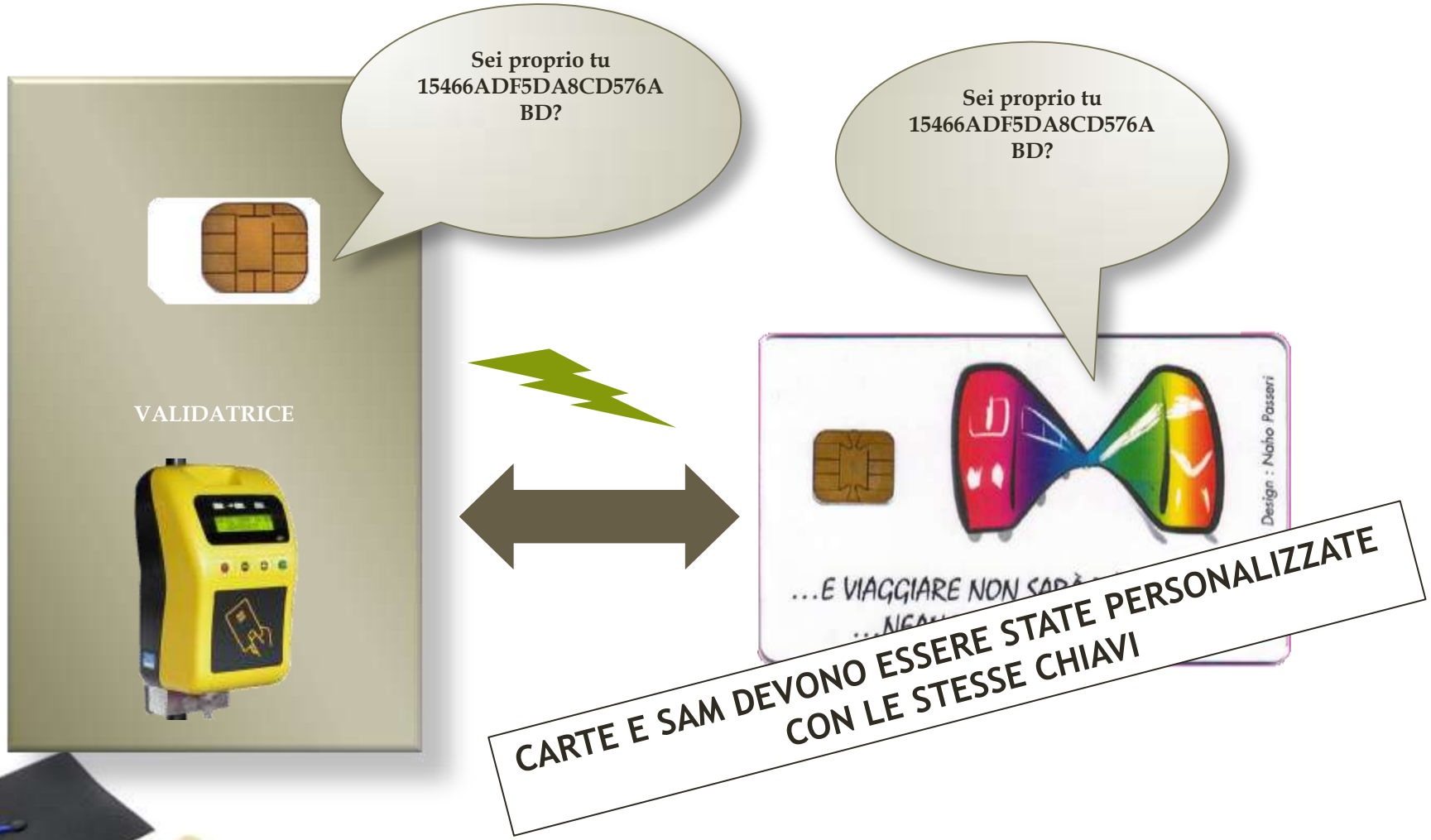
- I moduli SAM (Security Access Module) sono delle smart card a contatto che custodiscono le chiavi e che sono in grado di eseguire operazioni crittografiche



Funzioni dei SAM

- Custodia delle chiavi crittografiche;
- Esecuzione di funzioni crittografiche;
- Generazione o verifica delle firme digitali.

Mutua autenticazione

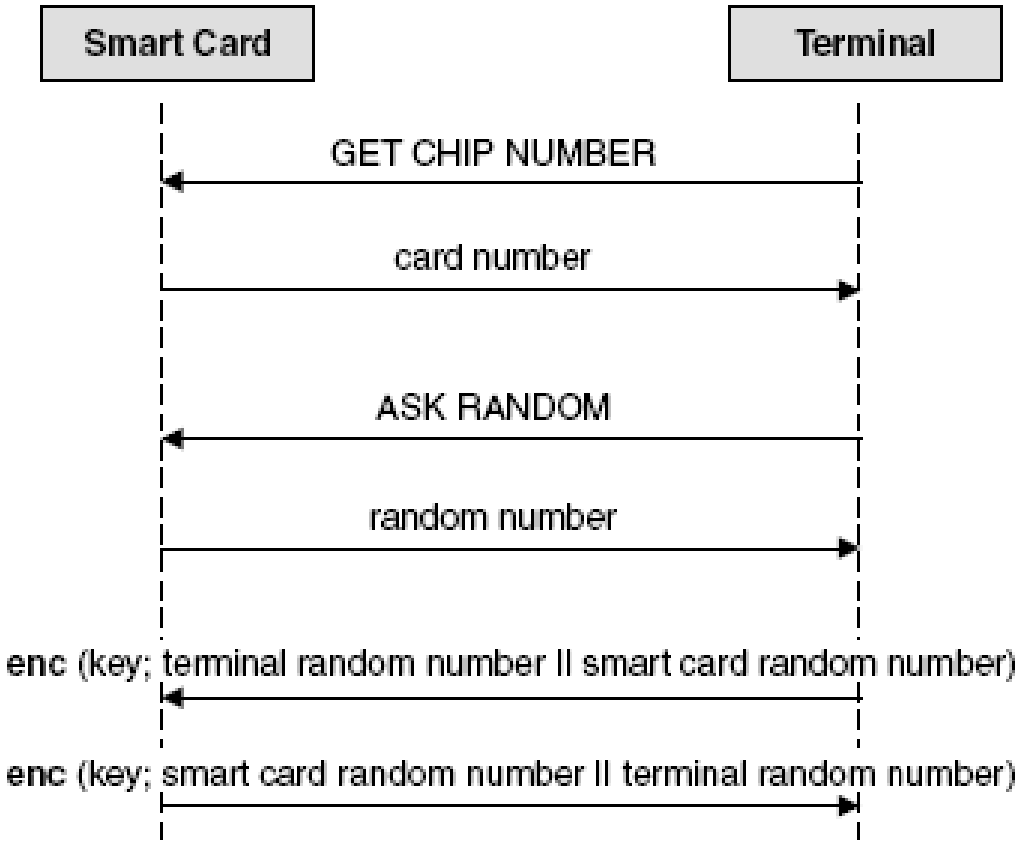


AEP Ticketing solutions

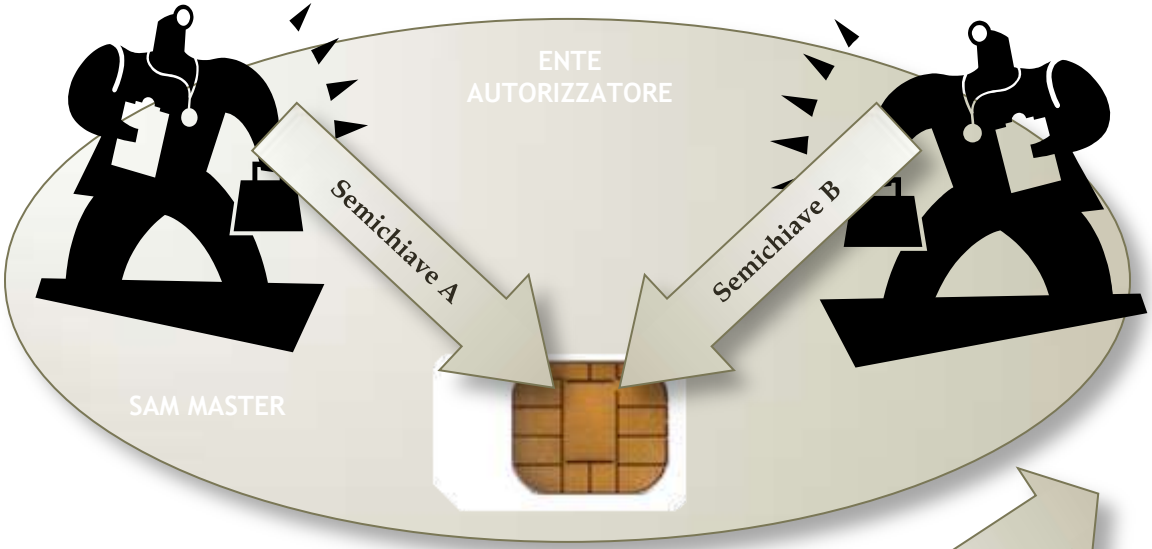
Ricarica

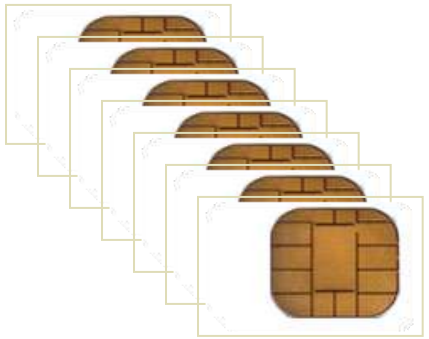
CARTE E SAM DEVONO ESSERE STATE PERSONALIZZATE CON LE STESSE CHIAVI

Una mutua autenticazione (ISO 7816)



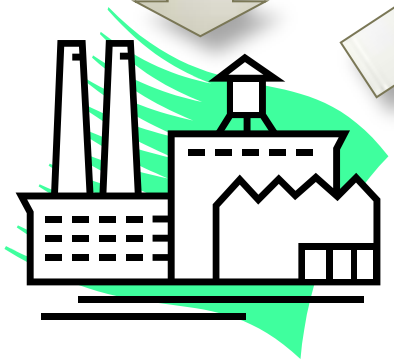
Processo produttivo





MODULI SAM
PER LE VALIDATRICI

PROCESSO
FABBRICAZIONE



CARTE
PER
LA
VENDITA

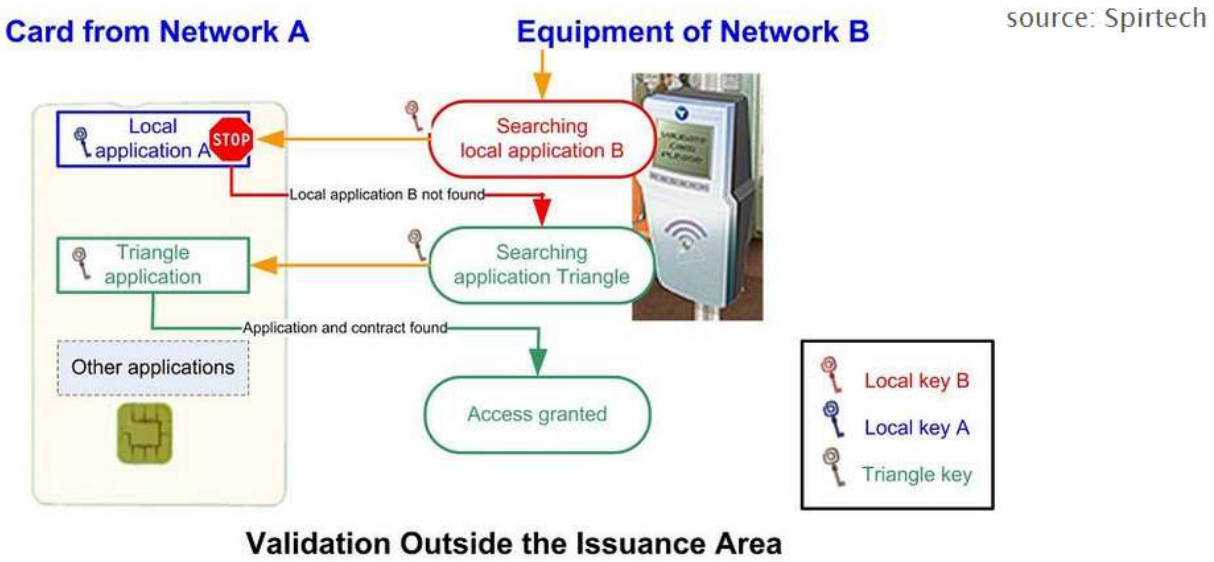
AEP Ticketing solutions

Tipi di chiavi

- E' possibile usare chiavi diverse per operazioni di ricarica, utilizzo ecc.
- Terminali diversi possono avere chiavi diverse; es. le validatrici dovrebbero avere solo chiavi di addebito.
- E' opportuno limitare la distribuzione delle chiavi alle funzioni strettamente indispensabili.

Calypso Triangle

- Definisce delle regole comuni per gestire le chiavi di sicurezza, la struttura file e il modello dati, con chiavi di protezione DESX e 3DES gestite da CNA



Carte Calypso

AEP Ticketing solutions

Carte Calypso

- **Fabbricanti**: ASK, Calmell, Gemalto, Oberthur Technologies, Sagem Sécurité, Watchdata ecc.
- **Caratteristiche**: 1-16K byte, interfaccia a contatti opzionale, crittografia DES, DESX o TDES.

Panorama Calypso

	Modelli	Fabbric.	Chip
Carte «storiche»	CD-97, CD Light, GTML	ASK	STM
Carte attuali	CD-21	Any	STM
	TanGO	ASK	ATMEL STM
	CiTi	Gemalto	Samsung
	CDS3	Oberthur	Infineon
	BMS2	Sagem S.	ATMEL
	TimeCOS	Watchdata	Infineon
Applet Java		Spirtech	

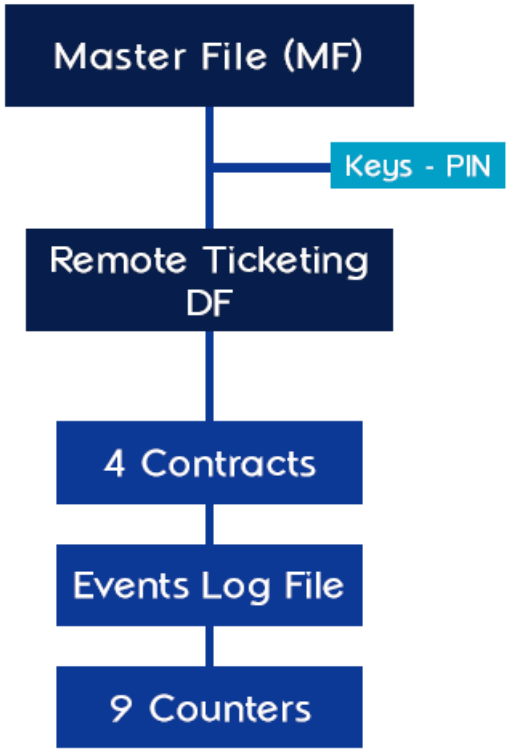
	GTML	GTML2	GTML+	CD97	CD97BX	CT2000	CT4000
File structure	Fixed	Fixed	TanGO	Fixed	Fixed	Custom	TanGO cust
Standard							
ISO7816	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISO14443	1-2-3 type B	1-2-3 type B	1-2-3 type A&B	1-2-3 type B	1-2-3 type B	1-2-3 type B	1-2-3 type A&B
Interface	Dual	Dual	Dual + Contactless	Dual	Dual	Dual	Dual + Contactless
Communication protocol							
ISO		Yes	Yes		Yes	Yes	Yes
Innovatron	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Speed (kBauds)	106	106	212/424	106	106	106	212/424
Security							
Hardware crypto-processor			Yes				Yes
DES	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DESX		Yes	Yes		Yes	Yes	Yes
Triple-DES			Yes				Yes
Number of key per DF	3	3	7	3	3	3	7

GTML ed altre carte ASK

(Fonte: ASK)

GTML

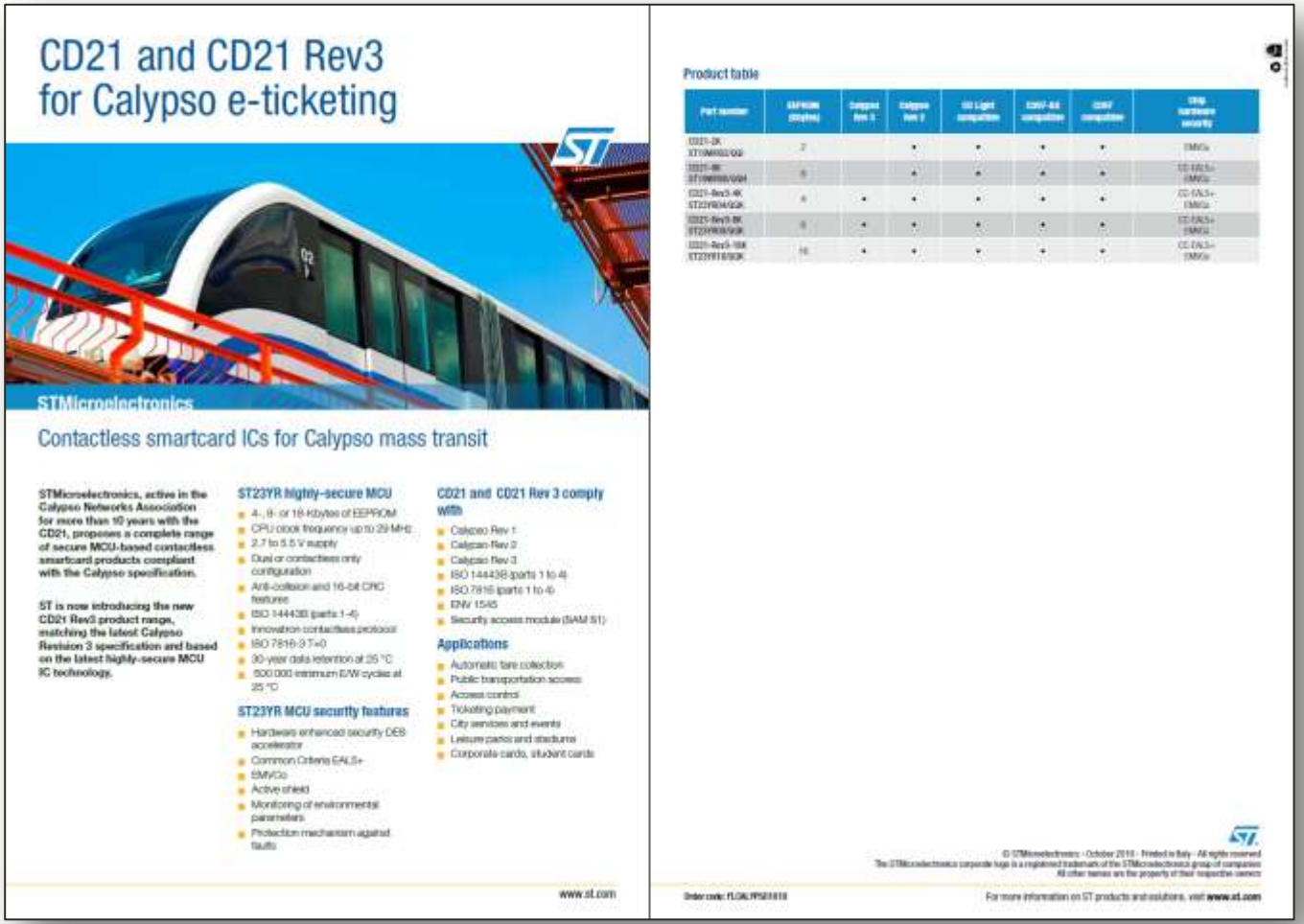
- 576 byte EEPROM
- ISO 14443B
- DES, X-DES, 3-DES
- struttura dati ENV 1545
- compatibile Calypso
- anti-collisione
- protezione contro allontanamento anticipato



GTML

- Nata come prodotto di ASK
- Non più prodotta, oggi emulata da nuove carte (es. CD21, TanGO ecc.)
- Molto usata anche in Italia: es. Milano, Regione Campania, Regione Umbria, ecc.

Prendiamone una attuale...



CD21 and CD21 Rev3 for Calypso e-ticketing

STMicroelectronics

Contactless smartcard ICs for Calypso mass transit

STMicroelectronics, active in the Calypso Networks Association for more than 10 years with the CD21, proposes a complete range of secure MCU-based contactless smartcard products compliant with the Calypso specification.

ST is now introducing the new CD21 Rev3 product range, matching the latest Calypso Revision 3 specification and based on the latest highly-secure MCU IC technology.

ST23YR highly-secure MCU

- 4-, 9- or 18-Kbytes of EEPROM
- CPU clock frequency up to 29 MHz
- 2.7 to 5.5 V supply
- Dual or contactless only configuration
- Anti-collision and 16-bit CRC features
- ISO 14443B (parts 1-4)
- Innovatron contactless protocol
- ISO 7816-3 T=0
- 30-year data retention at 25 °C
- 500 000 minimum E/W cycles at 25 °C

ST23YR MCU security features

- Hardware enhanced security DES accelerator
- Common Criteria EAL5+
- SMVCo
- Active shield
- Monitoring of environmental parameters
- Protection mechanism against faults

CD21 and CD21 Rev 3 comply with

- Calypso Rev 1
- Calypso Rev 2
- Calypso Rev 3
- ISO 14443B (parts 1 to 4)
- ISO 7816 (parts 1 to 4)
- ENV 1545
- Security access module (SAM S1)

Applications

- Automatic fare collection
- Public transportation access
- Access control
- Ticketing payment
- City services and events
- Leisure parks and stadiums
- Corporate cards, student cards

www.st.com

Product table

Part number	EEPROM (Kbytes)	Calypso Rev 1	Calypso Rev 2	ISO Light computation	CD97-64 computation	CD97 computation	Chip hardware security
CD21-2K ST1WM022/023	2		•	•	•	•	EMVCo
CD21-4K ST1WM068/069	5		•	•	•	•	CC EAL5+ EMVCo
CD21-Rev3-4K ST23YR04/02K	4	•	•	•	•	•	CC EAL5+ EMVCo
CD21-Rev3-8K ST23YR08/04K	8	•	•	•	•	•	CC EAL5+ EMVCo
CD21-Rev3-18K ST23YR18/09K	16	•	•	•	•	•	CC EAL5+ EMVCo

Order code: FLOBLYPS01010

For more information on ST products and solutions, visit www.st.com

STM CD21

STMicroelectronics, active in the Calypso Networks Association for more than 10 years with the CD21, proposes a complete range of secure MCU-based contactless smartcard products compliant with the Calypso specification.

ST is now introducing the new CD21 Rev3 product range, matching the latest Calypso Revision 3 specification and based on the latest highly-secure MCU IC technology.

ST23YR highly-secure MCU

- 4-, 8- or 18-Kbytes of EEPROM
- CPU clock frequency up to 29 MHz
- 2.7 to 5.5 V supply
- Dual or contactless only configuration
- Anti-collision and 16-bit CRC features
- ISO 14443B (parts 1-4)
- Innovatron contactless protocol
- ISO 7816-3 T=0
- 30-year data retention at 25 °C
- 500 000 minimum E/W cycles at 25 °C

ST23YR MCU security features

- Hardware enhanced security DES accelerator
- Common Criteria EAL5+
- EMVCo
- Active shield
- Monitoring of environmental parameters
- Protection mechanism against faults

CD21 and CD21 Rev 3 comply with

- Calypso Rev 1
- Calypso Rev 2
- Calypso Rev 3
- ISO 14443B (parts 1 to 4)
- ISO 7816 (parts 1 to 4)
- ENV 1545
- Security access module (SAM S1)

Applications

- Automatic fare collection
- Public transportation access
- Access control
- Ticketing payment
- City services and events
- Leisure parks and stadiums
- Corporate cards, student cards

Modelli

Product table

Part number	EEPROM (Kbytes)	Calypso Rev 3	Calypso Rev 2	CD Light compatible	CD97-BX compatible	CD97 compatible	Chip hardware security
CD21-2K ST19WR02/QQI	2		•	•	•	•	EMVCo
CD21-8K ST19WR08/QQH	8		•	•	•	•	CC-EAL5+ EMVCo
CD21-Rev3-4K ST23YR04/QQK	4	•	•	•	•	•	CC-EAL5+ EMVCo
CD21-Rev3-8K ST23YR08/QQK	8	•	•	•	•	•	CC-EAL5+ EMVCo
CD21-Rev3-18K ST23YR18/QQK	18	•	•	•	•	•	CC-EAL5+ EMVCo

ASK Calypso card

	Calypso Transit Cards						
Card Family	TanGO				CD21		
Card Name	CT4002 CTC4002	CT4004 CTC4004	CT4008 CTC4008	CT4018 CTC4018	CD21-2K CDC21-2K	CD21-8K CDC21-8K	CD21-3
Calypso compliance	Rev 2.4	Rev 2.4 / Rev 3.1			Rev 2.4		Rev 3.1
Emulation available	GTML/GTML2/CDLight/CD97				CDLight / CD97		
Interface	Dual / Contactless				Dual / Contactless		
Chip	ST19	ST23			ST19		ST23
ISO	ISO 14443 B1, 2, 3, 4 and ISO 7816-4						
EEProm	2 KBytes	4 KBytes	8 KBytes	18 KBytes	2 KBytes	8 KBytes	15 KBytes
Number of writes	100 000 cycles	500 000 cycles			100 000 cycles		500 000 cycles
Data rate	106 / 212 / 424 Kbps						
Unique S/N	32 bits	64 bits			32 bits (optional 64)		
Cryptography	DES / DES X / 3DES						
Key length	56 / 120 / 112 bits						
SAM	C. SAM and SAM S1						
Communication protocol	ISO Innovatron	ISO and Innovatron simultaneously on different domains			ISO Innovatron		
Number of keys	3 keys (up to 7 keys)				3 keys		
File structure	Customizable	Customizable after issuance Independant domains with different ATR			Customizable		

Carte EMV

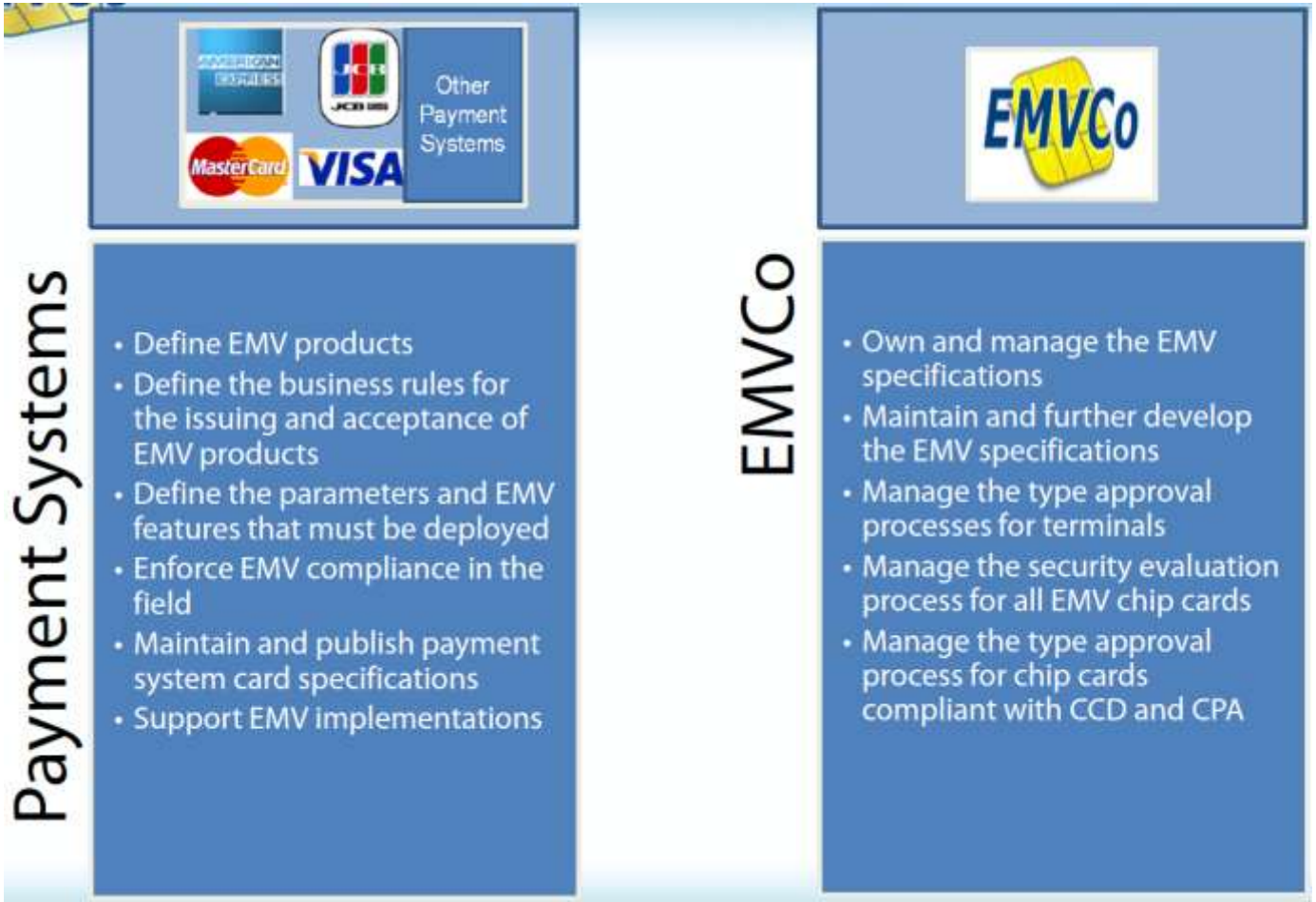
Le carte di credito oggi sono anche contactless

Specifiche EMV

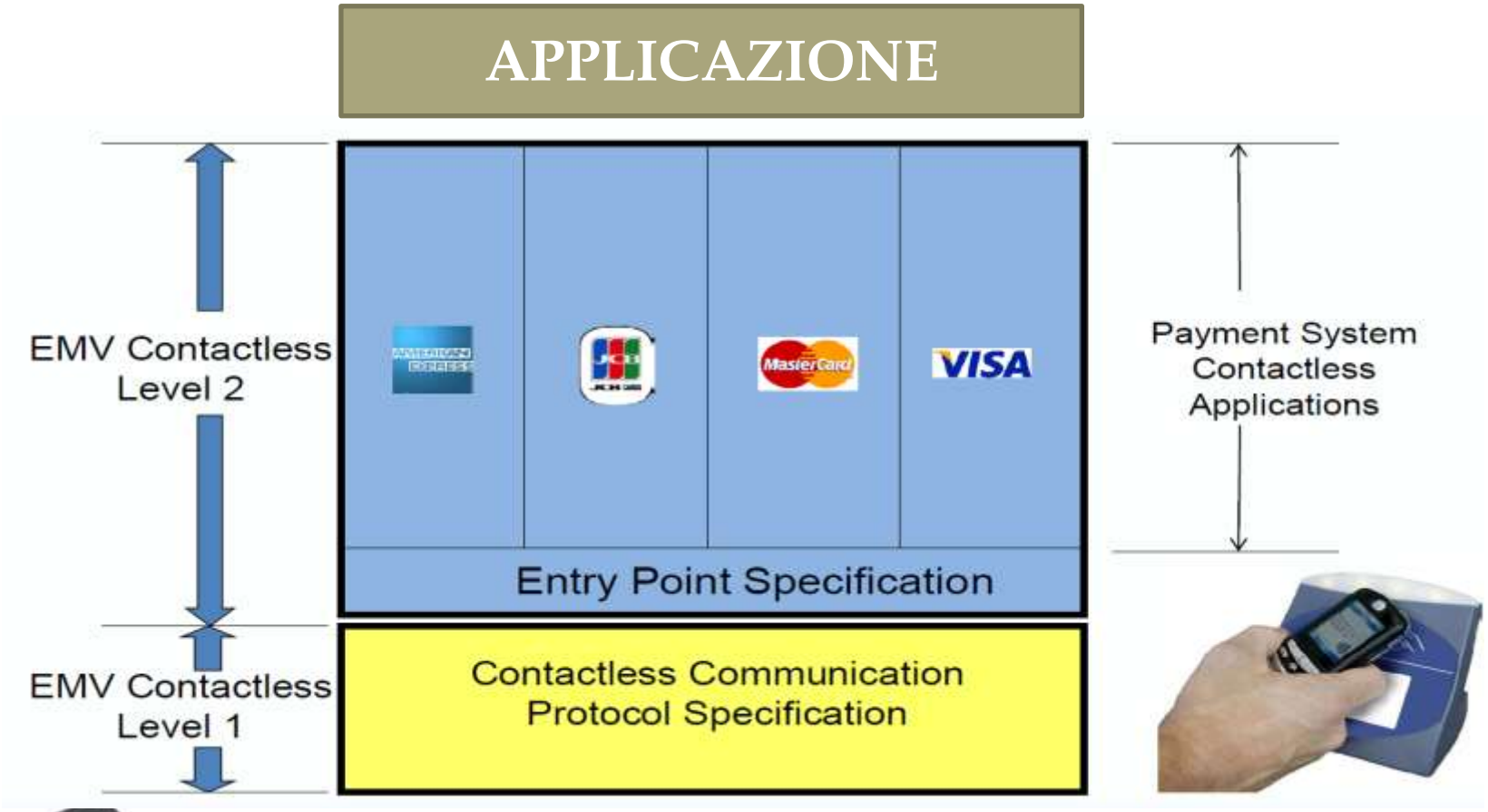
- EMV Integrated Circuit Card Specifications for Payment Systems (carte, POS, ATM ecc.)
- Sviluppate da Europay, MasterCard and Visa a metà degli anni '90
- Specifiche aperte per facilitare l'interoperabilità tra le smart card e i terminali per i pagamenti

- EMVCo gestisce, mantiene e migliora le specifiche EMV
- EMVCo inoltre stabilisce e amministra i processi di test e approvazione per stabilire la conformità alle specifiche
- EMVCo è oggi di proprietà di American Express, JCB, MasterCard e Visa.

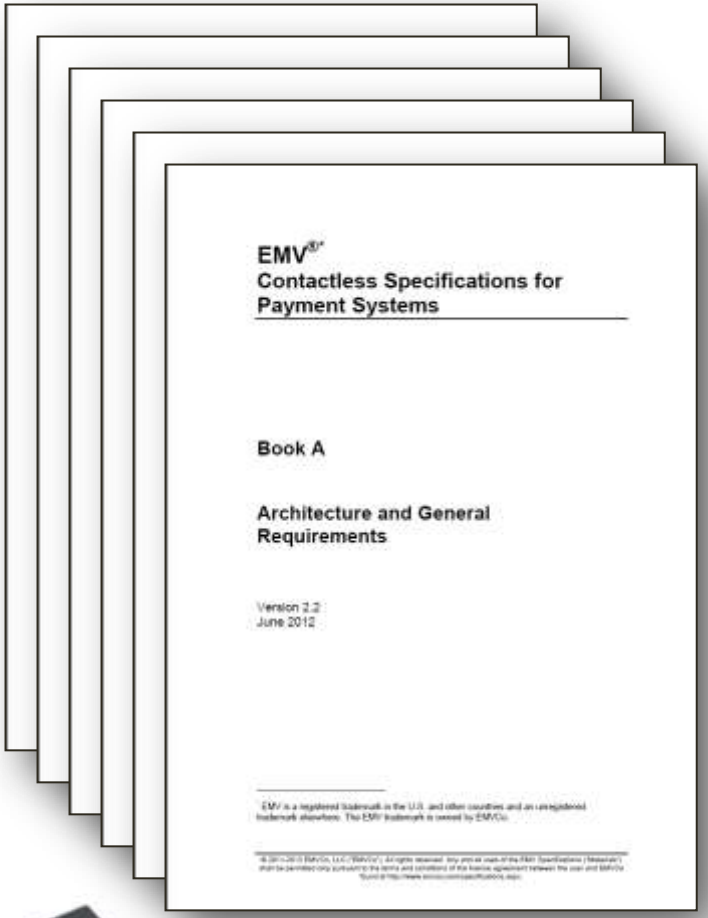
Principali soggetti

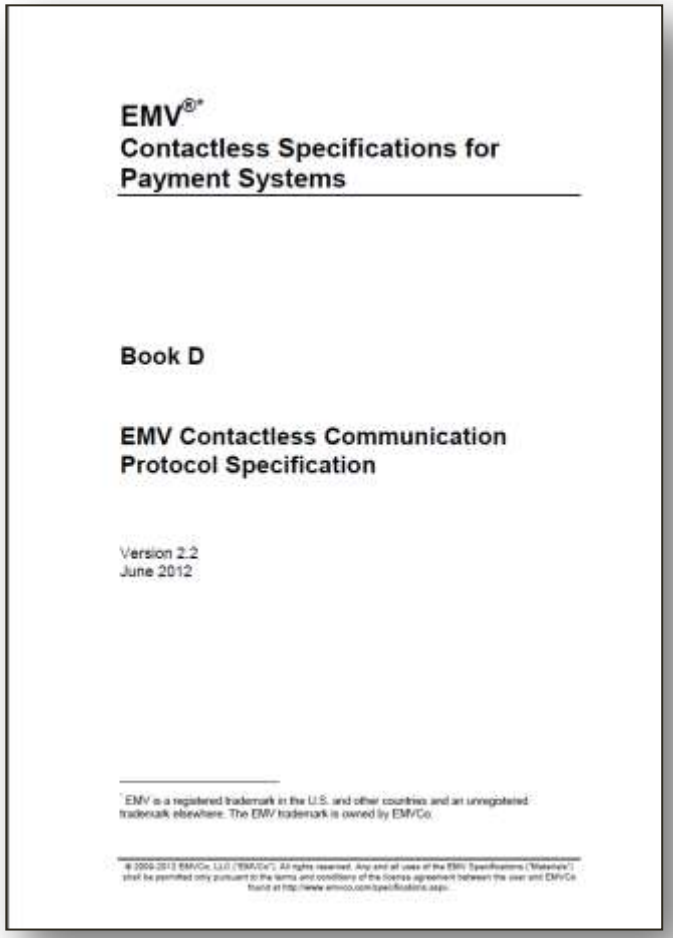


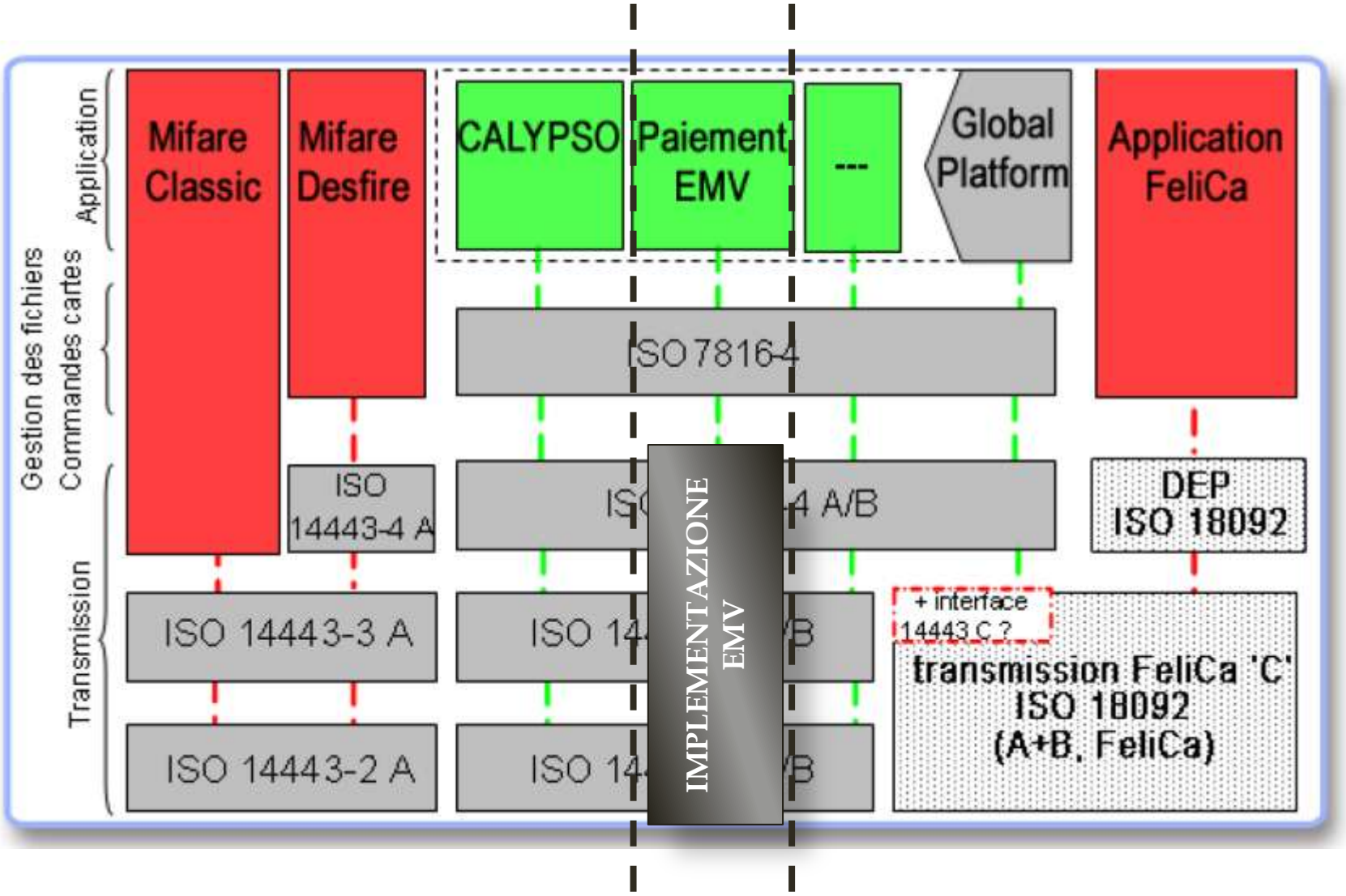
Estensione contactless



Nuove specifiche e certificazioni






Application
Gestion des fichiers
Commandes cartes
Transmission
Mifare Classic
Mifare Desfire
CALYPSO
Paiement EMV

Global Platform
Application FeliCa
ISO 7816-4
ISO 14443-4 A
4 A/B
DEP ISO 18092
IMPLEMENTAZIONE EMV
ISO 14443-3 A
+ interface 14443 C ?
transmission FeliCa 'C' ISO 18092 (A+B, FeliCa)
ISO 14443-2 A

GlobalPlatform

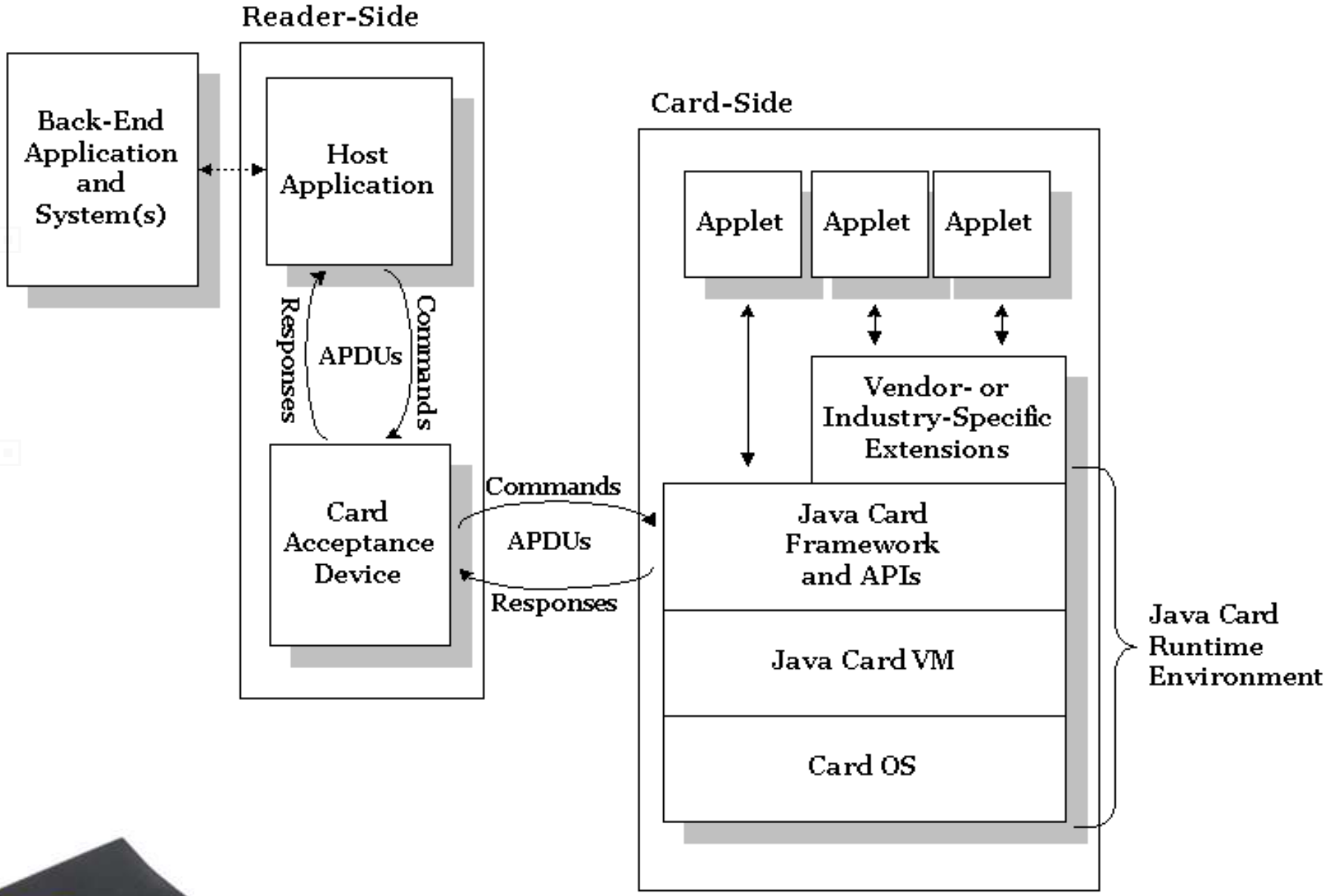
- E' un'organizzazione indipendente, non-profit, finalizzata a sviluppare e pubblicare le specifiche complessive per gestire più applicazioni su smart card in modo sicuro (es. Java card)
- Fondata nel 1999 per assumersi la responsabilità della specifica Open Platform di Visa Inc.'s

Java card

- È una tecnologia che consente di eseguire applicazioni basate sulla piattaforma Java, in maniera sicura, su smart card e dispositivi similari.
- È ampiamente utilizzata nelle SIM card (telefonia mobile) e nelle carte EMV.

Applet

- È una macchina a stati che elabora solo i comandi in entrata e risponde inviando dati o il proprio status al dispositivo di interfaccia.
- È un'applicazione che opera in maniera sicura.

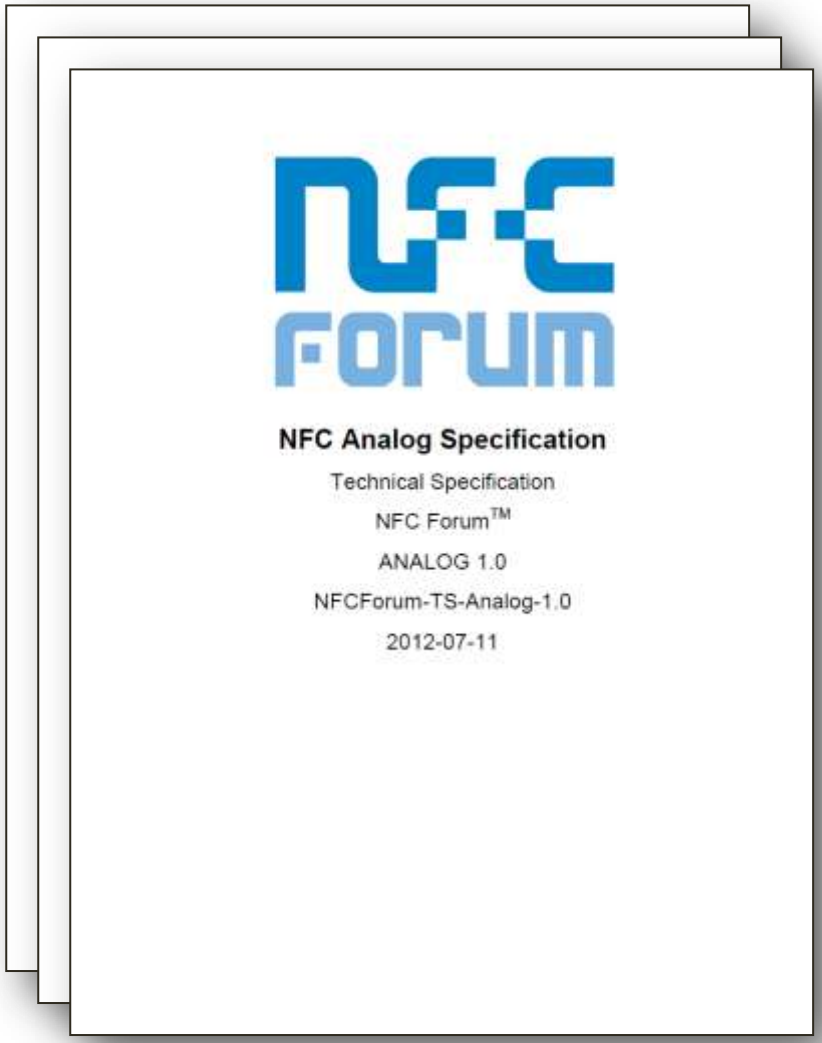

Reader-Side
Back-End Application and System(s)
Host Application
Responses
APDUs
Commands
Card Acceptance Device
Commands
APDUs
Responses
Card-Side
Applet
Applet
Applet
Vendor- or Industry-Specific Extensions
Java Card Framework and APIs
Java Card VM
Card OS
Java Card Runtime Environment

Near-Field Communication

- NFC è una tecnologia a corto raggio che opera sulla frequenza di 13,56 MHz, con trasferimenti di dati fino a 424 kbs
- Usata sugli smartphone per emulare smart card contactless, per eseguire transazioni di pagamento e trasferimenti dati

- NFC Forum è un consorzio di imprese operanti in vari settori (hardware, software, carte di credito, operazioni bancarie ecc.) interessati nel progresso e la standardizzazione di NFC

Nuove specifiche e certificazioni



Modalità NFC

- Listener (card, tag emulation)
- Poller (reader)
- Peer to peer ecc. (ISO 18092)

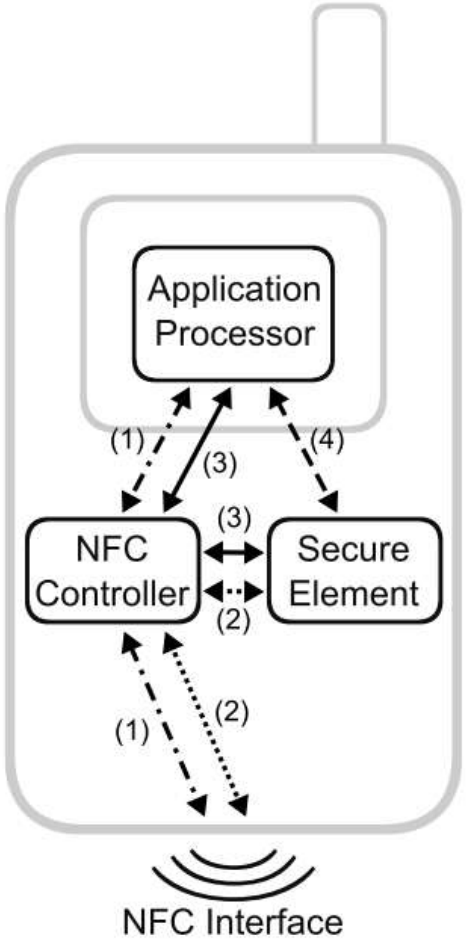
Secure Element

- È un chip che contiene un processore sicuro, a prova di manomissione, e la relativa memoria.
- Tipicamente è un ambiente Java Card che contiene le applicazioni che si basano su chiavi di sicurezza, in esecuzione.
- Il suo unico scopo è consentire transazioni sicure.

Dove sta il SE

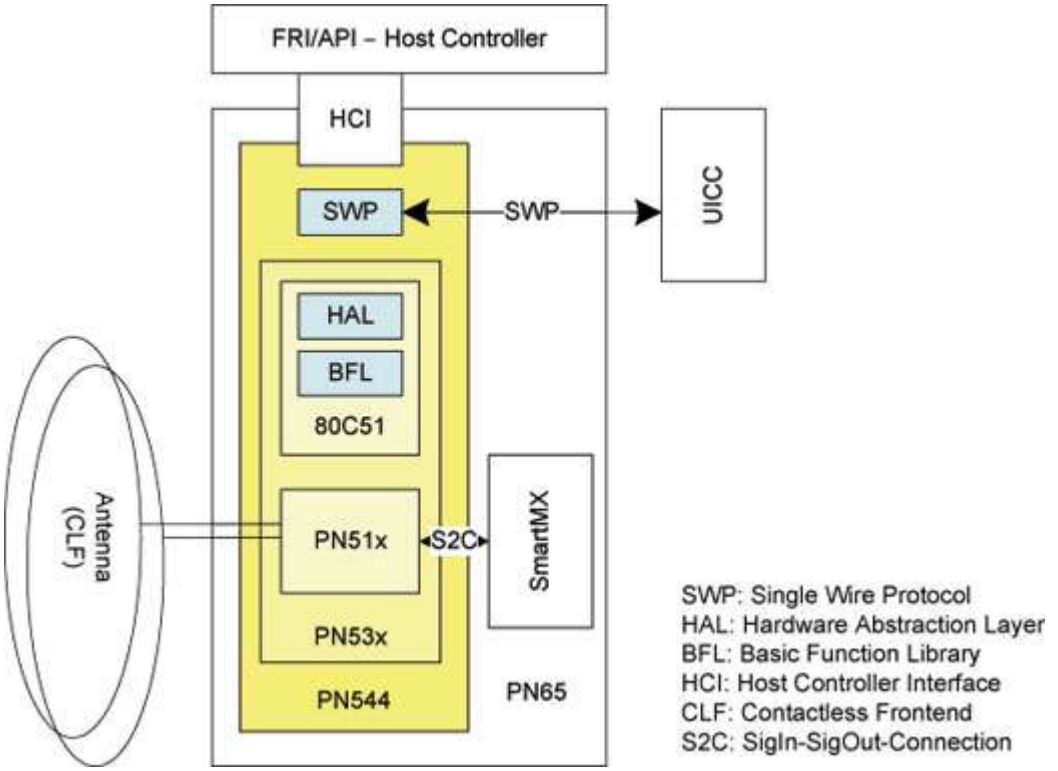
- Nelle smart card EMV sta nel chip della carta
- Nei telefoni può stare:
  - nella SIM del MNO (TIM, Vodafone ecc.)
  - nello smartphone
  - *(All'esterno, in una apposita scheda SD)*

Schema generale



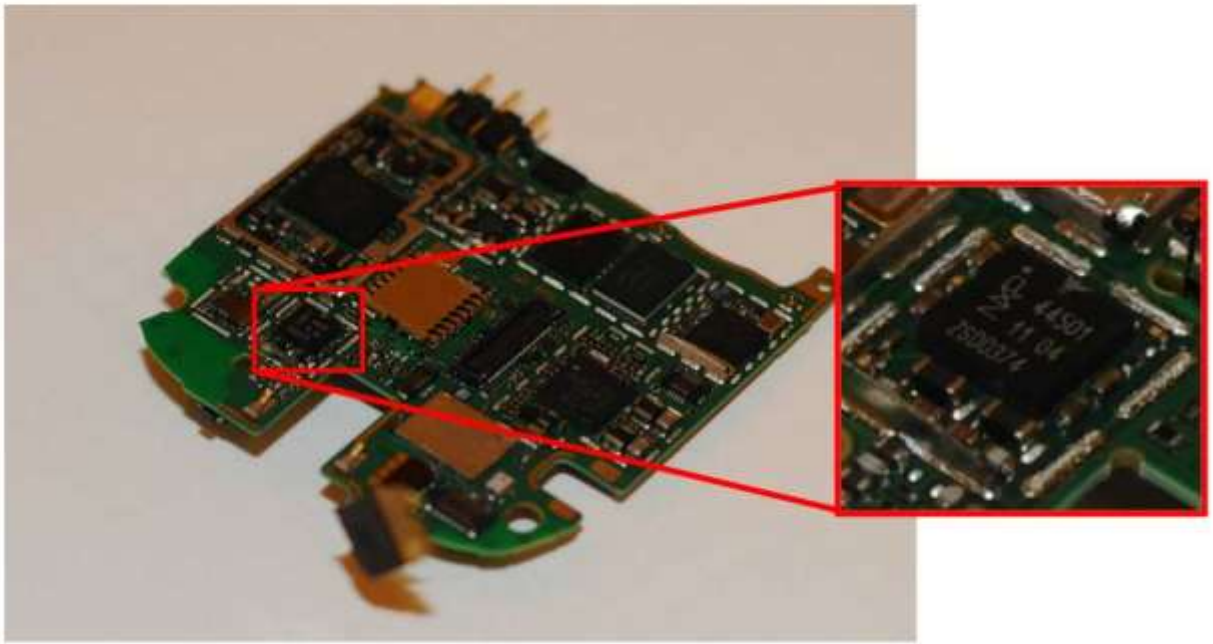
Esempio PN65 (Samsung Nexus S)

- **PN512** = contactless communication
- **80C51** = microcontroller
- **SWP** = interface to use a SIM card as the secure element.
- **SmartMX** = a secure smartcard chip used as Secure Element (a P5CN072 Smart Card Controller. Running a Java Card OS.

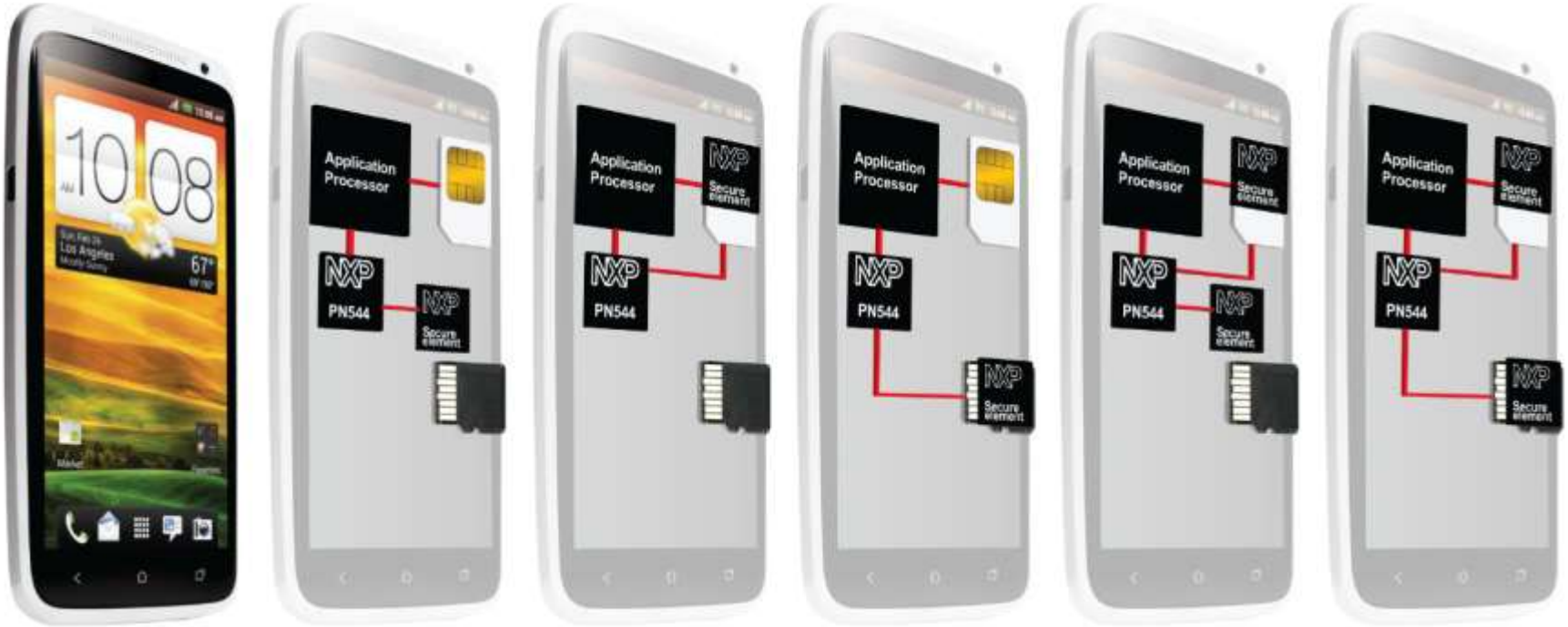


Un SE dal vero...

NXP PN544 in Nokia C7



Possibili situazioni



Possibili situazioni

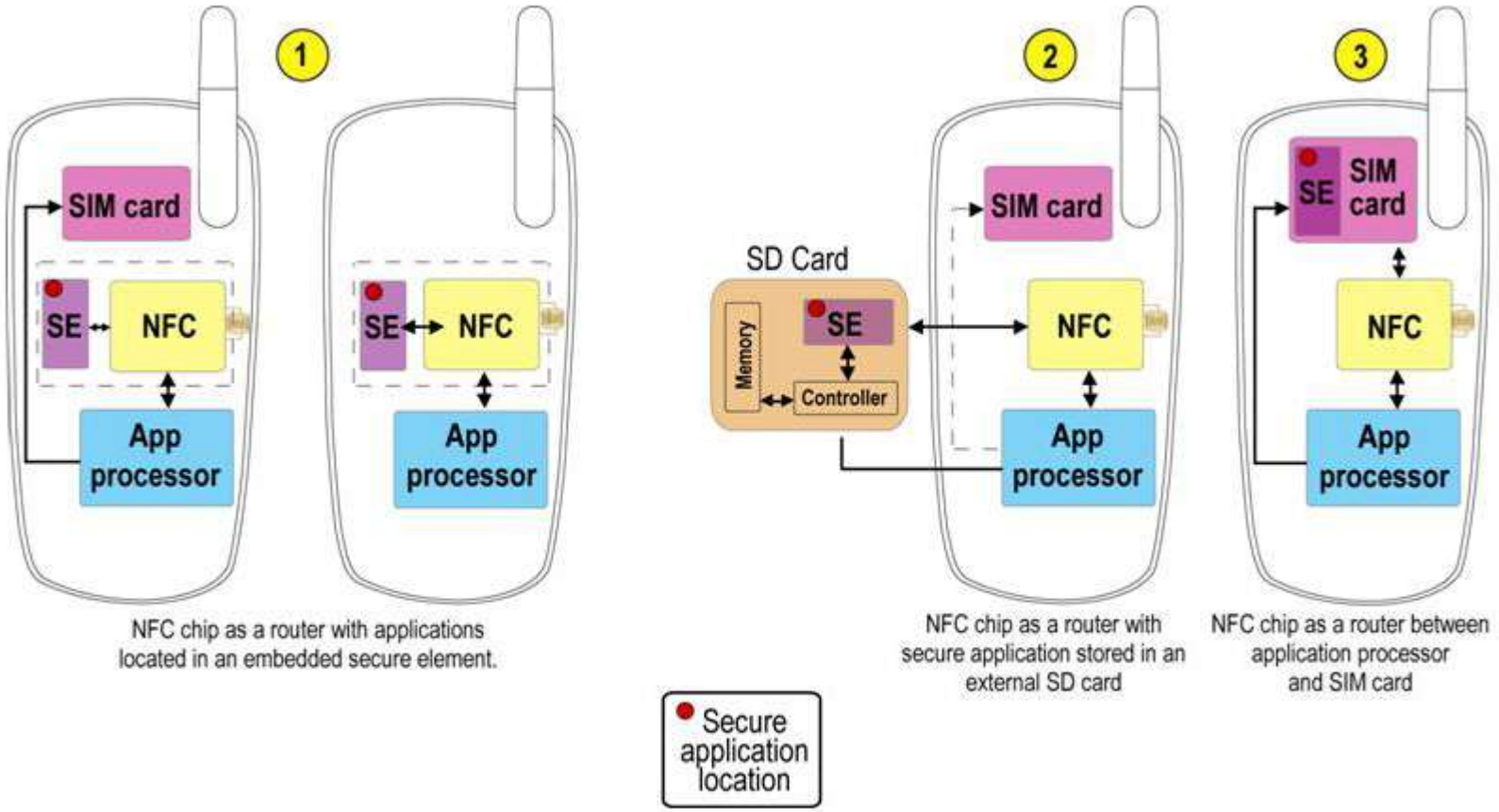
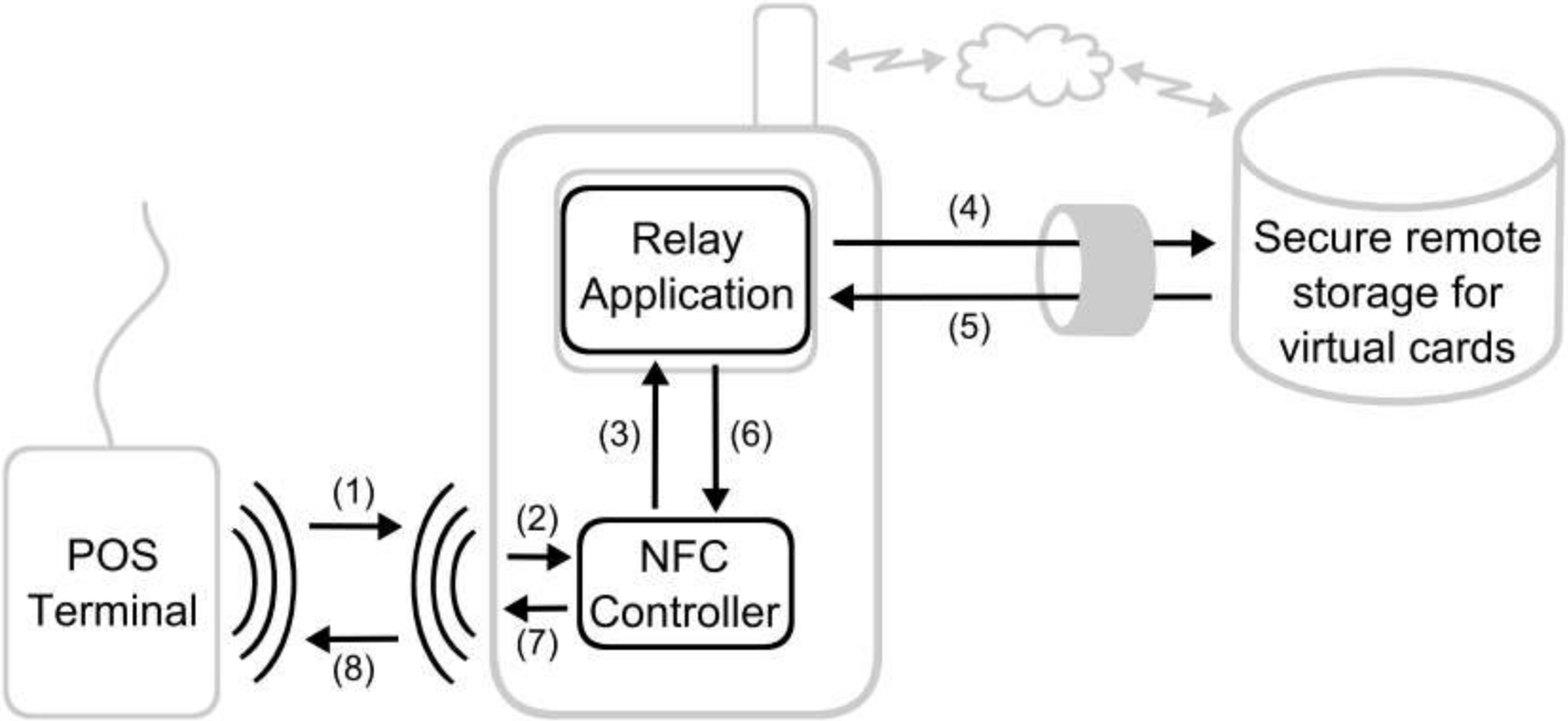


Figure 1: ① Embedded, ② SD Card-Based and ③ USIM Secure Element Solutions

Senza SE (on line)



Chi vincerà?

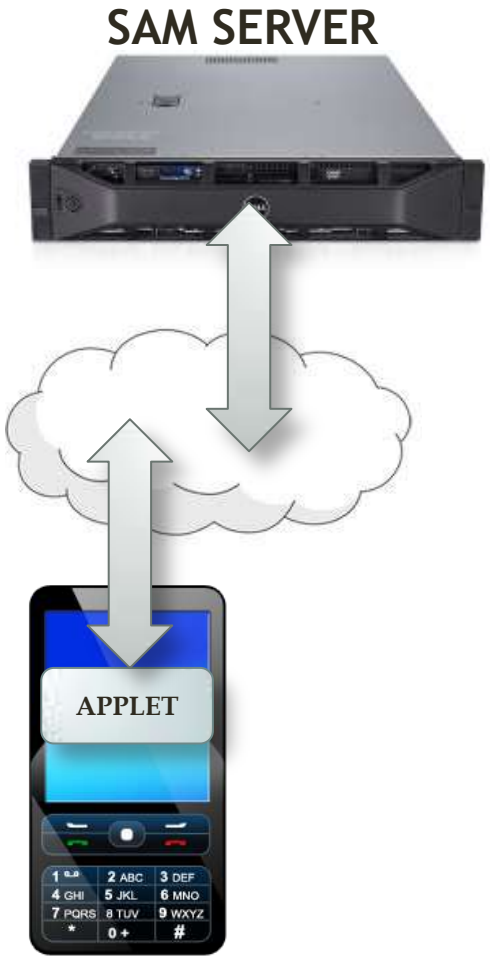
- *... Compagnie di Trasporto... mmmh....*
- Difficile usare la SIM o il chip SE come SE
- Quindi è necessario un elemento di sicurezza ulteriore:
  - Personalizzazione applet con chiavi TPL
  - Sistemi di SAM remota per le ricariche

Convalida

Anche l'applet deve essere personalizzata con le stesse chiavi!

SAM remota


Ricarica
SAM FISICA
BIGLIETTERIA
CARTE E SAM DEVONO ESSERE STATE PERSONALIZZATE CON LE STESSE CHIAVI
MASTER CLICKUTILITY NOVEMBRE 2012
AEP
Ticketing solutions


SAM SERVER
APPLET

Riepilogo del riepilogo

Sintesi estrema

Java

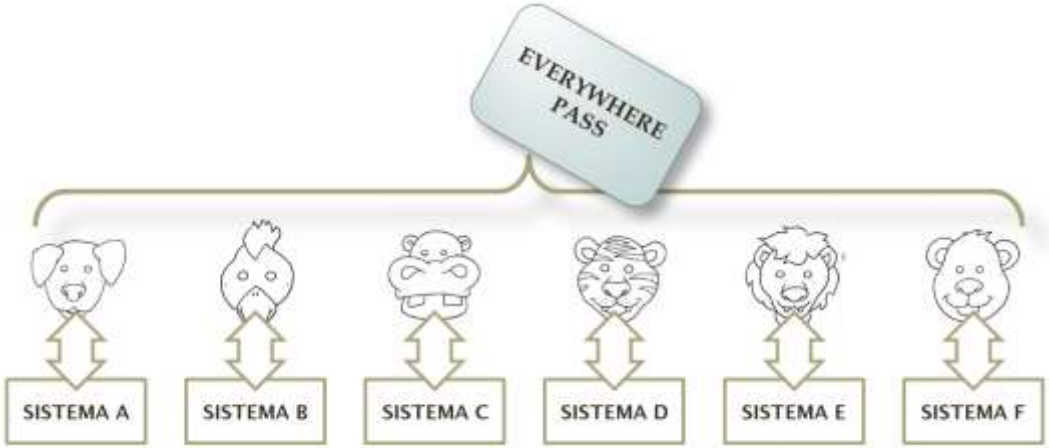
- Uno smartphone NFC o una carta di credito EMV sono entrambi basati su Java Runtime Environment
- Un'applicazione (*applet*) Java «gira» in maniera controllata e quindi sicura
- L'applicazione NFC può risiedere nella SIM o nel telefono
- Più applet possono convivere nel JRE
- Il terminale «vede» quello che l'applet fa vedere

Global Platform definisce

- L'ambiente deve operano gli applet
- La modalità di trasferire e caricare gli applet
- Ecc. ecc.

Quindi

- Applet EMV fa vedere la carta come EMV
- Applet Calypso fa vedere la carta come Calypso
- Ecc.
- Applet inviabili a distanza fanno presentare allo smartphone modelli esterni dinamicamente diversi



MASTER CLICKUTILITY NOVEMBRE 2012

Un telefono NFC

- Può emulare carte di credito contactless EMV
- Può emulare carte Calypso (o MIFARE, o altre)
- Riunisce in un solo oggetto più carte di tipo diverso

Il quadro generale

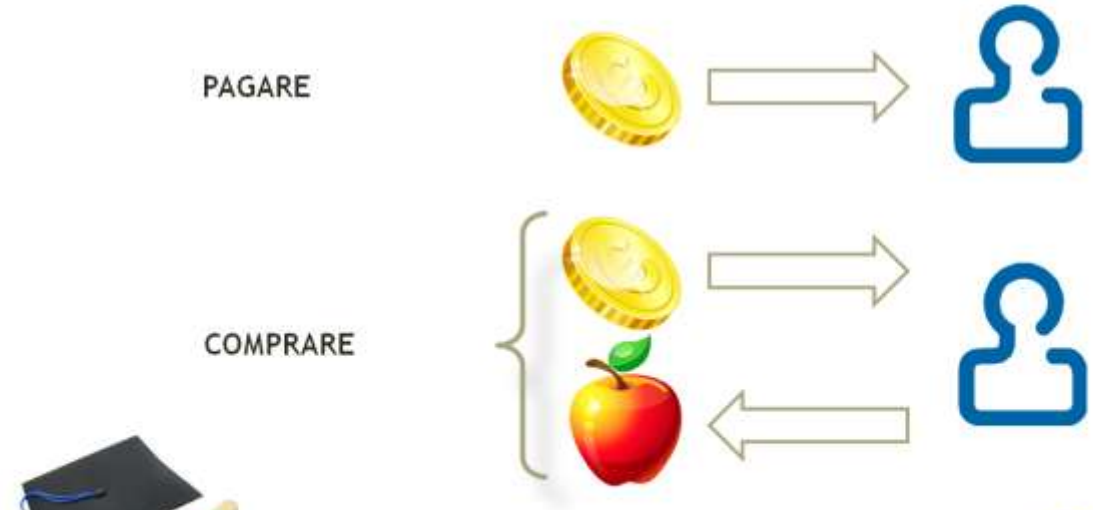
EMV nei trasporti

Meno facile di quanto sembra

Vi ricordate?

Niente è mai semplice 1

- Comprare è diverso da pagare



MASTER CLICKUTILITY OTTOBRE 2012

Acquistare con carte EMV

- Le carte saprebbero bene come pagare (su un POS) ma non sanno ancora dove mettere le cose acquistate
- Non offrono cioè un data model comodamente utilizzabile nell'ambito del trasporto pubblico
- La carta, insomma, non prevede ancora uno spazio dati scrivibile da parte della compagnia
- Molto opportuna quindi la strada degli applet trasporti
- Le validatrici, inoltre, non sono ancora dei POS

Pagare con carte EMV

- Le carte sanno bene come pagare ma solo su un POS EMV di un circuito esistente
- Le validatrici richiedono:
  - certificazione livello 1 (ci pensa il Costruttore)
  - certificazione livello 2 (ci pensa il Costruttore)
  - accordi con gli Istituti Bancari
  - creazione e certificazione della applicazione specifica e delle parti di sistema (comunicazione ecc.)

Comprare e pagare (1)

Comprare e pagare (2)

EMV da solo non basta

- La combinazione di più tecnologie convergenti rappresenta la tendenza più verosimile per i prossimi anni
  - ISO 14443
  - Calypso
  - EMV
  - Java
  - NFC
  - ecc.

Applet Java Calypso

- Un applet generico Calypso è disponibile, conforme alle specifiche Global Platform, utilizzabile dai fornitori di SIM e dai produttori di carte di credito.
- L'applet è scaricabile in un Secure Element basato JRE (es. telefono NFC o chiave contactless USB).

Portable Object

- Calypso rende sicure le transazioni contactless in modo indipendente dal layer di comunicazione (parte da ISO 7816-4).
- Quindi si adatta bene ai nuovi dispositivi multi-applicazione, dove le applicazioni «fisse» di un tempo cedono il passo ad applet scaricabili on-demand (Portable Object, non più smart card).

Nuove specifiche Calypso

- **Per descrivere** il modo in cui un applet Calypso può essere scaricato, attivato e personalizzato in modo sicuro all'interno di un Portable Object, in accordo alle specifiche di Global Platform.
- **Per descrivere** come il Portable Object può accedere a servizi remoti (ad esempio per ricaricare contratti).
- Il Portable Object nel dispositivo mobile si comporta come una carta rev. 3.1 (tempo di transazione maggiore) → nessun cambiamento richiesto nella infrastrutture esistenti.

Convergenza

- La convergenza tecnica EMV/Calypso è in fase di studio da parte di un gruppo di lavoro CNA.
- La specifica EMVCo Lev. 1 completa varie mancanze della ISO 14443 e trova riscontro nelle specifiche Calypso.
- Nuovi lettori Calypso/EMV potrebbero diventare terminali generici, in grado di gestire sia le carte di credito che i trasporti.

Google Wallet

- È il nuovo servizio di Google per semplificare i pagamenti, utilizzando uno smartphone al posto delle carte di credito.
- Il sistema sarà gestito in collaborazione con MasterCard e Citi
- Obiettivi: rendere più semplici e frequenti le transazioni attraverso denaro in forma elettronica
- Un solo smartphone compatibile, ad oggi, e limitazione al solo territorio degli Stati Uniti
- GW è un'applicazione che trasforma il telefono cellulare in un portafoglio, senza costi aggiuntivi.

Google Wallet (2)

- Il sistema conserva una versione elettronica delle tue carte di credito e dei coupon per ottenere sconti o fare acquisti con particolari promozioni commerciali.
- Basato su NFC con Secure Element nel telefono

Complementi

Quello che ancora non abbiamo riepilogato

Sicurezza fisica dei chip

- Il "Common Criteria for Information Technology Security Evaluation" (abbreviato in Common Criteria o CC) è uno standard internazionale (ISO/IEC 15408) per la certificazione di sicurezza dei computer
- Es. CC EAL5+ è il livello di sicurezza che resiste a tutti gli attacchi fisici ai chip

NXP

- E’ forse il più importante operatore mondiale nella progettazione e produzione di chip per smart card, per telefoni e per lettori.

MIFARE CLASSIC

- La carta trasporti più diffusa al mondo
- Caratteristiche di sicurezza: algoritmo crittografico Mifare®, CRC 16 bit per blocco, ogni settore protetto da due chiavi
- Organizzazione della memoria:
  - MF1K: 1 kByte EEPROM (16 settori di 4 blocchi)
  - MF4K: 4 kByte EEPROM (32 settori di 4 blocchi, 8 settori di 16 blocchi)
- Ormai tecnicamente superata, non è raccomandata per nuovi sistemi

ISO 7816 ISO 14443

NXP MIFARE™ Smart

Product Features	MIFARE Ultralight™	MIFARE Ultralight™ C	MIFARE™ Classic 1K	MIFARE™ Classic 4K	MIFARE Plus™ S 2K	MI
	MF0 IC U1X	MF0 IC U2X	MF1 S50	MF1 S70	MF1 SPLUS 60	MF
Memory						
EEPROM size [byte]	64	192	1024	4096	2048	40
OTP area [bit]	32	32	-	-	-	-
Write Endurance [cycles]	10 000	10 000	100 000	100 000	200 000	20
Data Retention [yrs]	5	5	10	10	10	10
Organization	16 pages à 4 byte	48 pages à 4 byte	16 sectors á 64 byte	32 sectors á 64 byte 8 sectors á 256 byte	32 sectors á 64 byte	32 8 s
RF-Interface						
Acc. to ISO 14443A	yes - up to layer 3	yes – up to layer 3	yes - up to layer 3	yes - up to layer 3	yes - up to layer 4	yes
Frequency [MHz]	13.56	13.56	13.56	13.56	13.56	13.
Baudrate [kbit/s]	106	106	106	106	106 … 848	10
Anticollision	bit-wise	bit-wise	bit-wise	bit-wise	bit-wise	bit
Operating Distance [mm]	up to 100	up to 100	up to 100	up to 100	up to 100	up
Security						
Serial Number [byte]	7 B UID	7 B UID	4 B NUID or 7 B UID with optional random ID#	4 B NUID or 7 B UID with optional random ID#	4 B NUID or 7 B UID, optional random ID	4 B opt
Random Number Generator	-	yes	yes	yes	yes	yes
Access Keys	-	1 key	2 keys per sector	2 keys per sector	2 CRYPTO1 or AES keys per sector	2 C sec
Access Conditions	per page	per page	per sector	per sector	per sector	per
MIFARE Classic™ Security (Crypto1)	-	-	supported	supported	supported in security level 1&2	sup
DES & DES3 Security	-	authentication	-	-	-	-
AES 128 Security	-	-	-	-	CMACing	CM
Anti-tear supported by chip	-	-	for value blocks	for value blocks	for AES keys, sector trailers and configuration	for cor
Special Features						
Multi-application	-	-	supports MAD*	supports MAD2**	supports MAD2**	sup
Special Functionalities	-	-	-	-	Multi-sector authentication	Mu
Purse Functionality	-	16-bit counter	Value block format	Value block format	-	-
Packaging						
Sawn Wafer	-	-	4 B NUID MF1S5035DUH	4 B NUID MF1S7035DUB	-	-
Sawn Wafer (Au-Bumped)	MF0ICU1001W/S7DL (17 pF, 75 µm) MF0ICU1101W/S7DL (50 pF, 75 µm) MF0ICU1001W/U7DL (17 pF, 120 µm) MF0ICU1101W/U7DL (50 pF, 120 µm)	MF0ICU2001DUD (17 pF) MF0ICU2101DUD (50 pF)	7 B UID MF1S500yXDUD## 4 B NUID MF1S503y(X)DUD#	7 B UID MF1S700yXDUD## 4 B NUID MF1S703y(X)DUD#	7 B UID MF1SPLUS6001DUD/03 4 B NUID MF1SPLUS6031DUD/03	7 B 4 B
MOA2 Module	-	-	4 B NUID MF1S5030DA3	4 B NUID MF1S7030DA3	-	
MOA4 Module	MF0MOA4U10/D	MF0MOU2001DA4 (17 pF) MF0MOU2101DA4 (50 pF)	7 B UID MF1S5000XDA4# 4 B NUID MF1S5030(X)DA4#	7 B UID MF1S7000XDA4# 4 B NUID MF1S7030(X)DA4#	7 B UID MF1SPLUS6001DA4/03 4 B NUID MF1SPLUS6031DA4/03	7 B 4 B
MOA8 Module			7 B UID MF1S5000XDA8# 4 B NUID MF1S5030(X)DA8#	7 B UID MF1S7000XDA8# 4 B NUID MF1S7030XDA8#		

*MAD: MIFARE Application Directory **MAD2: MAD Extension for 4 kbyte EEPROM size ***MAD3: MAD2 Extension for DESFire
Available from Q1 2011 onwards/X-Types available from Q2 2011 onwards ## «y» indicating the silicon source

MIFARE Plus™ S 4K	MIFARE Plus™ X 2K	MIFARE Plus™ X 4K	MIFARE DESFire™ EV1 2K	MIFARE DESFire™ EV1 4K	MIFARE DESFire™ EV1 8K
MF1 SPLUS 80	MF1 PLUS 60	MF1 PLUS 80	MF3 IC D21	MF3 IC D41	MF3 IC D81
4096	4096	4096	2048	4096	8192
-	-	-	-	-	-
200 000	200 000	200 000	500 000	500 000	500 000
10	10	10	10	10	10
32 sectors á 64 byte 8 sectors á 256 byte	32 sectors á 64 byte 8 sectors á 256 byte	32 sectors á 64 byte 8 sectors á 256 byte	flexible file system	flexible file system	flexible file system
yes - up to layer 4	yes - up to layer 4	yes - up to layer 4	yes - up to layer 4	yes - up to layer 4	yes - up to layer 4
13.56	13.56	13.56	13.56	13.56	13.56
106 ... 848	106 ... 848	106 ... 848	106 ... 848	106 ... 848	106 ... 848
bit-wise	bit-wise	bit-wise	bit-wise	bit-wise	bit-wise
up to 100	up to 100	up to 100	up to 100	up to 100	up to 100
4 B NUID or 7 B UID, optional random ID	4 B NUID or 7 B UID, optional random ID	4 B NUID or 7 B UID, optional random ID	7 B UID	7 B UID	7 B UID
yes	yes	yes	yes	yes	yes
2 CRYPTO1 or AES keys per sector	2 CRYPTO1 or AES keys per sector	2 CRYPTO1 or AES keys per sector	14 keys per application	14 keys per application	14 keys per application
per sector	per sector	per sector	per file	per file	per file
supported in security level 1&2	supported in security level 1&2	supported in security level 1&2	-	-	-
-	-	-	CMACing / Encipherment	CMACing / Encipherment	CMACing / Encipherment
CMACing	CMACing / Encipherment	CMACing / Encipherment	CMACing / Encipherment	CMACing / Encipherment	CMACing / Encipherment
for AES keys, sector trailers and configuration	for AES keys, sector trailers and configuration	for AES keys, sector trailers and configuration	yes	yes	yes
supports MAD2**	supports MAD2**	supports MAD2**	28 applications, MAD3***	28 applications, MAD3***	28 applications, MAD3***
Multi-sector authentication	Multi-sector authentication, Proximity Check, full virtual card support	Multi-sector authentication, Proximity Check, full virtual card support	Automatic backup mechanism Random ID (optional)	Automatic backup mechanism Random ID (optional)	Automatic backup mechanism Random ID (optional)
-	Value block format	Value block format	Value file	Value file	Value file
-	-	-	-	-	-
7 B UID MF1SPLUS8001DUD/03 4 B NUID MF1SPLUS8031DUD/03	7 B UID MF1PLUS6001DUD/03 4 B NUID MF1PLUS6031DUD/03	7 B UID MF1PLUS8001DUD/03 4 B NUID MF1PLUS8031DUD/03	MF3ICD2101DUD/05 (17 pF) MF3ICDH2101DUD/05 (70 pF)	MF3ICD4101DUD/05 (17 pF) MF3ICDH4101DUD/05 (70 pF)	MF3ICD8101DUD/05 (17 pF) MF3ICDH8101DUD/05 (70 pF)
			-	-	-
7 B UID MF1SPLUS8001DA4/03 4 B NUID MF1SPLUS8031DA4/03	7 B UID MF1PLUS6001DA4/03 4 B NUID MF1PLUS6031DA4/03	7 B UID MF1PLUS8001DA4/03 4 B NUID MF1PLUS8031DA4/03	MF3MOD2101DA4/05 (17 pF) MF3MODH2101DA4/05 (70 pF)	MF3MOD4101DA4/05 (17 pF) MF3MODH4101DA4/05 (70 pF)	MF3MOD8101DA4/05 (17 pF) MF3MODH8101DA4/05 (70 pF)

SmartMX2 MX2

Key benefits

- Unique security architecture meets current and future security requirements
- Multi-applications capability offers more value to your solutions
- Outstanding performance enables differentiation in terms of user convenience and transaction speed
- Fast time-to-market and smooth implementation

Key features

- IntegralSecurity™ architecture for best-in-class attack protection, CC EAL 6+
- High-performance SmartMX2 CPU with enhanced 8- to 32-bit application instruction set
- Power-efficient, high-speed crypto coprocessors for RSA/ECC and DES/AES
- Optimized ISO/IEC 14443 interface, including support for small antenna dimensions
- MIFARE DESFire™, MIFARE Plus™, and MIFARE™ Classic for applications convergence

Applications

- eGovernment
  - Passports, electronic IDs and credentials, health and social-security cards, driver's licenses
- Banking
  - Debit, credit, loyalty, ePurse, ATM
  - Different payment schemes combined with transport
- Transport
  - From stored value tickets to national transport schemes
- Access management
  - Access to buildings, logical access to PCs
- Mobile transactions
  - Payment, couponing, transport, access management
- Device authentication
  - Counterfeit protection of hardware, software and content
  - Cyber Security solutions to get access securely to service networks

Usa e getta

Dette anche *chip-on-paper* o *disposable*

MIFARE Ultralight EV1

Key applications

- Limited-use tickets in public transport
- Event ticketing (stadiums, exhibitions, leisure parks, etc.)
- Loyalty

Key features

- Fully ISO / IEC 14443 A 1-3 compliant
- Backwards compatible to MIFARE Ultralight
- 106 kbit/s communication speed
- Anti-collision support
- Fast read command
- 384 and 1024 Bits user memory product variants
- OTP, Lock Bits, configurable counters
- Three independent 24-bit one-way counters
- Protected data access through 32-bit password
- NXP Semiconductors originality signature
- Preparation for Virtual Card functionality
- Unique 7 bytes serial number
- Number of single write operations: 10.000

Benefits for solution developers

- Compliance to ISO / IEC 14443 A 1-3
- Backwards compatibility to MIFARE Ultralight
- Enhanced security for limited-use applications
- Ease of use and proven toolkits
- Fast time-to-market

Benefits for service providers

- Ability to check originality of tickets
- Improve transaction time using the Fast Read command
- Ideal for multi operator transportation systems with three independent counters (e.g.: bus, tram, metro)
- Availability of statistical data to optimize the system
- Efficient fleet management
- Higher customer throughput
- Reduction of maintenance costs
- Reduction of cash handling
- Fraud prevention
- System enhancement in limited-use applications

Product Features	MIFARE Ultralight EV1 384 Bit User Memory	MIFARE Ultralight EV1 1024 Bit User Memory
Memory		
EEPROM size [bits]	640	1312
OTP area [bit]	32	
Write Endurance [cycles]	100.000	
Data Retention [yrs]	10	
Organization	20 pages a 4 byte	41 pages a 4 byte
RF-Interface		
Acc. to ISO/IEC 14443 A	ISO/IEC 14443 A 1-3	
Baudrate [kbit/s]	106	
Anti-collision	bit-wise	
Security		
Unique Serial Number [byte]	7 B UID	
Memory Overwrite Protection	yes, per page	
Special Features		
Purse Functionality	3 x 24-bit one-way counter	
Special Functionalities	Fast Readout function NXP Originality Check	
Memory Protection	32-bit password protection	
Packaging		
Sawn Wafer 120µm on FFC (Au-Bumped) 17 pF	MF0UL1101DUD	MF0UL2101DUD
Sawn Wafer 75µm on FFC (Au-Bumped) 17 pF	MF0UL1101DUF	MF0UL2101DUF
MOA8 Module 17 pF		MF0UL2101DA8

	CTS-256-B	CTS-512-B	CTS-512-A	CTM-512-B	CTM-8k-A
RF Interface	ISO14443 B	ISO 14443 B	ISO 14443 A	ISO 14443 B	ISO 14443 A
Compatibility	Calypso	Calypso	Mifare®	Calypso	Mifare®
EEPROM	256 bits	512 bits	512 bits	512 bits	8192 bits
Security					
Unique S/N	64 bits	64 bits	56 bits	64 bits	32 bits
OTP area	12 bits	128 bits	32 bits	Variable	Variable
Memory Write protection	Yes per sector	Yes per sector	Yes per page or block	Yes per sector	Yes per sector
Authentication	Simple static	Simple static	Simple static	Simple dynamic	Mutual dynamic
Key length	N/A	N/A	N/A	80 bits diversified	48 bits
Other features				One way counter	Random generator
SAM	Optional	Optional	Optional	YES	MFRC500
Miscellanous					
Anticollision	No	Yes	Yes	Yes	Yes
Typical transaction time	<100 ms	< 100ms	< 100ms	< 200 ms	< 200ms
Typical communication distance	10 cm	10 cm	10 cm	10 cm	10 cm
Write endurance	1000 cycles	1000 cycles	1000 cycles	100000 cycles	100000 cycles

Carte CTS (Fonte: ASK)

Grazie dell'attenzione
Thanks for your attention

g.becattini@aep-italia.it