Posteitaliane

La Sicurezza in TITAN

Innovazione per Smartcard e Terminali PoI

Emiliano Sparaco - Alberto Ferro

Trento 08/03/2013

investiamo nel vostro futuro

Agenda

- Innovazione per Smartcard – JavaCard e GlobalPlatform
- Multi-applicazione: L'unione fa la forza
- Il modello S.T.R.I.D.E. applicato alla monetica
- S.T.R.I.D.E e GlobalPlatform
- Innovazione per Terminale PoI – Chip only
- Operazioni svolte dal layer crittografico
- Layer Crittografico: Algortimi TDES/RSA e AES/ECC
- Mitigazione dell'information disclosure

Posteitaliane

Modello Smartcard/SIM-card

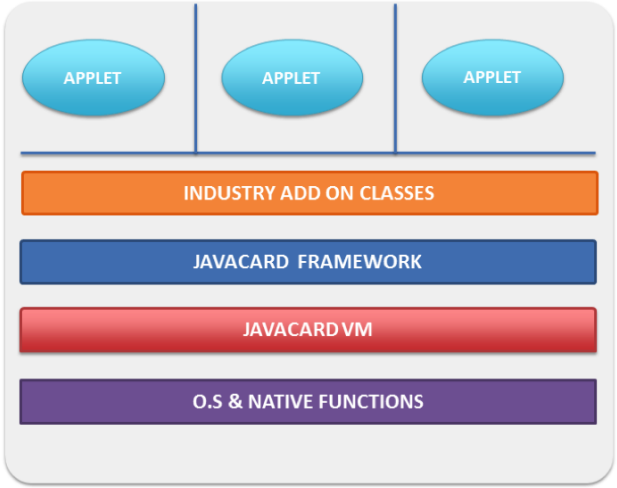
Emiliano Sparaco

Trento 08/03/2013

investiamo nel vostro futuro

L'utilizzo del framework **JavaCard** su una smartcard permette di eseguire e gestire le applicazioni (denominate applet) offrendo :

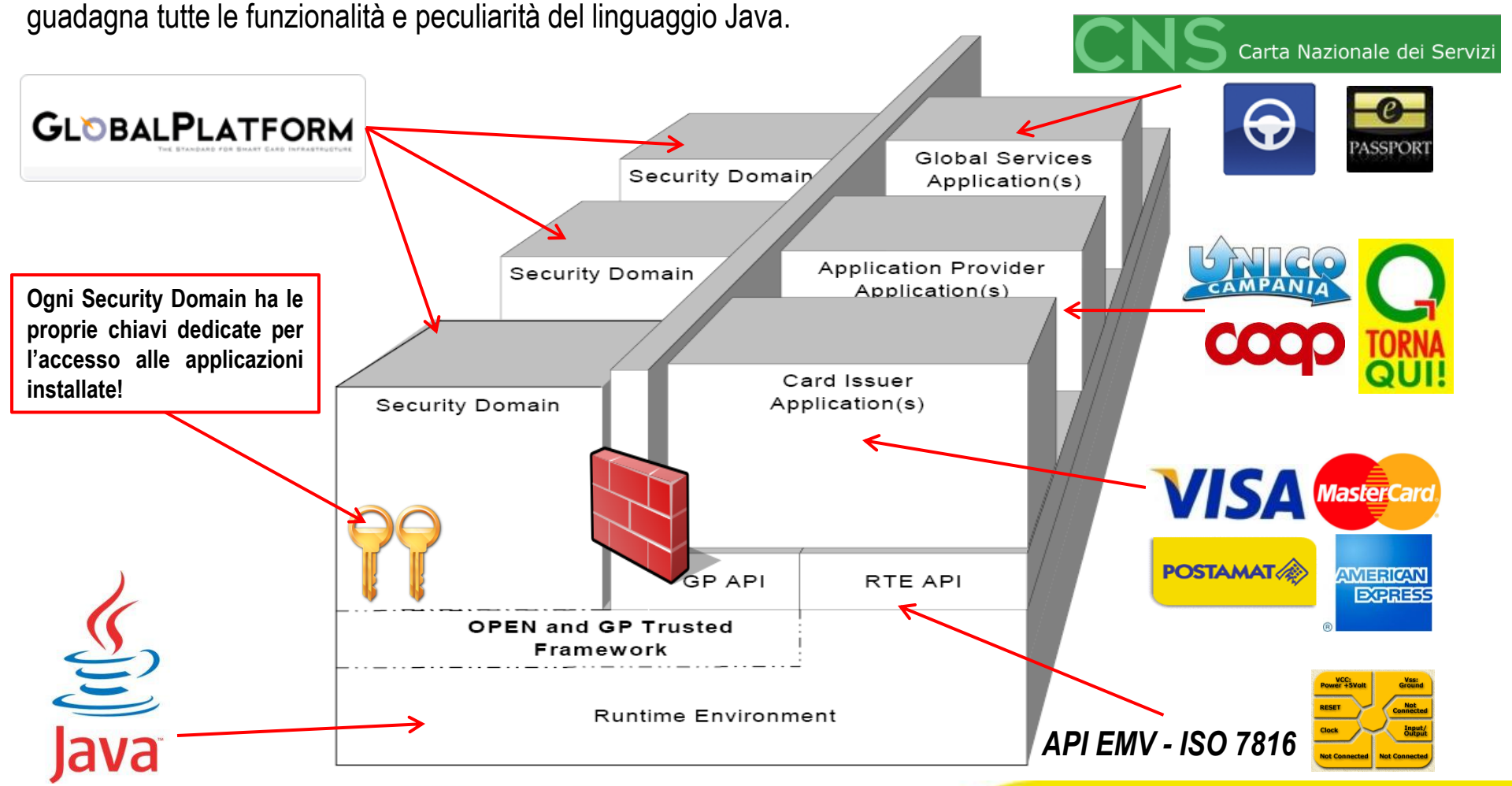
✓**Interoperabilità:** un applet può essere eseguita su qualsiasi prodotto JavaCard-based;
✓**Sicurezza:** il byte code interpretato e il firewall software tra contesti di installazione rendono l'ambiente di esecuzione sicuro;
✓**Dinamicità:** le applet possono essere installate in momenti diversi senza che la sicurezza venga compromessa.



GlobalPlatform è un'organizzazione indipendente fondata nel '99, dove ad oggi partecipano tutti i principali Circuiti di pagamento Internazionali e i principali provider tecnologici mondiali, che ha lo scopo di realizzare e standardizzare le procedure e funzioni, che permettano a tutti gli stakeholders coinvolti in un sistema di pagamento, di far coesistere diverse tipologie di applicazioni sulla stessa piattaforma. Alcuni membri:

Multi-applicazione: L'unione fa la forza

Grazie alla sua architettura logica suddivisa in domini di sicurezza, lo standard GlobalPlatform permette di gestire contemporaneamente sulla stessa piattaforma più entità differenti. E' possibile quindi avere servizi di diversa tipologia nella stessa smartcard, ognuno con un proprio dominio di sicurezza dedicato, e con proprie chiavi di accesso e autenticazione. L'architettura sfrutta principalmente come base il framework JavaCard, con cui il prodotto guadagna tutte le funzionalità e peculiarità del linguaggio Java.



Ogni Security Domain ha le proprie chiavi dedicate per l'accesso alle applicazioni installate!

Il modello S.T.R.I.D.E. applicato alla monetica

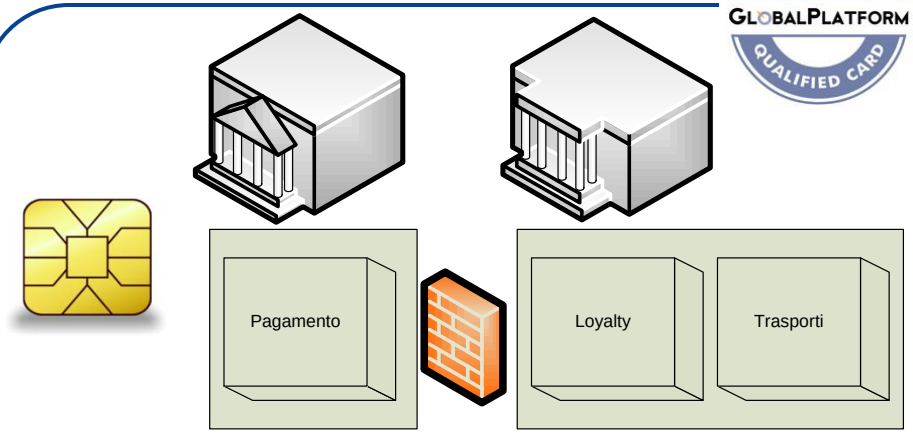
S.T.R.I.D.E. è un sistema sviluppato da Microsoft per studiare la sicurezza su sistemi prettamente informatici, principalmente usato per la modellazione delle minacce applicabili al sistema. L'acronimo deriva dall'iniziale delle minacce:

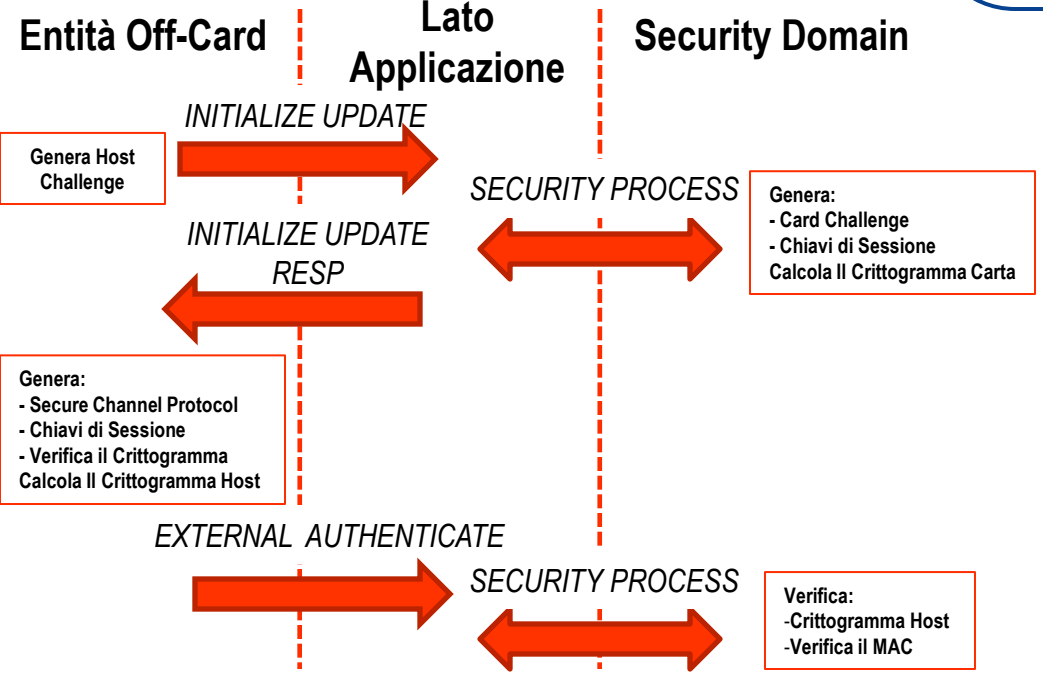
SPOOFING - Falsificazione dei dati per l'accesso al sistema**;**
TAMPERING **–** Modifiche non autorizzate e volontarie ai dati sensibili;
REPUDIATION **–** Esecuzione di un azione proibita provando l'integrità e l'origine dei dati;
INFORMATION DISCLOSURE - Esposizione di informazioni personali all'esterno del sistema;
DENIAL OF SERVICE (DoS) - Negazione totale del servizio solitamente tramite flooding;
ELEVATION OF PRIVILEGE **-** Ottenere illegalmente tramite bug l'accesso ROOT al sistema.

Il modo più semplice per applicare il modello S.T.R.I.D.E. ad un sistema è considerare come ciascuna delle minacce nel modello colpisce **ogni singolo componente**.

S.T.R.I.D.E. e GlobalPlatform

L'architettura logica GlobalPlatform, grazie alla suddivisione in più Security Domain, mitiga intrinsecamente le problematiche di **INFORMATION DISCLOSURE**; Inoltre i dati sono contenuti in una zona di memoria sicura, racchiusa dentro ai confini del Security Domain stesso e protetti da Firewall.
Questo meccanismo mitiga attacchi di tipo **REPUDIATION** poiché le aree di memoria non sono condivisibili.





L'accesso ai Security Domains è effettuato tramite mutua autenticazione tra entità Off-Card e Dominio di Sicurezza.
Le chiavi quindi sono in possesso solamente dell'entità che gestisce il relativo Security Domain (mitigazione **ELEVATION OF PRIVILEGE**).
Questo meccanismo, in aggiunta all'apertura del Secure Channel Protocol e alla generazione delle chiavi di sessione, oltre al principio di mutua autenticazione ISO9798, mitiga direttamente i rischi provenienti da attacchi di tipo **SPOOFING**.

Posteitaliane

Modello Terminale Pol

Alberto Ferro

Trento 08/03/2013

UNIONE EUROPEA
Fondo europeo di sviluppo regionale

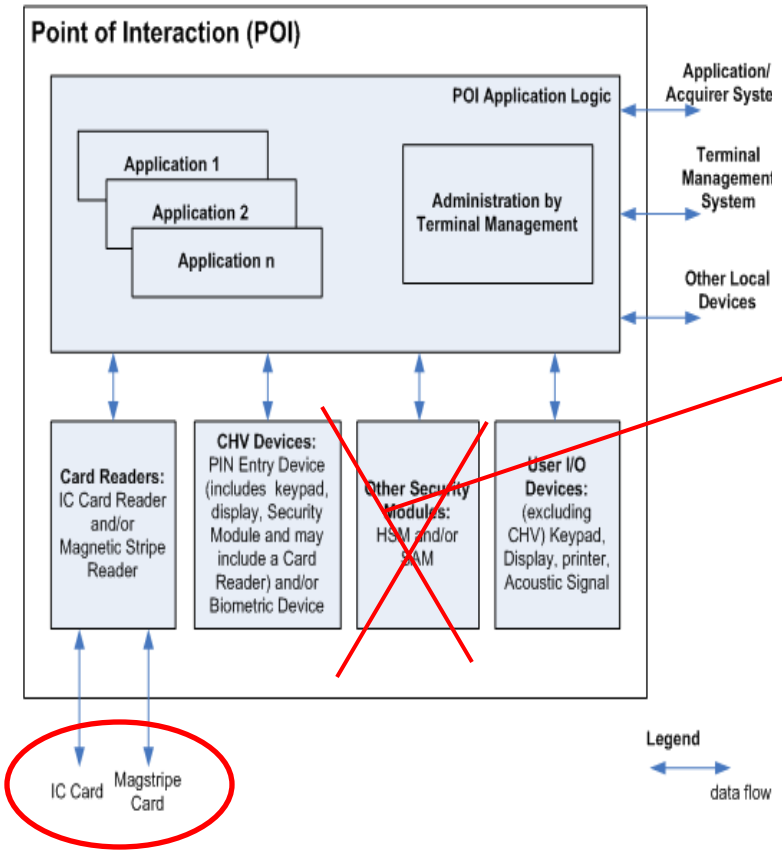
PON Ricerca e Competitività 2007-2013

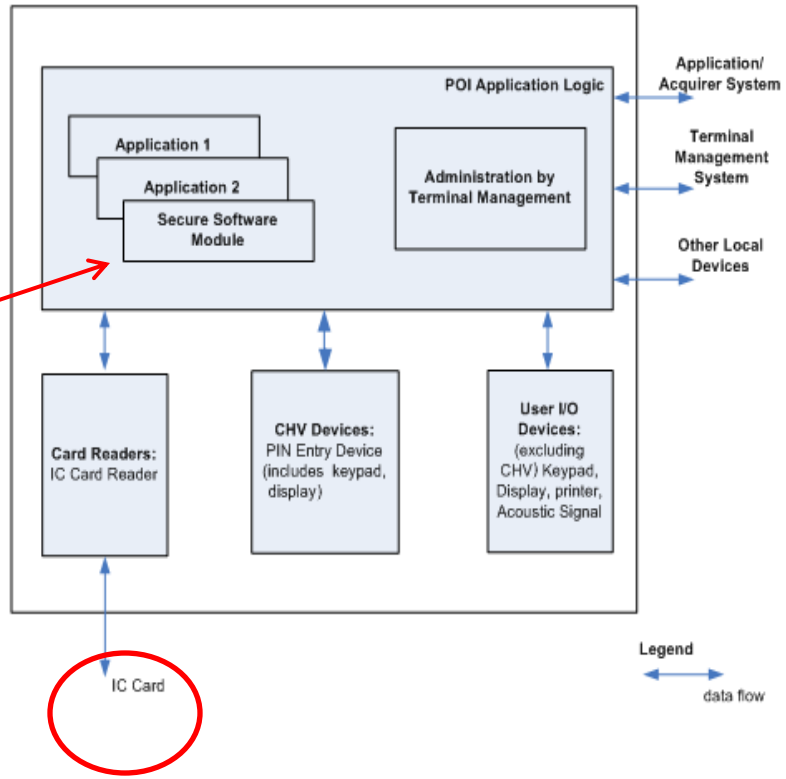
Ministero dell'Istruzione, dell'Università e della Ricerca

Ministero dello Sviluppo Economico

investiamo nel vostro futuro

Innovazione per Terminali PoI – Chip only

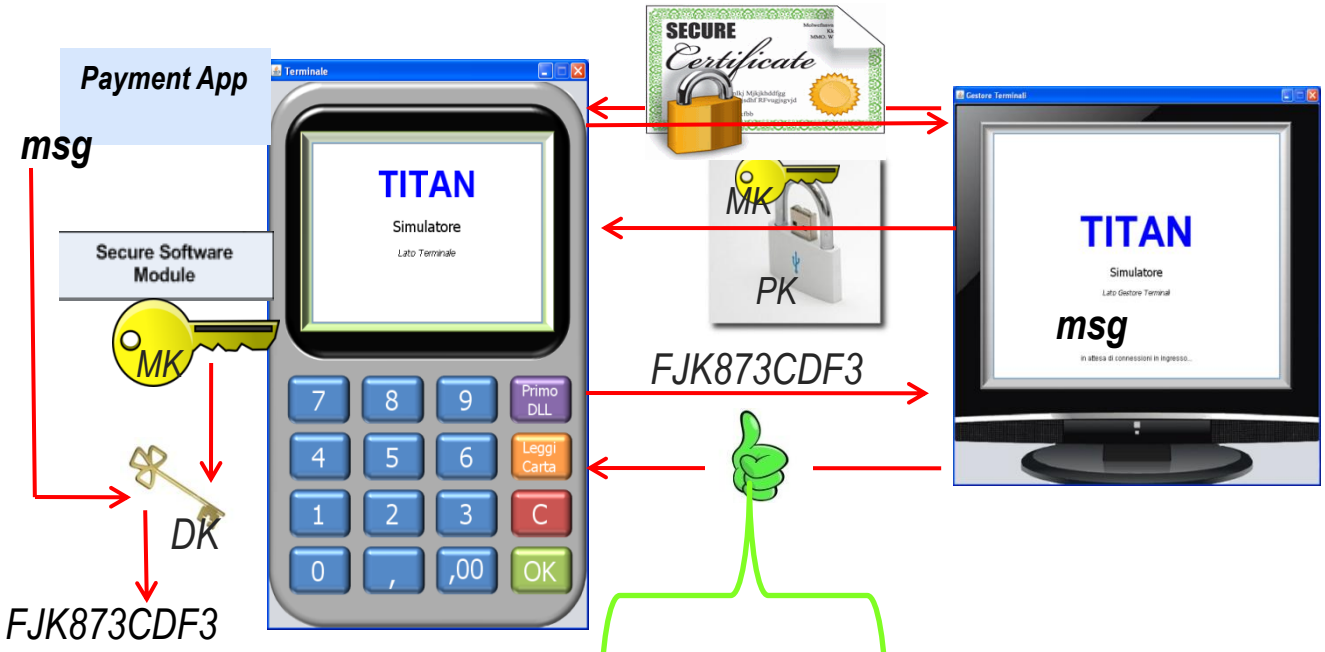




- ✓ *Favorire lo sviluppo della multi applicazione*
- ✓ *Ambiente Chip only intrinsecamente più sicuro rispetto all'ambiente banda-chip*
- ✓ *Riduzione costi hardware*
- ✓ *Aumento probabilità di accadimento della information disclosure*
- ✓ *Obiettivo1: Verifica di tutte le operazioni crittografiche svolte dal layer crittografico*
- ✓ *Obiettivo2: mitigazione alla information disclosure*

Operazioni svolte dal Layer Crittografico

✓ *Gestione di tutte le operazioni crittografiche svolte dal terminale attraverso il layer crittografico*



✓ *Memorizzazione MK*
✓ *Selezione MK dedicata*
✓ *Derivazione MK selezionata*
✓ *Cifratura del messaggio con la DK*

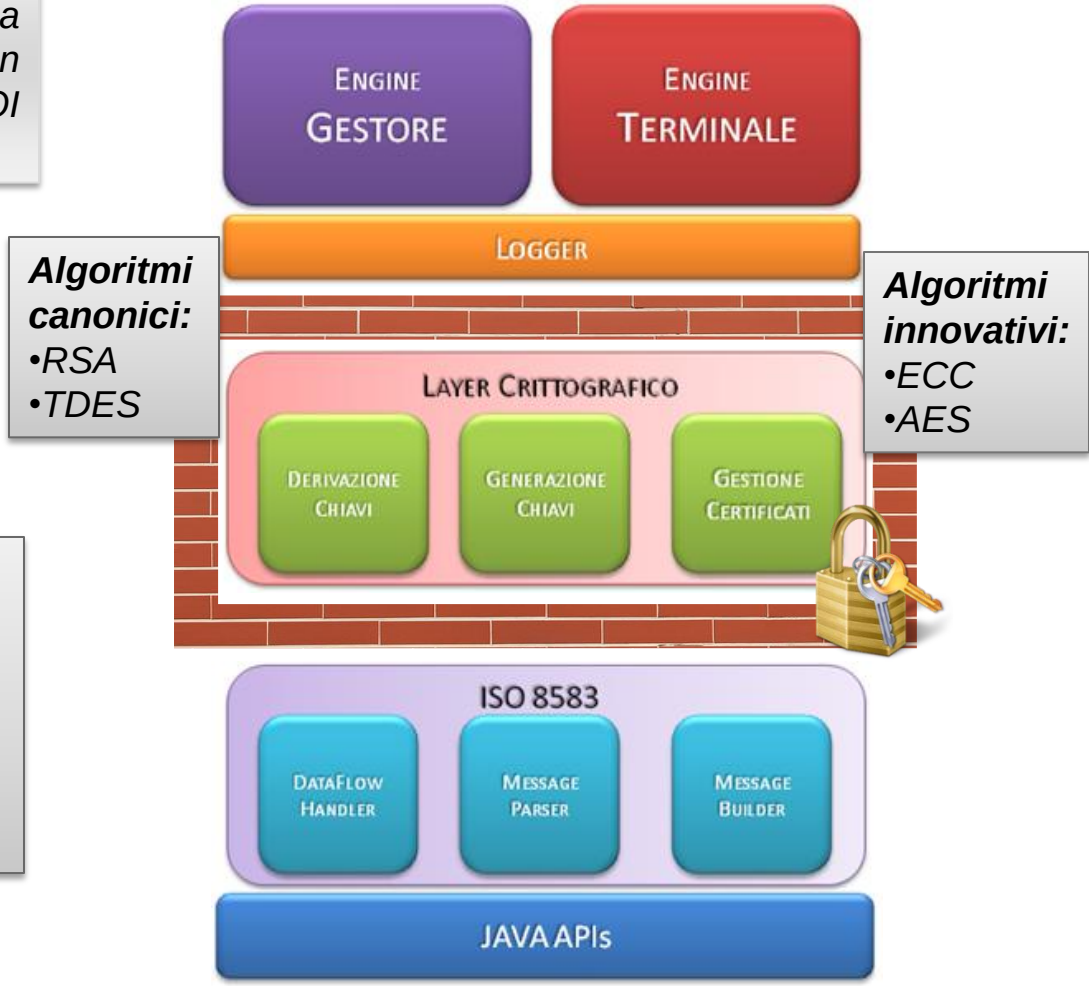
✓ *Crittografia simmetrica*

✓ *Verifica Certificato*
✓ *Estrazione chiave pubblica controparte*
✓ *Decifratura con la chiave privata*

✓ *Crittografia asimmetrica*

Layer Crittografico: Algortimi TDES/RSA e AES/ECC

La ricerca di mercato eseguita per reperire un terminale con l'architettura descritta, ha evidenziato il carattere innovativo della ricerca in quanto nessun produttore di Terminali POI dispone di un prodotto simile

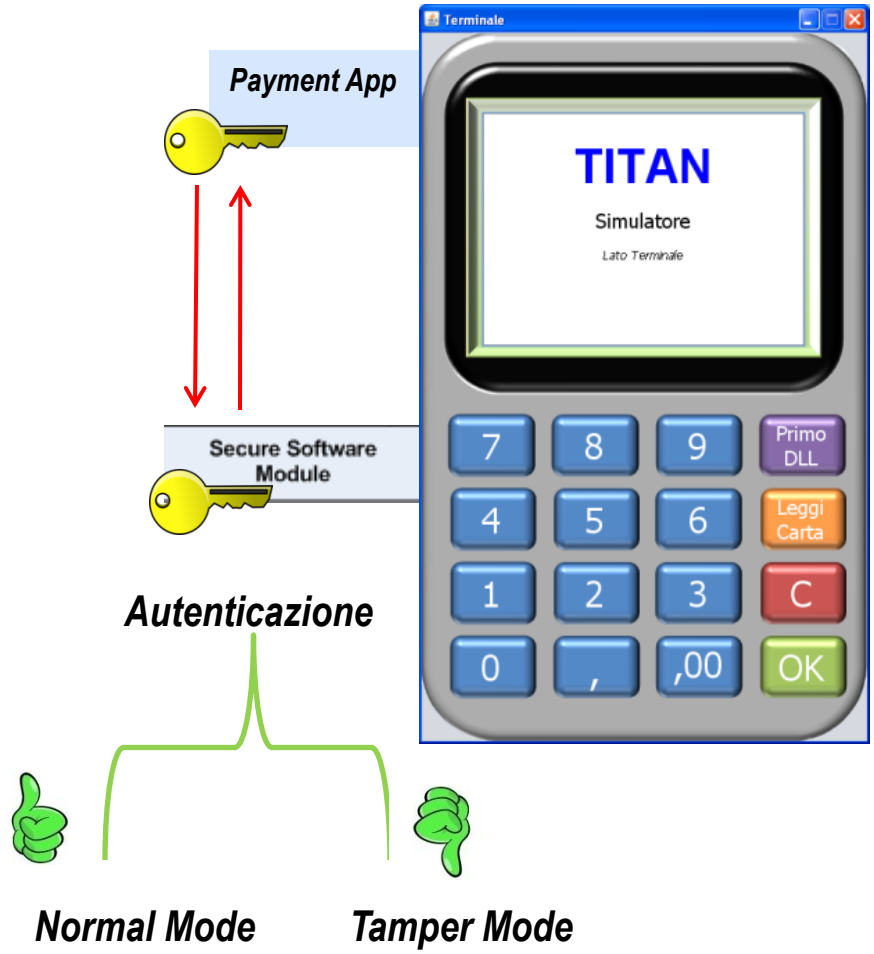


Algoritmi canonici:
- *RSA*
- *TDES*

Algoritmi innovativi:
- *ECC*
- *AES*

- *Simulazione in ambiente desktop*
- *Logica del Terminale e del GT*
- *Configurazione - Transazioni finanziarie*
- *Gestione del PIN solo online*
- *Simulazione relativa alla sola tratta bancaria*
- *Carta simulata da un file*
- ***Utilizzo algoritmi crittografici innovativi***

Mitigazione dell'information disclosure



✓*L'applicazione formatta il messaggio da inviare sulla tratta bancaria ed interagisce con il layer crittografico per effettuare la cifratura/decifratura del messaggio.*

✓*Ogni chiamata al Layer Crittografico avviene con un meccanismo di autenticazione basato su chiave* ***AES*** *a* ***256 bit****.*

✓*La chiave viene iniettata in entrambi i moduli software all'interno della Secure Room ed è nota solo al produttore.*

✓*Tale soluzione consente di mitigare gli attacchi di tipo* ***Information disclosure*** *poiché impedisce l'accesso alla memoria sicura alle applicazioni non autenticate.*

✓*Viene introdotto un meccanismo di* ***Tamper Responsive*** *di tipo software in quanto a un tentativo di accesso al layer crittografico da parte di un'applicazione non autorizzata, corrisponde un blocco dell'operatività del terminale.*

Le attività di ricerca sono state svolte in collaborazione con il **Prof. Massimiliano Sala, direttore del Laboratorio di Crittografia dell'Univ. di Trento**, che ha approvato quanto redatto e testato, in vista della visita ispettiva del M.I.U.R. durante la quale verranno presentati i test effettuati nel laboratorio di TITAN e i relativi prototipi realizzati.

Grazie per l'attenzione

Posteitaliane