e-payment: normative di sicurezza e best practice

Trento, 08 Marzo 2013

Vanni Galesso

Security Architect@IKS

www.iks.it
informazioni@iks.it
049.870.10.10

Il gruppo IKS

1999 — IKS

Capogruppo e azienda leader

Nata nel 1999 con focalizzazione sui temi della Governance IT e Security

2006 — daddoquadro

B2B application

Informatizzazione e dematerializzazione dei processi aziendali.

2008 — KIMA gruppo IKS

Compliance

Si occupa di security compliance.

Prima azienda italiana certificata PCI QSA e ASV

2009 — IKS TN

R&D

Ricerca e Sviluppo.

2011 — KLEIS

Fraud Management

Azienda leader per le tematiche frodi in ambito finanziario.

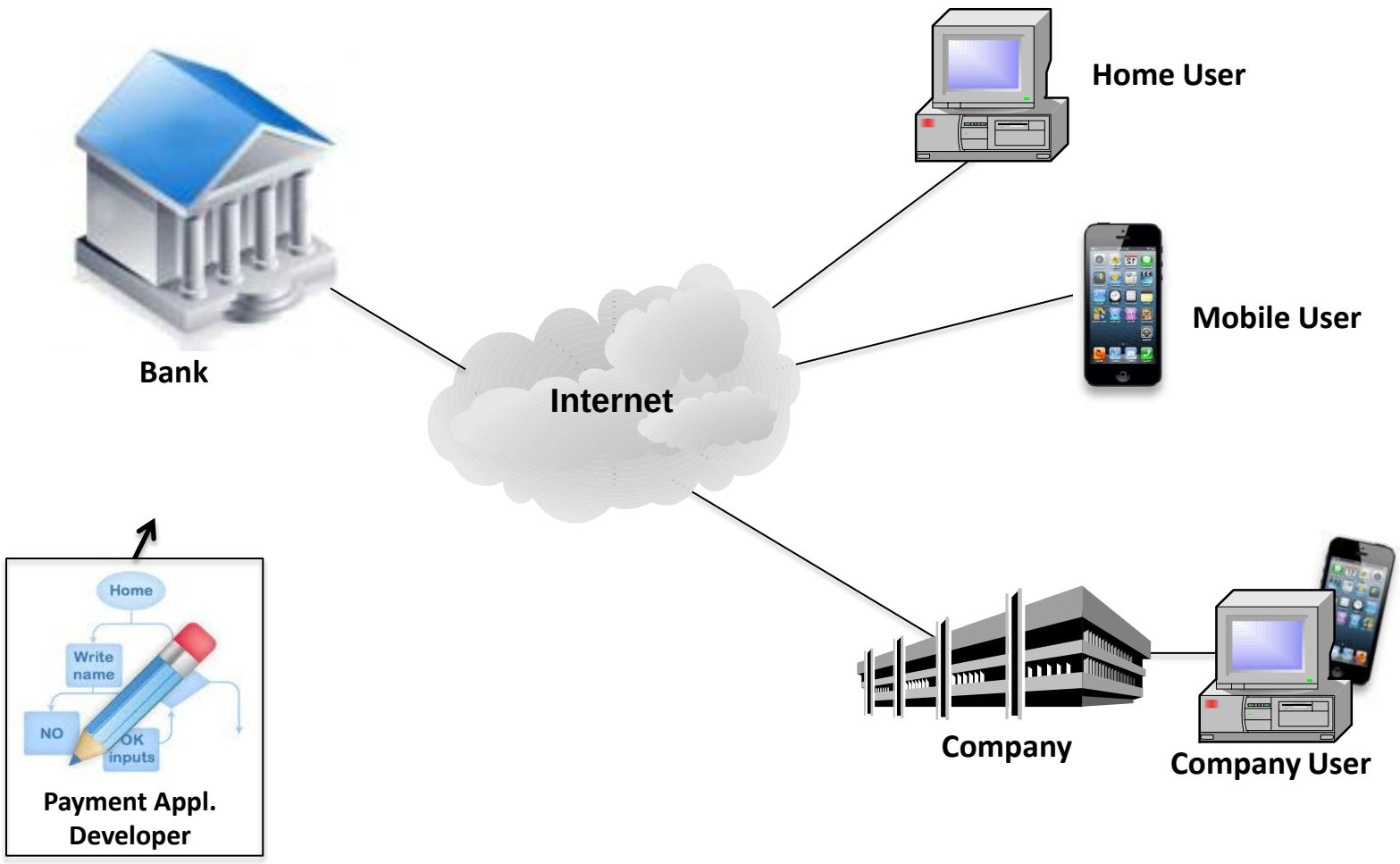
E-Payment

Si intende il **pagamento** per l'acquisto, la vendita di beni o servizi offerti attraverso **Internet**, o in linea di massima si intende il pagamento attraverso qualsiasi **linea dati**.

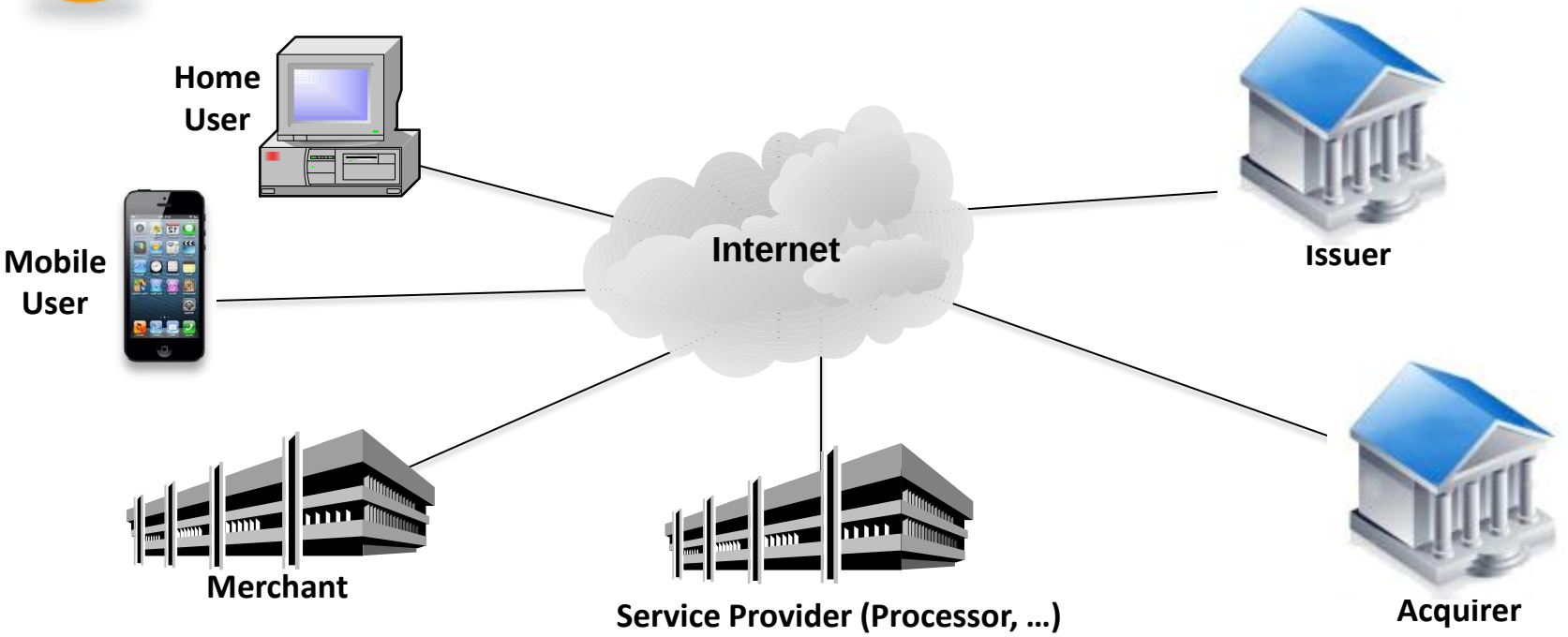
Cit. Wikipedia

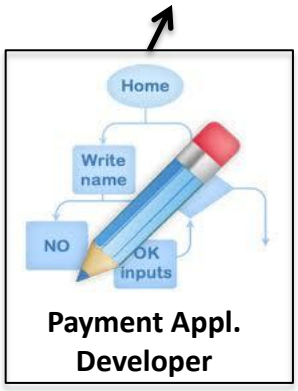
I molteplici scenari di E-Payment

Scenari: Home & Corporate Banking

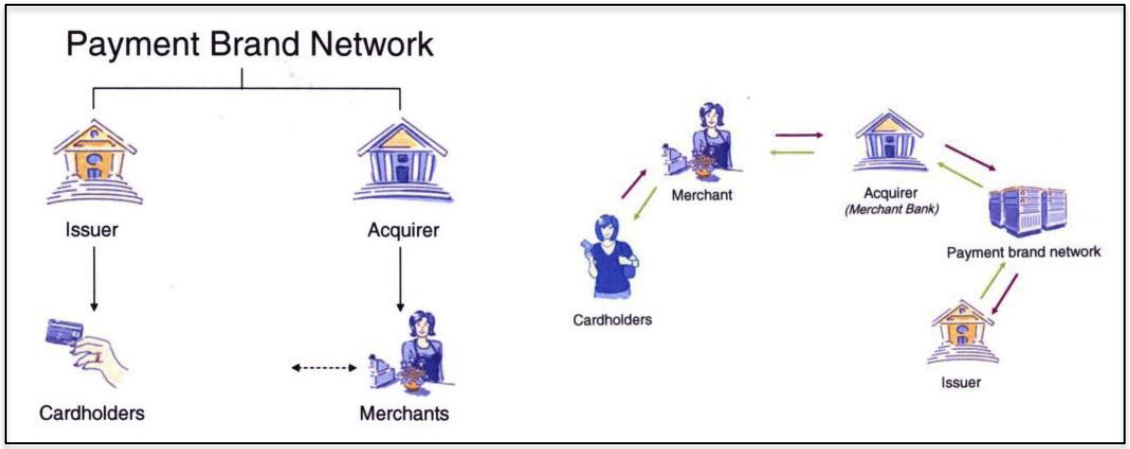


Scenari: E-Commerce

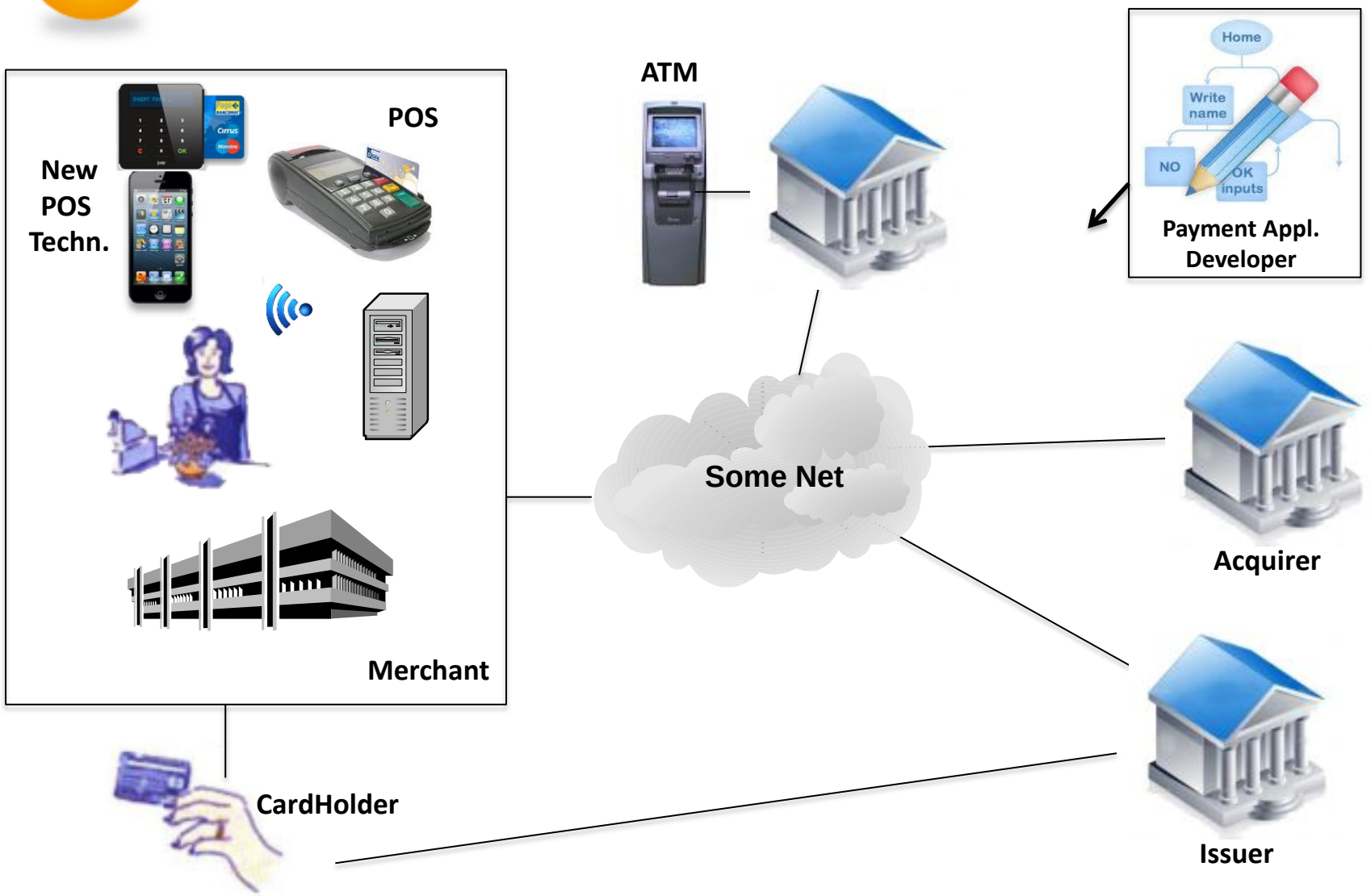




Payment Appl. Developer



Scenari: Card Present

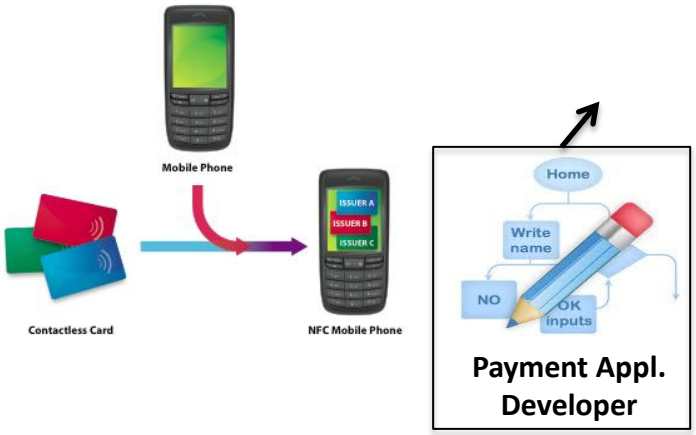


Scenary: Proximity MicroPayment

MNO: Mobile Network Operator
OTA: Over the Air supporting protocols which enable to address the UICC using the handset as a transparent communication means, as defined in "AFSCM: Guidelines for Interconnection of Service Providers' andMobileNetworkOperators' InformationSystems"
OTA functionality includes UICC management, applet issuance, UI application issuance, service management, mobile device management, applet personalization management, security domain management, and applet transport management.

UICC: Universal Integrated Circuit Card

NFC: Near Field Communication



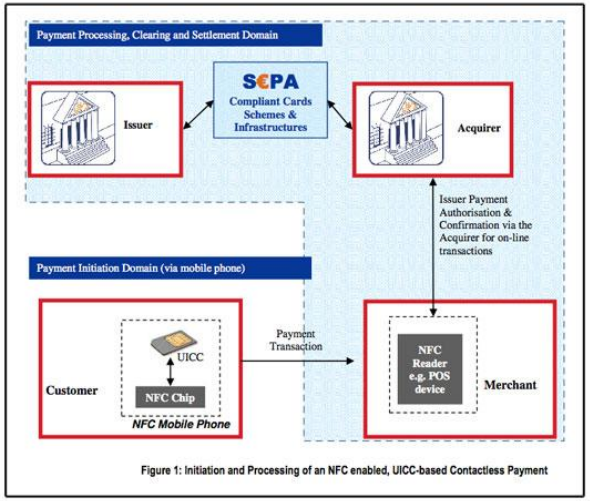


Figure 1: Initiation and Processing of an NFC enabled, UICC-based Contactless Payment

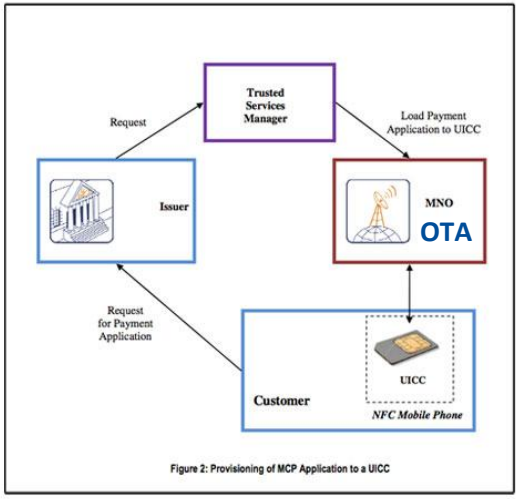
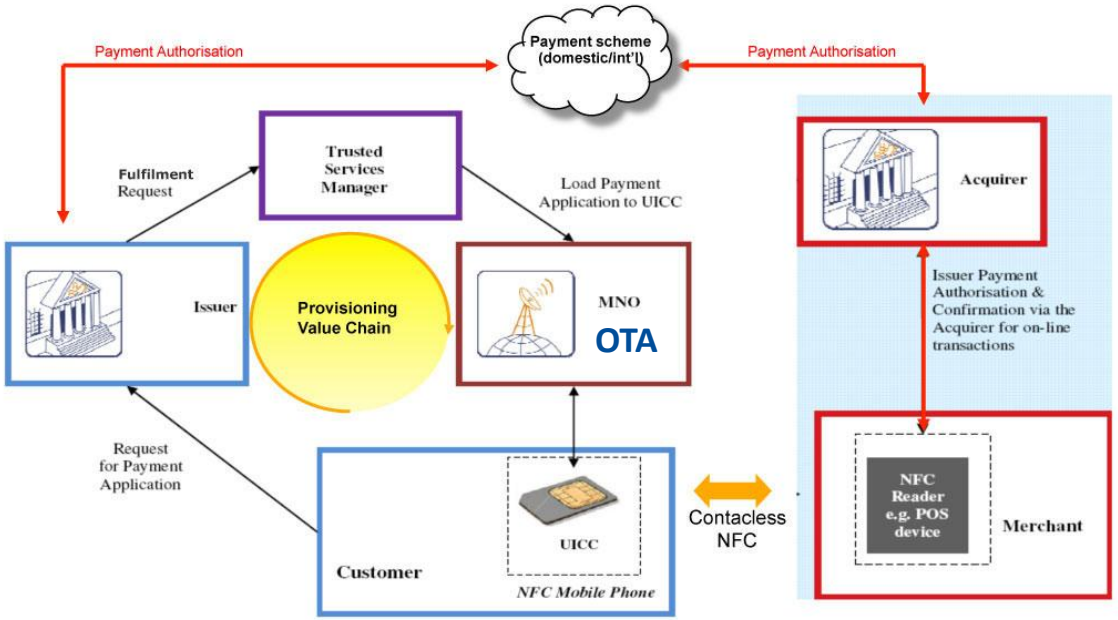


Figure 2: Provisioning of MCP Application to a UICC



Standard e best practices sono davvero utili ?

Casi reali di compromissione

Dopo i lunghi giorni di silenzio iniziali e le scuse, ora la ha deciso di passare al contrattacco per quanto riguarda la vicenda del blocco del causato da un grosso attacco hacker che ha portato alla violazione dei server di ed al furto dei dati sensibili di quasi **80 milioni di utenti** in tutto il mondo.

Il , infatti, ha scritto una **lettera ufficiale** di risposta al Congresso Statunitense che sta indagando sull'accaduto, anche alla luce delle denunce e delle possibili class action messe in atto dagli utenti.

Attacco hacker, rimborserà i clienti

E' ancora sospeso il servizio online della attaccato da degli hacker che hanno intercettato informazioni, anche bancarie, di 77 milioni di utenti. L'azienda ha ora annunciato un piano assicurativo per i clienti americani fino a una copertura di un milione di dollari a utente. Presto dovrebbe essere estesa ad altri paesi.

Ora, però, i guai sembrano non voler proprio abbandonare la che nelle ultime ore è stata vittima di un **nuovo attacco** da parte di un gruppo hacker, che sostiene di aver avuto accesso ai dati di milioni di utenti.

Hacker rubano 130 milioni di numeri di carte di credito

Online nel corso del quale un gruppo di cyber criminali non ancora identificato è riuscito ad entrare in possesso delle informazioni personali di oltre 100 milioni di utenti, è tornato ad affrontare il tema sicurezza.

Casi reali : non troppo standard

A fronte di una login il server restituisce sul dispositivo :

Quali standard usare ?

Non esiste un unico standard che copra tutte le tipologie

Ci sono standard, raccomandazione, best practices che coprono il mondo infrastrutturale, applicativo e hardware

Altri standard presenti

- SEPA (Single Euro Payments Area)
  - Standard per la razionalizzazione delle transazioni bancarie
- EPC (European Payments Council)
  - Organo che doveva implementare SEPA
- EMV (Europay, MasterCard e VISA per pagamenti con smart card, terminali POS e bancomat)
- ISO 27001
  - Standard più generale di gestione della sicurezza delle informazioni

Altri standard hardware NFC

NFC: Near Field Communication

- Can communicate with objects
- Magnetic field induction
- Contactless technology based on RFID 13,56MHz
- NFC is standardized ECMA-340 and ISO/IEC 18092
- Backward compatibility with ISO14443 and SmartCard
  - Millions of readers
  - Easy to use
- NFC-Forum (http://www.nfc-forum.org)

Altri standard sicurezza applicativa

- standard e linee guida NIST;
- standard e linee guida IETF;
- pubblicazioni Fraunhofer SIT;
- OWASP Mobile Security Project.
- Apple: “Secure Coding Guide”;

Il più completo standard sul mercato è : PCI

Il «PCI Security Standards Council» offre una serie di standard per aumentare il livello di sicurezza nei pagamenti con **carta di credito**, è composto da :

- Standard di protezione dei dati (DSS)
- Standard di protezione dei dati per le applicazioni di pagamento (PA-DSS)
- Sicurezza delle transazioni PIN (PTS).

è obbligatoria per tutte le organizzazioni che si occupano dell'elaborazione, dell'archiviazione o della trasmissione di dati relativi a transazioni effettuate con carte di pagamento.

PCI standard anche per mobile payment

EMV e PCI propedeutici per cless e mobile payments

VISA

VISA BULLETIN 9 August 2011

Visa Expands Technology Innovation Program for U.S. Merchants to Adopt Dual Interface Terminals

Visa is announcing plans to accelerate the migration to contact chip and contactless EMV chip technology in the U.S. The adoption of dual-interface chip technology will help prepare the U.S. payment infrastructure for the arrival of Near Field Communication (NFC)-based mobile payments by building the necessary infrastructure to accept and process chip transactions.

Not only will chip technology accelerate mobile innovations, it is also expected to enhance payment security through the use of dynamic authentication. Chip technology greatly reduces a criminal's ability to use stolen payment card data by introducing dynamic values for each transaction. Even if payment card data is compromised, a counterfeit card would be unusable at the point of sale (POS) without the presence of the card's unique elements. By eliminating static authentication, we reduce the value of stolen cardholder data, benefiting all stakeholders.

Visa's plan includes merchant incentives to upgrade to EMV chip-enabled terminals, requirements for acquirer processors to support chip acceptance and the introduction of U.S. liability shift policies.

Specifically, Visa will waive Payment Card Industry Data Security Standard (PCI DSS) compliance validation requirements to encourage merchant investment in contact and contactless chip payment terminals. Visa will also require acquirer processors to ensure that their systems support dynamic data acceptance (i.e., chip) and will institute a domestic and cross-border counterfeit liability shift.

Aree di copertura PCI

PCI as a part of overall Visa Security

VISA

POS Environment (ATM)	Online e-comm	Back office
		PCI PIN
Chip & PCI PIN	Verified by Visa	PCI DSS
PCI PTS/PED		PA DSS

Payment Appl. Developer

Altre raccomandazioni

ECB ripresa da Banca d'Italia ha pubblicato un documento :

RECOMMENDATIONS FOR "PAYMENT ACCOUNT ACCESS" SERVICES

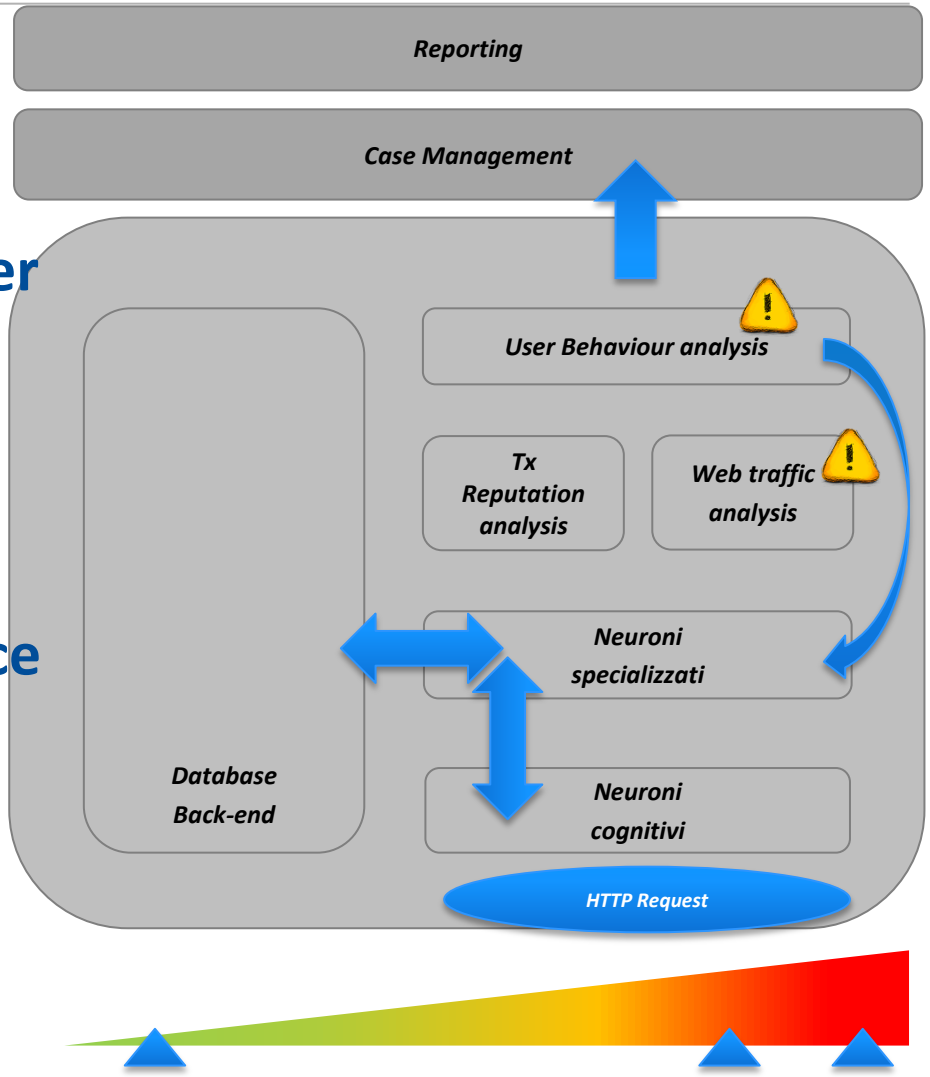
DRAFT DOCUMENT FOR PUBLIC CONSULTATION

1. Governance
2. Risk assessment
3. Incident monitoring and reporting
4. Risk control and mitigation
5. Traceability
6. Initial customer identification and information
7. Strong customer authentication
8. Enrolment for and provision of authentication tools
9. Log-in attempts, session time out, validity of authentication
10. Monitoring
11. Protection of sensitive payment data
12. Education and communication
13. Notifications, setting of limits
14. Customer access to information on the status

Contromisure più innovative

Monitoraggio delle transazioni per la Prevenzione delle Frodi:

- multicanale
- orientato all'analisi comportamentale
- controllo end-point e device mobili



Contromisure più innovative

Analisi del codice applicativo

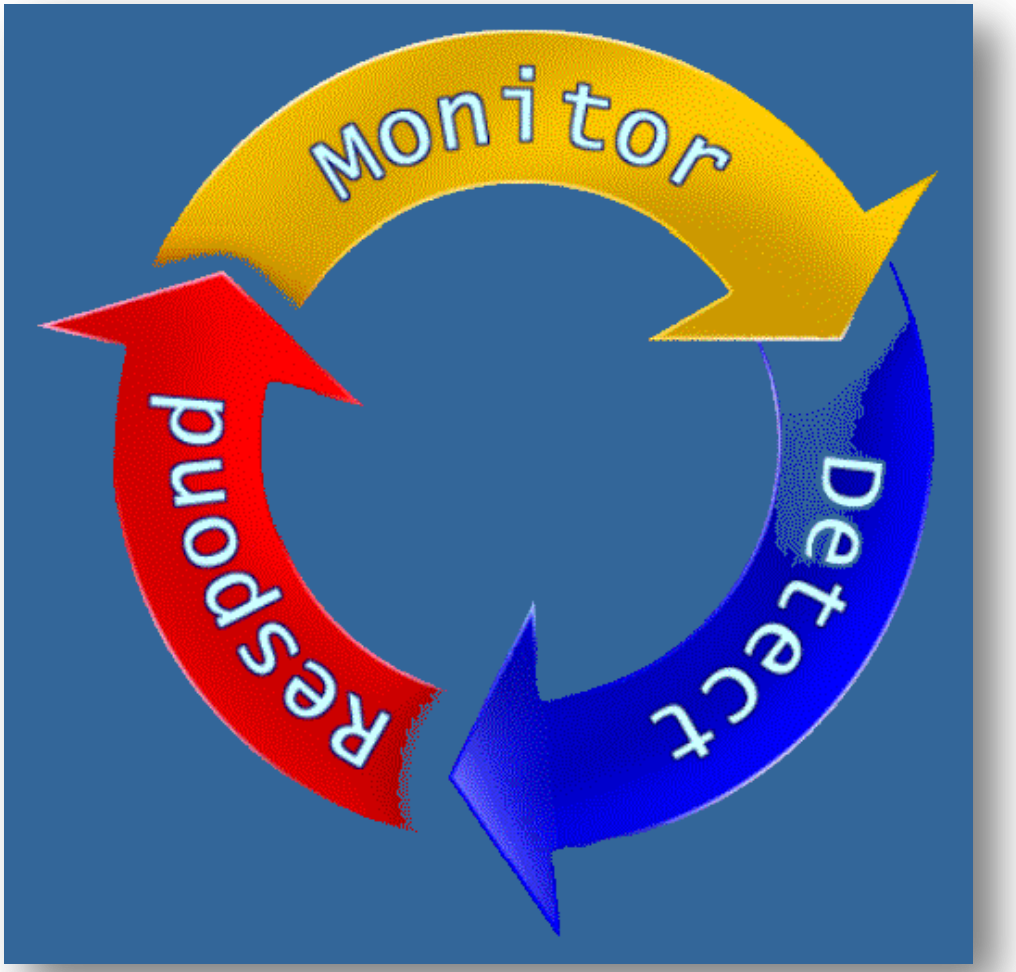
- Soprattutto in ambito mobile
- Sia statico che dinamico
- Come gestisco le informazioni sensibili

Contromisure più innovative

Rendi sicura la tua APP

- Analisi del codice
- Come gestisco le informazioni sensibili
- Utilizzo di plug-in di controllo per la verifica del livello di sicurezza del device

Ridurre il rischio



www.iks.it
informazioni@iks.it
049.870.10.10

appassionati all’eccellenza