BANCA D'ITALIA
EUROSISTEMA

La sicurezza tecnica dei pagamenti elettronici:
Il ruolo delle autorità finanziarie europee

"CARTE 2014"

Sessione A4: Security

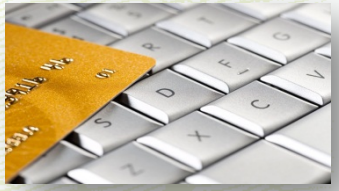
Roma, 19-11- 2014

Salone delle Fontane

Ravenio Parrini

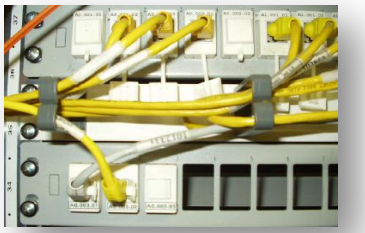
Servizio Supervisione sui mercati
e sul sistema dei pagamenti
- BANCA D'ITALIA -

BANCA D'ITALIA
EUROSISTEMA



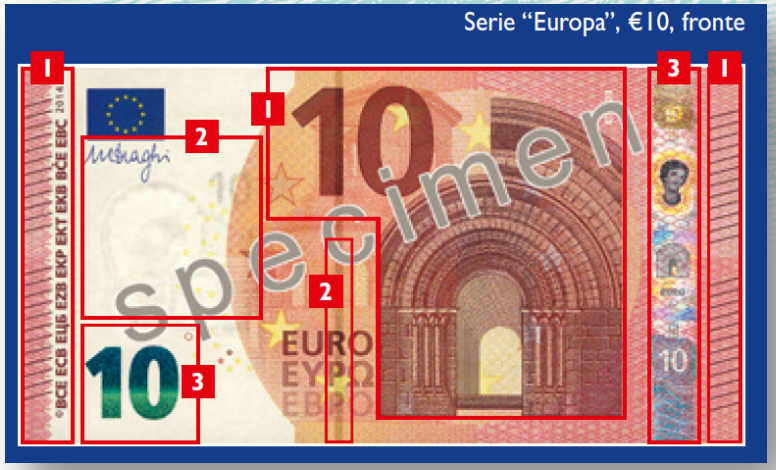
AGENDA

- Introduzione: i pagamenti elettronici
- Sicurezza tecnica: iniziative Autorità Finanziarie
- Profili evolutivi

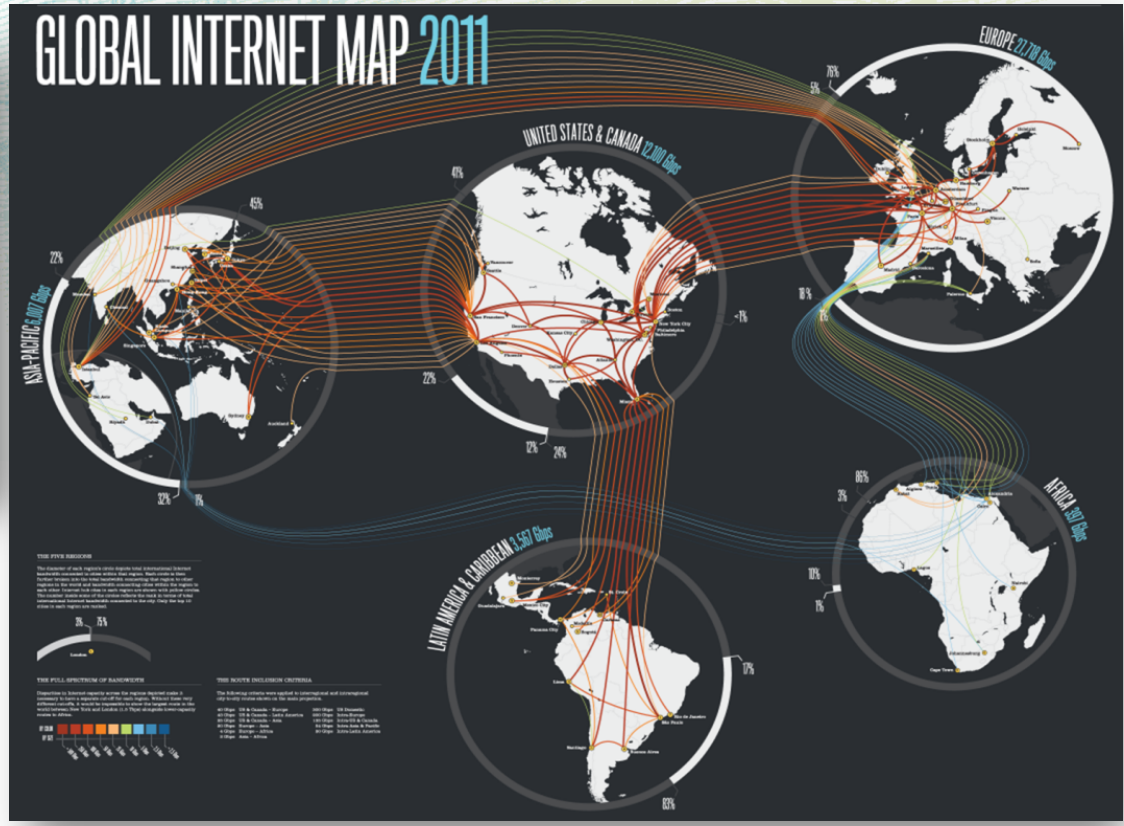


Cash vs. Pagamenti elettronici: caratteristiche

Banconota: elementi caratteristici a bordo dello strumento.



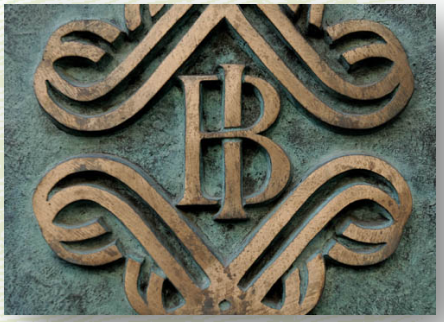
Come rappresentare uno strumento di pagamento elettronico?



Source: Telegeography

…. come una rete digitale!

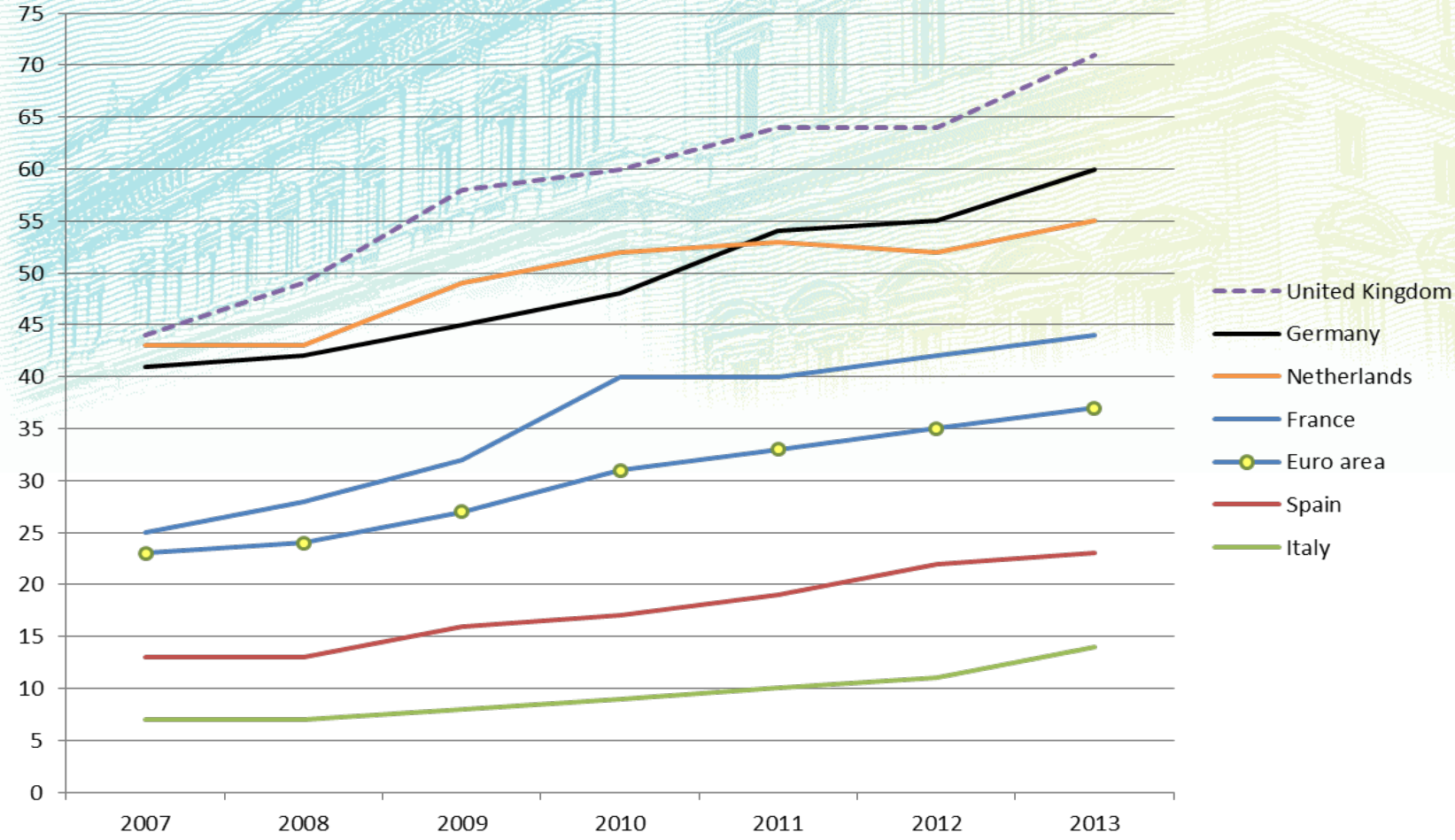
Sicurezza pagamenti elettronici



- **Cosa fa una Banca Centrale per la Sicurezza?**
- In sintesi:
  - Raccoglie dati e elabora statistiche;
  - Valuta evoluzione mercato, tecnologie e legislazione;
  - Definisce normativa di settore
  - Diffonde informazioni e promuove confronto/cooperazione
  - Effettua ispezioni e assessment sugli intermediari

Shopping on-line: Trend crescente

% individui che hanno acquistato on-line di recente



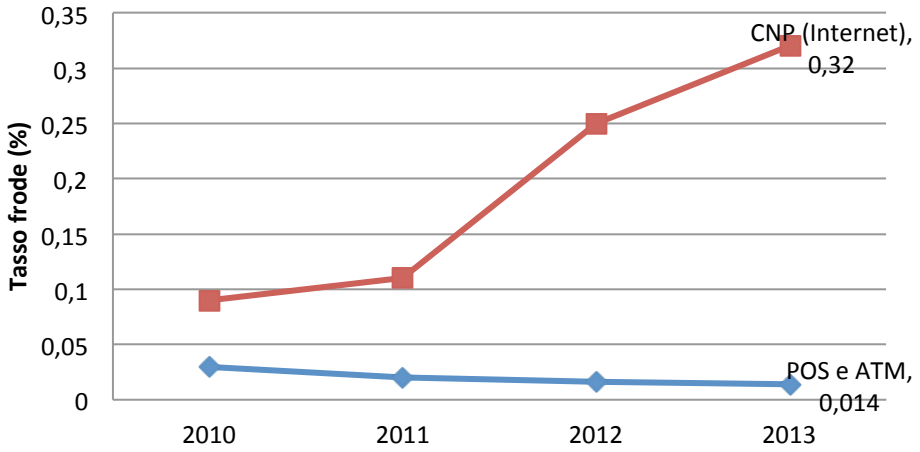
Source: Eurostat; Individuals having ordered/bought goods or services for private use over the Internet in the last three months

Carte di pagamento: i principali *Trends*

- CARTE - trend Frodi in Italia:

Tasso frodi % (* fonte: Banca d'Italia)	2010	2011	2012	2013	Trend
POS e ATM	0,03	0,02	0,016	0,014	↘
Card not present (Internet)	0,09	0,11	0,25	0,32	↗

Frodi settore carte - Italia



Tasso frode complessivo sulle carte:
~ 0,04 %
(gen. stabile nei 4 anni in linea con media UE)

Evoluzione Mercato/Tecnologia

- Innovazione guidata dalle tecnologie Mobile
  - *Vendita degli smartphone ha superato quella dei PC*
  - *Diversamente dalle carte di pagamento uno smartphone trascorre molta d… sua vita connesso !*

- Modello orientato alla facilità di uso
  - *Distribuzione Apps via «Stores»*
  - *(*) 30.000 nuove Apps al mese (scaricate milioni di copie)*

- Sicurezza ottimale ?
  - (*) 10% Smartphone con software di sicurezza (PC = 84 %)
  - (*) 62% Apps scaricate senza «checks» sulla genuinità dello store

* Source: Kaspersky, Canalys, Ponemon

Nuovi modelli di Business

- **E-Commerce** ? Non solo carte di pagamento…

Modelli	*Esempi*	Note:
Payments cards	Verified by VISA, MasterCard SecureCode	
Payments accounts	PayPal	Central platform
Direct debits systems	amazon payments	Central platform (US)
Redirection to bank website	MyBank, giropay, iDEAL	e-banking x e-commerce
Access on-behalf of costumer	sofort banking.de	e-banking x e-commerce
e-wallet/m-wallet	Google wallet	Mobile/ Internet (US)

Mobile payments .... la complessità aumenta !!

Business models:
- MNO centric model
- PSP centric model
- Collaborative model with potential for TSM
- Independent model (P2P)
- 3-party/4-party

Range:
- Local
- Domestic
- Cross-border
- Closed loop
- Open loop

Funding types:
- Card based solutions
- E-purse /Pre-paid accounts
- Bank account based
- Mobile wallet
- Direct carrier billing

Payment instruments:
- Payment Card
- CT, DD
- others

Technology/ Communication channels
- mobile internet
- SMS/USSD/voice response
- QR code
- NFC

Users base
- P2P
- C2B

Location
- POS
- Internet shops

- proximity
- remote

LevelUp

Google wallet

PayPal

DWOLLA

Pingit

DiGi CASH

NFC

ZONG

FeliCa

docomo

IKO

Zapp

PeoPay

Normativa: principali iniziative


EBA EUROPEAN BANKING AUTHORITY

EBA and ECB step up cooperation to make retail payments safer

20 October 2014

SecuRe Pay forum to provide input for the development of EBA regulatory and supervisory requirements, as well as European Central Bank oversight standards for retail payments. EBA meanwhile publishes consultation paper on the security of internet payments, also based on the SecuRe Pay recommendations.

The European Banking Authority (EBA) and European Central Bank (ECB) are stepping up their cooperation to increase the security of retail payments. The two institutions have agreed to use as a basis for their cooperation, the technical work developed in the European Forum for the Security of Retail Payments (SecuRe Pay), a voluntary cooperative initiative between relevant authoriti from the European Economic Area (EEA) that aims at facilitating knowledge and understanding of issues related to the security electronic retail payment services.

Related links:
- EBA consults on implementation of Guidelines on internet payments security
- Consultation EBA/CP/2014/31

Ottobre 2014

Cooperazione EBA- ECB per la sicurezza degli strumenti di pagamento retail, attraverso le iniziative del SecurePay Forum (nuovo Mandato).

Consultazione su implementazione Linee Guida per «Internet Payments».

Rapporti SecurePay Forum

- **Internet Payments**: gennaio 2013, **Assessment Guide**: febbraio 2014
- **Payment Account Access**: maggio 2014
- **Mobile Payments**: consultazione chiusa (31 gen. 2014).

- **PSD2**: Payment Service Directive revision (proposal COM(2013) 547)
- **NIS**: Networks and Information Security Directive (proposal COM(2013) 48)
- **eIDAS**: Regulation on Electronic identification and trust services (Regulation (EU) n. 910/2014 , 23 july 2014)
- **DPR**: new Data Protection Regulation (proposal COM(2012)0011)

SecurePay: le date rilevanti

- Internet Payments:
  - **31 Gennaio 2013**: pubblicazione raccomandazioni SecurePay per Internet Payments

    → **1 Febbraio 2015**: *applicazione volontaria* raccomandazioni da parte delle Autorità Nazionali partecipanti al Forum (BCN)

  - **Agosto 2014**: EBA decide di elevare raccomandazioni SecurePay a «*EBA Guidelines*»:

    → **20 Ottobre 2014**: EBA e ECB presiedono congiuntamente il SecurePay F.

    1 Agosto 2015: *applicazione armonizzata*: tutte le Autorità Competenti dei paesi UE devono garantire la applicazione delle Recc. SecurePay

    ** consultazione EBA su implementazione chiusa il 14.11.2014*

- Mobile Payments
  - **31 Gennaio 2014**: chiusa consultazione

    → **2015 –** *probabile rilascio all'EBA* delle raccomandazioni (*post PSD2*) per la loro inclusione nella normativa di Vigilanza Europea.

Le normative Europee di interesse

- PSD2: *(review of Payment Service Directive):*
  - **Negoziato ancora in corso**;
  - Focus specifico su Sicurezza Tecnica;
  - Autenticazione forte utente, ruolo EBA.
- eiDAS *(Regulation on e-Identity e Trusted Services):*
  - **Pubblicata il 23-07-2014**
  - Introduce il **mutuo riconoscimento (2018)** cross-border per e-ID e Trusted Services (Id. digitale, firma elettronica, sigillo elettronico, time-stamping, certificati elettronici, autenticazione siti Web).
- NIS *(Cybersecurity Directive):* **approvazione in corso**.
  - *Requirements* per operatori critici settore finanziario
  - Notifiche in caso di incidenti di sicurezza➔ «raccordo» con PSD2 e DPR
- DPR *(Data Protection Regulation):* **approvazione in corso .**
  - Limiti alla *profilatura* degli utenti ➔ impatti su sistemi «comportamentali» antifrode delle banche;

Cooperazione e Informazione

- Workshop e incontri con gli operatori

- Partecipazione ai Lavori presso EBA, ECB, Commissione Europea (PSD2 e IF) e altri Gruppi internazionali (es: ERPB*, CPMI**)

- Educazione finanziaria (diritti e obblighi) – guide informative, sito web – Migliore comprensione degli strumenti di pagamento per consapevolezza rischi e comportamenti «sicuri».

(*)Euro Retail Payments Board (ERPB)
(**) Committee on Payments and Market Infrastructures

Attività di valutazione

- SecurePay per **Internet Payments:**
  - Intermediari (PSP): recepite nelle Guide Ispettive di Vigilanza di Banca d'Italia (circ 263 - 2013);
  - Schemi e Circuiti: recepite nell'*Oversight Framework* della ECB per gli strumenti retail (*Carte, SCT, SDD, e-money*)

- **febbraio 2015:** valutazione rischio IT per intermediari e schemi includerà le Raccomandazioni SecurePay.

I trend evolutivi….

- Novità normative
  - Rafforzamento/armonizzazione sicurezza
  - Nuovi attori: *competizione crescente*

- Diffusione **piattaforma *Mobile***

  Questioni aperte:
  - Sicurezza del *Device* (nuovi modelli *anti-maleware*?)
  - Identificazione dell'utente (password insufficiente)
  - Convivenza APP con diversi livelli di sicurezza (es: Social network e Meteo, insieme a Banking e Firma digitale).

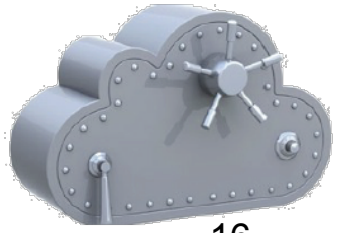
- Proposta di nuovi modelli di servizio

  (es. Faster Payment,..)

… e le sfide da raccogliere.

- ***Come coniugare «sicurezza» con «usabilità» e «privacy» ?***

- Le iniziative dei vari *stakeholders*:
  - Nuovi standard per rendere la piattaforma mobile sicura e interoperabile (es: TEE, HCE, FIDO, EMV Tokens, etc..);
  - Iniziative in tema di identità digitale e *authentication assurance* (es: ISO 29115, progetto STORK, etc..).
  - Iniziative e standard per rendere gli ambienti Cloud sicuri (gli ambienti Mobile in genere si appoggiano al Cloud per le componenti centrali) (es: iniziative ETSI e ENISA in tema di standard e certificazione).



BANCA D'ITALIA
EUROSISTEMA

Any questions?

RAVENIO PARRINI

ravenio.parrini@bancaditalia.it
Tel: +39 06 4792 5032