



BANCA D'ITALIA  
EUROSISTEMA

# La sicurezza tecnica dei pagamenti innovativi: Le raccomandazioni delle autorità finanziarie europee



**“CARTE 2013”**

***Sessione B2: Metodologie e Sistemi di  
Sicurezza evoluti per nuove soluzioni di  
pagamento***

Milano, 5-12- 2013

MiCo - Milano Congressi

---

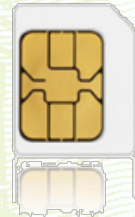
**Ravenio Parrini**

*Servizio Supervisione sui mercati  
e sul sistema dei pagamenti*

- BANCA D'ITALIA -



# AGENDA



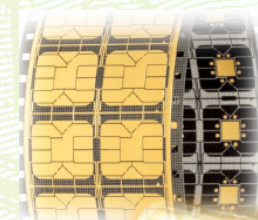
- **Lo scenario evolutivo**
- **I lavori del SecurePay Forum**
- **La revisione della Direttiva PSD (PSD2)**





# Strumenti di pagamento: il contesto

- Aspetti evolutivi:
  - **TECNOLOGIA**: convergenza piattaforme Internet, Telefonia cellulare, TV digitale.
  - **NORMATIVA** (PSD, D. “Salvitalia”, ..):
    - apertura verso soggetti “non bancari”;
    - Competizione, riduzione dei costi, interoperabilità, pagamenti elettronici, war-on-cash.
  - **MERCATO**: nuovi operatori =>
    - Telco operator
    - OTT (Google, Apple, Facebook, Paypal..)
    - Grande distribuzione (GDO).



➔ *Osservati progetti molto innovativi*

# IT security: un nuovo Framework ?



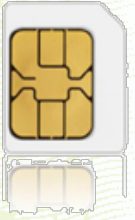
- **PSD2:** Payment Service Directive revision (proposal COM(2013) 547)
- **NIS:** Networks and Information Security Directive (proposal COM(2013) 48)
- **eIDAS:** Regulation on Electronic identification and trust services for electronic trans. in the internal market (proposal COM(2012) 238/2)
- **DPR:** new Data Protection Regulation (proposal COM(2012)0011)





# AGENDA

- Lo scenario evolutivo
- I lavori del SecurePay Forum
- La revisione della Direttiva PSD (PSD2)



# SecuRe Pay Forum: i membri

Members		Members	
BE	Nationale Bank van België/Banque Nationale de Belgique	MT	Central Bank of Malta
BG	Българска народна банка (Bulgarian National Bank)	NL	De Nederlandsche Bank
CZ	Česká národní banka	AT	Oesterreichische Nationalbank Österreichische Finanzmarktaufsicht
DK	Danmarks Nationalbank Finanstilsynet	PL	Narodowy Bank Polski Komisja Nadzoru Finansowego
DE	Deutsche Bundesbank Bundesanstalt für Finanzdienstleistungen	PT	Banco de Portugal
EE	Eesti Pank Finantsinspeksioon	RO	Banca Națională a României
IE	Central Bank of Ireland	SI	Banka Slovenije
GR	Bank of Greece	SK	Národná banka Slovenska
ES	Banco de España	FI	Suomen Pankki – Finlands Bank Finanssivalvonta
FR	Banque de France Autorité de Contrôle Prudentiel	SE	Sveriges Riksbank Finansinspektionen
<b>IT</b>	<b>Banca d'Italia</b>	UK	Financial Services Authority
CY	Central Bank of Cyprus		European Banking Authority European Central Bank
LV	Latvijas Banka Finanšu un kapitāla tirgus komisija		
LT	Lietuvos bankas		
LU	Banque centrale du Luxembourg Commission de Surveillance du Secteur Financier		
HU	Magyar Nemzeti Bank Pénzügyi Szervezetek Állami Felügyelete		



Observers	
IS	Central Bank of Iceland Fjármálaeftirlitið
LI	Liechtensteinische Landesbank 1861 Finanzmarktaufsicht Liechtenstein
NO	Norges Bank Finanstilsynet – The Financial Supervisory Authority of Norway
	European Commission Europol



# SecuRe Pay Forum: le attività



## Attività in corso

- **Internet Payments:** pubblicato 31 gen. 2013
- **Payment Account Access :** consultazione chiusa (aprile 2013)
- **Mobile Payments:** consultazione pub. [20 nov. 2013 – 31 gen. 2014 ]
- **Information sharing x IT security incidents:** in corso
- **Analisi spot :** domini Internet, incidenti sicurezza, segnalazioni Europol, etc.



# SecuRe Pay Forum: i principi

## 1. Security Policies

- documentation, roles/responsibilities, risk assessment );

## 2. Strong Customer Authentication

- two-factors-authentication;
- one dynamic factor (not *reusable*);

## 3. Real-time transaction monitoring

- transactions screening/evaluations;
- suspicious transaction *detection/blocking*

## 4. Data Protection

## 5. Customer awareness, support, and information.

Likelihood	Consequences				
	Insignificant (Minor) (Minor problem easily handled by normal day-to-day processes)	Minor (Minor) (Minor disruption possible, e.g. damage equal to \$500k)	Moderate (Moderate) (Significant time/resources required, e.g. damage equal to \$1 million)	Major (Major) (Operations severely damaged, e.g. damage equal to \$10 million)	Catastrophic (Catastrophic) (Business survival is at risk, damage equal to \$25 million)
Almost certain (e.g. >95% chance)	High	High	Extreme	Extreme	Extreme
Likely (e.g. between 50% and 90% chance)	Moderate	High	High	Extreme	Extreme
Moderate (e.g. between 10% and 50% chance)	Low	Moderate	High	Extreme	Extreme
Unlikely (e.g. between 3% and 10% chance)	Low	Low	Moderate	High	Extreme
Rare (e.g. <1% chance)	Low	Low	Moderate	High	High





# M-Payments: il draft del SecurePay F.

## □ Scope

- Proximity contactless (NFC, QR-Code,..);
- Remote Payments (App, )
- MNO channels (SMS, USSD,..)



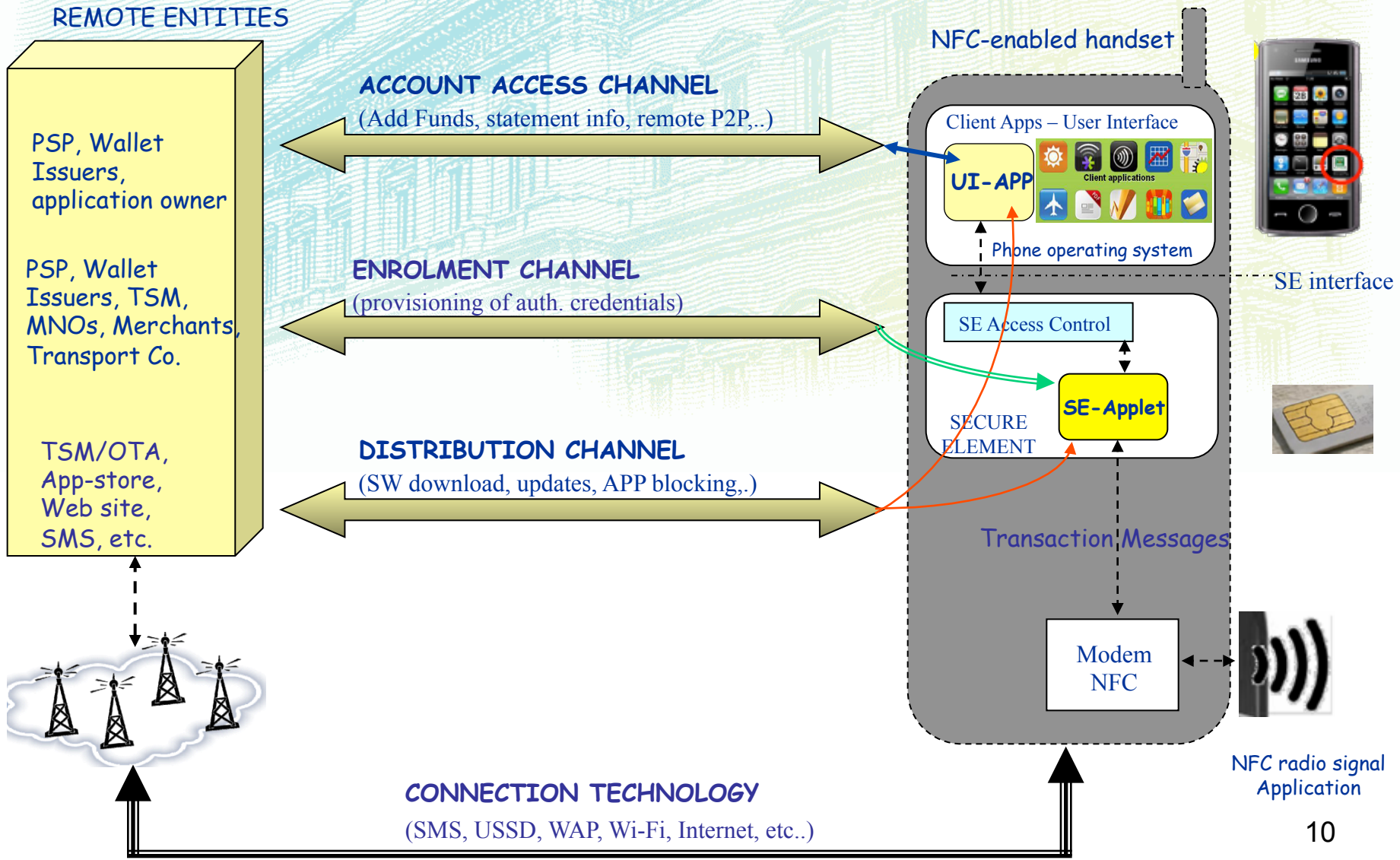
## □ 14 Raccomandazioni, suddivise in KC

## □ Peculiarità del mondo *Mobile*:

- Device «personale» dell'utente;
- Uso tecnologia wireless;
- Ecosistema complesso (Issuer, Telco, Hw vendors, TSM, etc..);



# ...Architettura M-Payments





# Secure Pay Forum: i documenti

Home · Site Directory · Glossary · Links · Contact · Disclaimer & Copyright · Search

Languages: English

The European Central Bank | Press | Events | Publications | Statistics | The Euro | Monetary Policy | Banking Supervision | Payments & Markets

Home > Press > Press releases > By date > 2013 > 31 January 2013

### PRESS RELEASE

**31 January 2013 - ECB releases final Recommendations for the security of internet payments and starts public consultation on payment account access services**

The European Central Bank (ECB) today released a comprehensive set of "Recommendations for the security of internet payments", following a two-month public consultation carried out in 2012. The Recommendations represent the first achievement of the European Forum on the Security of Retail Payments (SecuRe Pay), a voluntary cooperative initiative between relevant authorities from the European Economic Area (EEA) – supervisors of payment service providers and overseers in particular – formed with the objective of facilitating common knowledge and understanding of issues related to the security of electronic retail payment services and instruments and, where

**Recommendations**

- Recommendations for the security of internet payments. Final version after public consultation
- Recommendations for the security of internet payments: outcome of the public consultation
- Recommendations for "payment account access" services. Draft document for public consultation

**Invitation to comment**

→ Recommendations for "payment account access"

→ Internet Payments: *Rilasciate*

→ Accesso ai conti: *Consult. chiusa*

[http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131\\_1.en.html](http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html)

→ Mobile Payments  
(proximity, remote, SMS, .)  
Consultazione avviata  
novembre 2013

Home · Site Directory · Glossary · Links · Contact · Disclaimer & Copyright · Search

Languages: English

The European Central Bank | Press | Events | Publications | Statistics | The Euro | Monetary Policy | Banking Supervision | Payments & Markets

Home > Press > Press releases > By date > 2013 > 20 November 2013

### PRESS RELEASE

**20 November 2013 - ECB launches public consultation on Recommendations for the security of mobile payments**

On 15 November 2013 the Governing Council of the European Central Bank (ECB) decided to launch a public consultation on the "Recommendations for the security of mobile payments", in the context of the work undertaken by the European Forum on the Security of Retail Payments.

The Forum was established in 2011 as a voluntary cooperative initiative between relevant authorities from the European Economic Area – supervisors of payment

**Payments & Markets**

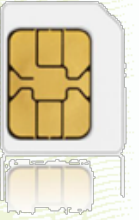
- Public consultations
- Consultation documents**
- Draft recommendations
- Template for comments

<http://www.ecb.europa.eu/press/pr/date/2013/html/pr131120.en.html>



# AGENDA

- Lo scenario evolutivo
- I lavori del SecurePay Forum
- La revisione della Direttiva PSD (PSD2)





# PSD I vs. PSD2

PSD1  
DIRECTIVE  
2007/64/EC



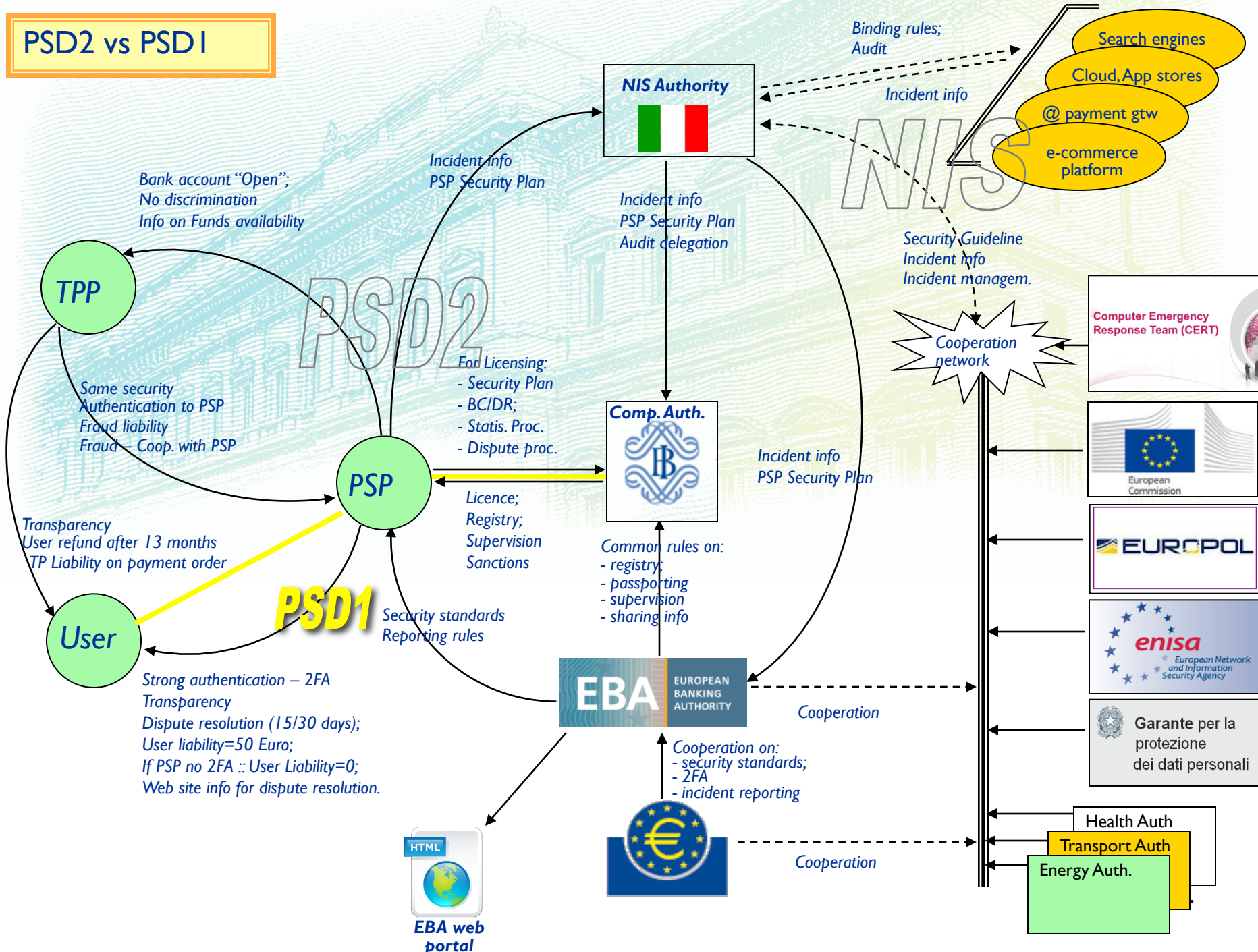
PSD2  
Proposal COM  
(2013) 547

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013PC0547:EN:NOT>

- Qualche numero...
  - 27 articoli aggiornati
  - 8 nuovi articoli
  - ~ 1/3 degli articoli impattati
- Nuovi Attori: TPP\*, EBA, NIS-Authority
- Focus delle novità:
  - Misure di sicurezza tecnica;
  - TPP (aspetti tecnici)
  - Ruolo EBA (aspetti tecnici)

*\*) "TPPs" (third party providers):  
Services based on access to payment  
accounts provided by a payment  
service provider who is not the  
account servicing payment service  
provider.*

# PSD2 vs PSD1





# Impatti sui vari attori

- Autenticazione 2FA

- *Coerenza con SecurePay Forum;*
- *Rapporto PSP - TPP e Autenticazione 2FA*



- Adeguamenti PSP

- *Sottoposti anche a Direttiva Cybersecurity (NIS Directive - COM(2013) 48 final);*
- *Report annuali su sicurezza e su incidenti*



- Autorità finanziarie

- *Definizione misure sicurezza;*
- *Ricezione notifiche incidenti;*
- *Ricezione/Analisi dei piani di sicurezza.*



BANCA D'ITALIA  
EUROSISTEMA





BANCA D'ITALIA  
EUROSISTEMA

*Any questions?*

**RAVENIO PARRINI**

[ravenio.parrini@bancaditalia.it](mailto:ravenio.parrini@bancaditalia.it)

Tel: +39 06 4792 5032

