EVOLUZIONI DELLE NORME SULLA SICUREZZA DEI PAGAMENTI ELETTRONICI

PCI-3DS e PIN, PSD2 e Bancomat

Fabio GUASCONI, Luciano QUARTARONE
@ BL4CKSWAN S.r.l.

Agenda

- Trend di mercato sui pagamenti elettronici
- Enti regolatori e schemi relativi
- Punti di contatto tra gli schemi
- Cosa ci riserverà il futuro
- Conclusioni

Introduzione

Negli ultimi mesi la tensione legata all'approssimarsi dell'entrata in vigore del GDPR è cresciuta progressivamente.
Gli aspetti di conformità al nuovo Regolamento non sono i soli a preoccupare organizzazioni di ogni tipo e dimensione: spesso **si verificano sovrapposizioni fra diverse attività di compliance** con differenti requisiti, a volte apparentemente molto distanti fra di loro.
Le organizzazioni spesso si chiedono se é possibile trovare un vantaggio operativo in queste attività, trasformando il rischio negativo di non riuscire ad essere conformi alle diverse normative, quando esaminate singolarmente, in **opportunità legate a spunti di miglioramento ed efficientamento complessivo**.

Trend di mercato sui pagamenti elettronici

Carte di pagamento

L'ultimo rapporto dell'**Osservatorio sulle Carte di Credito**, presentato a settembre 2017, ha evidenziato più pagamenti *cashless*, più transazioni con carte di debito che tolgono spazio alle carte di credito le quali registrano una lieve diminuzione.

Pagamenti elettronici in Italia	**+8,7%**
Transazioni effettuate con carte di credito	**+9,8%**
Carte di credito in circolazione	**-2,2%**
Carte di debito in circolazione	**+6,6%**
Carte prepagate in circolazione	**+3,7%**
Carte revolving in circolazione	**+2,2%**

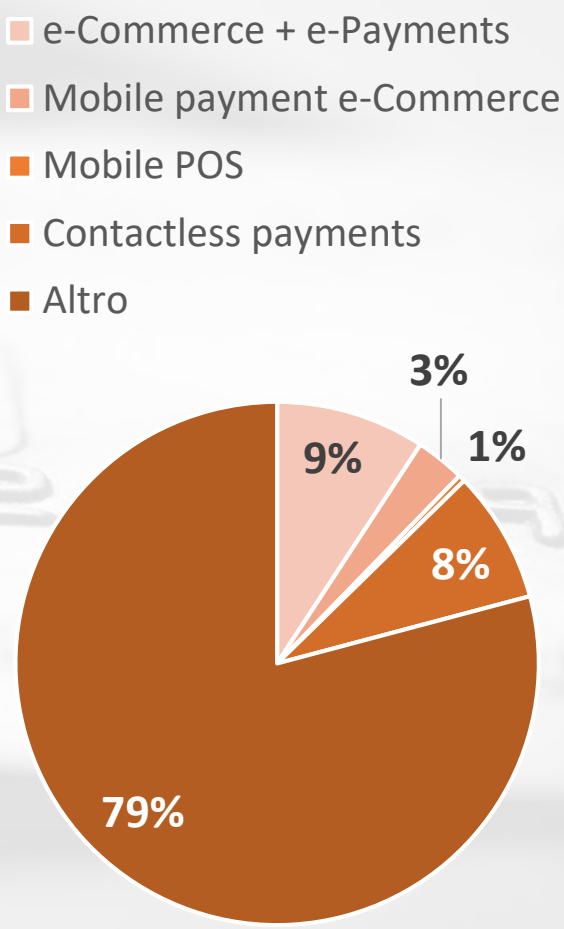
Trend di mercato sui pagamenti elettronici

Canali di pagamento innovativi

Trend 2017

e-Commerce ed e-Payments (9%)	+10%
Mobile payment e-Commerce (3%)	+60%
Mobile POS (1%)	+9%
Contactless payments (8%)	+150%

Tipologie di pagamenti elettronici 2017



Enti regolatori e schemi relativi

Autorità europea indipendente fondata nel 2011 che fornisce linee guida, standard tecnici, opinioni e report nell'ottica di uniformare il settore bancario tra i Paesi membri.

Il Payment Card Industry Security Standard Council è un organismo internazionale fondato nel 2006 da VISA, MasterCard, American Express, Discover e JCB cui è delegata l'emanazione e la gestione di schemi di sicurezza trasversali, in ambito pagamenti elettronici.

Società erede del CO.GE.BAN. che gestisce i circuiti di pagamento nazionali BANCOMAT® e PagoBANCOMAT®.

Enti regolatori e schemi relativi

Autorità europea indipendente fondata nel 2011 che fornisce linee guida, standard tecnici, opinioni e report nell'ottica di uniformare il settore bancario tra i Paesi membri.

- **Guidelines on Internet Payments**
- **Guidelines on ICT Risk Assessment**
- **Guidelines on incident reporting under PSD2**
- **Guidelines for security risks under PSD2**

Enti regolatori e schemi relativi

Il Payment Card Industry Security Standard Council è un organismo internazionale fondato nel 2006 da VISA, MasterCard, American Express, Discover e JCB cui è delegata l'emanazione e la gestione di schemi di sicurezza trasversali, in ambito pagamenti elettronici.

- **PCI DSS: Data Security Standard** (Merchants e Service Providers)
- **PCI PA-DSS: Payment Application – Data Security Standard** (Software)
- **PCI PTS: PIN Transaction Security** (Hardware)
- **PCI Card Production** (Produzione Carte e stampa PIN)
- **PCI PIN** (PIN nelle transazioni)
- **PCI 3DS** (3D-Secure)

Enti regolatori e schemi relativi

Società erede del CO.GE.BAN. che gestisce i circuiti di pagamento nazionali BANCOMAT® e PagoBANCOMAT®.

- **SPE-DEF** xxx
- **Security Verification Standard**

EBA Guidelines on incident reporting under PSD2

Generalità

Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)

Ambito d'applicazione

Incidenti operativi o di sicurezza dei PSP

Versione attuale

27/07/2017

Verifica

Vigilanza di Banca d'Italia

Certificabile

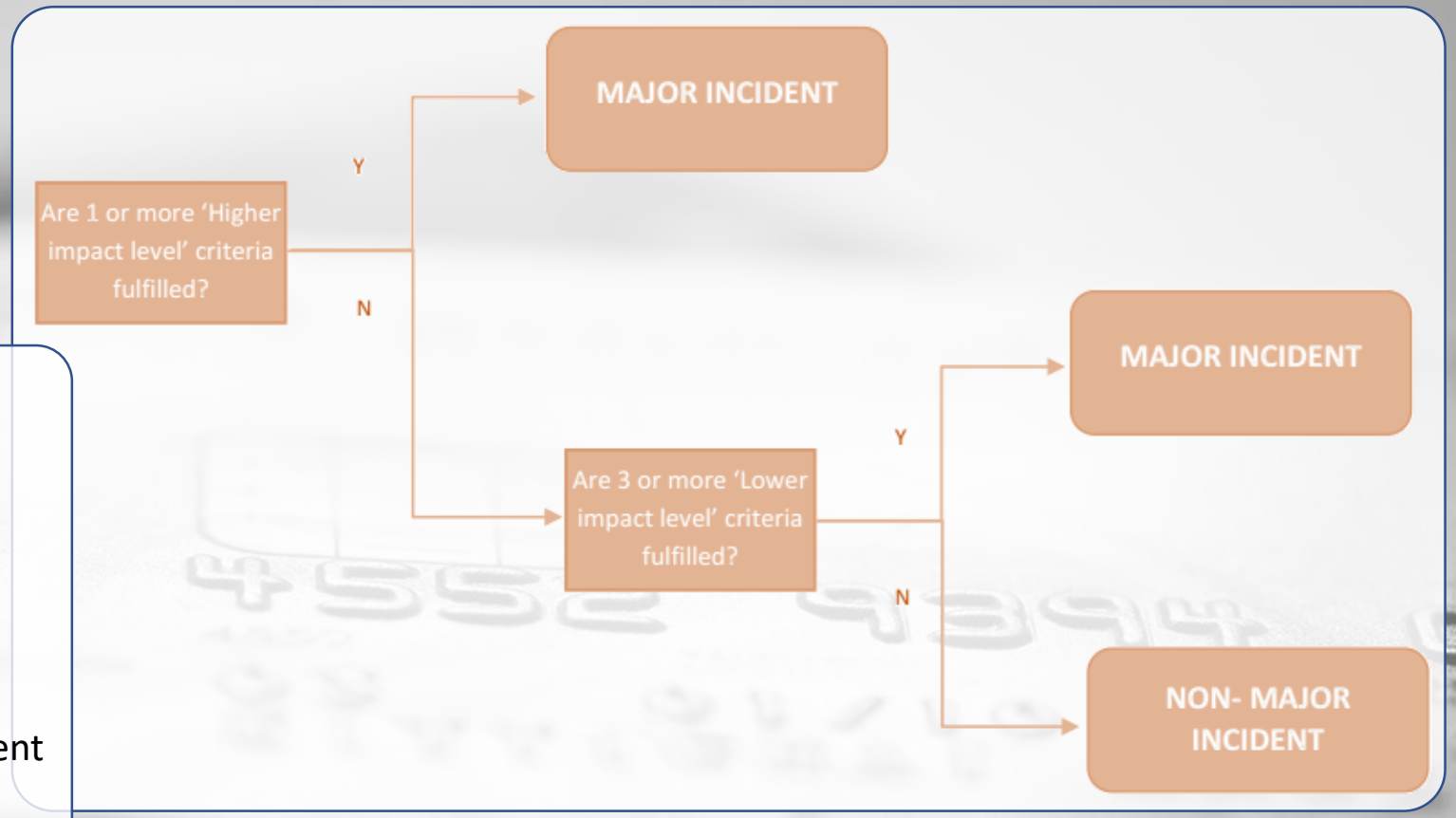
No

Note

Lo schema adempie al mandato di cui all'art.96 della Direttiva

EBA Guidelines on incident reporting under PSD2

Requisiti



Per i PSP

Guideline 1: Classification as major incident
Guideline 2: Notification process
Guideline 3: Delegated and consolidated reporting
Guideline 4: Operational and security policy

Per le authority vs altre authority locali

Guideline 5: Assessment of the relevance of the incident
Guideline 6: Information to be shared

Per le authority vs EBA

Guideline 7: Information to be shared
Guideline 8: Communication

EBA Guidelines on security measures for PSD2

Generalità

Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)

Ambito d'applicazione

Sicurezza dei servizi offerti dai PSP

Versione attuale

12/12/2017

Verifica

Vigilanza di Banca d'Italia

Certificabile

No

Note

Lo schema adempie al mandato di cui all'art.95 della Direttiva

EBA Guidelines on security measures for PSD2

Requisiti

1. COMPLIANCE AND REPORTING OBLIGATIONS

1.1 Status of these guidelines

1.1 Reporting requirements

2. GOVERNANCE

2.1 Operational and security risk management framework

2.2 Risk management and control models

2.3 Outsourcing

3. RISK ASSESSMENT

3.1 Identification of functions, processes and assets

3.2 Classification of functions, processes and assets

3.3 Risk assessments of functions, processes and assets

4. PROTECTION

4.1 Data and systems integrity and confidentiality

4.2 Physical security

4.3 Access control

5. DETECTION

5.1 Continuous monitoring and detection

5.2 Monitoring and reporting of operational or security incidents

6. BUSINESS CONTINUITY

6.1 Scenario-based business continuity planning

6.2 Testing of business continuity plans

6.3 Crisis communication

7. TESTING OF SECURITY MEASURES

8. SITUATIONAL AWARENESS AND CONTINUOUS LEARNING

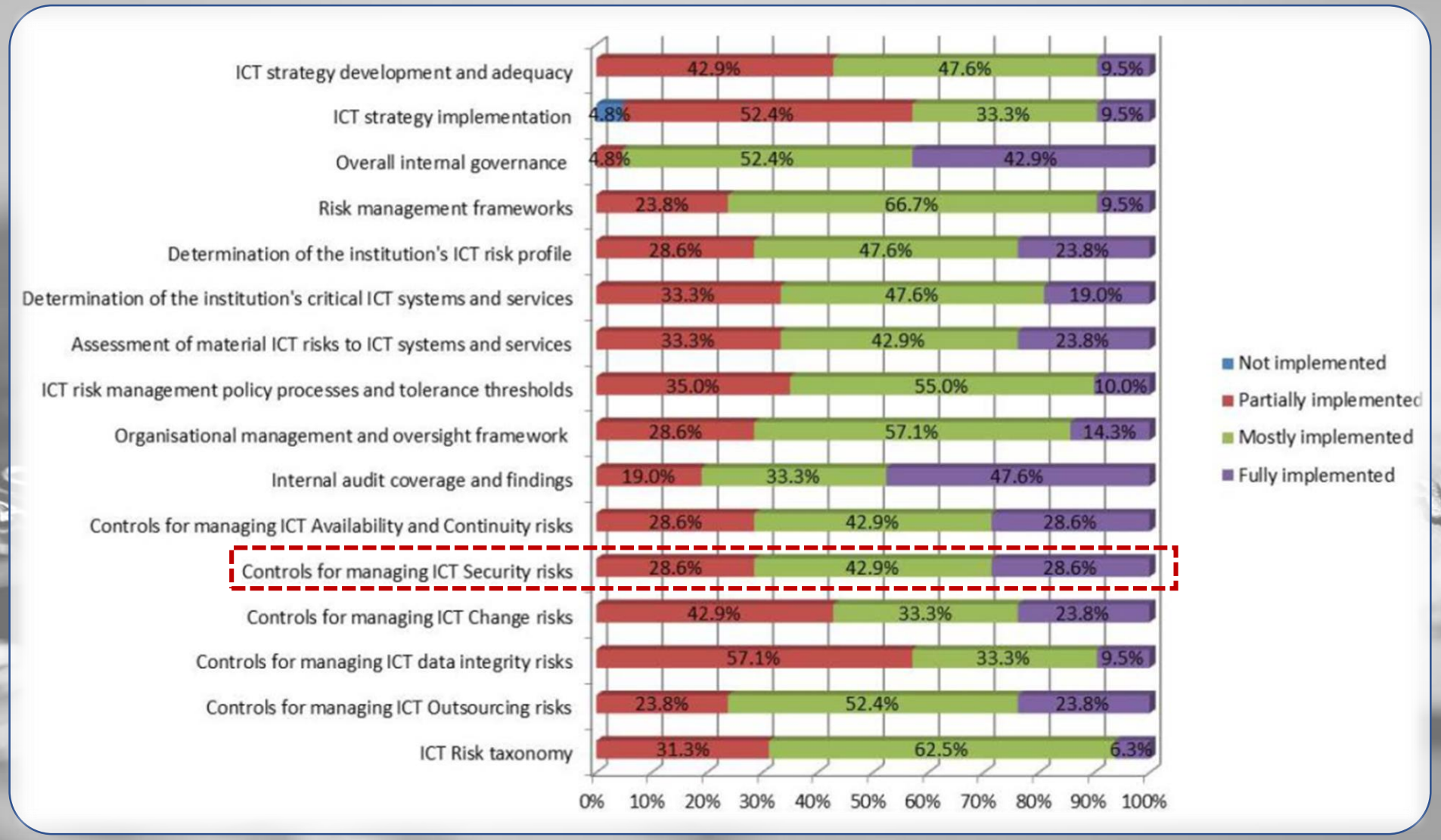
8.1 Threat landscape and situational awareness

8.2 Training and security awareness programmes

9. PAYMENT SERVICE USER RELATIONSHIP MANAGEMENT

9.1 Payment service user awareness on security risks and risk-mitigating actions

Survey EBA 2017



PCI PIN

Generalità

Payment Card Industry (PCI)
PIN Security

Ambito d'applicazione

Tramissioni di PIN/PIN Block durante le transazioni online e offline

Versione attuale

2.0, ad agosto 2017 è circolato un primo draft della versione 3.0.

Verifica

Richiesta dai circuiti tramite assessor qualificati per i loro programmi

Certificabile

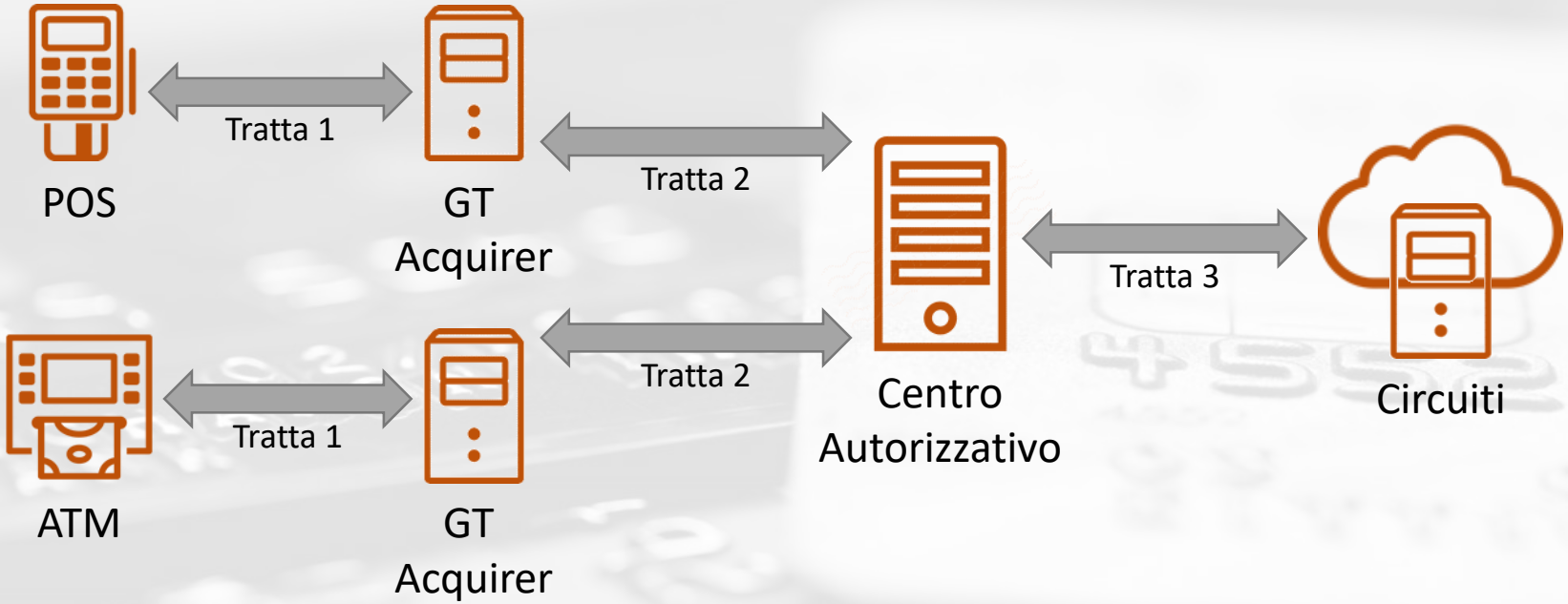
No

Note

Lo schema PCI PIN sostituisce il famoso VISA PIN su cui venivano effettuati i "PIN audit".

PCI PIN

Ambito "tipo" online con tratte di traslazione del PIN Block



Tratte 1 e 2 – comunicazioni regolata dalle specifiche "CB2" con possibili variazioni sul tema (e.g. GT Remoti, Multi-acquiring, Acquirer anche Centri Autorizzativi etc.)

Tratta 3 – comunicazione regolata dai circuiti internazionali

PCI PIN

Requisiti

Lo standard è fortemente **tecnico** ed incentrato sulla gestione delle chiavi crittografiche utilizzate a protezione del PIN/PIN Block.

Control Objective 1	PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.
Control Objective 2	Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.
Control Objective 3	Keys are conveyed or transmitted in a secure manner
Control Objective 4	Key-loading to HSMs and PIN entry devices is handled in a secure manner.
Control Objective 5	Keys are used in a manner that prevents or detects their unauthorized usage.
Control Objective 6	Keys are administered in a secure manner.
Control Objective 7	Equipment used to process PINs and keys is managed in a secure manner.

N.B. Nelle tratte POS/ATM – GT si sovrappone con le specifiche Bancomat che però, nella loro declinazione CB2, ne coprono completamente i requisiti con la sola eccezione del mandato per l'uso obbligatorio dei key blocks che inizierà ad applicarsi progressivamente a partire dal 2019.

PCI 3DS

Generalità

Payment Card Industry 3-D Secure (PCI 3DS)

Ambito d'applicazione

EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server

Versione attuale

1.0 (ottobre 2017)

Verifica

Richiesta dai circuiti tramite assessor qualificati dal Council

Certificabile

Sì

Note

Lo schema PCI 3DS sostituisce lo schema VISA 3DS Security Requirements.

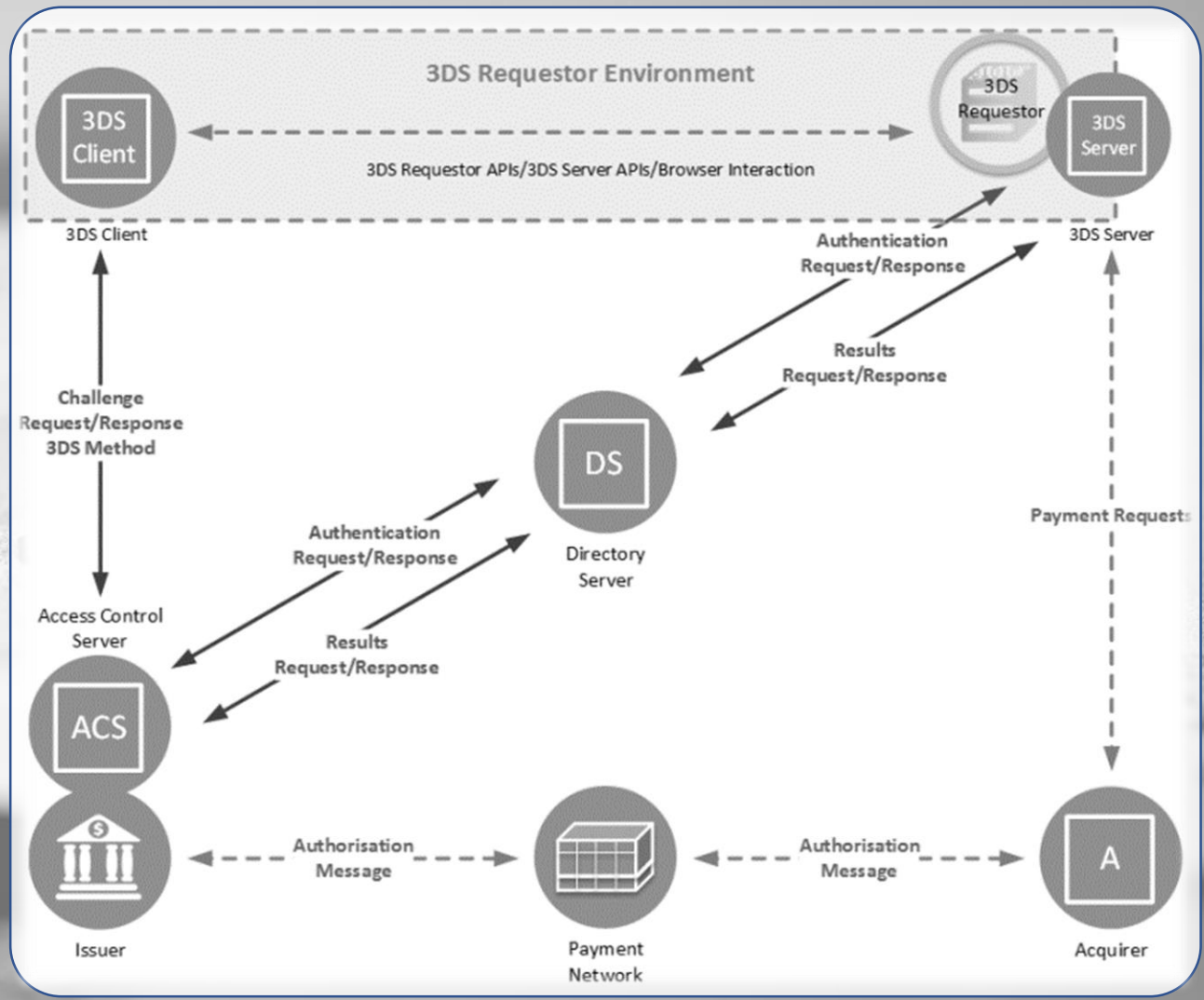
PCI 3DS

Rapporto con EMV

Secondo le **specifiche EMV versione 2.1.0**, le transazioni e-commerce soggette a 3DS devono funzionare secondo quanto riportato nello schema a destra.

Le versioni precedenti delle specifiche hanno elementi di semplificazione.

L'attestazione della conformità alle specifiche EMV (tramite "letter of approval") è un elemento complementare considerato necessario per poter ottenere la certificazione.



PCI 3DS

Requisiti

PCI 3DS Part 1: Baseline Security Requirements	
1. **Maintain security policies for all personnel**	1.1 Maintain security policies 1.2 Evaluate risk 1.3 Educate personnel 1.4 Screen personnel
2. **Secure network connectivity**	2.1 Protect 3DS systems from untrusted systems and networks 2.2 Protect 3DS systems from network threats
3. **Develop and maintain secure systems**	3.1 Secure application development 3.2 Configuration standards 3.3 Change management
4. **Vulnerability management**	4.1 Protect against malicious software 4.2 Address vulnerabilities and security weaknesses
5. **Manage access**	5.1 Access management 5.2 Account management 5.3 Authentication
6. **Physical security**	6.1 Restrict physical access 6.2 Secure media
7. **Incident response preparedness**	7.1 Incident response plan 7.2 Audit logs

Lo standard ha una struttura completa da un punto di vista **organizzativo e tecnico**.

La PCI-3DS utilizza un inedito **approccio a due parti**:

- La **parte 1** (a sinistra) deve applicarsi solo se gli elementi in perimetro non sono già sotto certificato PCI-DSS, ricalcandone gli aspetti principali.
- La **parte 2** (a destra) si applica sempre.

PCI 3DS Part 2: 3DS Security Requirements	
1. **Validate scope**	1.1 Scoping
2. **Security governance**	2.1 Security governance 2.2 Manage risk 2.3 Business as usual (BAU) 2.4 Manage third-party relationships
3. **Protect 3DS systems and applications**	3.1 Protect boundaries 3.2 Protect baseline configurations 3.3 Protect applications and application interfaces 3.4 Secure web configurations 3.5 Maintain availability of 3DS operations
4. **Secure logical access to 3DS systems**	4.1 Secure connections for issuer and merchant customers 4.2 Secure internal network connections 4.3 Secure remote access 4.4 Restrict wireless exposure 4.5 Secure VPNs
5. **Protect 3DS data**	5.1 Data lifecycle 5.2 Data transmission 5.3 TLS configuration 5.4 Data storage 5.5 Monitoring 3DS transactions
6. **Cryptography and key management**	6.1 Key management 6.2 Secure logical access to HSMs 6.3 Secure physical access to HSMs
7. **Physically secure 3DS systems**	7.1 Data center security 7.2 CCTV

Bancomat Security Verification Standard

Generalità

BANCOMAT S.p.A.

BANCOMAT® Security Verification Standard

Ambito d'applicazione

Transazioni BANCOMAT® e PagoBANCOMAT®

Versione attuale

Marzo 2016

Verifica

Self-assessment

Certificabile

No

Note

Nessuna

Bancomat Security Verification Standard

Requisiti

La gestione di POS e ATM è centrale per questo standard, che comprende i seguenti requisiti principali, scomposti in requisiti di ulteriore dettaglio:

1. **Governo dell'organizzazione**
2. **Governo della clientela**
3. **Governo della sicurezza nei rapporti con le terze parti**
4. **Sicurezza delle componenti hardware e software**
5. **Sicurezza ambientale**
6. **Sicurezza logica**
7. **Sicurezza dell'infrastruttura**
8. **Sicurezza nel trattamento dei dati**
9. **Gestione sicura delle chiavi crittografiche**
10. **Monitoraggio degli aspetti di sicurezza**
11. **Installazione, gestione e manutenzione dei prodotti**

Punti di contatto tra gli schemi

Considerazioni generali

Tutti gli schemi esaminati finora si focalizzano su aspetti diversi dello stesso ambito o di ambiti fortemente collegati tra di logo

Indipendentemente dall'Ente emettitore dello schema si possono notare ampie aree di sinergia:

- Centralità della gestione del rischio relativo alla sicurezza
- Messa in sicurezza del dato e delle chiavi con cui è gestito
- Gestione della sicurezza fisica e logica
- Monitoraggio e registrazione degli eventi
- Necessità di procedure per la gestione degli incidenti
- Garanzia della continuità operativa

Non vi sono indicazioni in contrasto l'una con l'altra ma esistono sovrapposizioni o requisiti specificati a un livello di dettaglio diverso a seconda dello schema

Probabilmente il livello di conformità con questi requisiti non è particolarmente elevato se si ravvisa la necessità di chiederne l'enforcement in modo così esteso

Punti di contatto tra gli schemi

Esercizio di mappatura di alto livello

EBA PSD2	PCI 3DS	Bancomat
	P.2.1 VALIDATE THE SCOPE	
1. COMPLIANCE AND REPORTING OBLIGATIONS		
2. GOVERNANCE	**P.2.2 SECURITY GOVERNANCE**	**1. Governo dell'organizzazione**
2.1 Operational and security risk management framework	P2-2.1 Security governance	
2.2 Risk management and control models	P2-2.2 Manage risk	
	P2-2.3 Business as usual (BAU)	**11. Installazione, gestione e manutenzione dei prodotti**
2.3 Outsourcing	P2-2.4 Manage third-party relationships	**3. Governo della sicurezza nei rapporti con le terze parti**
3. RISK ASSESSMENT	PCI-DSS 12.2	
3.1 Identification of functions, processes and assets		
3.2 Classification of functions, processes and assets		
3.3 Risk assessments of functions, processes and assets		
4. PROTECTION		
4.1 Data and systems integrity and confidentiality	**P.2.3 PROTECT 3DS SYSTEMS AND APPLICATIONS**	**8. Sicurezza nel trattamento dei dati**
	P.2.5 PROTECT 3DS DATA	
	P.2.6 CRYPTOGRAPHY AND KEY MANAGEMENT	**9. Gestione sicura delle chiavi crittografiche**
4.2 Physical security	**P.2.7 PHYSICALLY SECURE 3DS SYSTEMS**	**4. Sicurezza delle componenti hardware e software**
	P2-7.1 Data center security	**5. Sicurezza ambientale**
	P2-7.2 CCTV	
4.3 Access control	**P.2.4 SECURE LOGICAL ACCESS TO 3DS SYSTEMS**	**6. Sicurezza logica**
		7. Sicurezza dell'infrastruttura
5. DETECTION		
5.1 Continuous monitoring and detection	PCI-DSS 10.6	**10. Monitoraggio degli aspetti di sicurezza**
5.2 Monitoring and reporting of operational or security incidents	PCI-DSS 12.10	
6. BUSINESS CONTINUITY		
6.1 Scenario-based business continuity planning	P2-3.5 Maintain availability of 3DS operations	
6.2 Testing of business continuity plans		
6.3 Crisis communication		
7. TESTING OF SECURITY MEASURES	PCI-DSS 11	
8. SITUATIONAL AWARENESS AND CONTINUOUS LEARNING		
8.1 Threat landscape and situational awareness	PCI-DSS 6.1 & 12.10	
8.2 Training and security awareness programmes	PCI-DSS 12.6	
9. PAYMENT SERVICE USER RELATIONSHIP MANAGEMENT		**2. Governo della clientela**

Cosa ci riserverà il futuro

2018
Pubblicazione PCI-PIN 3.0

Maggio 2018
Applicazione del GDPR e probabile rinnovo dei provvedimenti nazionali collegati

Ottobre 2018
Aggiornamento PCI DSS

Novembre 2018
Designazione degli operatori di servizi essenziali per recepimento della direttiva NIS

2020
Rivisitazione della ISO/IEC 27002 per farla ritornare ad essere lo schema di controlli di riferimento

Coclusioni

Considerazioni generali

Il precedente esercizio di mappatura dimostra chiaramente che **è possibile mettere a fattor comune in modo proattivo i requisiti derivanti dagli schemi**, diversamente il loro numero sempre crescente renderà man mano più difficoltosa la loro gestione puntuale.

Un **valido processo di gestione del rischio** relativo alla sicurezza delle informazioni (**non basta più il questionario di self assessment di ORM!**) che sia in grado di scendere nel dettaglio delle misure di sicurezza da adottare è un pilastro fondamentale per poter dimostrare e giustificare degli interventi, per quanto la compliance rimarrà comunque un giustificativo valido.

E' necessario affrontare questi temi con il **supporto di specialisti in materia**, plotoni di consulenti generalisti non vi porteranno da nessuna parte e per giunta lo faranno anche in modo poco efficace.

Fabio GUASCONI, Luciano QUARTARONE

fabio.guasconi@bl4ckswan.com

luciano.quartarone@bl4ckswan.com