I nuovi standard per la sicurezza delle carte di pagamento

UNINFO

Relatore

Fabio GUASCONI

- ✓ Direttivo di **UNINFO**
- ✓ Presidente del ISO/IEC JTC1 SC27 UNINFO
- ✓ Direttivo **CLUSIT**
- ✓ CISA, CISM, PCI-QSA, ITIL, ISFS, Lead Auditor 27001 & 9001
- ✓ Partner e co-founder **BL4CKSWAN** S.r.l

UNINFO

Agenda

Key player

- UNINFO e SC27
- PCI-SSC

Standard PCI

- PCI-DSS
- PCI PA-DSS
- PCI PTS
- PCI Card production

UNINFO

UNINFO ed SC27

UNINFO è l'ente di normazione federato all' UNI ENTE ITALIANO DI NORMAZIONE che si occupa delle **tecnologie informatiche**.

Mantiene ufficialmente contatti in questo ambito con ISO, ISO/IEC JTC, CEN ed ETSI.

ISO International Organization for Standardization

IEC International Electrotechnical Commission

Il sottocomitato 27 (SC27), da cui nascono tutte le norme delle famiglie **27000** e **15408**, è da 25+ anni delegato ad occuparsi, nel Joint Technical Committee (JTC1) di ISO/IEC, della **sicurezza delle informazioni**.

Norme sulla sicurezza delle carte in SC27

ISO/IEC 27001 (2013)

Sistemi di gestione per la sicurezza delle informazioni

639 certificati in Italia, **22** nel settore Finance, **0** citazioni specifiche sulle carte

ISO/IEC 27015 (2012)

Information security management guidelines for financial services

0 certificati in Italia (sono guidelines), **21** citazioni specifiche sulle carte

UNINFO

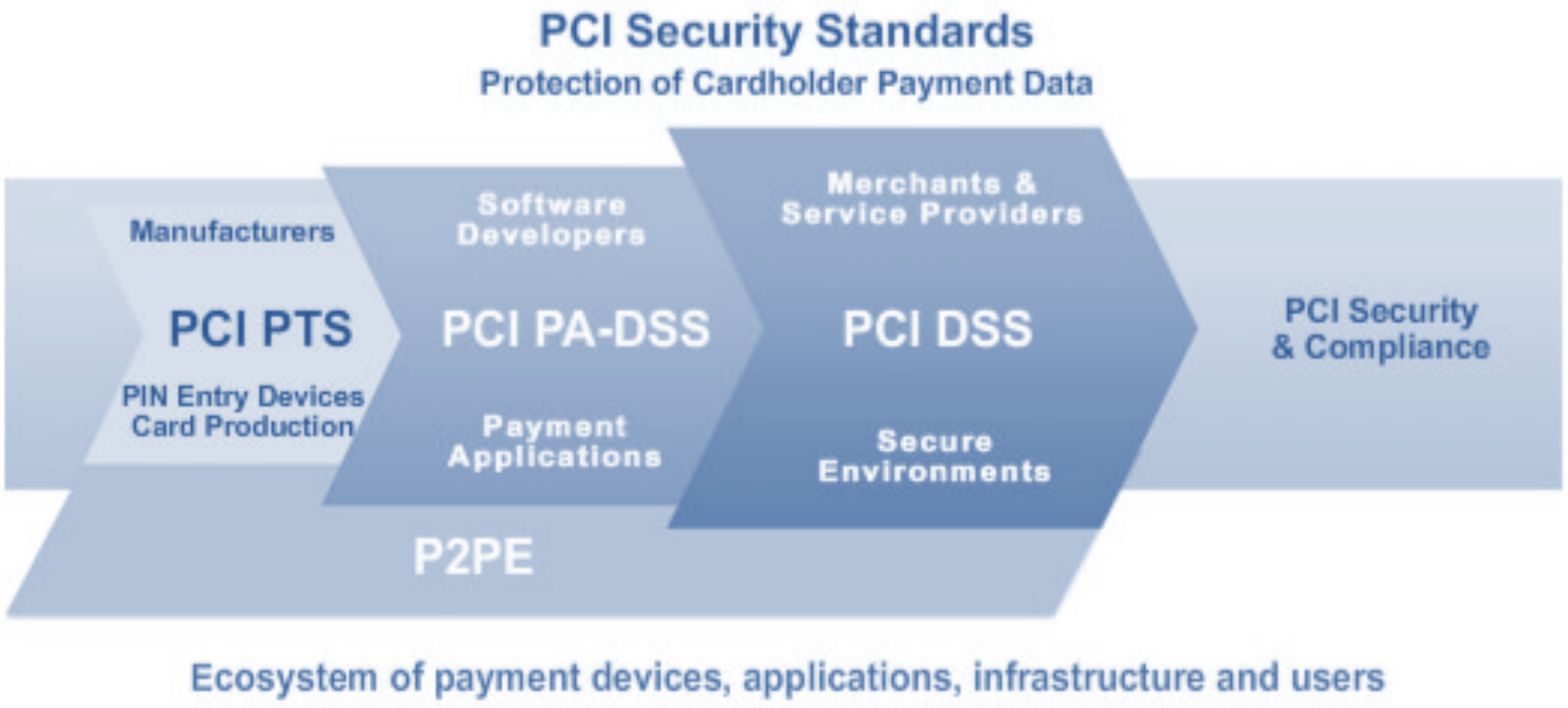
Da chi è formato il PCI-SSC

PCI Security Standards Council™

fondazione nel **2006**

UNINFO

Gli standard del PCI-SSC



Payment Card Industry (PCI)
Data Security Standard

Definisce i requisiti di sicurezza per **Merchant** e **Service Provider** circa

- **acquisizione**
- **elaborazione**
- **trasmissione**
- **memorizzazione**

dei dati relativi ai titolari delle carte di pagamento

- **PAN**

ma anche

- **CAV2/CVC2/CVV2/CID**
- **Tracce magnetiche**
- **PIN e PIN Block**

UNINFO

PCI-DSS v3.0

La versione 3.0 di PCI-DSS è una riedizione della versione precedente riorganizzata e chiarita

- Guidelines inserite nello standard
- Considerazione del "Business as usual"
- ROC reporting in un template separato
- Miglioramento delle procedure di testing

11 nuovi requisiti	**24 requisiti spostati**	**8 requisiti cambiati e chiariti**	**1 requisito dismesso**

PCI-DSS v3.0

Requisito 1 - Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta

Requisito 2 - Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione

Requisito 3 - Proteggere i dati dei titolari di carta memorizzati

Requisito 4 - Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche

Requisito 5 - Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus

Requisito 6 - Sviluppare e gestire sistemi e applicazioni protette

Requisito 7 - Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario

Requisito 8 - Individuare e autenticare l'accesso ai componenti di sistema

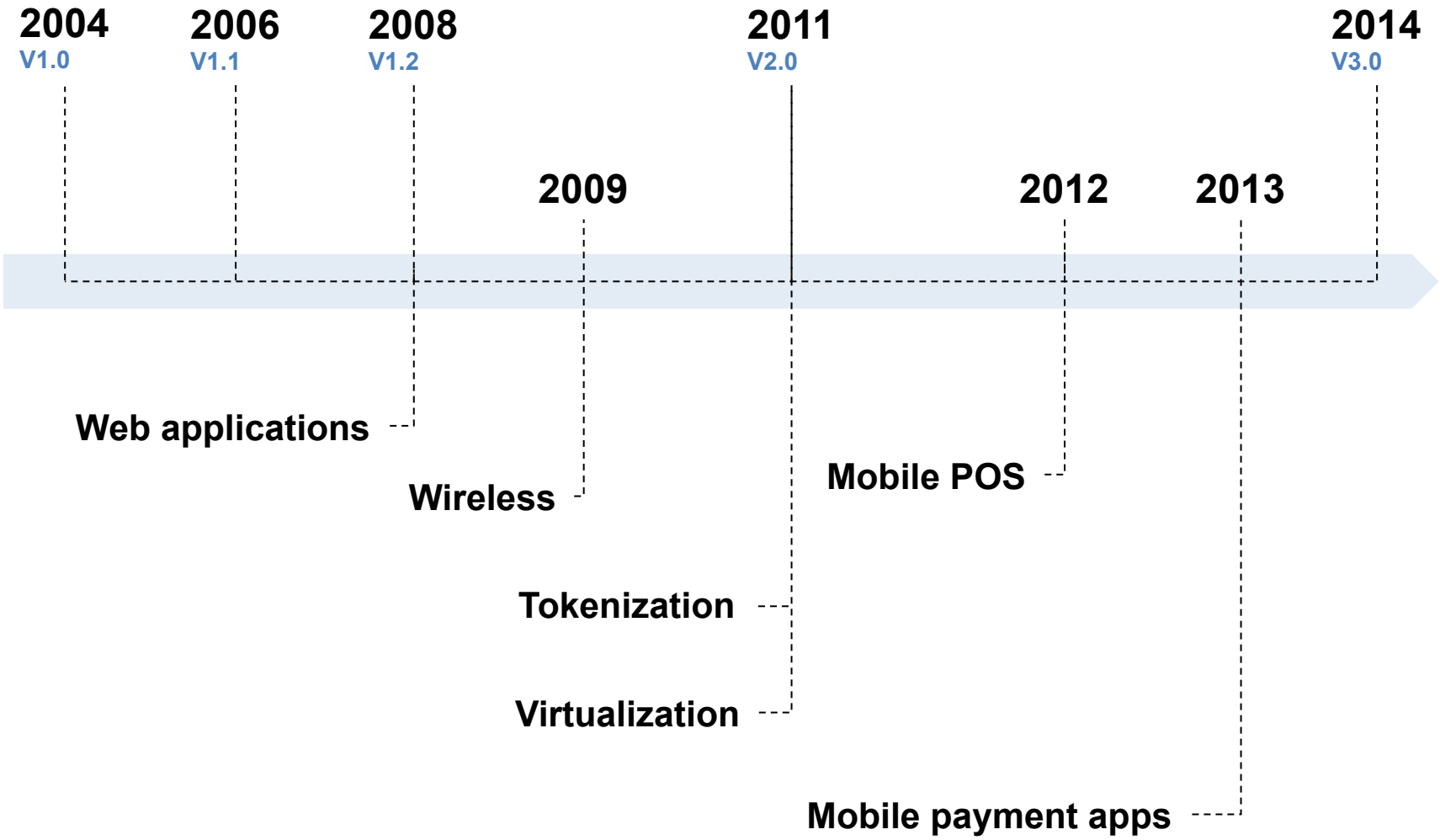
Requisito 9 - Limitare l'accesso fisico ai dati dei titolari di carta

Requisito 10 - Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta

Requisito 11 - Eseguire regolarmente test dei sistemi e processi di protezione.

Requisito 12 - Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale.

Guide di complemento a PCI-DSS



UNINFO

Payment Card Industry (PCI)
Payment Application Data Security Standard

Definisce i requisiti di sicurezza per gli **Sviluppatori di software** per le applicazioni che:

- sono coinvolte nell'**autorizzazione** o nel **settlement** di un pagamento
- sono vendute **"off the shelf"**
- **non sono personalizzate** per un solo soggetto
- **non sono sviluppate in house**
- **non sono fornite come servizio**

N.B. *Applicazioni non certificate PA-DSS richiedono una verifica più approfondita del loro sviluppo in caso di audit on-site richiesto da PCI-DSS*

Payment Card Industry (PCI)
PIN Transaction Security (PTS)

Definisce i requisiti di sicurezza per i **Produttori di hardware** che:

- permette l'**inserimento di PIN** come punto d'interazione presidiato e non
- non permette l'inserimento di PIN ma gestisce la sicurezza di **dati di account**
- viene integrato come **componente di sicurezza** nei terminali POS
- assolve funzionalità avanzate di cifratura (**HSM**)

N.B.1 *Gli ATM sono considerati oggetti particolari e hanno una linea guida dedicata*

N.B.2 *Hw certificato è richiesto per la gestione delle chiavi crittografiche in PCI-DSS*

Payment Card Industry (PCI)
Card Production

Sostituisce i programmi proprietari dei Brand **VISA PIN, MasterCard GVCP** etc.

Definisce i requisiti di sicurezza per i **Produttori, personalizzatori e fornitori di carte** relativamente ai processi di:

- Card manufacturing, personalization and storing
- Magnetic-stripe card encoding and embossing
- Chip initializing or pre-personalization, embedding, personalization
- Shipping & Mailing

Physical Security Requirements (maggio 2013)

Logical Security Requirements (maggio 2013)

UNINFO

Situazione del mercato

75.0% delle aziende in Asia è conforme a 80%+ dei requisiti

56.2% delle aziende in Nord America è conforme a 80%+ dei requisiti

31.3% delle aziende in Europa è conforme a 80%+ dei requisiti

Situazione del mercato

- Lo scudo "**stiamo lavorando su SEPA**" sta venendo meno per le banche europee
- I principali **acquirer italiani** iniziano a concludere le loro certificazioni
- Il mercato nazionale si sta arricchendo di **nuovi attori** che entrano nel settore
- Nuove modalità di pagamento (**mobile POS, NFC**) pongono nuove sfide per la sicurezza dei dati relativi alle carte di pagamento
- Alcune **associazioni** di settore stanno iniziando a mettersi insieme per cercare strade comuni e meno onerose d'accordo con i Brand
- Le controllanti e i partner stranieri iniziano a spingere per traguardare un allineamento a **PCI-DSS**
- Il **Garante per la Privacy** sta studiando misure per tutelare i dati personali tra i dati relativi alle carte di pagamento

Approfondimenti

http://clusit.it/download/Q08_ter.pdf

UNINFO

Contatti

fabio.guasconi@bl4ckswan.com
Tel. +39 3294656930

UNINFO

http://www.uninfo.it/
uninfo@uninfo.it
Corso Trento 13 - 10129 Torino
Tel. +39 011501027
Fax +39 011501837

UNINFO