



A Secure Profile for Tokenization in E and M-Commerce



Andreas Strobel
SPA Board Member



The Smart Payment Association addresses the challenges of today's evolving payment ecosystem. We offer leadership and expert guidance to help members and their financial institution customers realize the opportunities of smart, secure and personalized payment systems and services - both now and in the future.

Since 2004

Members:



What we do



► Providing a comprehensive portfolio of consulting, marketing and advocacy services

- An eye-growing library of expert technical resources and thought leadership collaterals to shape the future of payment
- The market's most accurate barometer of payment trends – annual analysis based on actual manufacturer data

► Defending member interests from a regulatory perspective, while addressing issues of standardization, certification and security to drive the technologies and business models that are shaping the future of payment.

- Engagement in industry bodies and standardization organizations across the world – offering guidance on best practices, providing the 'vendor' perspective and ensuring regulatory initiatives are beneficial to the efficiency of the ecosystem



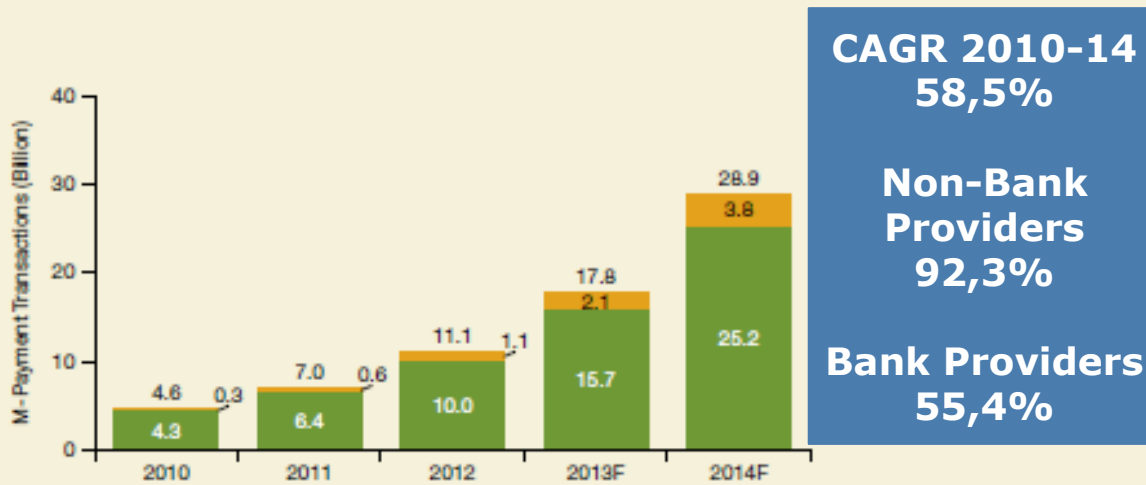
► Opening to encompass a rapidly evolving and broad payments community addressing new verticals and geographies

- Controlled expansion of membership – consolidating its influence on the payment issuing value chain and extending its support to a new generation of internet-based secure payment solutions and service providers.



The rise of e- and m-payments – more payments channels and non-bank providers

Figure 1.7 Number of Global M-Payments Transactions (Billion), 2010–2014F



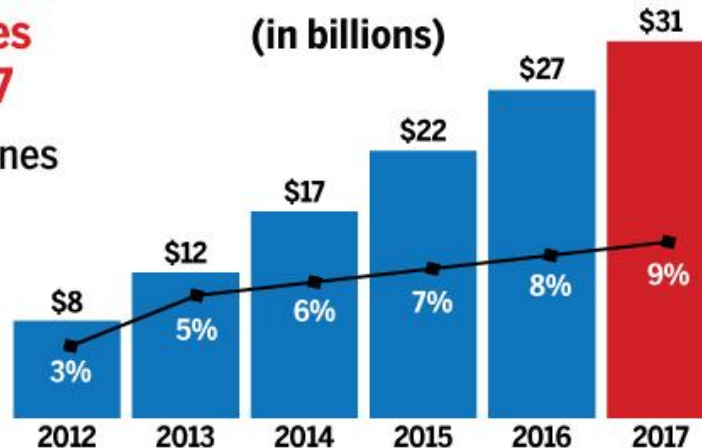
Source: World Payments Report 2013

- ▶ Driven by smart devices & connectivity
- ▶ Convenience and innovation
- ▶ New players and new usages
- ▶ Leading to asymmetry and fragmentation
- ▶ Need for accelerated standardization

U.S. Mobile Commerce Sales Via Smartphone, 2012-2017

Retail sales made on smartphones reached \$8 billion in 2012, 3% of total e-commerce sales, Forrester Research Inc. says.

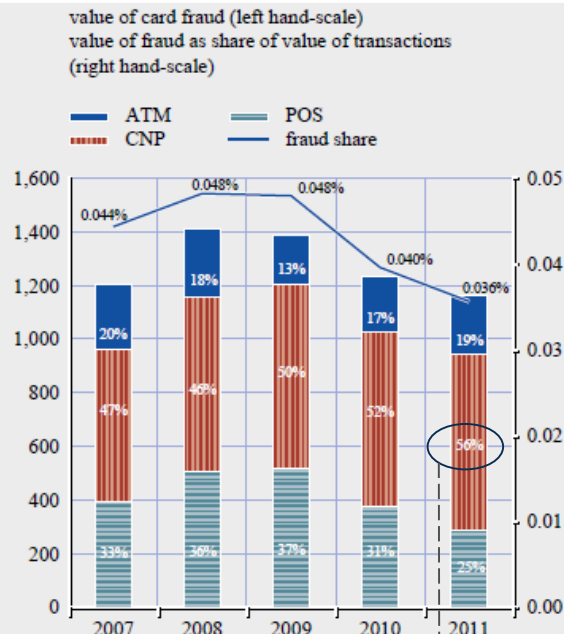
Source: Forrester Research, January 2013



In e-Commerce channel the card-not-present fraud (CNP) is dominant and further increasing

Evolution of the total value of card fraud using cards issued within SEPA ¹⁾

Value in millions of EUR / %



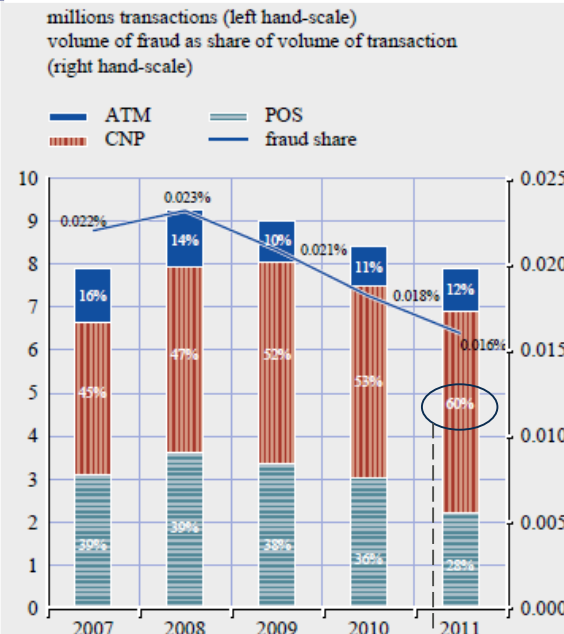
Source: All reporting CPSs.

1) Note that, as outlined in the introduction, total levels of fraud in the years 2008, 2009 and 2011 increased partly owing to the inclusion of data from additional CPSs.

CPSs: Card Payment Schemes

CNP 56 %

Transactions (millions) / %



CNP 60 %

- ▶ **Total level of fraud has reduced overall for the SEPA region**
- ▶ **However, card-not-present transactions now represent the biggest share and the biggest growth in terms of fraud**
- ▶ **Most of fraudulent F2F transactions with EU cards took place outside the EU**

■ Top 6 locations: USA, Dominican Republic, Colombia, Russian Federation, Brazil, Mexico) – Source: Europol

Source: ECB - Second report on card fraud, July 2013

Card technology to fight CNP fraud- Why ?

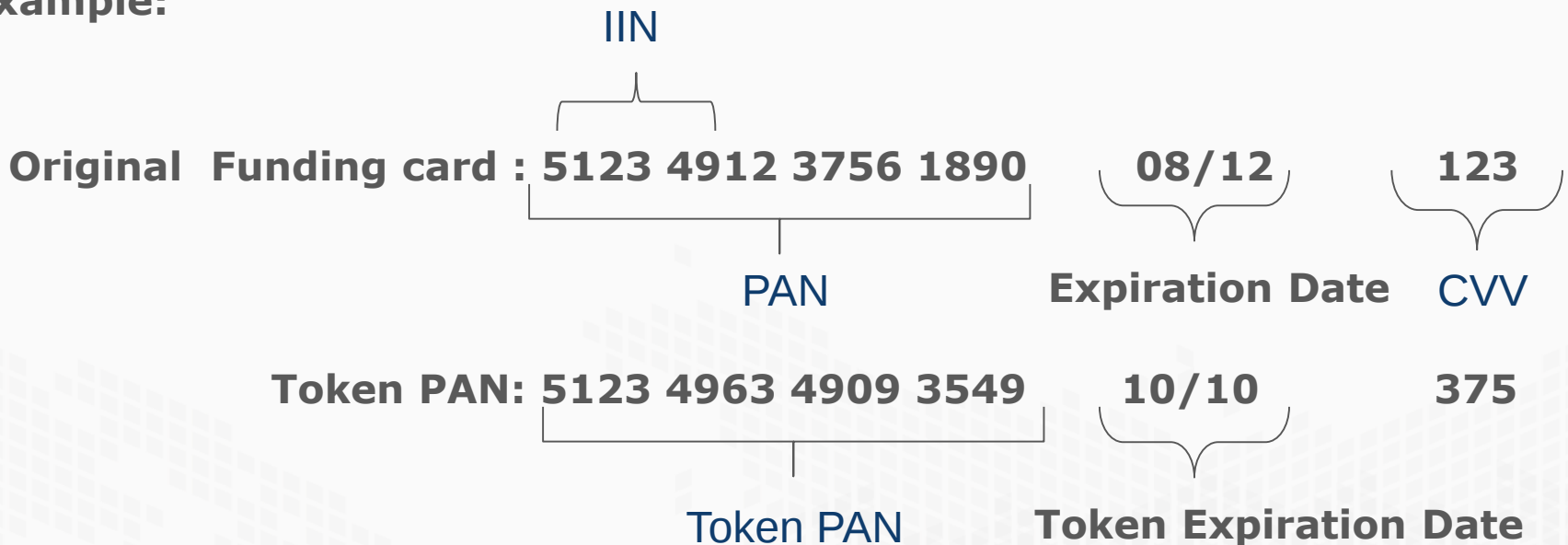
- ▶ **Chip & PIN EMVCo specifications means worldwide interoperability, security and convenience for F2F transactions**
 - Interoperability drives security
 - Without convenience no adoption by users
 - Trade-Off security –convenience was found for Chip&PIN F2F payment contexts
- ▶ **Different card form factors for « fixed » or « mobile » personal devices**
- ▶ **A rational way to come along is to export the basic security concepts of F2F transactions to the online payment context, meaning:**
 - The card and card data are to be authenticated
 - The cardholder is to be authenticated
 - The transaction terms are to be certified by the card
- ▶ **Reuse existing card payment infrastructures**
- ▶ **The risks for the users of electronic payment means should be equivalent regardless of the channel chosen to pay**

Several relevant CNP solutions , but ...

- ▶ A way is by using a personal reader connected to your PC and browser to pay with your card at home as you do in a physical shop
- ▶ OTP generation using a card also requires an additional device and solutions are proprietary, more suitable for e-banking
- ▶ 3D-Secure enables a more trusted cardholder authentication
 - But implementations have very different levels of security
 - Different adoption rates
- ▶ **At present however, most CNP solutions require the manual entry of visible card data but the card was not invented for that purpose !**
 - The static card sensitive data can be captured for fraudulent purposes
 - The cardholder authentication requires the use of an additional channel (eg, 3D Secure)
 - Online retailers need to go through complex and expensive PCI-DSS certification
 - Manual Entry is inconvenient specially in a mobile device
- ▶ **Tokenization is now being pushed by big players such as EMVCo**

What's Tokenization about ?

- ▶ Usually the Token is a standard Card Data structure but where the original card data (PAN, Expiry Date, CVV) are replaced digit by digit
- ▶ The structure of the card data is maintained so the token may be routed using payment system protocols
- ▶ However, in order to be routed to the right Issuer the IIN part of the PAN is the same as in the original PAN
- ▶ Example:



Tokenization overview

- ▶ Both, merchants and cardholders have to be enrolled
- ▶ The token generation is requested in principle by the merchant, but it could also be requested by the cardholder
- ▶ The aim of tokenization is to remove the card information from the merchant environment as completely and quickly as possible
- ▶ Address the root cause of data security issues
- ▶ Maintains existing business processes
- ▶ The token can be used just like the original card number for returns, sales reports, marketing analysis, recurring payments, and so on
- ▶ Can't be used for a fraudulent transaction outside the merchant environment

What challenges for EMVCo Tokenization?

► **Develop an effective technical solution**

- Appropriate choice the underlying technology
- Right tradeoff enhanced security with ease of purchase
- Enabling for competition between EMVCo members anyway, and with solutions from disruptive players

► **Time-to-market: how long will take the standard to be published ?**

- Certification and Type approval procedures to be agreed and put in place

► **Incentive retailers to sign on (liability shifts, other advantages)**

► **Incentive consumers adopting**

Interoperability architecture compatible with existing card payment systems

Customer-Merchant Domain

Token Service Provider Domain

Card Issuer Domain



2. Generate Token (PAN)



4. Token



5. AUTH Request (Token)



6. AUTH Request (PAN)

1. PAN



3. **Strong** User Authentication



But Key security issues to be addressed

- ▶ where the token will be generated
- ▶ which party will secure the token
- ▶ which methods to identify and verify a user before issuing a token
- ▶ what form will the actual token take
- ▶ which security properties for the token
- ▶ which lifecycle for the token
- ▶ standard distinguishability mechanism
- ▶ new data fields for richer transactional information to help improve fraud detection and expedite approval
- ▶ common API for tokenization request and redeem

... and SPA recommends:

- ▶ Security, interoperability, good user experience and a robust business model for the token issuer and the other players of the tokenization framework
- ▶ Specify the security services required for the generation and operation of tokens, as well as the certification framework for components of the framework
- ▶ Specify early the security properties to be featured by the token
- ▶ Standardize protocols and message structures on the retailer to Trusted Service Provider
- ▶ Mandate strong cardholder authentication to protect tokens for high value transaction
- ▶ Position the Secure Element for cardholder authentication, storage and generation of tokens
- ▶ Better collaboration between PCI, EMVCo and ANSI X.9 in order to avoid different standards covering the same needs

Download our Tokenization whitepapers at
www.smartpaymentassociation.com

Thank You

www.smartpaymentassociation.com

#SmartPayment

