The Evolution of Payment Specifications and Tokenization

Smart Card Alliance and EMVCo Webinar

November 4, 2015

Presenters and Agenda

- **Tokenization as a Layered Security Approach for Secure Payments**
  - Randy Vanderhoof
  - Executive Director
  - Smart Card Alliance & EMV Migration Forum

- **EMVCo Payment Tokenization**
  - Clinton Allen, American Express
  - Chair of EMVCo's Tokenisation Working Group

Smart Card Alliance

Tokenization as a Layered Security Approach for Secure Payments

Randy Vanderhoof
Executive Director

Technologies to Mitigate Fraud

- **EMV chip technology**
  - Use of chip cards/devices and POS chip acceptance devices that comply with the global EMV specification

- **Encryption**
  - Encryption of cardholder primary account number (PAN) and/or transaction data while at rest and/or in transit

- **Tokenization**
  - Replacement of a card's PAN with an alternative card number that is used in the transaction process

Smart Card Alliance

Tokenization

- Tokenization is the replacement of a card's PAN with an alternative card number that is used in the transaction process
  - Tokens vary in format and in methodology for generation
  - Tokens may be merchant- or channel-specific and single or multi-use
  - If compromised or stolen, tokens reduce the impact of fraud since they have no value outside a specific merchant or acceptance channel

Smart Card Alliance

Types of Tokens*

- **Acquirer Tokens**
  - Created within the closed environment of the merchant and acquirer and used to remove sensitive account data from the merchant environment
  - Provides protection for data at rest and in transit between the merchant and acquirer
- **Payment Tokens**
  - Created by token service provider on behalf of the token requestor to substitute for a PAN during the entire transaction process
  - Provides protection from transaction initiation until de-tokenization
- **Issuer Tokens**
  - Created by issuers to serve as “virtual card numbers”

*Terminology is still being defined among industry stakeholders

Example Use Cases for Tokens

- **Mobile Contactless Transactions**
  - Tokens stored in mobile device and used at contactless terminals
- **Mobile Remote Payment Transactions**
  - Tokens stored in mobile device and used for in-app or e-commerce transactions
- **E-commerce / Card-on-File Merchants**
  - Tokens replace stored customer PANs
- **Other Use Cases**
  - Tokens used by merchants for other related applications (e.g., loyalty or returns)

Smart Card Alliance

What Does Tokenization Solve?

- **Security**
  - Distributed copies of PANs is a security problem waiting to happen
  - One PAN across multiple technologies reduces the value of the more secure technologies
- **User Experience**
  - Customers don't want to do data entry
  - Card replacement has become a major pain point

Smart Card Alliance

EMV + Tokenization: Security Layers

	Card-Present Transactions			Card-Not-Present Transactions
Counterfeit cards	✓	EMV chip: unique cryptogram replaces static data		Not applicable
Lost/stolen cards	✓	EMV chip + PIN: cryptogram plus PIN for stronger CVM		Not applicable
Prevention of stolen data re-use	✓	Mobile token: Specific- or limited-use token replacement for card data	✓	Tokenization: Specific- or limited-use token replacement for card data
Theft of data at rest	✓	Mobile token: Specific- or limited-use token replacement for card data	✓	Tokenization: Specific- or limited-use token replacement for card data
Theft of data in transit	✓	Mobile token: Specific- or limited-use token replacement for card data	✓	Tokenization: Specific- or limited-use token replacement for card data

Best Practice Guidelines: Layered Approach

- Complete migration to EMV chip cards with dynamic authentication data in the card-present environment
- Protect data-at-rest and data-in-transit through the payment process in both card-present and card-not-present environments with tokenization and encryption
- Remove sensitive payment data present across multiple domains and isolate where and when tokens are used
- Wrap entire transaction environment in secure IT best practices

Payment Tokenisation

Clinton Allen, EMVCo Tokenisation Working Group (TWG)

EMVCo & Smart Card Alliance Webinar – November 4, 2015

Agenda – Payment Tokenisation

- Payment Tokenisation Overview
- EMV Payment Tokenisation Explained
- Industry Feedback and Evolution

Overview of EMV Payment Tokens

EMV Payment Tokens further enhance security of digital payments and simplify purchase experience when shopping on mobile, computers or other smart devices

- Replaces a traditional Primary Account Number (PAN) with a unique EMV Payment Token
- Restricts the use of an EMV Payment Token by device, merchant, transaction type or channel

Fraudulent activity reduced because:

- EMV Payment Tokens are limited to a specific acceptance domain
- EMV Payment Tokens can be unlinked from (PAN) as required
- Merchants that accept EMV Payment Tokenised transactions will not have access to full PAN

Evolution of Tokens

The term tokenisation is used to mean many different things…

- **'Non-Payment' tokens are generally used to protect data at rest in a specific environment**
- **EMV Payment Tokenisation is an interoperable framework that works throughout the payments ecosystem**

Traditional tokenisation seen in the industry revolves around 'non-payment' tokens which are primarily used to protect account numbers utilised in merchant business operations

Replaces a traditional PAN with a unique 'non-payment' token, typically after payment has occurred	PANs are less attractive in a compromise scenario

Data protection measure can be an effective layer of security, however, it is not designed as a replacement for the PAN

Examples of EMV Payment Token Activity

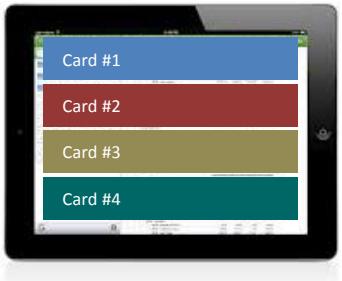
Broad proliferation of models (remote and proximity) has accelerated EMV Payment Token usage:

Card-on-File Merchant

Merchant uses Payment Tokens in lieu of PANs in card-on-file database

Digital Wallet

Branded Digital Wallet presents “Pay with Wallet” in front of card-on-file



QR and Bar Code

QR or Bar Code supplier put a “bar-code” in front of card-on-file

NFC

Payment Tokens in NFC device

EMV Chip Card

Payment Tokens in EMV chip device

Role of EMVCo in Payment Tokenisation

EMVCo Does

- Develop specifications that support secure and globally interoperable transactions - Version 1 published March 2014
- Enhance the specifications based on industry feedback
- Maintain relationships with vendors / service providers
- Collaborate with other industry bodies e.g. PCI DSS, ISO, etc.

EMVCo Does NOT

- Develop EMV Payment Token solutions or services
- Implement EMV Payment Token solutions or services
- Maintain ecosystem implementation and governance requirements
- Mandate, incentivise or shape policies for EMV Payment Token solutions

Complementary Payments Technology

EMV Payment Tokenisation protects against misuse in other domains / channels and can be used with EMV cards & NFC devices

EMV allows secure authentication of payment applications

EMV Payment Tokenisation and EMV-based payment applications improve the payments experience across all channels

EMV Payment Tokenisation Explained

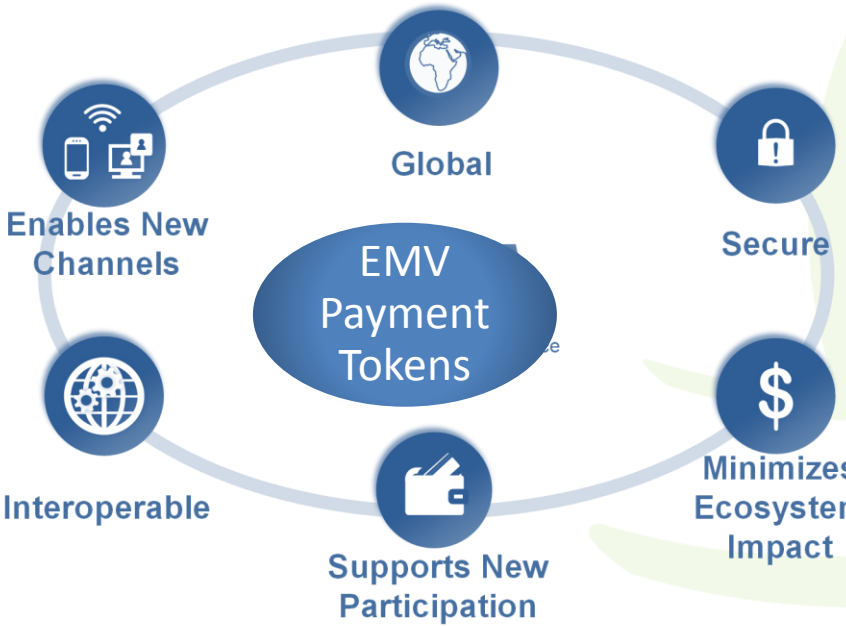
PAN Usage: Need for a Replacement

EMV Payment Tokens will:

- Not ‘collide’, or conflict, with an actual card issuer assigned PAN
- Pass basic validation rules of an account number, while reinforcing interoperability
- Be mapped and associated with an underlying PAN by the entity that generates it, and issues it to the requestor
- Be accepted, processed and routed by the entities within the ecosystem (merchants, acquirers, payment processors, payment networks, card issuers)
- Be a 13 to 19 digit numerical value that conforms to the account number rules of an ISO message (‘like-to-like’ formatting)

EMV Payment Token Attributes

EMV Payment Tokens add value to its processing environment while improving visibility and protecting cardholder information



- Global & multi-channel
- Interoperable with BIN enabled payments
- Bound, mapped or affiliated with underlying credential
- Distinct and identifiable in systems
- Able to be passed through or routed by existing ecosystem players
- Compatible with current payment technologies (web, NFC, POS standards, ISO 8583)
- Capable of supporting future payment channel technologies (QR code, TBD)
- Deployable as static or dynamic (limited use, time limits)
- Able to support authentication by different entities and types (card issuer, wallet, merchant, etc.)
- Supports all regulatory obligations (e.g. routing decisions)

Entity Participation

The EMV Payment Tokenisation Specification must be compatible with the existing payment processing ecosystem. There are five key stakeholders (entities) that must be supported by the new service, and two new entities that will be introduced.

Entities	Category	Description
Cardholder	Current	Consumer enrolled card issuer / payment network
Card Acceptor	Current	Merchant enrolled acquirer / payment network
Card Issuer	Current	Financial institution / processor
Acquirer	Current	Financial institution / processor
Payment Network	Current	Card payment network / processor
Token Requestor	New	Enrolled entity requesting EMV Payment Tokens
Token Service Provider	New	Authorised entity providing EMV Payment Tokens

BIN / PAN Utilisation Principles

Any interoperable EMV Payment Token solution will require increased usage of existing BINs and PAN ranges and remain compatible to ISO Specifications

Utilisation Principles:

- EMV Payment Token BINs / PAN ranges require mapping to base / core credentials
- EMV Payment Token BINs / PAN ranges must reflect product attributes (e.g. debit, signature)
- New BINs / PAN ranges may be introduced at payment network level for EMV Payment Token use
- Current BINs / PAN ranges may be reallocated at a card issuer level for EMV Payment Token use
- Token service providers (TSPs) will store and manage EMV Payment Token BINs / PAN ranges
- TSPs may be managed by a card issuer, payment network or authorised 3rd party

EMV Payment Token Related Data

An EMV Payment Token will be defined by standard data elements, which are passed and where applicable, preserved between the parties

- EMV Payment Token – format preserving, looks like a PAN, but guaranteed not to overlap
- Token expiry date – identical format, may be the same value or different from PAN expiry date
- Token requestor ID – included in some transaction types
- Token cryptogram – included in some transaction types
- Token assurance level – provided to card issuer from TSP
- Token assurance data – provided to card issuer from TSP
- Token request indicator – used during identification and verification only

Identification & Verification Binding Principles

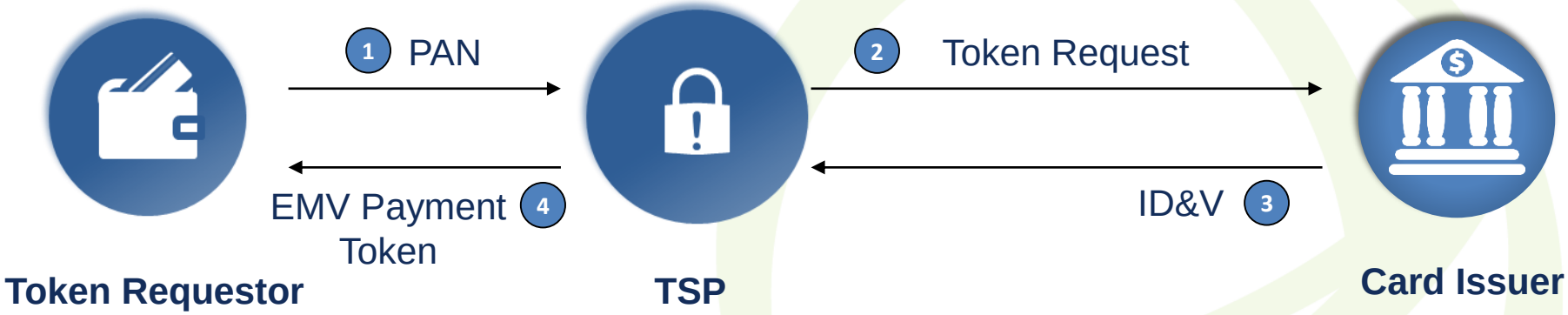
Identification and verification (ID&V) of the consumer and card credentials during EMV Payment Token issuance is a critical step for increasing trust, particularly in card not present environments

Principles:

- Card issuers provide the highest level of ID&V
- There are other parties that may provide ID&V services on behalf of card issuers
- Increasingly token requestors have robust ID&V capabilities
- A good ID&V program supports multiple levels of assurance (multi-party)
- Card issuers and payment networks may assign or adjust risk / authorisation metrics (scores) based on token assurance levels and performance over time

EMV Payment Token Interactions: Token Request

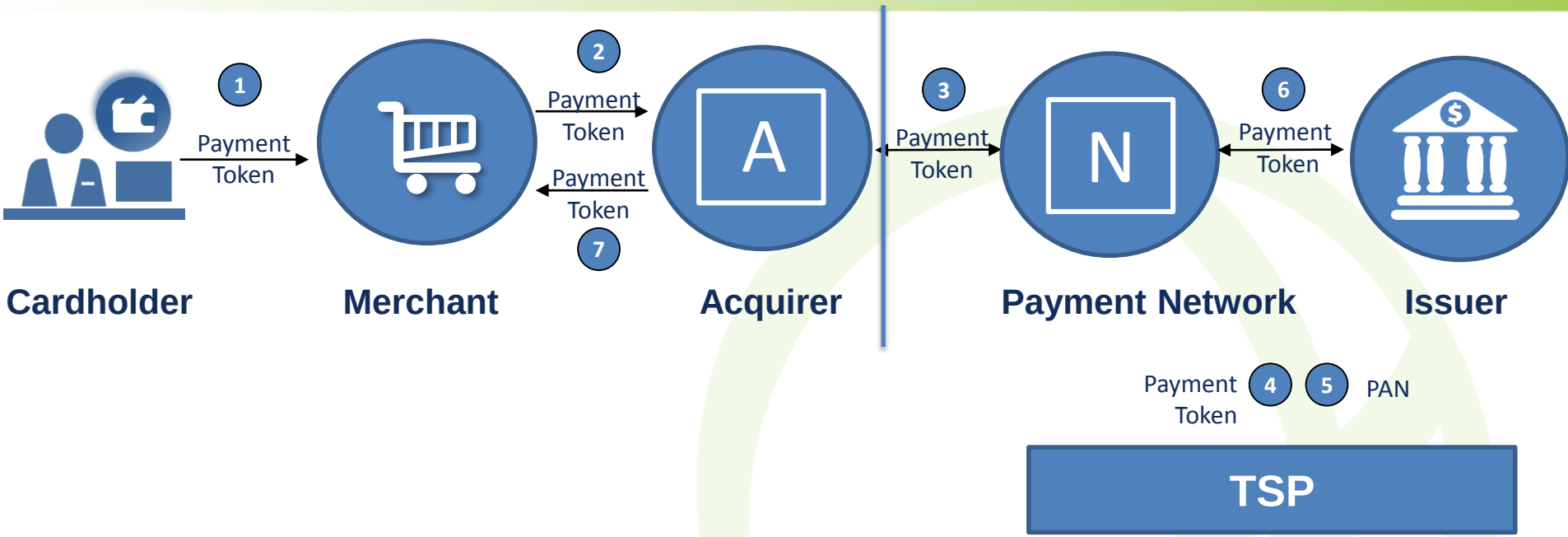
EMV Payment Token requests are made to a TSP. The token requestor, TSP and card issuer can all participate in ID&V. A token requestor can be a wallet, merchant, etc.



1. Token requestor sends a cardholder PAN to the TSP (a request)
2. As part of the token request process, the TSP alerts the card issuer that ID&V is needed
3. Card issuer (or TSP on issuer's behalf) performs ID&V and passes results to the token vault ('binding')
4. TSP passes the registered EMV Payment Token to the token requestor

Example and Illustrative Use Case Only – Not Exhaustive

EMV Payment Token Interactions: Authorisation Processing



1	Cardholder initiates a purchase with a payment instrument i.e. EMV Payment Token
2 3	EMV Payment Token flows through the merchant and acquirer as if it were a PAN
4 5	Payment token is de-tokenised into a PAN by the TSP; card issuer makes authorisation decision and returns PAN to TSP
6 7	TSP re-tokenises the PAN and the authorisation response flows back through the acquirer to the merchant

Example and Illustrative Use Case Only – Not Exhaustive

Industry Feedback and Evolution

Common Feedback and Questions

Summary of feedback key points and answers to common questions:

- There is flexibility designed in the EMV Payment Tokenisation Specification – Technical Framework that allows for entities to innovate beyond current payment acceptance methods and to not prevent interoperability amongst traditional and emerging solutions.
- PCI SSC's / ANSI's current efforts on tokens do not conflict with EMV Payment Tokenisation, instead they are complementary. Areas for cooperation exist and the EMVCo TWG is working with PCI SSC on this to explore data security standards for TSPs.
- TSPs are entities that must have authorised access to issue EMV Payment Tokens from actual BINs. These can traditionally be payment networks or card issuers as well as third party providers acting on behalf of a card issuer or payment network. Ultimately, TSPs are responsible for their own interfaces and vault to support token issuance and lifecycle management.
- Token assurance levels can be used by card issuers for fraud risk scoring and enriches the data currently available for ID&V and authorisation.
- EMV Payment Tokens may be deployed on EMV chip cards and help prevent account misuse. Future use cases will consider this amongst a number of potential areas.

EMVCo is nearing finalisation of the TSP Code Registration process.

In Nov 2014 the EMVCo TWG reviewed with the EMVCo Associates, areas to consider for 'certification' and determined the EMV Payment Tokenisation Specification – Technical Framework was far different to other EMV Specifications

Based on feedback from EMVCo Associates workshops, it was determined to focus on a registration and listing programme

As a result, three areas within the process were defined as candidate requirements, including: registration, renewal and listing management

TSPs that become registered will be provided a 3 digit TSP code by EMVCo, which will be used by token requestors and card issuers to determine the TSPs where EMV Payment Tokens will be issued and managed from

In terms of timing*, the EMVCo TWG will have a process defined in late 2015, with operational readiness thereafter

Format of Token Requestor ID:
Comprised of TSP code, followed by a unique 8 digit numeric identifier assigned by the TSP for the token requester

3 digit numeric, TSP Code

8 digit numeric, Unique Identifier

**The timeline and milestones presented are provisional and subject to change*

PAN Usage: Need for a Replacement

With the introduction of EMV Payment Tokenisation, acquirers and merchants are unable to link transactions performed using EMV Payment Tokens to those performed using underlying PANs

Until a resolution is in place, acquirers and their processors may require full or partial PAN in the interim for a number of internal reasons, including:
- Pre-authorisation fraud checks
- Anti-money laundering checks
- Other merchant operations such as receipt-less returns and transit ticketing

The EMV Payment Tokenisation Specification – Technical Framework v1.0 does recognise this need in the constraints section (heading 2.1). In order to avoid data leakage, it is clearly stated that merchants must not get the full PAN data back in authorisation response messages

A new data element is proposed to replace PAN over the long term. This is referred to as the Payment Account Reference (PAR)

PAR Characteristics and Principles

Feedback from the industry and associates has been consistent about PAR

PAR must have these characteristics:

- Not 16 digits in length, too easily confused with PAN, but needs to be consistent length across all network entities
- Actual method of generation by network entity does not need to be consistent
- Can be read at the terminal before the transaction, where practical and should not force hardware terminal upgrades

PAR must meet the following principles:

- Must be unique across and within network entities
- Must be unique to the PAN, not the cardholder
- Must exist outside of the TSP environment and not create a dependency on it, as PARs are needed for PANs (even those without affiliated payment tokens)
- Cannot be reverse engineered to obtain the PAN
- Provide consistent definition for use within the acceptance community

PAR Data Field Proposal – Proposed Approach

Efforts to develop the PAR concept and underlying principles have been underway since late 2014. A draft specification bulletin was made available in mid-May for finalisation, this draft is not to be used for development at this time until finalised

Format of PAR:

- Fixed 27 characters, uppercase, Roman, alphanumeric (2 + 25)
- Comprised of 2 character, uppercase, Roman, alphanumeric Network Identifier value (assigned by EMVCo)
  Followed by a unique 25 character uppercase, Roman, alphanumeric value

Network Identifier assigned by EMVCo

Unique 25 character value for each PAN

Completed:

- Included feedback from broader EMVCo Associates and EMVCo Advisors
- EMV personalisation = Tag ‘9F24’
- ISO working group assigned composite or dataset TLV Field
  Field 56 for ISO 8583 (1987), Field 112 for ISO 8583 (1998), Field 51 for ISO 8583 (2003)
- Collection of PAR feedback

EMV Payment Tokenisation - Industry Engagement

DEFINE

Identify core components:

- Define payment token ecosystem
- Define new actors in ecosystem
- Establish new definitions / interoperable data elements

- **2013 – Oct-Nov:** Sessions held to determine scope of effort
- **Dec:** Task force scope defined, PR issued

REFINE & RELEASE

Refine core areas:

- Token Assurance Data
- ISO data fields
- Use cases in card present and card not present environment

- **2014 – Jan:** Scope v1.0 spec framework defined, dialogue with X9 and PCI SSC begins **Feb-Mar:** TTF refines v1.0 spec framework
- **Mar:** v1.0 spec framework released, PR issued March 11

FEEDBACK

- **2014 – Mar:** UK Cards Association engagement
- **Apr:** Advisors meeting, TTF becomes TWG
- **May:** PCI SSC engagement
- **June:** TA workshop
- **July:** NGTF engagement
- **Aug:** PST engagement
- **Sep:** TA meeting, MPWG engagement
- **Oct:** US Fed Reserve MPIW engagement, Advisors meeting, further PCI SSC engagement
- **Nov**: Ad-hoc TA+BA Associates workshop

- **2015 – Mar**: TA face-to-face
- **Apr:** Advisors meeting
- **May**: EMV Seminar
- **July**: Ad-Hoc Associates session
- **Sep**: TA Workshop

EMVCo Payment Tokenisation Roadmap*

Q1-4 2015

Ongoing industry engagement:

- Regional payments bodies
- Global standards bodies
- Merchants, processors, issuers, acquirers
- Payment innovators and others

Tokenisation Engagement Opportunities:

- Oct 21, 22: EMVCo Board of Advisors | Boston, USA
- Oct 15: Seminar | Barcelona, Spain
- Nov 3: Seminar | Jakarta, Indonesia
- Nov 4: Webinar in conjunction with SCA

Q4 2015

TSP registration & listing programme management:

- List and registration process to be made available on the EMVCo website
- Ongoing work with PCI SSC for investigation of industry standard TSP security requirements

Dec 2015

PAR Special Bulletin:

- PAR
- Network Identifier registration and programme management

Q2 2016

Payment Tokenisation Specification – Technical Framework Updates:

- Integration of PAR
- Clarifications – including more clarity on token assurance levels and aggregator concept
- Expanded EMV Payment Token use cases
- Consider impacts to special transactions

**The timeline and milestones presented are provisional and subject to change*

EAP Connects EMVCo to Industry Leaders

Benefits:

Access
Engage and connect with EMVCo's Executive Committee, Board of Managers and Working Groups

Insight
Learn more about EMVCo's work programme, including future initiatives

Influence
Contribute to the future evolution of the EMV Specifications by sharing expertise, experience and requirements

Foresight
Receive advanced updates on EMV Specifications and technical amendments

Thank You!

For more information visit www.emvco.com or join us on LinkedIn

Smart Card Alliance

Wrap-Up

Wrap-Up

- **Events**
  - Smart Card Alliance Payments Summit, April 5-7, 2016
    - http://www.scapayments.com/
- **Resources**
  - EMVCo web site, http://www.emvco.com
  - Smart Card Alliance web site, http://www.smartcardalliance.org
    - Technologies for Payments Fraud Prevention: EMV, Encryption and Tokenization white paper
  - EMV Connection web site, http://www.emv-connection.com
  - GoChipCard.com web site, www.gochipcard.com

Smart Card Alliance

Q&A

Randy Vanderhoof
rvanderhoof@smartcardalliance.org

Clinton Allen
clinton.r.allen@aexp.com

www.smartcardalliance.org
www.emv-connection.com/emv-migration-forum
www.gochipcard.com

www.emvco.com