Mobile Payments Industry Workgroup Meeting

Discussion on Tokenization Landscape in the U.S.

June 2-3, 2014

Susan Pandy and Marianne Crowe
Federal Reserve Bank of Boston

September 23, 2014

Susan Pandy is a Director and Marianne Crowe is a Vice President in the Payment Strategies Group at the Federal Reserve Bank of Boston.

The authors would like to thank the speakers at the June meeting and the members of the MPIW for their thoughtful comments and review of the report. The views expressed in this paper are solely those of the authors and do not reflect official positions or endorsements of the Federal Reserve Bank of Atlanta, the Federal Reserve Bank of Boston, or the Federal Reserve System.

I. Introduction

The Federal Reserve Banks of Boston (Payment Strategies) and Atlanta (Payments Risk Forum) convened a meeting of the Mobile Payments Industry Workgroup (MPIW) on June 2-3, 2014 to discuss several industry tokenization initiatives[1] being developed for digital and mobile retail payments.

The key objectives of the meeting were to: (1) obtain an overview of the different industry tokenization initiatives under development (Accredited Standards Committee (ASC) X9,[2] EMVCo,[3] the Payment Card Industry Security Standards Council (PCI SSC),[4] The Clearing House (TCH),[5] and the credit card networks (Visa, MasterCard, and American Express (AmEx)); (2) begin to understand the business and operational perspectives of the tokenization schemes and implementation models; (3) lay the groundwork for conducting an analysis of the similarities and differences across these models; and (4) identify potential risks and gaps that may require industry coordination or input to standards.

This paper provides an introduction to tokenization for the payments industry; summarizes the discussion on payment versus non-payment industry tokenization initiatives and identifies some of the key issues and considerations underlying any tokenization models or related technical specifications for payments.

II. Defining Tokenization

A token is a randomly generated substitute value used to replace sensitive information through a process called *tokenization*.[6] When used for financial transactions, tokens replace payment credentials, such as

[1] A number of "initiatives," referred to as models or specifications throughout this paper were not considered to be industry "standards" at the time of writing, although some have been published specifically to achieve that distinction.
[2] For more information, see http://x9.org/.
[3] EMVCo is owned by the six major global card payment brands (Visa, AmEx, MasterCard, Discover, JCB, and China Union Pay). It facilitates worldwide interoperability and acceptance of secure payment transactions by managing EMV® Specifications and related testing processes. This includes card and terminal evaluation, security evaluation, and management of interoperability issues. There are EMV Specifications for contact chip, contactless chip, common payment application, card personalization, and tokenization. For more information, see http://www.emvco.com.
[4] The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. For more information, see https://www.pcisecuritystandards.org.
[5] The Clearing House (TCH) operates payment systems for the banking industry and works with commercial banks to create new capabilities for the next generation of payments. For more information, see https://www.theclearinghouse.org.
[6] Other industry bodies, such as PCI and X9, define a token as a surrogate value used in place of the original value and note that not all tokens are randomly generated, but may be generated using deterministic methods. The MPIW maintains that a token is *not* an encrypted or hashed value that can be mathematically re-engineered to determine the original value. Both PCI SSC and Visa identify two tokenization generation methods that use: 1) a known strong cryptographic algorithm, or 2) a one-way irreversible function.

bank account and credit/debit card numbers. The ability to remove actual payment credentials from the transaction flow can improve the security of the payment and is a key benefit of tokenization.[7]

The key goal of tokenization is to protect the Primary Account Number, or PAN. A PAN is a 13 to 19[8] digit number embossed on a plastic bank or credit card and encoded on the card's magnetic strip.[9] The PAN identifies the card issuer in the first six digits, known as the Bank Identification Number (BIN), as well as the individual cardholder account (generally the final four digits), and includes a check digit for authentication. Tokenization eliminates the need for merchants to store the full PAN on their network systems for exception processing or to resolve disputes. Replacing PANs with tokens can reduce the financial impact resulting from data compromise, theft, or unintended disclosure during disposal. While data breach prevention is the key to reducing the risk of compromise, tokenization has the benefit of making the compromised data less valuable.

While tokenization is not a new concept,[10] emerging proximity and remote payment types, such as card-on-file merchant,[11] digital wallet, QR code, NFC and chip, have accelerated demand for payment-related token usage. EMVCo has proposed using these types as representative use cases for tokenization deployment. What is new about tokenization is the need for interoperable, open standards, and the increasing desire to replace payment card or bank account numbers with tokens for point-of-sale (POS), online, or mobile payments. Tokenization enhances the ability to protect the payment information in both card-not-present (CNP) and card-present (CP) transactions. It addresses the vulnerabilities inherent in the magnetic stripe credit card and enhances the security of EMV.[12] Furthermore, it enables retailers to not store sensitive payment information in their systems, which can reduce the impact from a data breach and potentially minimize their compliance requirements with the PCI Data Security Standard (PCI DSS).[13]

---

[7] Payment information that is protected through tokenization and encryption is much safer than a plain-text credit card number or other payment account information. Because a token can be specific to each transaction, it provides little value to fraudsters. The token would have to be decrypted by the tokenization provider to be useful.

[8] According to ISO/IEC 7812-1:2006 *Identification cards -- Identification of issuers -- Part 1: Numbering system*, while most PANs are 14 or 16 digits, some are shorter and some are longer (up to 19 digits are allowed). For more information, see http://www.iso.org/iso/catalogue_detail?csnumber=39698.

[9] A PAN can also be encrypted on a chip for an EMV-enabled card.

[10] Credit card data was first tokenized in 2005, but lagged in adoption until October 2009, when Visa published guidelines for encrypting card data and recommended the use of tokens to replace the PAN in payment-related business functions. Visa published best practices for tokenization in 2010, which noted the benefits of tokenization in reducing the scope, risks, and costs of ongoing compliance with PCI DSS. EMC[2] (n.d.) *Tokenization: What's Next after PCI?* Retrieved on July 24, 2014 from http://www.emc.com/collateral/white-papers/h11918-wp-tokenization-rsa-dpm.pdf.

[11] Merchants use tokens in lieu of PANs in card-on-file databases.

[12] EMV is a global specification for credit and debit payment cards based on chip card technology that defines requirements to ensure interoperability between chip-based payment cards and terminals. The primary use for these chip-based cards is to perform payment transactions. The encrypted dynamic data supplied by the chip provides a higher level of protection against counterfeiting than magnetic striped cards. For more information, see http://www.emvco.com.

[13] PCI DSS provides an actionable framework for developing a robust payment card data security process-including prevention, detection, and appropriate reaction to security incidents. Available at: https://www.pcisecuritystandards.org/security_standards/. PCI SSC has not announced a position on all types of tokenization and the impact on PCI DSS obligations.

There are several obstacles to developing a common set of standards for tokenization for the payments industry. First, different tokenization models are being developed (e.g., EMVCo, TCH, card networks, PCI SSC, and ASC X9). At this time, it is not clear how the different payment models (EMVCo, TCH, and the card networks) may complement each other as they remain in different stages of development and coordination. Second, the models do not use consistent terminology, which is necessary to develop common standards. MPIW members and others in the payments industry have suggested the need for stakeholders to collaborate to develop common terminology for the different tokenization models, which requires a better understanding of how each model will work in various transaction venues. The MPIW is evaluating this effort as part of a multi-stakeholder assessment to understand the key issues surrounding tokenization in the payments industry.

III. Payment Tokenization Initiatives

Tokenization is used to solve many different problems, which explains the existence of several models. EMVCo, TCH, and the card networks (Visa, MasterCard, and AmEx) are considered *payments* tokenization efforts, while ASC X9 and PCI SSC are characterized as *non-payment*[14] tokenization efforts. Non-payment tokenization initiatives aim to protect data at rest (when it is stored), so, these proposed ASC X9 and PCI SSC specifications focus on the security and protection of sensitive information versus the creation of a token to replace a payment credential in a financial transaction.

EMVCo

EMVCo, the EMV chip card standards body, published *The EMV Payment Tokenization Specification – Technical Framework v1.0*[15] (EMVCo spec) in March 2014 as a framework for tokenizing credit card numbers. It was designed to help merchants, acquirers, payment card issuers, and mobile and digital payment providers develop globally interoperable tokenization solutions for online and mobile environments. It includes details on the payment tokenization ecosystem, the types of entities whose participation is needed to support payment tokens, and key responsibilities and controls specific to each entity within the ecosystem, along with the benefits of adopting a unified approach.

The EMVCo spec contains details on implementing different use cases, including mobile NFC at POS, mobile/digital wallet ecommerce, card-on-file ecommerce, and scan at POS (i.e., QR codes). It also includes definitions and data message formats to ensure the interoperability of tokens and outlines the

[14] This terminology was suggested by EMVCo, but has not been accepted by ASC X9 or PCI SSC.
[15] Download available at http://www.emvco.com/download_agreement.aspx?id=945.

consistent approach that should be used to route and authenticate payment tokens.[16] Although an EMVCo representative did not attend the June 2014 MPIW meeting, other guests and MPIW members were familiar with the effort and discussed the similarities, differences, and key considerations.

EMVCo published minimum requirements for the creation and use of payments tokens, which include:[17]

- Token format should be similar to a credit card number: 13-19 digit numeric value that must pass basic validation rules of an account number, including the Luhn[18] check digit. Payment tokens must not have the same value or conflict with the real PAN.
- Tokens can be used to initiate payments, and differ from financial tokens addressed in the PCI SSC requirements that protect data at rest.
- Tokens are merchant- or payment-network specific, and are only relevant within a specific domain.
- For most use cases, the PAN is known only to the payment card issuer and customer. The token becomes a payment object[19] shared between merchants, payment processors, the customer, and other relevant parties to the transaction.
- Process to validate the identity of the token requestor each time a token is requested.
- Type of token generated varies based on risk analysis – higher risk factors mean a low-assurance token.

These requirements will impact the entire payments environment, where many stakeholders operate a mix of legacy and contemporary infrastructure. If the EMVCo spec becomes the dominant industry standard, it may be difficult for businesses with legacy systems to adopt it, as they may not be able to accept all features. Whether the tokenization standard adopted is EMVCo or non-EMVCo, businesses will need efficient and compatible solutions that have minimal impact to their operations.[20] Tokenization platforms that include format-preserving protocols, tokenization and encryption of data and files, centralized policy control, and simplified key management may help to address this issue.

The EMVCo spec also includes requirements for the Token Service Provider (TSP) and Token Requestor. The TSP is an entity authorized to provide payment tokens to Token Requestors who are traditional payments participants, including card-on-file merchants, acquirers, acquirer processors, payment gateways, and payment enablers, such as device manufacturers, digital wallet providers, and card issuers.

---

[16] Arnfield, Robin. (2014). Mobile Banking and Payments Security: What Banks and Payment Service Providers Need to Know to Keep their Customers Safe. *Mobile Payments Today*. Available for purchase at www.mobilepaymentstoday.com.

[17] For a detailed explanation of these requirements, refer to EMVCo (2014, March). *EMV Payment Tokenization Specification – Technical Framework*. Available for download at http://www.emvco.com/specifications.aspx?id=263.

[18] The Luhn algorithm or formula is a simple checksum formula used to validate a variety of identification numbers, such as credit card numbers. For more information see http://en.wikipedia.org/wiki/Luhn_algorithm.

[19] Per the EMVCo specification, when tokens are used as payment objects, there are "data elements" (i.e., metadata describing the token–to-buttress security), which include a cryptographic nonce, payment network data, and token assurance level.

[20] For a discussion of infrastructure impacts to various stakeholders, see http://www.bobsguide.com/guide/news/2014/Jul/22/tokenization-the-future-of-payments-security.html.

TSP requirements cover development and operation of a token vault,[21] payment token generation, issuance and provisioning, security and controls, token requestor registration, token assurance, and token domain restrictions.

In October 2013, Visa, MasterCard,[22] and AmEx proposed a framework for a global tokenization specification (spec) for digital payments as a starting point and began working together. Realizing that implementation of this spec would require support from the broader payments industry, they shifted responsibility for the effort to EMVCo.[23] The framework proposed by the card networks basically overlays the EMVCo spec, but allows for customization typically required by the networks. For example, EMVCo may require a minimum of five fields, but a network could specify seven fields to accommodate more proprietary information. The EMVCo spec will need to maintain compatibility with the existing payments infrastructure and complement existing specs to ensure consistency across all payments environments.

The card networks' proposed specifications will be available to all payment networks to share with their business partners. Key elements include:

- New data fields to provide richer information about each transaction to help improve fraud detection and expedite the approval process;
- Consistent methods to identify and verify a consumer before replacing the traditional card account number with a token; and
- A common standard designed to simplify the process for merchants to tokenize contactless, online, or other transactions.

The Clearing House (TCH)[24]

In 2012, several members of TCH[25] initiated a project to improve the trajectory of mobile payments. They developed the Secure Token Exchange (STE) tokenization spec, (originally known as "Secure Cloud"), and proposed it as a possible industry standard in July 2013. The goal of the STE is to address the problem of the proliferation of exposed payment account credentials, which is expected to accelerate

[21] A token vault stores tokens and the credit card or bank account numbers they represent. The vault is the only location where a token value can be exchanged for the real number.
[22] MasterCard and Visa did not attend the MPIW meeting. Comments are based on input from other participants and publicly available information.
[23] Paybefore. (2014, August 5). *Token Efforts on Security are more than Gestures.* Retrieved from http://paybefore.com/finance-and-strategy/token-efforts-on-security-are-more-than-gestures/ [Requires subscription].
[24] David Fortney, Senior Vice President, Product Management and Strategy at TCH, represented TCH at the MPIW meeting.
[25] TCH was established in 1853 and is the oldest banking association and payments company in the U.S. It provides payment, clearing, and settlement services on behalf of its member banks. TCH is owned by more than 20 commercial banks.

with mobile payments. Initially, the debit card number served as the token for the Demand Deposit Account (DDA) since it was an entirely different number. However, merchants and customers found it inefficient and inconvenient to key-enter the debit card number for every purchase, which is why TCH is creating a standard, tokenized payment card number to make the mobile device more secure for payments. TCH considers tokenization a viable alternative to storing customer payment credentials in the mobile wallet (e.g., using the secure element).

The STE model is intended to be open to encourage innovation and not impede any current practices in the payments industry. To test the concept, TCH launched a low-volume pilot in 4Q 2013 with a token switch, a single issuer, a single acquirer, and a small number of merchants. The issuer developed the token vault. The pilot tested for the creation of one token, but allowed for a spare token (e.g., to allow the token to be replenished if a user has no connectivity, for example, on a plane). This option allows for either the first token to be re-used multiple times or to make use of a spare token. The pilot supports token lifecycle management for payment card numbers (strings of digits that mimic the length of the actual number but are randomly determined), so they cannot be linked to the actual payment card number.

TCH originally approached the card networks to participate in the pilot, recognizing that their participation is ultimately needed to achieve market scale, but the card networks preferred a global solution and decided to work with EMVCo instead to develop a spec.

TCH plans to expand the pilot to more member banks in late 2014, and develop a plan for online venues. TCH employs a dynamic tokenization process, and stores tokens on the mobile phone. TCH is also adding support for static tokens used in conjunction with a dynamic cryptogram.

TCH is building a bank-owned multi-issuer token vault to support STE. The vault will issue tokens, decide how to identify and verify the customer, and determine what standards will be needed. While some TCH member banks are building their own token vaults, many will not, largely because of the complexity and investment involved.

Similarities and Differences Among Payment Tokenization Efforts

TCH evaluated differences between the STE and EMVCo specs and identified key disparities in token formatting, lifecycle management, PAN ownership, and the use of static versus dynamic tokens. TCH defined and developed a set of messages to support token formatting, which EMVCo does not include. TCH also has a lifecycle management process to handle a stolen payment card or mobile phone, including

identification of messages that need to be exchanged to cancel the tokens and ensure the customer experience is not negatively impacted.

TCH and EMVCo view ownership of the real PAN differently. Acquiring bank participants in the TCH pilot expressed a strong need to access the real PAN, which the STE spec addressed by assigning PAN ownership to the acquirer. PAN access provides the ability to track purchases across mobile and non-mobile use cases, facilitate loyalty and returns, and provide fraud services. Although TCH discussed the PAN issue with the card networks, the current EMVCo spec does not address ownership of the PAN.

Both TCH and EMVCo are considering adjustments to their specs. TCH plans to modify its spec to incorporate several EMVCo requirements. For instance, TCH may publish information on how to prevent re-use of tokens. TCH also plans to maintain its distinct capabilities in the STE model and is hopeful that these capabilities will be incorporated into the EMVCo spec in the future.

IV. Non-Payments Tokenization Initiatives

Payment Card Industry Security Standards Council (PCI SSC)[26]

In August 2011, the PCI SSC issued *Information Supplement: PCI DSS Tokenization Guidelines*. These guidelines are intended for merchants that store, process, or transmit cardholder data and are seeking information on how implementing a tokenization solution may impact the scope of their compliance efforts with the PCI DSS. PCI SSC is now in the process of developing a tokenization spec, the *Non-Payment Tokenization Technical Standard*, for release in late 2014 or early 2015. The goal of the PCI SSC tokenization spec is to protect data at rest by defining methods for generating *security* tokens. Therefore, the spec will address technical and security requirements for a tokenization process and commercial token solutions, whether software- or hardware-based, that would replace storage of the PAN value with a token.

The PCI SSC and EMVCo objectives for developing tokenization specs differ in several ways. First, PCI SSC addresses security tokens, while EMVCo addresses payment tokens. Security tokens are issued internally (i.e., by the data owner), while payment tokens are issued externally (i.e., by the TSP) and used to authenticate a transaction. Second, PCI SSC wants to prevent fraud if the holder of the token is compromised, so its tokens are not intended to pass through the payments ecosystem. Third, PCI SSC tokens do not need to be format-preserved. Merchants often utilize third party (acquirer or processor) token solutions that offer Format Preserving Encryption (FPE), which allows tokens to be stored in place

[26] Ralph Poore, Director, Emerging Standards with the PCI SSC, represented PCI at the MPIW meeting.

of payment card numbers without modifying existing business applications and databases. FPE is applied to PAN data in order to generate the substitute value which must pass the Luhn check digit algorithm and a PCI SSC scan. Additionally, PCI SSC requires a mechanism to show that the value is a token and not a PAN.

PCI SSC tokenization supports irreversible and reversible token models (where de-tokenization is possible).[27] Similar to TCH, the PCI SSC guidelines cover a broad range of use cases to allow for innovation.

American National Standards Institute (ANSI) Accredited Standards Committee X9

X9 is the American National Standards Institute (ANSI) committee responsible for developing the American National Standards for the financial services industry.[28] X9 is currently working on a standard (X9.119 – Sensitive Payment Data) to define requirements for the secure implementation of tokenization.[29] When work on X9.119 began in 2009, its goal was to write a standard for encryption and tokenization methods to protect sensitive payment card data. To make the process more efficient, X9 split the standard into two parts and created X9.119-2 specifically for tokenization.

X9.119-2 defines a token as "a surrogate value used in place of an Underlying Sensitive Value (USV) [30] in certain, well-defined situations, but not in every way that the USV is used." The standard also distinguishes between token attributes and token utility. Token attributes refer to the structure of the token, whereas the utility refers to what can be done with the token. The utility of a token replacing a PAN can range from a unique value mapped to the USV to a "higher utility" value used to approve certain financial transactions. X9.119-2 only covers tokens with minimal utility.

X9.119-2 provides guidance on how to securely generate tokens without identifying the type of underlying token generated. By contrast, PCI labels tokens based on what type of token was generated (e.g., cryptographic versus non-cryptographic, reversible versus irreversible, and authenticated versus non-authenticated). The prospect of different usage "tiers" being assigned to specific transaction venues,

---

[27] Random tokens map to "Reversible Non-Cryptographic Tokens" and PAN encryption maps to "Reversible Cryptographic Tokens." For a discussion of tokenization techniques and PAN to token map techniques, see Voltage Security. (2014). *Tokenization/Point to Point Encryption/EMV and PCI: Cutting Through the Confusion*. Retrieved from https://macmember.org/library/public/MAC%20Presentation%20-%20Tokenization.pdf.

[28] X9 is responsible for the industry standards for financial cryptography and data protection including payment card PIN management, credit and debit card encryption, and related technologies and processes.

[29] This work is taking place in the X9F6 group that works on "Cardholder Authentication and ICCs (Integrated Chip Cards)." X9.119-2 defines tokenization as "the act of generating and mapping a token to an underlying sensitive value (USV)."

[30] X9.119-2 defines **Underlying Sensitive Value (USV)** as the value that the token replaces. For example, when a token replaces a PAN, the PAN becomes the USV for that token. X9.119-1 requires the USV for a 16-digit PAN to be at least six digits.

risks, and purposes, may encourage X9 to further analyze and assess the need for global tokenization standards.

X9.119-2 supports merchant and acquirer tokenization use cases. It enables the merchant to store the token instead of a credit card number, but allows the merchant to request the real credit card number (PAN) if needed. It should be noted that the X9 standard will only cover tokens used to protect the USV of the PAN, or other payment card elements. Therefore, the token is considered to have no utility with respect to payment transactions.[31] Any token that can be used to approve a payment transaction in its raw form, without converting it back to its original USV, will be treated as if it were the USV and protected using methods described in Part 1 of the standard.

X9.119-2 also outlines some of the key business drivers for implementing tokenization, such as a reduction in audit costs by reducing the PCI audit scope. The standard will also address in detail the following: 1) how a token should be generated; 2) what security requirements should support token generation; and 3) what security requirements are needed to request a token.

While X9.119-2 and PCI are similar, X9.119-2 has a broader focus, aimed at building a standard around all the existing tokenization implementations. Both the PCI and X9 standards are in draft form and are open standards processes (i.e., anyone can join and participate).[32]

V. Key Considerations

As the industry moves forward to develop tokenization standards, there are several key issues to resolve:

1. Static versus dynamic tokens
2. Token-tiering by venue and use
3. Prevention of fraudulently created tokens
4. Impacts to infrastructure and interoperability
5. Role of tokenization in host card emulation (HCE)[33]
6. Approaches to managing tokenization process
7. Consumer usability
8. Other uses of tokenized PAN
9. Implications of proprietary tokenization approaches

[31] The token acts as a placeholder for the PAN (or USV) and cannot substitute for the PAN (such as being used to approve financial transactions).

[32] For more information on how to join X9, see http://x9.org/join-x9/membership-application/. For more information on how to join PCI SSC, see https://www.pcisecuritystandards.org/get_involved/join.php.

[33] **Host Card Emulation** makes it possible to perform NFC card emulation without using the secure element (SE) in mobile handsets. HCE enables NFC card emulation communications to be routed through the mobile phone's host processor versus from the POS terminal through the NFC controller to the SE.

10. Other

1. Static versus Dynamic Tokens

Dynamic tokens change with every transaction. Static tokens do not change until the token expiry date, and then can be renewed "as is" at each expiry date in perpetuity. Some tokens are neither completely dynamic nor completely static.

A dynamic token is valid either for a single transaction or for a limited number of transactions occurring in a very short time interval, during which a new token is generated and provisioned to the mobile wallet.[34] If a dynamic token is intercepted by malware residing in a retail POS system, the ability to use that token for a subsequent fraudulent purchase is nearly impossible because it would require the fraudster to be in the same immediate vicinity, and would be rapidly detected.

Despite the fact that dynamic tokens are considered more secure in the payments industry, they present challenges which need to be addressed. For instance, some large issuers may consider static tokens because dynamic tokens impact how they perform fraud prevention, which occurs before the token enters the back-end system.

The EMVCo spec supports static, domain-specific[35] payment tokens with a token cryptogram.[36] The TCH model also plans to support static tokens with cryptograms. A key consideration for merchants with the use of static tokens is the potential for increased risk of re-use in fraudulent transactions. It is also unclear as to whether static tokens will allow merchants to usefully track transaction history for customers.

2. Token-Tiering by Venue and Use

Token tiers categorize different token options, venues, uses, and values to help assign the appropriate risk assurance level to the token. Risk assurance levels are negotiated between the TSP and the Token Requestor. EMVCo defined four use cases (NFC at POS, ecommerce purchases, ecommerce with stored

[34] The MPIW acknowledges that dynamic tokens can be used by other form factors as well; however, the MPIW is primarily focused on the use of dynamic tokens as related to mobile and digital wallets/payments.
[35] The EMVCo spec outlines a set of parameters or controls for payment token issuance by a TSP that allow for the appropriate use of payment tokens in payment transactions. Examples of these controls include: use of a payment token with a particular presentment mode, such as contactless or ecommerce (e.g., POS Entry Mode as defined in ISO 8583), merchant entry modes, and verification of the presence of a token cryptogram that is unique to the transaction.
[36] A token cryptogram is generated using the payment token and additional transaction data to create a transaction-unique value. The calculation and format may vary by use case. The Token Requestor generates the unique token cryptogram to validate authorized use of the token. It is carried in different fields in the transaction message based on the type of transaction and associated use case, and is passed in the authorization request and validated by the TSP and/or the card issuer. See *The EMV Payment Tokenization Specification – Technical Framework v1.0*, pp. 14, 31, 66-68, 70-72, and 74-78.

accounts, and use of QR codes at POS) as initial applications of tokens, but left open the possibility of more use cases.

Non-EMVCo examples include: pseudo-PAN tokens used for online purchases (e.g., Braintree/Venmo, Stripe, and WePay); processor-provided tokens used by merchants internally; second log-in tokens (PayPal, 3-D Secure, and Visa Checkout); and proprietary tokens that support new business models for POS payments. Other potential use cases that need to be investigated include digital content, host card emulation (HCE) applications working with NFC, fingerprint-reading/verifying authentication to obtain purchasing tokens, and use of Beacon[37] technology to pass tokens for payments.

A comprehensive assessment of the tokenization landscape is needed to understand the wide range of token types and how risk levels will be assigned to them.

3. Prevention of Fraudulently Created Tokens

The purpose of front-end fraud prevention is to block the creation of counterfeit tokens that can be used to make unauthorized payments. Global tokenization standards should address front-end fraud, but none of the current models do (beyond EMVCo developing assurance scores and card networks' vetting of token requestors). Payment standards should address strong authentication of the account holder on the front-end when the credentials are being shared (e.g., with a wallet provider). Therefore, it is critical that tokenization solutions incorporate fraud detection mechanisms (e.g., collecting and checking data on mobile device location and identifiers when tokens are requested) to prevent theft and counterfeiting of legitimate tokens prior to the transaction initiation and during the process flow.

Merchants want assurances that fraud will be prevented at the point of entry. Visa's *Best Practices for Tokenization* does not address how to prevent fraudulent tokens from being obtained when stolen account credentials are used for enrollment. However, MasterCard's tokenization program proposes to include tools using mobile or other digital information for issuers to authenticate account enrollments.

4. Impacts to Infrastructure and Interoperability

It is still unclear as to how tokenization standards will impact existing infrastructure and what changes will be required by payment stakeholders. Tokenization can be implemented on top of the existing infrastructure. However, legacy card systems have complicated data flows and processes which make it more difficult to improve the security of the payments infrastructure. For example, the card networks use

[37] Beacons are low-cost hardware components, small enough to attach to a wall or countertop, that use battery-friendly, low-energy Bluetooth connections to transmit messages or directly prompt a smartphone or tablet. Beacons can potentially transform how retailers communicate with customers in their stores.

card emulation to minimize changes that merchants, processors, networks, and issuers would have to make to accommodate full, end-to-end encryption and tokenization for payments, but it causes some account credentials to be passed "in the clear" (i.e., unencrypted or not protected) at the POS terminal. If this issue is not resolved, it will impact interoperability and might incent new mobile payment providers to consider building their own token systems and process their own returns and chargebacks.

Further analysis should be done to determine what is needed to ensure broad adoption of tokenization by financial institutions, merchants, and other stakeholders and to achieve interoperability. If EMVCo becomes the prevailing technical specification for tokenization in the payments industry, then riding the newly emerging EMV rails at POS should pose few challenges to interoperability. But some industry stakeholders forecast that EMV will take several years to gain a substantial portion of payment card transactions. There are other technologies emerging which could be viable alternatives to the EMVCo approach.[38]

5. Role of Tokenization in Host Card Emulation (HCE)

To secure cloud-based mobile payments and protect sensitive information without burdening the user experience, HCE can use multiple techniques. The general opinion among payment industry stakeholders is that tokenization is one of the primary security measures being considered. Other measures include limited use keys, account replenishment, and risk assessment scores.

One way to secure HCE payments is to store the PAN in the mobile phone's secure hardware (e.g., processor chip, extended chip, etc., not the SE). Another approach is to develop the software protection capacity on the phone to affect the required level of security—e.g., creation of a Trusted Execution Environment (TEE), incorporation of cryptographic algorithms in the operating system software and/or cloud configurations, or combination of an HCE token with a transaction token. Most designs for HCE security assume a pairing with tokens, so that the true PAN does not reside on the mobile device.

6. Approaches to Managing the Tokenization Process[39]

There are several approaches to managing the tokenization process. One approach is for each issuer to manage its own tokenization process (and vault for managing the token issuance life-cycle), which requires the issuer to make significant changes to its internal systems. Another approach would allow

[38] With HCE, Beacon, or other options, the merchant only needs an authorization with a promise to pay from a trusted entity to complete the purchase transaction. The authorization may come from a cloud (or other virtual source) in a multitude of configurations that do *not* use the existing or evolving POS infrastructure.

[39] Arnfield, Robin. (2014). Mobile Banking and Payments Security: What Banks and Payment Service Providers Need to Know to Keep their Customers Safe. *Mobile Payments Today*.

issuers to select a third party token service provider, much like they outsource personalization functions today. A third option is a network-based tokenization process where the card networks create and manage the tokens/token vault for multiple issuers within a given payment network. The network approach does not require issuers or acquirers to change their internal systems for individual issuers.

7. Consumer Usability

Many industry stakeholders are using multi-factor authentication, registration of the mobile phone, and/or biometrics/fingerprinting to engage the consumer and improve cardholder identification and verification and overall transaction security. A key consideration is what is required to change consumer behavior. If the consumer links multiple wallets or solutions, and the tokenization schemes are not connected or interoperable, what will happen? How should differences between non-interoperable and fully updated systems be explained to the customer to avoid confusion or frustration? For example, newer systems display the last 4 digits of a card number on a receipt (printed or electronic) and may provide online payment confirmation. Do customers need to be trained to expect some variances on their receipts and changes to purchase confirmations? How much consumer education is required to explain the use of tokens for enhanced payment security and to build confidence? Do customers need to be aware that the industry is driving tokenization or is it simply enough that they have been advised in recent announcements, such as with the launch of Apple Pay? As with other features, any changes need to factor in consumer privacy.

8. Other Uses of Tokenized PAN

In addition to serving as an account identifier, some retailers, acquirers, and cardholders use the PAN for other purposes. The first 6 digits (BIN), are extensively used for routing in today's POS infrastructure—not only for open-loop (multi-issuer) systems, but increasingly for closed-loop alternatives as well (e.g., AmEx, Discover, private label, etc.). The PAN can also help recognize frequent shoppers, and a partial PAN (usually the last 4 digits) is printed on a receipt to aid consumers in reconciling their accounts.

In the trucking industry, the PAN prompts drivers to enter mileage and/or a driver ID when getting fuel. Drivers cannot purchase fuel without keying the middle nine digits of the PAN on the reader. While it might be helpful to separate these types of data elements from the PAN, PCI requires that certain components of the PAN be present to determine if it is a token. This creates questions about how much of the PAN can be used for everyday transaction management purposes and still protect the overall account.

A number of merchants encrypt the PAN when they first receive it at the swipe or order-entry stage. Tokenizing the PAN before sending it to the acquirer adds another layer of security. However, this is not a consistent practice yet. Some MPIW members would like to see a use case for a merchant with PAN present in addition to PAN not present included in industry tokenization standards. The EMVCo spec mainly addresses PAN not present.

9. Implications of Proprietary Tokenization Approaches

Proprietary tokenization approaches raise concerns related to portability for clients (whether merchants or issuers) and issues of safety and soundness for regulated institutions.

10. Other

Efficiency considerations such as transaction processing speed, redundancy, disaster recovery, etc. should be factored in to the development of tokenization approaches. Also, the practical application of tokenization schemes should not limit competition.

VI. Benefits of Payment Tokenization

While there are issues to be resolved, there are several key benefits of tokenization for payments, including:

- Use of properly-constructed tokens to reduce a merchant's PCI scope.
- Tokenization can limit the spread of cardholder data across the enterprise through good planning, design, and implementation.
- Tokenization significantly reduces the financial impact that can result from a data breach by removing value from the payments data. If the customer's payment credentials are tokenized and fraud occurs (i.e., the token is stolen), the customer is protected. As a result, sensitive data is less likely to be compromised if it is rendered useless to the fraudster. Devaluing the payment data also diminishes the incentive to attack processing environments.
- Tokens cannot be reversed back to their original values without access to the original "look-up" table that matches tokens to their original values.[40]
- Tokens can be formatted to maintain the same structure and data type as their original values.
- Issuers can turn off a token and reissue a new one within seconds if fraud is discovered.

[40] These tables are typically kept in a "hardened" database in a secure location inside a company's firewall.

- Tokenization will help get ahead of the anticipated shift in fraud from CP to CNP with the U.S. migration to EMV.

VII. Conclusions and Recommendations

The developments around tokenization should help to instill confidence in a payments environment challenged by more frequent data breaches. However, it is important to note that tokenization alone is not a panacea to the security challenges faced by the payments industry. Any approach to security must be layered in order to prevent future compromises. Both ASC X9 and PCI SSC aim to provide value by enhancing security as the industry moves forward. It is expected that TCH and EMVCo standards will become harmonized in the future. Companies are still evaluating the new tokenization models to understand impact their businesses. Many probably already use some type of tokenization scheme, paving the path for broader adoption.

In moving towards an interoperable and open industry standard for tokenization, several considerations have been noted that need to be addressed. One outcome from the June 2014 MPIW meeting was to create a Tokenization Subgroup to evaluate the different tokenization approaches and determine how industry stakeholders can coordinate efforts to achieve the optimal approach. The Subgroup's objective is to assess and document payment industry stakeholder perspectives on challenges and opportunities surrounding payment tokenization initiatives, to identify potential gaps, and to recommend possible solutions. The final product will be an analysis of the state of tokenization in the payments industry and the role tokenization can play in securing the mobile and digital payments ecosystem. It will include a common set of definitions and help to educate the industry on the similarities and differences between the different token use cases. The latter point addresses growing concern over the lack of precision and understanding of what is meant with respect to tokenization "specifics" (e.g., a need to evaluate the advantages and disadvantages to both static and dynamic types of tokens and to understand what is necessary to move the payments ecosystem toward support of dynamic tokens).

Finally, in order to achieve interoperability, all of the use cases need to be evaluated on an end-to-end basis, which can best be accomplished through a multi-stakeholder assessment. This end-to-end perspective will dovetail with the evaluation and incorporation of encryption as an added component of transaction security.