Secure Remote Payment Council (SRPc)

Tokenization: Risks to Consider - Position Paper #3

August 13, 2015

The SRPc's starting position for this white paper began with a discussion on the potential of token vaults as honeypots and the role of the token service provider (TSP) as the safe keeper of the data contained in these vaults. Currently there appears to be a limited set of TSPs that can play this role, which includes the Global Card Brands and a few others, and there are outstanding questions about the level of security used to protect cardholder data through the tokenization process.

Is the additional security provided by the use of TSPs outweighed by the additional risk introduced by the existence of token vaults, i.e., as honeypots? To understand the underlying issues of the question, we must provide a background discussion on tokenization and the industry standards for implementation.

Tokenization is defined as a process that replaces the Primary Account Number (PAN) and expiration date found on a payment card with a surrogate value or payment "token" and token expiration date. The PANs and their corresponding tokens are stored in a token vault which is a database designed to securely house cardholder information. The tokens and PANs are stored and accessible to external services and applications through the use of an API. Ideally, the storage and management of the vault will be consistent and based on industry best practices as recommended by NIST or PCI, for example. The TSP manages the interaction within the token vault. The token vault maintains the ability to encrypt/decrypt a card number and/or match it to its surrogate PAN and expiration date.

The Payment Card Industry Security Standards Council offered a tokenization primer in its 2011 document, PCI DSS Tokenization Guidelines and an update in 2015 entitled: Tokenization Product Security Guidelines. In March 2014 EMVCo LLC released its first payment tokenization specification entitled: EMV® Payment Tokenisation Specification – Technical Framework. The PCI guideline is directed at Acquirer/Processors and Service Providers whereas the EMVCo specification is directed more towards the Networks and Card Issuers. Both have similar tokenization constructs.

The April 2015 PCI document "Tokenization Product Security Guidelines" appears to supersede the "Information Supplement: PCI DSS Tokenization Guidelines." In the 2011 document, PCI stated: "In a tokenization system, the card data vault (or "data vault") is the central repository for PANs and tokens, and is used by the token-mapping process. Whenever data exists, it must be managed and protected in accordance with PCI DSS requirements. Because it contains PANs as well as tokens, the data vault often presents the most attractive target for attackers. Compromise of the data vault could potentially result in the compromise of the entire tokenization system, and additional security controls above and beyond those required in PCI DSS may be warranted."[1]

In the 2015 document, suggested security practices for the card data vault are outlined without any mention of the relative risk of card data vaults compared to other tokenization methods. However, certain specific requirements are presented detailing the normative method to secure PANs and tokens in a variety of contexts. It is recommended that future versions of PCI's token vault-only approach provide comparative solutions risk assessment and consistent guidance.

[1]PCI Data Security Standard DSS V.2, Information Supplement: Tokenization Guidelines, August 2011, p. 7

Concerns about Proprietary Specifications

EMVCo is setting a proprietary standard that is being implemented at the Network (i.e., Visa and MasterCard) level, not the Processor level. Since the Global Card Brands, operating under the auspices of EMVCo, own the specification, they have significant influence on the way that tokenization is implemented and thus how the industry may move forward. For example, the EMVCo technical framework rules prescribes a centralized approach for tokenization where the tokenized PANs are assigned by the Card Brands to a token requester (e.g., wallet provider, Merchant, etc.) for use within a specified period of time.

They have mandated that the tokenized PAN utilize a token BIN (necessitating new data elements be added to the ISO 8583 message specification) which will route to the TSP who will then map it to the true BIN for presentment to the Issuer.

EMVCo is regarded as a standard setting body but it has moved forward as a de facto standard rather than a consensus standard. The SRPc is concerned that the current standards process precludes all stakeholders from participating except with the proprietary standard set forth by the Card Brands. A closed environment inhibits competitive and innovative solutions.

Who can be Token Service Providers?

EMVCo is also in the process of establishing the technical framework for the token service providers, allowing the first four Global Card Brands to join.[2] Others must apply and at this time only a small number of large banks are approved to provide token vault services. This means that today's implementation of tokenization and the ability to perform tokenization services is supported only by the Global Card Brands thereby creating a competitive advantage for them and requiring other unaffiliated Networks to utilize their services because of the proprietary and limited availability of TSPs.

In order for tokenization to maintain flexibility and choice and be Durbin compliant, the Issuer must support at least two unaffiliated network routes for authorization. Since the Global Card Brands are the only debit card token service providers, all the other Debit Networks must submit "call-out" transactions to the Global Card Brands to translate the tokens to real PANs. To accept these tokenized PAN transactions, the Debit Networks must certify to the Global Card Brands in order to translate the tokens to real PANs. This adds an extra step to the authorization process and allows competitors to see a record of every transaction that occurs on alternate Networks.

Furthermore, industry stakeholders have concerns that the development of these functional requirements to enable "call-outs" for alternative Networks will not be a priority, thereby entrenching the GlobalCard Brands as the only token service provider for financial institutions. Once rooted in a solution with a partner, it is much more difficult for a financial institution to deconvert and switch to another partner due to the heavy impact on resources and IT priorities.

Apple Pay Tokenization

Since the primary implementation of a global Brand based tokenization service in the market today is Apple Pay, a closer examination of how this works may help to elucidate the honeypot potential.

Apple Pay leverages the security benefits of EMV® contactless for card present transactions as well as the benefits of tokenization for card present and card-not-present, using similar cryptography. Apple Pay utilizes a static token established by the TSP at the time of card enrollment. The initial enrollment or provisioning process for Apple Pay occurs on the iPhone. The consumer either takes a picture of his card or enters it manually. The TSP is responsible for preparing the information that will be sent to the Secure Element, a device-based

[2] Visa, MasterCard, and American Express solutions are currently deployed, and Discover is scheduled for Fall 2015.

component embedded in the iPhone. A fabricated magnetic stripe is stored on the phone; this is not the actual magnetic stripe data from the “real" card.

This fabricated magnetic stripe is used with the PIN offset at the host to support debit transactions. At the time of purchase, the static PAN token is combined with a generated cryptogram from the Secure Element in place of the card's static CVV/CVC. This cryptogram uniquely identifies the device that created the token, and is comprised of encrypted data from the token, the device and transaction information such as the Merchant ID and amount being transacted.

At a retail POS, the transaction is considered a card present transaction which utilizes a fabricated magnetic track to send the transaction to the Network for authorization without any actual Issuer discretionary data. This forces Issuers to move to an environment supporting host-based PINs (if utilizing a PIN debit transaction) in order to play in the tokenization ecosystem.

The cryptogram and PIN block on an authorization request are not being tokenized. Instead, they are being passed in the transaction along with the surrogate PAN token for de-tokenization by the TSP and authorization by the Issuer. The TSP takes this token and converts it to the real PAN. Where this real PAN is stored is the actual honeypot. Millions of PANs in one place is the ultimate challenge for a hacker!

EMV® Tokenization Specifications are Issuer and Global Card Brand Biased

The current implementation of tokenization is highly proprietary and, as such, produces systemic impacts that increase the cost and complexity of implementation for all stakeholders. Here are some problems with the current EMV® tokenization specifications:

Dependence on the PAN – The EMVCo framework is dependent on the use of the existing PAN field to create tokens, and thus future expansion of the token is limited to the existing 13-19 digit PAN structure. EMVCo tokenization schemes are using existing BINs/IINs, creating a new set of token BIN ranges that are effectively controlled by the Global Card Brands. Obviously, this situation favors those that administer the BINs and hampers the emergence of competing TSPs.

Unique or exclusionary implementations of tokenization are not good for the industry. Rather, the industry should be adopting the ANSI and ISO standards for protection of PAN data, like the standards making process the ANSI X9.119 Working Group is using.

Missing Business Case Tokens – Merchants, acquirers and processors need a variety of tokens to support their business activities. These tokens could have different attributes depending on their use. For example, a CRM token is useful to greet a customer, track patterns and suggest new products. It doesn’t need to be reversible. Fraud analysis and recurring payments often need a token that can be reversed to display the PAN. Voids, refunds and chargebacks should always have a transaction token, totally unrelated to the PAN that can be used to amend a transaction without having to request or know the PAN. Unique transaction ID tokens, unrelated to the PAN, are the safest tokens to use, but they do not fit every business need. They should be used wherever possible because any time a token can be associated or reversed to expose a PAN, the honeypot is sweetened.

The EMVCo token is not a one-size-fits-all use case token. It’s a static token, specific to a merchant, for a finite period, that can only be detokenized by a single party and that does not satisfy the business needs of many payment stakeholders.

Requirement to Support New Numbers – To address the above token usage issue, EMVCo has created a new number called the Payment Account Reference (PAR) which needs to be supported in the message structure. The PAR is an alphanumeric replacement for the PAN in the Internet ecosystem. This new field is being introduced to allow Merchants to tie transactions back to a single payment account since there can be multiple tokens related to one PAN. Further complicating the situation, each wallet provider will have a different token in the EMVCo framework.

Support for these new numbers is no more than a work around to create a token based on the PAN. The SRPc argues that, if a new field is required, why not deliver a field that can contain a token that does not look like a PAN and is not controlled by the Card Brands?

Proprietary Interfaces - There are no standard interface definitions in the EMVCo specifications for either Issuers or Merchants to interface to the TSP. The interfaces supported are proprietary in nature, thus limiting participation to the current tokenization service providers.

Lack of Support for PIN Offset - In the current tokenization scheme, a tokenized PAN is being routed rather than the real PAN. This means the Networks are not receiving the original track data which contains the PIN offset or verification value. Instead they receive a fabricated magnetic stripe where the PIN offset cannot be captured. Thus, the link between the real PAN and the PIN is broken.

This is a problem if the Issuer has a PIN offset on the magnetic stripe because there is no way that the token service provider at the Network level knows what the PIN offset is. Issuers who put a PIN offset on the magnetic stripe will not be able to use this form of tokenization because it will not work for transactions where the PIN is prompted. If the PIN cannot be read, the PIN debit customer's transaction will be declined.

While many Issuers have moved to support host-based PINs to enable customer PIN selection, there are a significant number of Issuers that still issue magnetic stripe cards with a PIN offset. These Issuers will face major customer service challenges as implementation of these EMVCo tokenization schemes unfold.

CALL TO ACTION

The SRPc acknowledges that provisioning tokens for cards on file is a worthy endeavor, but the SRPc still believes that concerns about proprietary token vaults as honeypots are valid. The honeypots will become only more attractive when populated with PANs related to cards on file. A massive exposure of PANs in a token vault could have catastrophic ramifications to the payment industry. For our formidable, organized adversaries, the concentration of such valuable data will prove irresistible, as has been demonstrated in the recent past.

More Token Service Providers

More token service providers are needed in the ecosystem. Issuers, EFT Processors and Core Processors are equally well positioned to be TSPs because they see all the transactions. The construct for a token service provider must be attainable by any party with a secure and auditable solution.

The limited number of token service providers creates an attractive target for hackers because a central repository or honeypot creates the potential for a single point of failure. If the token service provider role were expanded to include other stakeholders, then more token vaults would be created. This may increase potential for a honeypot compromise, but fewer tokens will be exposed should a breach occur, thus mitigating the impact of any single compromise.

End-to-End Solution for Tokenization

The SRPc believes that the lack of an end-to-end solution for tokenization is a fundamental requirements flaw. Industry best practices require an end-to-end solution for tokenization which must include Issuers, EFT Processors and Core Processors as token service providers.

In the current tokenization schemes, the token vault does not leverage a host security module or industry accepted cryptography to create the token. Thus the vulnerability lies in that there is a single location for all token to PAN mappings and if the token vault is compromised so too are the PANs in the vault.

In an effort to ensure security in a card-not-present environment, the industry should be moving forward to protect the PAN in the mobile and Internet environment in accordance with acceptable or approved schemes

similar to what the industry uses for PIN encryption. Each PIN is sent as a token encrypted using ANSI standards. The strength lies in the combination of keys, encryption, and hardware security modules to do the encryption and decryption services plus standardized values passed between the different Networks and Processors. The importance of a tokenization scheme is to protect the PAN from end-to-end. We should not care how it is protected but the solutions should leverage industry standards allowing for choice, innovation, and flexibility (e.g., encrypted in AES, etc.).

Furthermore, tokenization will be more secure if the process entails de-tokenizing and re-tokenizing at each stage in the payment process, until ultimately reaching the Issuer that has access to the original PAN. This method of tokenization would mirror the successful approach currently used for the end-to-end protection of PINs, would ensure security over the entire payment flow and require far less effort and expense on the part of merchants, acquirers and processors than an implementation of EMVco tokenization.

Adopt a Federated Approach

The principle issue here is *choice*. If the Global Card Brands control the tokens and their usage, they will dictate the token schemes including the types of tokens and the associated response codes. The Global Card Brands are making the decisions on behalf of the industry about how tokenization is going to work. A honeypot is a good example of what happens when all market players are not involved in the technical process, particularly as described by the EMVCo standard.

Open standards that apply to all stakeholders must be an industry imperative. The Federal Reserve of Kansas City recently published The Economics of Retail Payment Security in which the authors address the need for open standards to level the playing field for market competition.

> "Profit-oriented firms may compete for the market by employing proprietary security standards rather than participating in open, consensus-based standards development. Although proprietary standard may support incentives of firms to innovate, they may reduce interoperability." [3]

On the subject of standards of tokenization, the authors further comment that "although tokenization uses open standards, due to the proprietary environment in which the standards were developed, global card brands may have a competitive advantage at least in offering vault services compared with U.S. domestic card networks or processors." [4]

One might question why EMVCo is involved in the development of tokenization standards since this is not a part of EMVCo's historic mission to promulgate a chip card payment standard. Alternatively, tokenization focuses on protection of card data. If EMVCo is expanding its charter to include the development of standards for tokenization, it should be developing open standards that apply to all stakeholders.

The SRPc recommends that EMVCo's process for developing tokenization standards be modeled like the ANSI and ISO standards organizations where all participants get an equal vote. As it currently stands, other organizations can attend EMVCo meetings and provide suggestions and comments, but ultimately have no say in the final specifications and thus no voice in the outcome. If EMVCo were to voluntarily remodel itself like ANSI and ISO, the recommended federated approach would be possible.

Furthermore, the SRPc recommends a federated approach for encryption services using public standards and strong encryption algorithms. The SRPc would like to see regulation for tokenization such that tokenization schemes could be validated to meet a generally accepted industry standard and approved for widespread usage.

[3] https://www.kansascityfed.org/publications/research/pscp-2012
[4] Ibid.

Should the industry succeed in the endeavors outlined above, SRPc additionally recommends that a task force be assembled to develop a migration plan that considers the needs of all stakeholders in the payment industry. Without this final commercialization effort, inertia and other priorities can doom the best of intentions.

Industry best practices should consider the needs of all stakeholders, not just a subset of them. Industry stakeholders must sit at the table and provide their input on the tokenization infrastructure to ensure that all stakeholders are making the decisions on the specifications. Any stakeholder that wants to create and adopt a tokenization scheme should be able to, so as long as the scheme meets industry best practices, is auditable as compliant and deemed safe.

New Security Approaches

It is important to understand what is happening in the marketplace. Tokenization schemes being presented today are just further entrenching the existing payment system infrastructure. Format Preserving Encryption, which tokenizes the middle digits of the card number, merely reinforces the weaknesses in the existing infrastructure and further bolsters the incumbents. Patching schemes based on bit mapping, ISO 8583 message formatting and the associated operating rules and business relationships have their limitations. Moreover, current solutions focus on protecting static data. Fraudsters may be able to gather sufficient transaction data to hack the algorithm or compromise the key in the online environment, or may be able to bypass the Secure Element in a rooted mobile phone. Dynamic data adds an extra layer of protection and a disincentive to fraud.

Unfortunately, the current proprietary tokenization process does not leverage a hardware encryption algorithm to generate tokens. The token vaults contain the look up pairs that associates a token with an encrypted PAN which requires key management. Despite this encryption, the concentration of encrypted PANs in the token vault makes it an exceptionally attractive target to hackers. This target would not exist if the tokens being generated at the time of provisioning and authorization were based on a hardware encryption algorithm such as AES or Triple DES. A distributed token vault solution which leverages open industry hardware encryption standards and algorithms reduces complexity, costs, improves scalability, and ensures a robust defensible security architecture that can change and adapt as encryption algorithms and routines improve over time.

About the Secure Remote Payment Council

The Secure Remote Payment (SRPc) is a nonprofit, inter-industry trade association that supports the growth, development and market adoption of debit based internet eCommerce and mobile channel payment methods that meet or exceed the security standards for pinned based card present payments. It will accomplish this by encouraging and supporting those activities that accelerate the implementation, adoption and promotion of these payments. The SRPc's members include merchants, financial institutions, merchant processors, issuer processors, payment brand companies, payments authentication hardware providers, payments authentication software providers and payments consultants. This document does not necessarily express the views and opinions of every member of the SRPc. For additional information, visit www.SecureRemotePaymentCouncil.org.