Tokenization and Protection of Card Data for Online Payments

An SPA Position

15th May 2014

1. Introduction

Tokenization in payments has been around for years.

However, in recent months tokenization has once again become a buzzword within the financial industry which is looking to add tokens to the list of alternative payment methods using card data (cloud-based accounts, mobile wallets, Google HCE).

The SPA considers that what's different this time round is the standardization efforts taking place for online payments using tokens (for example, EMVCo, US Clearing House and new ANSI X.9 standard, PCI-DSS) and the fact that these efforts are being aligned with upcoming legal frameworks for e-commerce, m-commerce and data protection in several regions of the world.

However, it is not always clear how these new payment methods are positioned with respect to existing card payments; in other words, whether these are complementary or a replacement. Are these new payment methods and technical drivers bound to make profound changes in the way we do payments? The SPA's opinion is that payment innovation breakthrough is only possible when both trust and convenience are achieved. Yet trust and convenience must be compatible with a business case for the issuers of new payment methods. Finally, the terminology used for tokens is not always consistent, which in turn contributes to the generation of additional confusion. For instance, what do we really mean by "tokens"?

In this paper, the SPA discusses the business and technical drivers for tokenization, provides initial feedback on the EMVCo Draft Framework for tokenization, and suggests ways to develop secure and interoperable online payments with a great user experience.

2. What kind of problems are tokens trying to solve?

2.1. Securing online payments

Two key security objectives of card based payments are to eliminate card fraud and avoid the repudiation of legitimate transactions. In face-to-face payments this is achieved through three different, yet interrelated, authentication stages:

1. Customer authentication
2. Card payment data authentication

3. Generation of a certificate for an authorized transaction.

Steps (1) + (2) and the corresponding risk analysis lead to a decision by the card issuer to authorize or reject the payment. If the payment is authorized, then the card/secure element generates a transaction certificate to be delivered to the merchant for the payment to be cleared and settled (3).

The implementation of this authentication framework in face-to-face transactions has proved highly efficient in achieving the two central security objectives highlighted above – customer authentication and card payment data authentication. The payments industry has therefore tried to extend the benefits of this experience in the context of online acceptance, where fraud is increasing.

Within the constraints of the need to maintain a good user experience, achieve cost-efficiencies and ensure liability issues are shared, the main challenges to secure online payments can be summarized in the following six 'how to' requirements:

- make sure that the customer connects to a legitimate merchant
- authenticate the customer
- transfer in a secure way card data to the merchant
- protect the customer's card data at rest in merchant's computers
- protect card data in transit over networks facilities
- minimize chargeback risks for merchants

This paper assesses to what extent tokenization is likely to provide a cost-effective solution to the above points in order to secure remote payments. At first sight, the ability to process transactions using non-sensitive data, strong access-control systems, and the creation of a trusted entity able to authenticate, verify and coordinate the communication exchanges, all appear as central components for the design of a secure architecture using tokens.

2.2. Defining tokens

A token is a randomly generated surrogate of the Primary Account Number (PAN) that is used to execute the transaction, instead of the original plaintext card data (for example, the PAN). Tokens designed properly do not provide information on the original PAN and are therefore useless for fraudsters. Matches between the tokens and the original PAN are exclusively maintained by a Token Service Provider, a trusted third-party according to EMVCo.

By processing tokens, instead of real card data, the merchant is no longer storing highly sensitive data that is a target for attackers. Thus, when the token is received, the merchant can proceed to delete the original card data sent by the customer and use only the token to identify and settle the transaction. As tokens are limited in scope and potentially in time (duration) and credit risk, the potential liability of merchants is greatly reduced.

Tokenization eliminates the need for online retailers, e-commerce web sites and operators of digital wallets to store sensitive payment card data on their systems. The high security constraints for the certification of the merchant's processing facilities when they store, process, and transmit cardholder data can be relaxed. From the cardholder perspective, the use of tokens avoids unauthorized access to his/her card data, both at rest and in transit. That's a good point.

To summarize: tokenization certainly helps make payment data less interesting for criminals. It remains a fact, however, that a tokenization infrastructure must be built, certified and plugged into the already complex acquisition chain for card payment processing. This inevitably adds extra complexity for new incomers offering a tokenization service. Taking into account that issuers of digital wallets are also part of the token value chain, the business case and revenue share models are so far unclear.

3. The EMVCo standard on tokenization

3.1. Standardization and regulatory ecosystem

EMVCo has recently drafted a tokenization standard for securing online payments using tokens via consumer controlled devices (such as mobile devices and personal computers). The SPA recognizes the need for a worldwide standard to improve the security of online payments. Remarkable data breaches and resulting fraud have become international issues. EMVCo is taking the lead in ensuring cooperation and coordination at global level on tokenization, and that's good news.

Standard tokenization schemes are only one of the potential solutions for securing e-commerce payments. Since the mid-1990s, protocols such as SET have been proposed and later on 3D-secure schemes have been deployed, offering different levels of security in terms of user authentication.

At present online payment fraud is perceived as a major risk among national and regional law enforcement agencies and governments, yet there may be divergence on the recommended technical solutions they approve to prevent fraud.

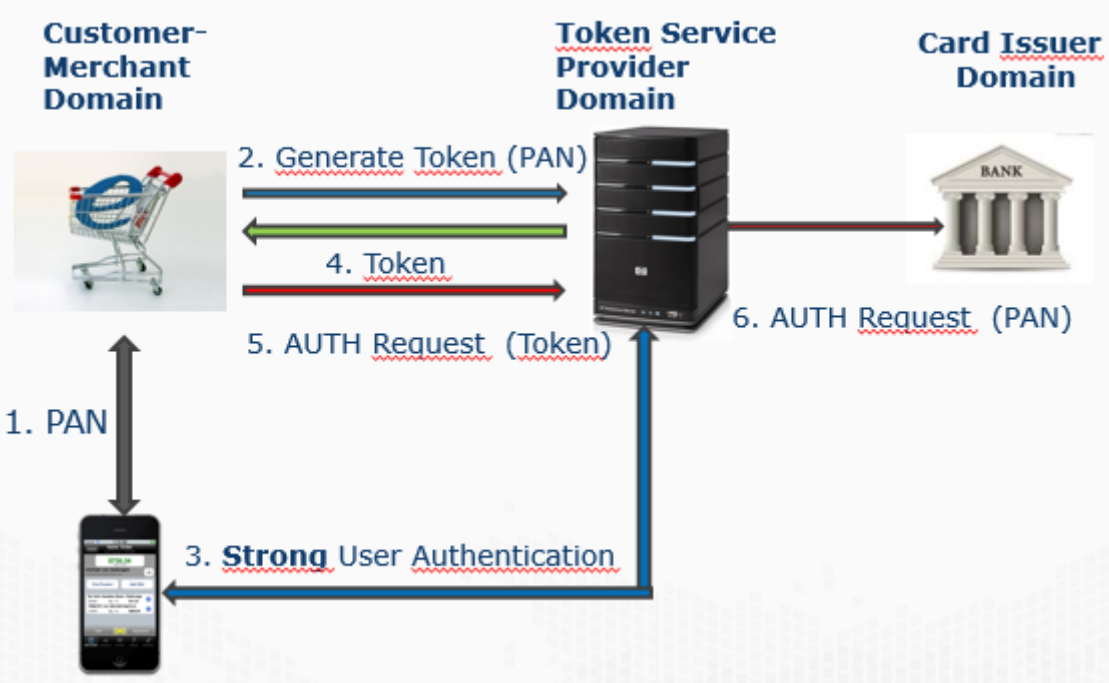
The reality is that the payments industry is in a cycle of rapid rulemaking across multiple jurisdictions and, in some of those jurisdictions, across multiple regulators. The aggregated impact of this (for example, data protection, KYC, interchange fees, security requirements) represents a very significant concern for the industry. The automatic support of financial authorities to proprietary specifications should not be taken for granted. EMVCo is well aware of this and in their draft they recognize that "governing requirements supersede any industry standard".

Not surprisingly, the Clearing House initiative and the ANSI X9 standards body are working on developing tokenization standards for the US payment industry. X9 is focused on developing standard terminology for tokenization and the central processes for generating and validating payment tokens. But nothing prevents X9 from proposing an ISO fast-track for the international adoption of the original US standard.

3.2. Positioning players in the token value chain

The EMVCo draft standard relies on a series of roles played by entities, which may be either traditional card payment system players or newcomers. A central role is played by the Token Service Provider (TSP) which provides the processing backbone for token system users (merchants and cardholders). The TSP is actually a role tailored to individual payment schemes, because the processing of the token as specified requires interoperability between the TSP and the international scheme processing system. In a consistent way with this approach, the specification recognizes that the TSP role might be also played by a card issuer.

This central role of the TSP has several interesting consequences, from both a business and security assurance perspective.



1. Since tokenization is done in a central way, only a small portion of the processing network knows how to generate and reverse a token.
2. The TSP has a privileged position. It is the only role which directly interfaces with all stakeholders of the system; more pertinently, the TSP may decide on its own policy and business practices for enrolling Token Requesters.
3. The TSP has the central responsibility to manage the "Vault" enabling de-tokenization. The security of the Vault is key to the security of the Token System. Vault management is going to generate a huge amount of information about consumption patterns by the cardholders.
4. A TSP may launch its own tokenization system, using the EMVCo specification for interoperability and security, by setting governance rules to which independently Token Requesters, Card Issuers and Trusted Service Providers may adhere.
5. EMVCo acts as the registration authority for TSPs, so ultimately they keep the control of any tokenization system endorsing the specification.
6. To facilitate the connection of the merchant (Token Requester) to any TSP (e.g., one by a major card brand), EMVCo sets forth an API of Token-related services. Any merchant acting as a Token Requester must support the API.
7. EMVCo recognizes, however, that the implementation of the API may then be outsourced by a merchant (or merchant consortium) to a third party ("the aggregator"). But the merchant will remain the ultimate token requester and must therefore be registered by the TSP.
8. The tokenization scheme, as specified, mirrors somehow the EMVCo security architecture for card data authentication. The Token may be perceived as a certificate signed by the TSP with an expiry date. This signature of the Token may be verified by the Token Requester (the merchant) with a

TSP certificate (proving that the TSP is authorized to act as a Token Issuer) which in turn is signed by a Scheme.

3.3. Technology choices

3.3.1. At processing level, make it easy for interoperability

The EMVCo architecture for interoperability relies to a maximum extent on the existing payment systems protocols for authorization, clearing and exception processing. These protocols are all based on the ISO 8583 standard, but schemes have often profiled them in not-interoperable implementations. Whilst the protocols will remain as they are, common Data Elements have been defined by EMVCo to support the Token and Token-related data.

On the other hand, the tokenization follows the classical "Three Domain" interoperability model used for instance by 3D-secure solutions, with the Issuer Domain (the TSP, which may be a Card Issuer), the Merchant-Acquirer Domain (the acquirers will process payment by tokens as they do with card payments) and the Interoperability Domain (based on a new API for the Token Request –TSP communication + the support by the acquirer of a set of new data elements related to tokens).

To summarize, EMVCo proposes an architecture for token services that is:

1. Backward compatible with existing systems, provided that a minimum extension of the processing functionalities is supported.
2. The standard data elements required for token management are mapped in existing protocol data units.

3.3.2. Token generation, storage and verification

A Token can only be issued to a registered Token Requestor. At token issuance, EMVCo introduces a concept of "Token Assurance Level". This Assurance Level is negotiated between the Token Requester and the TSP and, amongst other considerations, is dependent on the requested Token Location (where the Token will be stored) and the Token Domain (which channel will be used for the token transaction – for example, NFC).

The Token Assurance Level is implemented by selecting a set of Token Identification and Verification Methods (ID&V) as set forth in the EMVCo specification, ch6. The ID&V are security controls under the responsibility of the TSP. It requires an assessment of the risk associated with a Token Request on the grounds of the information provided by the Token Requester. If appropriate, the TSP requests the card issuer to authenticate the cardholder. The EMVCo specification provides examples of authentication methods without mandating any of them. The only exception is the strong recommendation not to use static authentication data. This is in line with the European Central Bank's recommendations for e-commerce payments.

Other than the above pre-issuance security controls, the EMVCo specification does not provide information on the security properties of the Token.

3.3.3. SPA members' technology for tokenization

Token provisioning may be implemented using TSM. The Token Requester is typically a retailer of a cardholder. The cardholder may then decide to store the Tokens in a Secure Element or a TEE (other options include remote server or cloud based storage) for later use.

SPA considers that there is a case for the generation of tokens using a token application stored in a secure element. The token is generated from the PAN and auxiliary unique information that might be stored in the token application in the secure element. The secure element would, in that case, transmit the token and an authenticator to the retailer to generate and send a payment authorization request to the token application issuer. That way, the retailer should not be storing cardholder confidential information and the payer would only be transmitting dynamic information not useful for fraud purposes.

NOTE: in the payments industry usually two different forms of tokens are referred to, namely (1) the token as an authentication mechanism and (2) the token as an object that can be mapped to your card or bank account. In a consistent way with our above description, EMVCo differentiates between "The Token" and "Token Data". Token Data are generated by the TSP as well, but are intended to secure token transactions with an authenticator.

4. SPA committed to the financial industry for a secure online payment framework

Card-based technology, using different form factors, has proved to be the undisputed best security/cost approach for retail payments. The SPA is fully committed to supporting the financial industry in addressing the security challenges raised by innovative online payment methods. The SPA will put every effort in getting the EMVCo tokenization standard-setting process right. In particular, the security objectives for the tokenization framework should be clearly formulated. This will help to define second step concrete implementation aspects, such as:

1. Where the token may be generated. If several options are considered, the corresponding pros and cons, based on different business models, will be clarified.
2. Which entities in the framework will secure and verify the token.
3. Which methods of authenticating the user are acceptable before issuing a token.
4. Which security properties should be provided to the token.
5. What structure and coding will provide the security properties to be assigned to the token.
6. Which standard lifecycle will be specified for the token and what are the security implications of this.
7. Which metadata are needed to help improve fraud detection.
8. Whether or not common protocols for token request, generation, transport and lifecycle management are suitable.

Due to the hard competition context, the SPA believes that implementation aspects should be considered soon. At present, it is unclear whether tokens will be used exclusively for e-and m-commerce transactions, for cardholder present transactions, or for both. Depending on the use case, the points 1-8 outlined above may need to be adapted.

The SPA also considers that, at present, a clear picture outlining the benefits of the tokenization framework compared with existing online payment solutions and alternatives is lacking. Similar to the EMVCo Next Generation program, a document setting forth the business requirements for tokenization should be produced. In particular, migration considerations should be addressed. A possible way moving forward is to upgrade the EMVCo Next Generation document to include online payments, which were excluded from the original scope.

On the other hand, SPA members consider that market fragmentation should be avoided. In this respect, we encourage EMVCo to coordinate with other on-going standardization efforts (ANSI X9, EPC-CSG, PCI e-Commerce). Because of the growing driving role being adopted by payment regulators, the integration of the constraints imposed by regional legal frameworks should be considered in priority.