Is there a case for the regulation of Tokenization services?

An SPA Position

May 2016

1. Introduction

The initiation of a card payment first requires the transmission of the card's Payment Account Number (PAN) to the payment acceptor; this PAN is then automatically retrieved from the card in a physical terminal or manually entered by the cardholder in the website of an online merchant. However, the increasing use of cards has boosted the proliferation of PAN databases which, if compromised, will result in increased fraud. Indeed, the European Central Bank's recent fourth report on card fraud (2015) confirms that (1) the level of fraud for Card Not Present (CNP) has grown steadily; and (2) that this level is above the total increase in the number of CNP transactions. To mitigate this fraud risk, EMVCo recommends the use of a payment token for vulnerable payment contexts: typically, online payments or mobile payment using Host Card Emulation (HCE). A payment token is a card PAN surrogate; it replaces the card payment PAN and enables the transaction to be processed according to card payment system rules.

Tokenization, the process for the issuance and management of payment tokens in card transactions, creates a new role in the processing chain: The Token Service Provider (TSP). Upon request, the TSP creates a Token associated to a PAN and records the freshly created peer (PAN Token) and metadata in a secure database called "the Vault"; the Vault is the only location where de-tokenization of the transaction may take place in order to generate the authorization request. The TSP either directly operates or outsources management of the Vault.

The Eurosystem has called for the development of a framework for the interoperable processing of card payments. The technical interoperability of card processors and card schemes using European standards is a central objective for SEPA. As tokenization will become part of the payment process, integration of tokenization-related infrastructures must be respectful of (1) this generic interoperability principle and, (2) the separation of the processor and scheme activities according to Article 7 of the Interchange Fee Regulation (2015).

The migration towards tokenized card transactions does, however, raise a number of interesting issues for financial regulators in relation to the provision of tokenization services; issues that this paper discusses. This topic is not new, during the Money 2020 conference held in Las Vegas in 2014, the regulation of tokenization in US was extensively debated – but discussions were inconclusive.

For the purposes of this paper, the term "regulation" is being considered in the context of recommendations that might promote the existence of an efficient and sustainable market for token-related services, with adequate incentives for innovation and investment. These recommendations might eventually be incorporated into a new regulatory technical standard, or implemented as an extension to those already drafted by the European Banking Authority (EBA). With this respect the SPA outlines that the EBA Consultation paper for a Draft Regulatory Technical Standard on the

separation of payment card schemes and processing entities which exclusively addresses accounting, organization and decision-making processes, not technical content.

2. Tokenization standards

Tokenization is a good case to analyze the relationships in the retail payment market between innovation, trust, regulation and standards – despite the fact that token technology is not exactly new. The initial PCI Tokenization specification was released almost 20 years ago, but PCI tokens were not designed to replace the PAN generated for payment transactions. Instead, PCI tokens were designed as an identifier to keep track of transactions for commercial purposes once the payment had been made. In 2014, however, EMVCo published its first version of a new Tokenization Framework for payment tokens. Therefore both PCI and EMVCo approaches complement each other in protecting the customer.

Because payment tokens used in different payment contexts (a smartphone, a card, a wearable) may originate from the same PAN, there is a business need for the merchant to know that those tokens actually came from the same customer. EMVCo has provided an elegant solution to this problem with the specification of a data object specific to tokenized transactions; this is known as the PAR (Payment Account Reference). The price to pay for the merchant to get rid of PAN storage is the acceptance of Tokens and their associated PAR, and possibly also the PCI token in addition to its role as a Token Requestor. The PAR has been standardized by EMVCo in a specification bulletin.

Almost simultaneously, and after a public consultation, PCI-SSC has also released a Set of Requirements for Token Service Providers for use with PCI DSS v3.1. It's worth noting that these requirements apply exclusively to EMVCo payment tokens, not to PCI ones. This new PCI specification, along with the updated version of the EMVCo Tokenization Framework (including the PAR bulletin), should provide a robust core for the implementation of tokenized systems.

In addition to these industry specifications, two other open standardization initiatives are under way:

1. ISO TC68 RMG has published a set of standard ISO 20022 messages for use with tokenized transactions. These standardized messages convey the token-related information to be used by processors and provide interoperability for the exchange of data, as set out in the EMVCo framework implementations.

2. ANSI x9 is an initiative led by big US retailers, among others, and is aimed at developing open generalized standards which apply to Token Service Providers, so that other entities besides EMVCo are eligible to provide competitive services.

Finally, the European Card Stakeholders Group (ECSG) has initiated workings in the specification of functional and security requirements for tokenization, and has released a taxonomy with the different types of tokens available. The ECSG ensures a democratic representation of all the stakeholders of the card payment industry. This work has currently halted, awaiting publication of the new version of the EMVCo Tokenization Framework that should inspire the next steps forward. The objective remains to avoid unnecessary duplication of effort, provided that fair access-to-market conditions are met.

3. The case for regulation

In theory, regulation in the financial industry usually serves two primary objectives: ensuring a level playing field to enable competition; and enhancing security to reduce fraud and protect the consumer in order to facilitate adoption of the regulated services. "Fair" market conditions, however, remains, an ambiguous term and many actors don't believe in the ability of regulation to prompt innovation, but rather the opposite. Yet this opinion is also disputable:

1. New market entrants have to capture market share and existing players need to defend their existing positions – by innovating.
2. Regulation pushes for stronger security mechanisms to protect the freedom of choice for the consumer in regard to new payment devices.
3. Compliance with regulation brings about new trade-offs in terms of user experience, security and data protection.

Regulations are first and foremost largely legal texts that give little detail in relation to technical implementations and typically try to be agnostic from a technology perspective The payments industry, however, has expressed the need for further clarifications, for product and solution development purposes. For the sake of PSD2 and the Interchange Fee Regulation (IFR) implementations, the European Banking Authority (EBA) has decided to publish a limited number of regulatory technical standards (RTS) in 2016.

Innovative payment solutions, regardless of whether these are based on cards or other payment instruments, will have an impact on consumer payment behaviors – provided that the user experience is good. As a minimum, payment tokens must be secure, easy to use, universally accepted and designed according to well-identified use cases. Furthermore, the general acceptance condition requires technical standards for interoperability. Whether or not the payment regulatory authorities should drive the standardization effort is another debate. It is true that in cyberspace, any government intervention on how communication between computing systems is organized is considered an anathema. But it is also certain that today's regulatory authorities are more proactive in standardization efforts than in the past, and that seems to be a global trend.

The usual solution for this type of conundrum is a standardization process that is open to all stakeholders through a standards-setting body, with regulators acting as active observers. As described above, EMVCo has already taken the initiative to develop an interoperability framework for payment tokens that is likely to become a de-facto industry standard. For this reason, it is important to understand whether or not the EMVCo specification promotes and facilitates a fair competition field, or if it is a scheme-centric framework. If the latter is the case, an alternative could be the development of an open regulatory technical standard (RTS) applying to Token Service Providers (TSP). This RTS would keep the conceptual principles and functional roles proposed by EMVCo, but would aim to ensure that market players, other than the schemes, may compete as becoming a TSP for card issuers.

By "scheme-centric" we refer to the situation where the Token Requestor (such as a merchant, or a mobile device manufacturer) needs to connect directly to a scheme infrastructure for the provisioning of the token. In this case, the scheme acts as a privileged TSP, possibly after a contractual agreement with the manufacturer of the mobile device where the token will be stored. The scheme then, upon approval by the card issuer, conveys the token request to a "by-default" token provisioning facility.

The TSP as such constitutes "a processor within the existing processing chain"; an independent role ensuring a set of extra-functionalities for the card transaction (acceptance of token requests, token provisioning and life-cycle management, Vault operation, de-tokenization, authentication of the payment device, the cardholder and the token requestor, enrollment and management of token requestors). The TSP typically has to offer interfaces to at least four stakeholders of the card payment circuit (the merchant acting as token requestor, the acquirer, the issuer, and the card scheme). From a competition perspective, the question is whether the legal principle of "separation of payment card scheme and processing entities" should be extended to "separation of payment card scheme, processing and token-processing activities".

4. Is there a case to regulate Tokenization Services?

The SPA recognizes that the EMVCo framework is flexible enough to accommodate competing implementation specifications by EMVCo members and covers a broad range of use cases. That's fine. To avoid excessive market fragmentation it is also important that there are not multiple standards, and the EMVCo initiative helps to limit the number of outsiders. But the framework should also accommodate offers from other capable market players. Of course, any workable TSP solution should easily and efficiently be integrated into existing business infrastructures. It should also allow for implementation of the TSP at different points in the processing circuit of payment data. Indeed, the TSP may be implemented in different domains: Acquirer domain, Issuer domain, Acquirer-to-Issuer domain, or Acquirer-to-Merchant domain.

The decision to develop a regulatory technical standard approach for TSPs may depend on the following factors, which somehow match the "three-principles" that justify a regulatory initiative (fair market access conditions, fight against fraud, and consumer protection):

1. If the Token Requester is the end-user (cardholder and/or merchant) or not.
2. The existence or not of technical specifications/de-facto standards for the interoperability of token processing, based on open interfaces to be implemented without discrimination by any legal entity willing to enter this market.
3. Whether these specifications enable all the technology providers to compete equally, not just the payment schemes; and more specifically, do not impose high-entry barriers for TSP services.
4. If implementations compliant with the framework conform to Article 7 of the Interchange Fee Regulation, assuming that TSP is a processing service according to the definition of Article 2 (27) of the Interchange Fee Regulation.
5. If strong authentication is required for token provisioning, which entities have to be authenticated and by whom.
6. Token ownership and liability shift policies applicable to tokenized card transactions.
7. The existence or not of a security evaluation and certification process for the TSP.

As previously discussed, the TSP is a "processor within the processing circuit" and as such may be a bank or a third payment service provider (e.g., a payments processor), as the service may be offered by an independent legal entity having contracted with a payment system. In this "modular" approach the TSP may not necessary need to be licensed as a payment institution. Yet, the added security provided by the use of tokens to pay is reliant on the integrity of the Vault. The tokenization internal process and Vault management by the TSP could be subject to monitoring, including specific testing to evaluate resistance against cyber-attacks.

Next to the TSP, some frameworks recognize the role of "Token Requestor", which in principle is a legal entity contracting with the TSP and not an individual. It is unclear which type of entity qualifies as a Token Requestor, or how to ensure that non-discriminatory, non-exclusivity practices apply to the Token Requestor as well as the PCI perimeter for security certification, dependent on the nature of the requested token and any additional services associated to the token. This is an area where national regulators may specify the rules that govern the operation of a Tokenization system.

As mentioned, the EU payments industry 'privileges' the way of self-regulation as a means to create a competitive market for the provision of Tokenization Services. Obviously the success of a self-regulatory process relies on the existence of real business incentives to collaborate in the development of technical standards for tokenization. An agreement on the business principles and requirements to act as a Token Service Provider could also be in the scope of industry-led initiatives; an agreement recognized by the regulatory authorities.

There are many potential TSP business models, because any stakeholder of the card processing circuit may act either as a Token Requestor or play the role of TSP. In addition, the operation of a TSP brings about a complex organization, where individual roles can be identified and fair competition conditions must be ensured. However, in the end it is likely that only a few models will actually prevail. Therefore it is important to guarantee that this "market decision" is not biased from the beginning, and that the inevitable simplification of this very complex picture is actually the result of good technical and commercial practices.

5. Five points to conclude

1. The complex business relationships between different payment service providers make it difficult to evaluate the impact of new regulations in the efficiency of payment systems. Thus, many experts consider that regulation should focus more on security and consumer protection aspects rather than enforcing an artificial level of competition, not taking into account the specific characteristics of the retail payments market itself.

2. Compared with other SEPA retail payment instruments (SEPA Credit, SEPA Direct Debit), card transactions are processed through multiple interfaces operated by different entities – which all adds up to a complex processing circuit. This complexity makes it appealing to pursue the bundling of payment processing services in order to simplify the transaction flow and to decrease processing costs. Tokenized card transactions add complexity and therefore reinforce the trend towards further vertical integration (which disintermediates SPA members).

3. Collaboration in building infrastructures and setting common standards is a key business concern, and network effects put a limit on the level of competition in payment systems because it creates high-entry barriers. Tokenization is not an exception to this rule. Card payments are two-sided markets, and so is the market for TSP services. TSPs must compete to enroll token requestors and bank issuers to generate a sufficient number of transactions. This competition should not be impaired by processing-centralized practices.

4. The EBA regulatory technical standards (RTS) constitute a timely opportunity to investigate the market access conditions for the provision of token-related services. In particular it is crucial to verify whether the industry self-regulated approach is sufficient and if the existing de-facto standard frameworks (for example, EMVCo) don't create direct or indirect barriers to market entry. The existence of open interfaces for capable parties that want to

serve as token providers is fully in line with the PSD2 principles, and the RTS publication by EBA may provide implementation details on the processing side.

5. Tokenization is in the program of work of the European Card Stakeholders Group (ECSG) which enables democratic representation of all stakeholders, and results in public consensus for standards laying down both functional and security requirements in the Volume Book of Requirements. The integration of new requirements in the Volume specific to Tokenization should guarantee that roles and market entry conditions for the provision of tokenization services is open to all sectors represented in the ECSG.