Secure Remote Payment Council (SRPc)
Tokenization Position Statement
October 22, 2014

The Secure Remote Payment Council (SRPc) released a position statement in July 2014 stating that tokenization standards must embody three major points:

1. *Standards must be open, enabling all to compete equally.*
2. *Standards must support end-to-end tokenization for all use cases.*
3. *Standards must cover both the card-present and card-not-present environments.*

The recent Apple Pay announcement challenges the SRPc's mandate for open standards for tokenization and a level playing field for all stakeholders to compete.

There is no doubt that the Apple Pay announcement made a profound impact on the payments business. The offering uses Near Field Communication (NFC) to support credit and signature debit transactions performed in-store at a point-of-sale device and/or in-app on iPhones and iPads. How debit and network routing will be supported in Apple Pay is still undefined. In Apple Pay's implementation of tokenization, the tokens are restricted to transactions with a specific device, namely the mobile phone, or applications specific to the iPhone and the Apple Wallet.

The Apple Pay offering will support a proprietary tokenization technology and the major card brands will serve as the primary token service providers (TSPs) and the token vault provider (TVP).

- The token service provider (TSP) supports those activities related to servicing the token to access the clear PAN. TSPs enable services such as issuer enrollment, token provisioning, mapping tokens to the primary account number (PAN), token/PAN exchange to the issuer, and life cycle management of the token. Token provisioning refers to the process of getting a physical token device into the hands of the end user. When the consumer loads card information onto the mobile phone, the provisioning application requests a token value. The use of the token minimizes the risk of fraud in the event the device is compromised.

- The token vault stores the tokens and supports the mapping of the tokens back to the real PANs that they represent. The opportunity to provide vault services appears to be limited to the card brands, a few processors and a couple of large banks. The exclusion of network participants as TVPs will influence the routing and cost of debit transactions.

Equal Opportunity for Competition

Apple Pay's initial implementation of tokenization is based on EMVCo's proprietary tokenization framework. This implementation does not support the use of an industry standard that would enable issuers, issuer processors and alternative networks to provision, load and provide services. The implementation of unique token solutions specific to individual networks creates important competitive implications for many existing payments stakeholders that will likely be competitively disadvantaged by EMVCo's approach to tokenization. Tokenization should be implemented in accordance with ANSI or ISO standards so that it can scale throughout the industry - similar to the ANSI PIN standard. The opportunity for issuers and merchants, as well as their processor or network partners, to provide token vault and token services is important to maintain industry competition and innovation.

There are also concerns about how Regulation II routing is maintained and whether merchants, their service providers and the networks might be inhibited in routing transaction economically if some parties are precluded from serving as token service and vault providers. While an EMV credit transaction requires routing across only one network for authorization, a merchant must have the option to route a debit transaction via two or more networks. Debit routing choice is limited if the transaction has to access network-specific vaults for token services.

Competitive concerns arise if the crucial role as token service provider and the specifications for becoming a token service provider are left in the hands of EMVCo or any party other than a traditional open standards body.

Moreover, the standards for tokenization must be flexible enough to cover all technologies, and not be limited in scope to one or two options such as NFC. They should support dynamic tokenization, i.e., one-time or limited use tokens, rather than static, domain specific, cryptograms as proposed by EMVCo.

Call for Open Standards

The SRPc believes that tokenization is an important component in the overall security requirements for the safety and soundness of card and card-not-present transactions. Solutions for tokenization should subscribe to an open standards approach to payments security, such as those developed and governed by ANSI and ISO standards bodies. It is essential that the standards are accepted by all industry participants. It is equally important that all industry participants have the opportunity to provide token vault and token services. The current roll out of Apple Pay does not provide this opportunity, and moreover pushes a proprietary approach that will create competitive issues if adopted more broadly.

History suggests some stakeholders may be seriously injured by their lack of inclusion in the creation of pseudo-standards. For example, the merchant community contends it has suffered significant damages from the imposition of pseudo-standards by PCI and EMVCo. The industry as a whole only benefits when standards are created and realized through collaboration and acceptance of all of the parties with a stake in the outcome.

The payments industry needs to move in a deliberate manner toward making substantive changes that enable interoperability and scalability instead of a solution that limits participants and as a result, routing choice. The SRPc's goal is the use of an ISO or ANSI standard that provides ubiquitous and universal access to the PAN for all industry stakeholders.

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.