Secure Remote Payment Council (SRPc)
Tokenization Position Statement
July 24, 2014

The Secure Remote Payment Council (SRPc) is dedicated to improving security and consumer confidence in ecommerce payments. We call upon all stakeholders in the payments industry to come together to ensure open and efficient data security standards to better protect U.S. businesses and consumers from cyber-attacks.

The deployment of a security technology called tokenization is one major step in the right direction; however, the SRPc has serious concerns with ongoing developments being put forth by EMVCo (EMVCo, LLC, manages, maintains and enhances the EMV™ Specifications for Payment Systems). The SRPc strongly recommends the development of tokenization standards in an open and accredited process with equitable participation by all stakeholders.

Tokenization refers to the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data, such as account or identity information, without compromising its security. Tokenization has been used for many years in an enterprise manner, but recent developments have focused on the utilization of tokenization in an end-to-end, multi-enterprise manner.

There are two major standards bodies that govern developments in the payment industry, namely ANSI (ASC(X9) in the U.S.) and ISO. These fully accredited standards bodies promote an open solutions approach to payments security. Solutions for tokenization should subscribe to an open standards approach, covering both the global brands and all other network brands. The intellectual property should also be governed by industry standards.

The SRPc believes that tokenization standards must embody three major points:

Standards must be open, enabling all to compete equally.

The standards must allow participants to develop proprietary frameworks that inter-operate with each other in adherence to a standard.

Any form of tokenization adopted by the industry should enable all industry stakeholders to compete on equal footing, and moreover should provide equal access or even partial ownership to the supporting technology. The goal must be to create an open industry-consensus standard. That standard should be supported by all networks, brands and payments types (credit, debit, prepaid, ACH, etc.), and should not be unique to any specific network. Ideally the issuers, merchants, and acquirers would have a single standard accepted by all networks and brands allowing for issuer and merchant choice.

The current EMVCo framework does not pass the normal definitions of a standard, and is in fact a specification. Token-granting entities are limited by global brand rules and token processing is controlled by these global brand rules. Currently, global brands require that all participants, including network competitors, utilize token-generating entities that global brands approve. This restricts competition and innovation.

Historically, the nature of the payments system including the cards, computer-to-computer communications, and messages formats have been derived under an open standards process that involves ISO and ANSI standards in the US. To foster market competition, the market needs to continue in this way.

Standards must support end-to-end tokenization for all use cases.

Any movement toward end-to-end tokenization must support all use cases in a manner agreed upon by all payments participants.

The EMVCo framework does not support a complete solution. Use cases are limited to the two circumstances: (1) for consolidation when an ecommerce merchant uses tokens to replace cards on file; and (2) when a mobile device obtains a token in a face-to-face merchant transaction using NFC as the transport layer.

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.

There is also the need for choice among token service providers (TSP), which an issuer, merchant, processor, or network can utilize for tokenization services. In order to be effective worldwide, tokenization should deploy a distributed architecture, a common application programming interface (API) for all parties to access, and highly secured credentials and authentication standards to use it. Additionally, the federated, distributed architecture must allow networks, processors, third parties, merchants, and financial institutions to serve as token service providers.

Standards must cover both the card-present and card-not-present environments.

We should not rush to market with a solution that doesn't address the entire problem. The lessons learned from the implementation of EMV™ in other countries have shown a shift of fraud from the physical space to the online environment. As such, the industry solution for tokenization must address both the card-not-present and the card present environments.

Call to Action

The SRPc calls all interested parties to come together to work toward a solution that will meet the requirements of a standard as set forth above. The development of such a tokenization standard is the best way forward to ensure that all stakeholders participate in a solution that is equitable, safeguards competition and encourages innovation.

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.