SUMMARY OF ANS X9.119-Part 2
USE OF TOKENS TO PROTECT SENSITIVE CARD DATA

September 2017

X9, the US accredited standards body for the Financial Services Industry, recently adopted a standard that defines the minimum security requirements for designing and implementing a tokenization system for post-authorization payment data. X9.119 – Part 2, entitled "Retail Financial Services - Protection of Sensitive Payment Card Data: Tokenization," was also approved by ANSI and becomes the US national standard to protect data that may disclose the identity of the cardholder (e.g., Primary Account Number, Cardholder Name, Expiration Date, Service Code), and Issuer Discretionary Data or Track data, which typically refers to the data stored on the magnetic stripe of a payment card, as well as "Equivalent Track Data" when that data is stored in IC Cards and other electronic media (e.g., a mobile wallet).

The standard deals exclusively with so-called "data security" tokens (i.e., tokens used by merchants, either issued by the merchant itself, or by an acquirer, and some cases, by an issuer). The standard does not deal with EMVCo tokens used in the authorization of payments. In other words, the tokens described in the X9 standard are used to protect sensitive card data after a transaction is completed, but they are not used as a replacement for the Primary Account Number (PAN) in a card authorization transaction.

As defined in the X9 standard, a "token" is a surrogate value used in place of the original value (or underlying sensitive value) in specific situations, even though the token is not used in place of the original data value in every way that the original value is used. Post-authorization tokens are not produced until after the initial payment authorization is accomplished using the related original data value (i.e. sensitive payment card data) and cannot be used to initialize a payment transaction. Post-authorization tokens are instead used to protect the original data during the payment process workflow by replacing those original data values in various data repositories. The standard describes multiple use cases to demonstrate the use of post-authorization tokens.

The standard provides support for data encryption and data integrity protection, as well as for key management services that are required to protect sensitive payment card data during the tokenization and de-tokenization processes and for the protection of any such data when it is stored within a tokenization system. The objective of the standard is to maintain the secrecy and integrity of sensitive card data protected by tokenization from unauthorized disclosure and modification. It also provides requirements and guidance about the tokenization environment, including:

- A review of the evolving uses of tokens and tokenization to protect sensitive payment card data;
- A description of and requirements related to, a model tokenization generation system involving the use of a Tokenization Service Provider securely distributing a token to an interface between the tokenization requestor and the tokenization service on the behalf of an entity requesting a token;
- A description of acceptable token generation methods for use by a Tokenization Service Provider;
- Security requirements for processes requesting tokens from a tokenization services;
- Security requirements about the establishment and maintenance of a Tokenization Service; and
- An informative set of use cases describing the role of the entity requesting a token within a tokenization system.

A key element of X9.112-Part 2 is that is often used in conjunction with Part 1 of X9.119, which involves protecting sensitive card data through the use of Point-to-Point Encryption (P2PE). That standard was adopted by X9 in 2013 and revised in 2016; Conexxus has developed a specification for implementation of P2PE technology for petroleum/convenience retailers. The ability to combine both P2PE and tokenization provides merchants with significant security tools to better protect sensitive data.

Specifically, the Standard is required to have a Tokenization Security Policy and is required to document all of the potential weaknesses/risks in the Tokenization Service it implements, as well as how it adheres to its Security Policy in implementing and operating its Tokenization Service.

Conexxus and the International Forecourt Standards Forum (IFSF) have articulated specific recommendations they feel should be part of the tokenization landscape. Those recommendations include the following concepts that are met by the X9 standard:

- Tokenization standards should be owned and managed by a national standards organization or by an ISO accredited standards body, which enables democratic representation of all stakeholders, and results in public consensus standards, not proprietary ones.
- Tokenization standards should cover the greatest number of potential use cases, in order to apply to existing and emerging technologies.
- Tokenization standards should enhance competition and promote a free market, and should focus on roles and requirements, rather than "who" provides the service.
- Tokenization messages must be generic and NOT be limited to proprietary technology.
- Security tokenization should be standardized in an open and flexible way that does not dictate how interfacing with any token service provider has to occur, allowing for implementation of tokenization at multiple points in the flow of data.
- Data captured through tokenization should only be used to secure sensitive data, and any secondary uses of data must respect the appropriate privacy and permission requirements that apply to that data.

While this X9 standard only deals with sensitive payment data and is not wholly generic to cover other types of data (e.g., employee data, such as SSNs or health data), the security principles embodied in the standard can be used by retailers for non-payment data.

Technical Editor for the project, Steve Schmalz of RSA, commented on the value of this standard to the existing body of tokenization standards, noting, "This effort involved input from across the financial industry and security community at large and provides a true synthesis of competing views on tokenization and its implementation."

As mentioned earlier, this standard is part of a broader X9.119 Protection of Sensitive Payment Card Data standard. Part 1 covers Using Encryption Methods and Part 2 covers Tokenization. Both standards are available on the X9 website in the Standards Store, X9 Standards Store, or at the ANSI Webstore: http://webstore.ansi.org.