Tokenization: The Future of Payments Security?

INDUSTRY INSIGHT

Background

The Payment Card Industry Data Security Standard (PCI-DSS) was created to increase controls around cardholder data to reduce credit card fraud via its exposure. From nearly the beginning of its introduction, the standard has been criticized for the expense associated with annual certification and for security being less than advertised. The recent increase in public data breaches has underlined concerns around whether the investment required provides the level of security needed.

Many conversations around options for security have suggested use of tokenization, which substitutes sensitive cardholder information with tokens. Since the tokens contain no cardholder or card data, they present no value to criminals and improve consumers' level of trust. In addition, issuers avoid the expense associated with notification, loss reimbursement, and legal action. Furthermore, by removing the need to store actual card details, this approach significantly reduces the costs and hours associated with the compliance requirements.

By eliminating the need to store sensitive information, a successful tokenization strategy would also enable merchants to shift many business processes and IT systems to the cloud realizing significant advantages in IT efficiency, costs and flexibility provided in that environment.

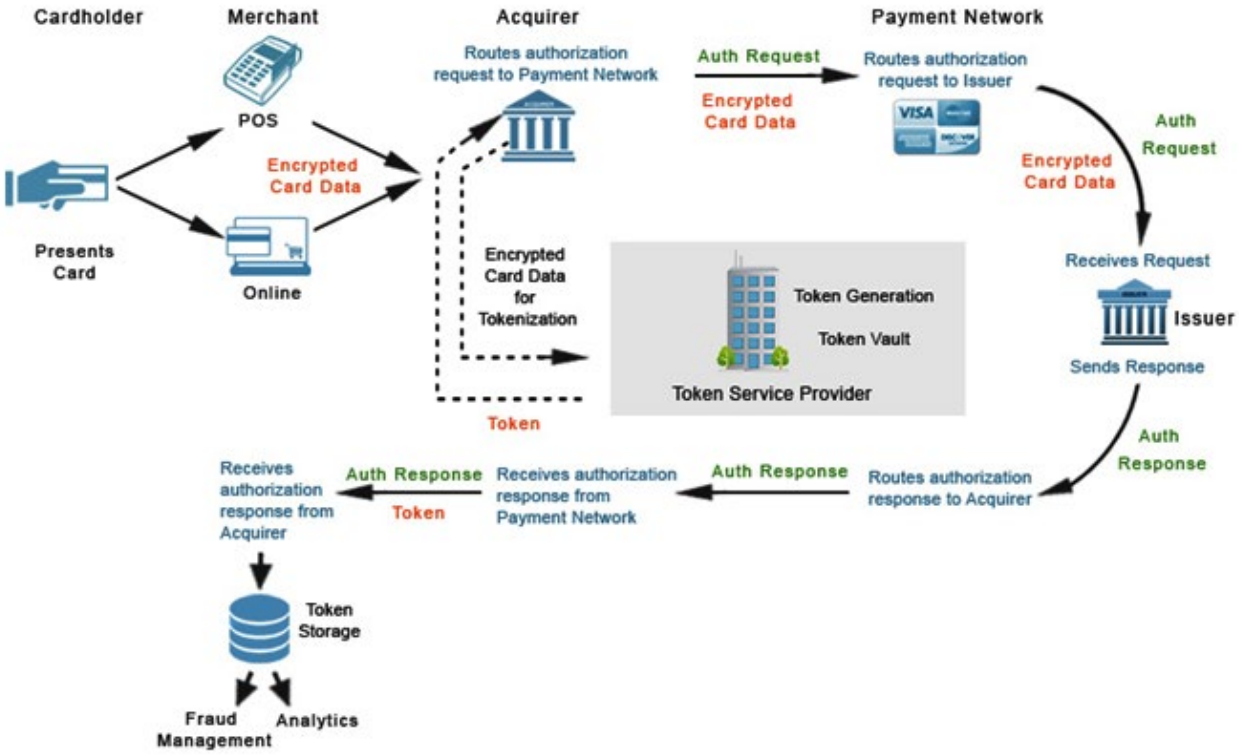
Impacts to Stakeholders

For tokenization to be possible, the organizations involved in payment processing need to make modifications to their existing systems.

- **Merchants:** Tokenization requires merchants to change the PAN and expiry date information in their databases to token and token expiry date information. Tokenization allows for additional messages

to be embedded in transactions, thus increasing merchant discounts. Merchants using on-premise token solutions would experience a greater impact in terms of infrastructure and change in business processes than those who use a tokenization service.

- **Token Service Providers (TSP)**: There are two major areas of setup for a TSP: infrastructure preparation and information preparation. Infrastructure preparations include setting up the token vault, firewall and strong access control measures. An encryption system for the vault, a token provisioning platform, and access APIs also need to be set up. Information preparation involves defining and codifying token presentment modes for token-based transactions at the point of sale. Supported domains with restrictions and controls, assurance levels and Token BINs used to distinguish tokens from each other need to be established.



- **Merchant Acquirer/Processor**: A merchant acquirer or processor first needs to select a TSP and register as a token requestor (TR). Once this step is taken, impacts for the merchant acquirer or processor include implementation of new token POS entry modes, token domain restrictions and controls, new token acquisition APIs, related exceptions, and token acceptance processes. In addition, merchant acquirers and processors need to reconfigure their PAN analytics strategy to accommodate the fact that posttokenization data is segmented by domain.

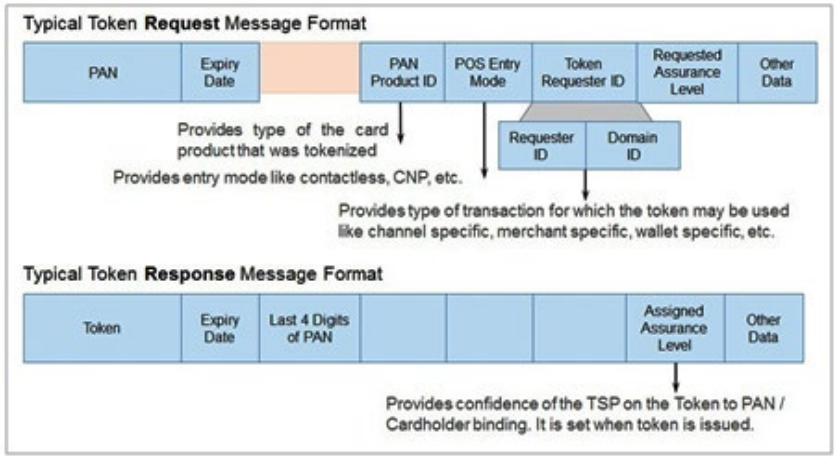
- **Network**: Payment networks typically play the role of a TSP. However, other entities in the payments supply chain can also apply to be registered as a TSP and provide the services. Fulfilling this role requires networks to consider how they will distinguish tokens, what parameters they will use for token assurance, the domains to be provided (e.g., NFC only, contactless, e-commerce, CNP, merchant specific, wallet specific or combinations), and changes that need to be introduced to merchant on-boarding to support token registration.

- **Issuer**: Issuers need to make modifications to log the token / PAN mapping for transactions to allow merchants using tokenization to refer to a transaction using a token and not PAN. In addition, issuers may wish to consider alterations to authorization scoring.

Impacting the Ecosystem

Token creation and storage, the primary responsibility of the TSPs, serves as the standard foundation for the tokenization process. However, the approach to tokenization taken by various payment processing intermediaries is not standardized. For example, some merchants have implemented tokenization as an on-premise solution that tokenizes data before it is passed to the payment gateway, network or processor.

Another common approach involves the merchant utilizing a tokenization service provided by the processor. This approach requires the cardholder data to be encrypted through the application of an algorithm and key before being passed to the processor. Then the encrypted data is accepted, decrypted and tokenized by the processor. The card is then processed for authorization and the response paired with the token and then sent back to the merchant. A processor providing this service generally partners directly with a TSP or purchases the service from the network that, in turn, would partner with a TSP.



Many tier 1 and tier 2 retailers work with multiple payment processors and thus need an on-premise solution that is vendor agnostic. However, a hosted solution frees merchants from the complexities and costs of creating and maintaining the tokenization engine and the secure token vault. In addition, an outsourced solution shifts the risks and costs of PCI compliance to trusted third parties with proven capabilities for securing card data. However, if merchants use a tokenization service provided by an acquirer, migrating to a new acquirer will require that all card-on-file information be migrated to the new service provider since merchants do not retain the card information when tokenization is used in this manner.

Key Considerations

Regardless of the approach taken towards tokenization, most organizations are demanding a solution that allows for multiple uses of the token values. In this scenario, tokens can potentially be used for repeat purchases, recurring payments, and even chargebacks and refunds. In addition, multiple use token values can be utilized for post-processing functions such as sales analysis, velocity checking, or customer relationship management.

Other areas for consideration also come into play, either directly or indirectly depending on the role of the intermediary, when considering a strategic solution for tokenization.

- **Token Values**: Token values can be generated randomly or customized for the merchant. The customization of the token must be done under a set of established guidelines and can include the last four digits of the card number or be a format-preserving token designed to cater to the merchant's legacy applications. The specific operational and business needs of merchants will determine which of these methods are most viable for their organizations.
- **Single Pay vs. Multiple Pay Tokens**: A multi-pay token is unique to a specific card used with a specific merchant. Multi-pay tokens are especially useful in CNP transactions (e.g. e-commerce purchases) that tend to store payment card information in a mobile wallet or on a website for repeat customers. Merchants using multi-pay tokens with a hosted payment page also provide an environment hostile to CNP fraud removing the need to capture card data within their environment and minimizing the risk of card data being stolen.
- **Legacy Data in Storage**: To help prevent potential breaches and reduce PCI scope and maintenance costs, merchants can use tokens to completely remove legacy and stored primary account numbers (PANs) in the card data environment (CDE). When adopting this approach, it is important to ensure that the tokenization solution selected provides the capability to tokenize existing cardholder data in the merchant environment and not just data acquired going forward.

In addition to these primary areas, related subjects for consideration include token lifetime, distinguishability, domain setup and assurance levels.

RS Software

When considering implementing a tokenization solution, it's important to carefully consider the impact on your system's performance, the commitment of vendors to encryption and NIST certification, and the ability to store data tokens separate from production data.

RS Software has participated in the evolution of the payments industry for more than two decades working with industry leaders including major card associations, large and small acquirers and other participants in the payments industry in North America, Japan and the UK.

The RS School of Payments and RS Payments Lab are cornerstones for our vertically integrated approach to assisting our clients. We engage with customers in the consulting stage to plan the

necessary downstream priorities including custom application development, upgrades, implementation and integration.

RS Software has the ability to do a comprehensive analysis of how implementation of tokenization impacts services like authorization cycle (token extraction, token generation, etc.), clearing and settlement, dispute management and downstream value-added services such as the evaluation of where PANs potentially impact tokenization. Our deep understanding of tokenization stems from experience in end-to-end lifecycle of transactions, EMV enablement, parsing and routing, authorization, clearing, settlement, and dispute management. In addition, RS Software provides additional services for consulting, scoping and requirements definition, development, testing implementation and support.

RS Software wrote "Tokenization: The Future of Payment Security?" For more than 20 years, RS Software has been a leading provider of electronic payment solutions for issuers, acquirers and processors. Today, many of the world's best-known brands in the payments space utilize RS Software's vertically integrated approach of providing solutions to gain a competitive advantage.

RS Software