RS Software

FACT SHEET

Tokenization: A Capability Note

Why Talk About Tokenization

The Payment Card Industry Data Security Standard (PCI-DSS) was created to to reduce credit card fraud by increasing the security measures used to protect cardholder data. From nearly the beginning of its introduction, the standard has been criticized for the expense associated with annual certification and for security that did not deliver as promised. These facts have caused various players in the payment industry to question whether the standard delivers value, given the investment required and the increasing number of data breaches reported.

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. This technology improves the consumer's level of trust and helps issuers avoid the expense associated with notification, loss reimbursement, and legal action.

Furthermore, by removing the need to store actual card details, tokenization may reduce the costs and hours associated with the compliance requirements. Finally, by eliminating the need to store sensitive information, a successful tokenization strategy could 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.

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

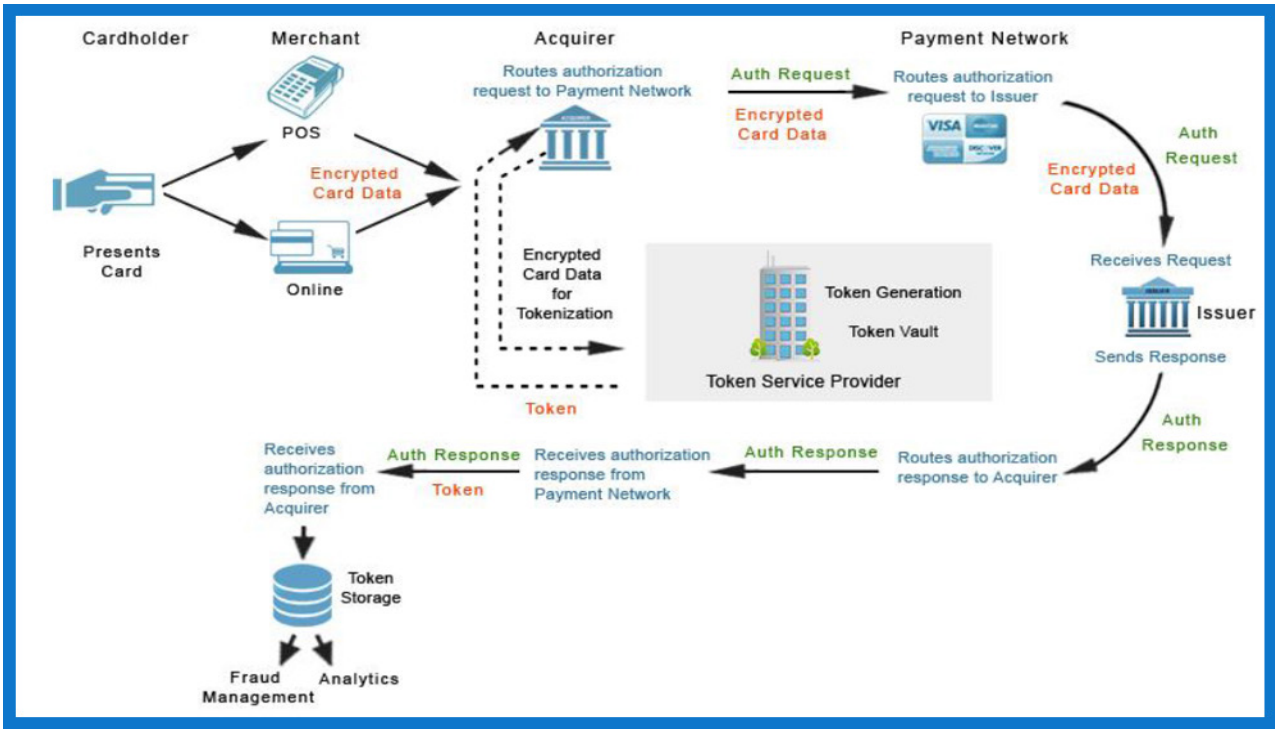
Merchants: Tokenization requires merchants to substitute the PAN and expiry date information in their databases with token and token expiry date data. Tokenization allows for additional messages to be embedded in transactions, thus making it possible to increase merchant discounts. Merchants using on-premise token solutions will have more options for improving security and efficiencies 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 put in place. Information preparation involves defining and codifying token presentment modes for token-based transactions at the point of sale. In addition, 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. Merchant acquirers and processors also need to reconfigure their PAN analytics strategy to accommodate the fact that post-tokenization 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. 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 the 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.



Now that as card asassociations are becoming TSPs, the business relevance that existed in the past for acquirers to be a TSP has been considerably reduced. However, even today tokenization is not pervasive and there are networks that do not support card on file, as of today. So, an ecommerce merchant connected to the acquirer will still benefit if the latter rolls out tokens for them.

If acquirers become a TSP, as First Data has, their internal systems will have one system (vault) that is PCI compliant and their merchants would not need to have any system that has sensitive data to protect.

RS Capabilities in Tokenization

When considering the implementation of a tokenization solution, it is important to comprehensively assess the impact the solution will have 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 adding the necessary tokenization will impact various aspects of a system's performance, such as the authorization cycle (token extraction, token generation, etc.), clearing, settlement, dispute management and downstream value-added services such as the evaluation of where PANs potentially impact the tokenization process. Our deep understanding of tokenization stems from experience in the 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 definition of requirements, development, testing implementation and support.

Here is a representation of our portfolio of services that we offer:

Consult

Evaluate business drivers and identify appropriate business use cases to implement tokenization

Gap Analysis on compatibility of new products/channels

Strategize on roadmap ahead and provide a SME-driven domain edge to thought process

Review the use cases to identify gaps in implementation

Develop

Enable architecting, design and development of tokenization for new products/channels from ground up

End-to-End Token Life Cycle Management

Design core Tokenization Components like Token Service Interface, Token Vaults, Token Generator

Actuate Tokenization business cases like HCE based payments and in App payments with Apple Pay

Buy/Integrate

Evaluate, Implement, Customize and Integrate a 3rd party TSP solution with current system

Build, Test, Implement and Migrate to the composite solution with apt scalability

Provide Post-deployment support like Token service interfacing, support for issuers in implementing Tokenization and support

RS Accelerators and Reusable Assets

Over the last two decades, RS Software has developed a framework to leverage the cumulative knowledge from our past e-payments experience delivering this to our clients in a comprehensive package of reusable assets. Our engagements involving tokenization have yielded the following set of these types of assets:

- Business use cases and test scenarios capturing different message flows. All the test scenarios in functional and end to end testing are documented for use as a reference for any future testing. This serves as a good basis of ensuring requirements and test coverage by a functional testing team for any payment network wishing to integrate their tokenization solution with Apple Pay
- A checklist corresponding to different functionalities of a message flow associated with key message components and their contents
- A consolidated list of lessons learned including common pitfalls and error prone areas
- Test tools that are technology specific withdesign and pseudo code can be used, for example, to simulate functionalities of a DWP, HSM, TSM to fast track unit testing for the authorization system
- Extensive experience in Agile and hybrid methods that can accelerate implementations of Apple Pay technology by allowing development, functional testing and integration testing to happen in parallel. The process and methodologies can be leveraged in any similar endeavor by any payment network or card issuer.

All of this is packaged in our RS-TKF (Tokenization Knowledge Framework) for reuse.

RS Tokenization Knowledge Framework (RS-TKF)

RS-TKF is a Proprietary Tokenization Knowledge Framework based on the EMV-Co specification and enriched with best practices knowledge we have gained in dozens of such implementations worldwide. It consists of validators that serve key reference points for the developed solution and accelerators that improve time to market.

The content of RS-TKF is based on the following:

- Use cases (40+)
- Message flow and structure
- Sequence diagrams
- Component diagrams
- Internal and external APIs and their associated parameters
- Class diagrams
- Integration diagrams
- Known-error database and FAQs related to tokenization implementation related issues

RS Experience in Tokenization

This section will provide an overview of some of our recent tokenization engagements.

Development and testing partner in tokenization initiative for a leading payment network

Engaged as the key partner to develop and implement a tokenization solution for a leading network , we delivered services such as token provisioning, overall lifecycle management, token vault setup and maintenance, service monitoring,reporting and detokenization. We collaborated with the network's key stakeholders from the business side and its architecture teams to identify, design, develop and implement the changes required in the core processing applications specificallypayment gateway authorization, risk prediction, fraud reduction, member configuration management, data services and dispute resolution.

Working with this flagship client, we delivered the following key components for their tokenization projects:

- A comprehensive set of TSP functionalities
- The changes to the core system require to accommodate tokenization
- The identification of changes required for all downstream systems
- All system and integration testing

Description of the major functional changes that we implemented for this client in addition to the above are documented in the subsections below.

HCE Based Tokenization

Historically, the network's mobile transactions required account credentials to be stored in a secure chip on the mobile device called the secure element. Although secure elements offered similar security benefits to physical chip cards, they presented numerous technical and commercial complexities that limited the technology's scalability. The network developed a cloud-based payments program using the Host Card Emulation (HCE) technology introduced by Google in Android™ 4.4 KitKat to remove many of these complexities and provide the payment ecosystem a more flexible and scalable way to make secure mobile transactions without the requirement for a secure element.

PANs are not directly used for HCE-based transactions. Instead, payment tokens are used for HCE payments. The following restrictions help to mitigate a variety of threats:

- Presentment channel restriction: Tokens utilized in an HCE cloud-based Payments program are domain restricted to the contactless NFC payment channel. This means that a token can only be used at contactless NFC-capable POS terminals and cannot be used for magnetic stripe, e-commerce, card on file, or similar transactions. Therefore, HCE data cannot be used for CNP or CP fraud through other presentment channels.
- Single user restriction: A separate payment token is issued to each mobile application account enrollment. This allows risk management to track transactions to the specific mobile application, making it easier to restrict fraudulent activity since HCE transactions are usually initiated by a single consumer.
- Limited issuance restriction: Payment tokens can be only issued to approved token requestors (e.g., issuers, digital wallet providers, etc.). Some of these requesters are prominent names in the world of third party digital wallet providers.

Testing

RS Software managed the project testing including: 1) defining the test strategy 2) designing the test cases 3) establishing of the test environment and controls, 4) designing the test execution framework and 5) formulating the metrics for integration testing and UAT. Our company also provided the following elements to support the testing process:

- Comprehensive test program management requiring coordination and planning with diverse teams throughout the organization, including scheduling, budgeting, resource planning, issue monitoring and status reporting.
- Testing and validation of several encryption services involved in the different stages of provisioning a card includingRSA-2048, TDES, CBC (i.e, cipher block chaining), AES-128, ECC-256 encryption – including the different stages of check card, consumer authentication, link and Provision and application of provisioning scripts through SEI-TSM.
- Test design and planning for network message flows, cryptographic functionalities and token life cycle management.
- Test execution across various risk rules and profiles, data feeds and updated to rule profiles.
- Functional testing using simulated issuing in the test environment and On-Behalf-Of (OBO) services to issuer during provision requests.

Apple Pay Integration

A notable extension of the digital platform development during this project happened when the Apple Pay integration services were kicked off. Our team identified several features and impact points across core functional areas and worked towards weaving them into the overall solution design and development.

We participated with Apple in the end-to-end testing of all the involved applications and devices including the iPhone, the Apple wallet app, Apple Pay, the payment network, and TSM. With Apple teams creating integration test artifacts (e.g., design, scenario etc.), our team reviewed the same and recommended modifications to ensure better test coverage. We also recommended changes in the configuration and provided the required configuration values to ensure that the tests achieved the desired test objective.

One of the most challenging areas in testing was the user acceptance testing. We worked closely with both Apple and the payments network to define the user acceptance test strategy and associated test plans. The user acceptance testing was executed within the network's production environment using test cards and test handsets. The test cards were sourced from a variety of issuing banks and utilized to make actual purchases. RS provided complete oversight and management of the process and implemented then tracked the fixes required for Apple, the network, the TSM and the Issuer.

For the subsequent eight months post implementation, we provided the requisite support to Apple teams on different message flows and HSM-related issues. Our team also analyzed incidents raised by Apple and provided solutions for those. Lastly, our team was involved in complete design and end-to-end implementation of the portal required, including a multi-threaded messaging service for the backend integration.

White-Labelled application for IN-APP Payment with Apple Pay

This project involved working with a payments service provider in the education space to build a mobile application that would allow white-labelling and support of in-app payments using Apple Pay and an Apple partner's SDK. The white-label app needed to allow for customization via a partly automated process and subsequently publishing to the Apple store on behalf of a client for download and usage by the client's end-users to make payments.

The functional categories contributed by our team included:

- Development of a framework that renders itself to fast white-labelling and customizations (e.g., embedded end client Identity and secret key, branding and skin etc.) and publishing to the app store as an end user application
- The ability to keep manual intervention to a minimum and allow a non-technical audience to complete the customization process that aligns with limitations imposed by Apple publishing procedures
- Integrated authentication, leveraging a proxy service and standard biometrics
- Transaction reporting services
- Apple Pay integration using third party payments libraries and SDKs

Validation and refining of the Tokenization roadmap

It is our practice to leverage the cumulative knowledge from our past experience and translate the same into a comprehensive package of reusable assets. Based on our prior experience and understanding, our competency team has been instrumental in creating business use cases, test scenarios, checklists, and known error databases corresponding to different functionalities and components of a message flow.

This allowed us to engage with another large payments network and card issuer taking the first step towards realization of a tokenization platform. We delivered the following services in this particular engagement:

- Review of business requirements, specifications and design documents providing value added recommendations based on our best in breed experience with tokenization in a variety of settings.
- General consultancy on token reuse, IIN range allocation, lifecycle management and HCE application
- Test coverage for business test scenarios

Why 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 lifecycles 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.