Best Practices For Tokenization Projects In The Payments Industry

INDUSTRY INSIGHT

The Payment Industry's Move To Tokenization

While EMV is effective for securing card transactions at point-of-sale terminals, it is less useful for online payments, card-not-present transactions and for protecting card data at rest in merchant systems. That is one of the major reasons why payment card fraud has migrated from point-of-sale systems to online channels in Europe and other places that have already adopted EMV.

With online payments, card tokenization is one way to address this gap and a number of organizations in the industry have come out in support of tokenization as a risk management strategy. The major card networks such as Visa and MasterCard have been vocal with their endorsement of this approach as have powerful organizations such as The Clearinghouse – representing 22 of the largest banks in the United States. The recently published EMVCo standards also have helped by providing a standard for stakeholders to follow as previously there was none.

Replacing a card's Primary Account Number (PAN) with a unique, randomly generated sequence of numbers, alphanumeric characters or a combination of a truncated PAN and a random alphanumeric sequence presents a significant barrier for criminals moving from counterfeiting cards to exploiting vulnerabilities in online and in merchant systems.

In addition, the token is usually the same length and format as the original PAN, so it appears no different than a standard payment card number to back-end transaction processing systems, applications and storage. The random sequence, or "token", acts as a substitute value for the actual PAN while the data is at rest inside a retailer's systems. The token can be reversed to its true associated PAN value at any time with the right decryption keys. Tokens can be either single use tokens or multi-use tokens.

Most payments organizations that are considering serving as a Token Service Provider (TSP) are going to want a solution that allows for multiple uses of the token values and is flexible enough to support new payment methods in the future. In this scenario, tokens can potentially be used for repeat purchases, recurring payments, 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.

What Payments Organizations Should Consider Regarding Tokenization

There are several other areas for consideration that also come into play, either directly or indirectly depending on the role of the intermediary, when payment organizations are considering their approach to 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 is 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, organizations will need to explore related subjects such as token lifetime, distinguishability, domain-setup and assurance levels. These various options and associated variables will require many TSPs and other organizations operating in a tokenized environment to seek partners that have proven methodologies and domain expertise in this area.

These partners will use best of breed practices tailored specifically to the issues and challenges involved in delivering a solution that addresses the complexities associated with tokenization. They will structure their work with clients around several phases tailored to the deployment of a tokenization environment. Each phase will need to be comprehensive in cataloging and addressing all the impacts tokenization can have on a payments organization.

Consultative Phase

There are several other areas for consideration that also come into play, either directly or indirectly depending on the role of the intermediary, when payment organizations are considering their approach to tokenization.

The partner chosen should have a vertically integrated approach to the project, starting with the ability to catalogue and comprehend the business drivers for the TSP service the client wishes to deploy. The following steps should be part of an initial consultative phase of the project.

Understanding the business drivers: Working with the key client stakeholders, the partner should document the organizational goals and market drivers to identify the business cases for implementing tokenization.

Evaluating the prioritization from both business and technology perspectives: Using the outcome from establishing the baseline business case, the solution provider should map the organizational goals and market drivers to a set of possible use cases for the client to implement and define the associated implications for the business and its IT infrastructure.

Establishing a gap analysis: Once the business case is approved and the use cases are established, a gap analysis is then conducted that includes an analysis of the "build versus" options for the client. The options should include various scenarios (e.g., hybrid options that include product and customized components of the solution) and their implications for initial and ongoing costs.

Solution providers who have domain expertise around tokenization will use a framework as part of this initial phase of the project to understand, document, evaluate and present their recommendations. This framework should feature a set of critical criteria that serve as the key reference document in the remaining phases of the project.

Requirement Phase

During the requirements phase of a tokenization project, the following areas will need to be reviewed and the information noted gathered to define the overall needs of the organization relative to the solution:

Checklist for requirement analysis (functional and non-functional):

Checklist should have the key points to cover in the requirement analysis reducing the iteration and rework on the detailed requirement specification and integration definition. For instance, the checklist should cover specific needs on:

Member profile management application

- Number of token bins and token ranges to be provisioned
- Token requester registration related changes
- Token service participation related changes

Authorization System

- New message type creation
- New data element creation
- New data element values for existing/new data elements
- Business rules corresponding to domain control
- Business rules corresponding to token assurance level
- Existing authentication services that require de-tokenized PAN
- Transaction monitoring process
- Transaction logging process

Clearing & Settlement and Dispute Management System

- Token-PAN distinguishability
- New message creation
- New service request creation

Data Services System

- New token data elements
- Token-PAN distinguishability

Questionnaire to enable faster identification of specific needs:

A comprehensive questionnaire should be the supporting artifact to establish key requirements, as well as the primary approach to the build, integrate and implementation phase for the solution. Focusing on the areas below in the questionnaire will help maximize the time of subject matter experts (SMEs) and architects working on the project:

- Token bin provisioning process
- New message and data element creation process
- Any specific database management related guidelines to be followed for Token Vault creation and commissioning
- Mode of communication between Authorization, C&S, DMS systems etc.
- Technical documentation related guidelines
- Message types and data elements to be defined for Token generation and de-tokenization requests/ responses in case of ISO/XML API parameters for web-based service calls

Build, Integrate and Implement Phase

There are several other areas for consideration that also come into play, either directly or indirectly depending on the role of the intermediary, when payment organizations are considering their approach to tokenization.

Depending on the outcome of the previous phases, this phase could be a build, buy and integrate or a hybrid of the two. Whatever the decision, the partner should provide an independent Verification and

Validation (V/V) service that provides a complete traceability from the business case and use cases to the requirements, design and testing.

A solution provider with an established practice in tokenization will utilize reusable artifacts during implementation to accelerate establishing a baseline for design and speed the start of development and testing with specific alignment with client's requirement. These artifacts should include:

- Baseline data model and interface definitions
- Use cases and data flows for different transaction scenarios
- Interface API with required and optional parameters
- Integration test scenarios
- Test matrix for functional testing
- Test matrix for integration testing
- Verification
- Traceability matrix for making sure the use cases are properly integrated into the requirements and the requirements are properly covered by the test cases.

In addition to considering a partner's specific expertise in tokenization and best practices associated with it, a client should consider that company's specific expertise in the payments industry. The client should seek partners with a proven track record that features delivering solutions that can be maintained and expanded easily in an environment that requires continuous availability and high performance.

RS Software's Proprietary Tokenization Knowledge Framework (RS-TKF)

RS Software has developed a proprietary Tokenization Knowledge Framework (RS-TKF) based on the EMVCo specifications. This RS-TKF is one of several strategic initiatives sponsored at the RS School of Payments™ and RS Payments Lab™, both of which constitute an integral part of the RS Global Execution Methodology (GEM™).

RS-TKF: Proprietary Tokenization Knowledge Framework

- Accelerators for time to market
- Validators as key reference points to the developed solution

Use cases covering the lifecycle from token provisioning, lifecycle management and service monitoring

Detailed artifacts including sequence diagrams, detailed interface definition to create design documents

Test scenarios and test cases to validate tokenization solution including changes and impacts to the core system

Artifacts to identify the downstream impact including disputes, analytics, billing, reporting

The RS-TKF assesses the impact to Token Service Provider (TSP) system architectures when compensating for volume, capacity and scalability. The framework also offers technology use cases for implementing tokenization for a TSP; e.g., how to reduce possibility of token collision, and how to reduce latency within the token vault by choosing the right token formats.

In addition, the RS-TKF provides descriptions of message flow and structure, testing scenarios and test cases as well as downstream impacts to disputes, analytics, billing and reporting. Lastly, with the RS-TKF, clients are provided with an understanding of APIs and their internal and external parameters in a TSP environment, class and integration diagrams and data modelling options.

RS Software has conducted a comprehensive analysis focused on the implementation of tokenization and its impact on services like authorization cycle, clearing and settlement, dispute management and downstream value-added services. We have a deep understanding of tokenization stemming from numerous projects in the areas of the end-to-end transaction lifecycles, EMV enablement, parsing and routing, authorization, clearing, settlement, and dispute management.

RS Software has 20+ years of experience providing technology solutions to the electronic payments industry. From payment networks to processors, from acquirers and issuers to ISOs and retailers, we have helped our clients address the convergence of payment types, the proliferation of mobile devices, the move to cloud computing and the introduction of new strategies, such as behavioural targeting. No other custom software provider delivers more industry-specific knowledge and experience to organizations that compete for market share globally in the electronic payments industry.

We serve a client list that includes the world's leading payment brands, major acquiring processors and issuers. Our company has successfully provided solutions to customers throughout the world proving our payments-focused project methodology in a variety of regulatory environments. Our global delivery model and knowledge transfer disciplines ensure that the cross-culture experience of RS brings maximum value to the customer from start to finish.

RS Software, the sponsor of this report, is a company of 1,000 resources focused specifically on the acquiring, issuing and payment processing space. For more than 20 years, RS Software has served this space with a vertically integrated approach to providing solutions to many of the leading brands in it.

RS Software