Tokenization: A Fraud-free Payments Landscape in the Making

Abstract

Banks are under pressure to meet customers' demands for convenient and frictionless digital payments. At the same time, they are required to ensure the security and safety of such transactions – an effective tokenization solution is fast emerging as the answer. There are various approaches to implementing a tokenization solution depending on the diverse payment offerings offered by banks and the extent of their participation in the larger ecosystem. This paper describes the considerations, impacts, and implications of build and buy approaches to implementing tokenization solutions.

Tokenization: What is in it for Banks?

An effective tokenization solution will enable banks to ensure the safe and secure conduct of payment transactions in any context of money movement or commerce. With new payment form factors, channels, and payment models driven by open APIs, and real-time payment schemes driving payment initiatives, tokenization is no longer restricted to card payments. By removing sensitive data from the transaction process, tokenization makes it impossible for fraudsters to misuse transaction data. With increasing regulatory focus on consumer protection, the potential use cases and business models for tokenized account-based instant payments will increase. An effective tokenization solution will help banks acquire the necessary agility to leverage new payment form factors and allow customers to make secure payments, in turn unlocking exponential value for banks.

Implementation Approaches and Models

Depending on their size and scope of operations, banks may choose to either maintain all the tokenization components in-house or opt for a combination of outsourcing and in-house operations or outsource the complete process. For example, large banks may choose to manage all the tokenization elements such as issuance, storage, transaction processing, and even risk authorization services in-house, while mid-sized players may restrict themselves to building risk authorization services. Small banks, on the other hand, may collaborate with a strategic partner for the complete solution.

Implementation models vary across the industry with three standard variants:

- On-premise tokenization: managed within the financial institutions' IT infrastructure delivering a high degree of security but with significant overheads
- Hybrid: mix of on-premise and outsourced components for niche use cases but with longer time-to-market
- Cloud-based APIs for as-a-service models: outsourced to service providers outside the institutions' IT infrastructure but with limited flexibility and control

In our view, cloud-based tokenization services will become dominant in the next few months and transcend well beyond the cards segment. It will facilitate overlay services on faster payment networks enhancing convenience and creating

exponential value for customers through social commerce and Internet of Things (IoT) enabled payments. Non-financial use cases such as the use of tokens for loyalty coupons abound and multiple providers will grab the opportunity to offer such services.

Key Considerations for Building a Tokenization Solution

Tokenization is a secure and cost-effective alternative to data encryption as it minimizes application level changes and reduces the potential for data exposure. Some key aspects that must be considered while building tokenization solutions include:

- **Flexibility –** to support varied formats keeping in mind the sensitive data they will need to handle. Tokens must have the capability to adapt to additional format constraints; for example, tokenization of credit card numbers may require the actual last four digits of the number to be retained in the token.
- **Synchronization services –** to ensure data recovery and data availability in applications that use token services through periodic replication as servers may be distributed across different data centers.
- **Architecture –** appropriate design to ensure superior performance, increased scalability, and higher security. Tokenization and de-tokenization services should be available through APIs to enable integration of new applications and support secure data exchange.
- **Authentication –** bi-directional authentication for all applications prior to servicing requests to verify that the connection was started with a trusted certificate from an approved application and to validate the user who issues a request.
- **Encryption –** of the sensitive data for storage in the token database. When a de-tokenization request is made, the original sensitive data should be erased immediately from the temporary memory and the log files should record only the last four or X digits of the original data for tracking purposes.

Putting it all Together: Approach to Implementation

Before embarking on implementation, banks must ensure a clear understanding of the existing state, analyze the business requirements, conduct system analysis, and identify possible use cases.

Requirements gathering: Identify the key capabilities required including but not limited to PCI DSS compliance, data security, and encryption and the various use cases for which the tokenization solution can be leveraged.

System analysis: Analyze and map the systems that store and access sensitive data (platform, database and application configurations), and identify the processing dependencies between upstream and downstream applications.

Application-specific requirements: Identify specific requirements mandatory for integrating the tokenization solution with other systems, the database platform to be used, languages to be used for writing applications, the authentication methods, and the APIs to be developed to facilitate data exchange between applications.

Define solution capabilities: Based on analysis of how the credential data is to be used by different applications, assess whether single- or multi-use tokens are required. Also, determine the expiry timelines for single-use tokens and check whether multi-use tokens can be used for different transaction contexts such as in-store purchase, ecommerce, or peer-to-peer (P2P) money transfer.

Implementation options: Based on business requirements, use cases, analysis of the application systems within the payment processing platform, and application integration requirements, decide whether to build and deploy the solution in-house or choose one of the various solutions available in the market after a well-rounded analysis. Banks that choose to use a third-party solution must also decide whether to host it on-premise or partner with a service provider.

Several third-party tokenization solutions are available in the market. Some of the top players in this space are Gemalto, TokenEx, Hosted PCI, Thales eSecurity, SafeNet Tokenization, Vaultive, Inc., and Spreedly. These solutions are cloud-compatible and have the capability to provide vault and vault-less token services. Banks looking at third-party tokenization solutions must conduct a proof-of-concept (PoC) to ensure that the chosen product meets compatibility and fulfillment

requirements for key features. Typically, a tokenization solution must meet the following requirements:

- Integration with identity and access management systems to ensure verification and control of users who place tokenization and de-tokenization requests
- Token server with embedded data store encryption, key management services, transaction monitoring, securing communications, and verification of de-tokenization requests
- Scalability across geographies and products to provide the same level of service performance despite increased volume and variety of data
- Quick response to new token requests and eliminating delays in fulfilling tokenization and de-tokenization requests
- Support for multiple token vaults (MS SQL, Oracle, MySQL), API services for token service consuming entities, and vendor token server failover capabilities

Making the Right Choice: Build or Buy?

Banks will need to take into account multiple considerations while deciding on whether to build the solution in-house or opt for a third-party solution. Table 1 depicts a high-level comparison of both options across some key parameters.

Serial No.	Solution Parameters	Build	Buy
1	Ability to embed into existing applications	●	◐
2	PCI scoping and compliance liabilities	◐	●
3	Brand reputation risks due to data breaches	◐	◕
4	Omni-channel experience strategies	◕	◐
5	Flexibility to connect to multiple processors	●	◐
6	Change implementation and customization	◕	◔
7	Extensibility and scalability	◐	◐
8	Implementation cycle time	◐	◕
9	Competitive advantage with bespoke use cases	◕	◔
10	Integrated reporting and customer servicing	◐	●
11	Maintenance and monitoring of token platform	◔	◕
12	Retain business and functional expertise	◔	◕
13	Return on investment	◐	◕
14	Data portability, change of TSP	◕	◔
15	Total cost of ownership	◐	◕

Unfavorable ← ○ ◔ ◐ ◕ ● → Favorable

PCI – Payment Card Industry
TSP – Token Service Provider

Table 1: Build versus Buy Comparison for Tokenization Solution Implementation

Based on an evaluation of specific requirements like preference for single or multi-use tokens or different token formats, organizations will need to decide on whether to build or buy the solution. Building the solution in-house will reduce long-term costs of token operations and render the flexibility required to customize the solution. Moreover, it will also provide banks an opportunity to white-label the solution to their partners. However, in-house development will take a longer time to roll out and entail higher initial investment. As depicted in Table 1, each option comes with its own set of strengths and weaknesses. Banks must make a choice based on an assessment of their critical parameters and strategic objectives.

The Bottom Line

The proliferation of digital payments has been one of the most prominent outcomes of the digital revolution. However, this has increased the onus on banks to ensure secure and safe customer payments underscoring the need for a holistic tokenization strategy. Moreover, meeting rising customer expectations in digital payments will require banks to leverage extended partner ecosystems and offer overlay services, which will help create exponential value for customers as well as businesses However, a robust tokenization solution is a prerequisite to offering overlay services, and banks would do well to incorporate tokenization into their digital payment strategies.

About The Author

Debasis Thakur

Debasis Thakur is a Senior Payments Consultant with the Cards and Payments group within TCS' Banking, Financial Services, and Insurance (BFSI) business unit. He has over 20 years of experience in working with global banking clients in the areas of business development and solution design focusing on cards and payments. Thakur has anchored several transformational projects for TCS' clients the world over, and is currently focusing on innovations in the digital payments space to help global financial institutions reimagine their payment processes.

Contact

Visit the Banking & Financial Services page on www.tcs.com

Email: bfs.marketing@tcs.com

Blog: Drive Governance

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty. IT Services
Business Solutions
Consulting

TCS Design Services I M I 10 I 18