Tokenization: The future of Secured Payments

January 2019

pwc

Foreword

Dear Readers,

It is our pleasure to bring to you the latest edition of our Payments newsletter.

With a need for enhanced security in the payments transaction environment, tokenization holds substantial promise to address this critical need. This newsletter aims to provide key insights into origination of tokenization, the typical use cases of card tokenization and the impact of RBI's recent circular on implementation of card tokenization.

I hope you will find this to be an insightful read.

For details or feedback, please write to

vivek.belgavi@pwc.com or mihir.gandhi@pwc.com

pwc

In this issue

Introduction

The payments industry is progressing to support new payment form factors that require intensified protection against counterfeit, account misuse, and other forms of frauds. Thus security is needed for card-not-present, card present and hybrid transaction environments to help minimize unauthorized use of cardholder account data and prevent cross-channel fraud. Tokenization as a concept holds substantial promise to address this need.

In **2001,** Trust Commerce created the concept of Tokenization to protect sensitive payment data for a client, Classmates.com.[1][2] Further the application of Tokenization was applied to payment card data by Shift4 Corporation and released to the public during an industry Security Summit in Las Vegas, Nevada in 2005.[1] Card tokenization has gained acceptance across the world with Apple Pay, Samsung Pay and Google Pay facilitating retail payments through mobile devices, with involvement of card networks like VISA, Mastercard, American Express, Discover, JCB etc.

Card tokenization made entry into India with launch of Samsung Pay using which customers with Samsung Mobile devices could make payments at PoS terminals (NFC & non-NFC enabled). As others players keenly watched the space, Reserve Bank of India (RBI) with its latest circular has laid down the rules for card tokenization which is still in a nascent stage even after its launch 2 years ago.

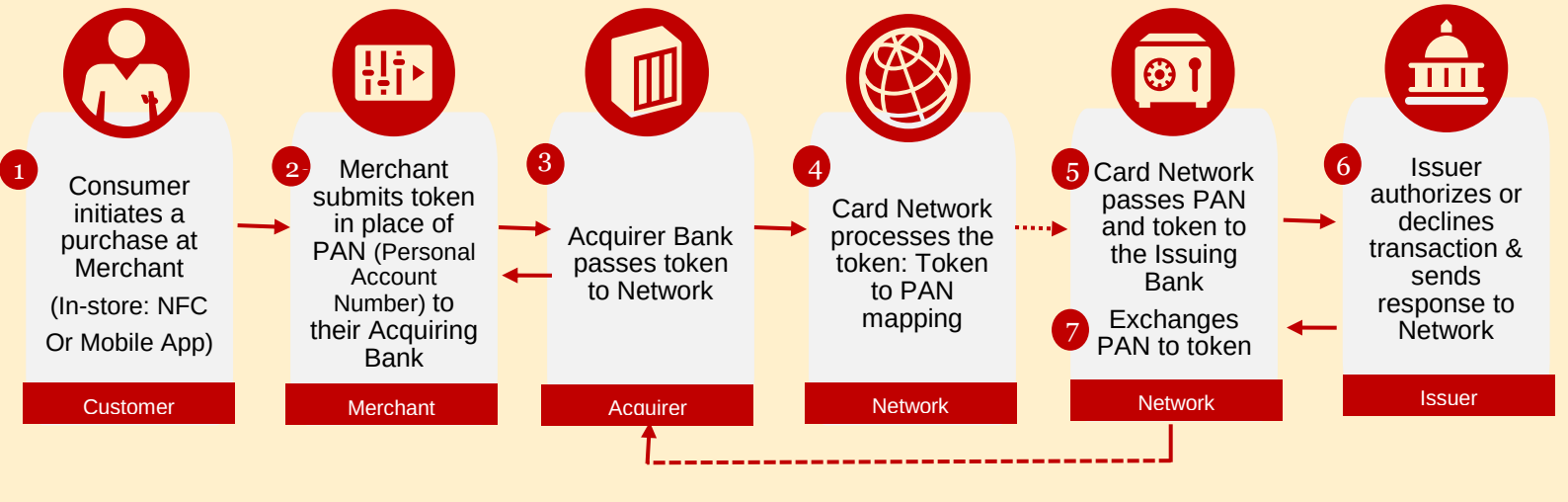
[1] https://en.wikipedia.org/wiki/Tokenization_(data_security)
[2] https://www.trustcommerce.com/blog/where-did-tokenization-come-from/
[3] https://townsendsecurity.com/sites/default/files/Tokenization.pdf

At present Tokenization is currently in standards definition in ANSI X9 as X9.119 Part 2 .X9 is responsible for the industry standards for financial cryptography and data protection including payment card PIN management, credit and debit card encryption and related technologies and processes.[1]

Card tokenization is the process of replacing sensitive information, such as a debit card or credit card number, with a surrogate value called token that will be issued by a bank.[3] The original value of the card may be stored locally in a protected data warehouse, which is placed at a remote service provider, or not stored at all. The goal of tokenization is to reduce or eliminate the risk of loss of sensitive data, and to avoid the expensive process of notification, loss reimbursement, and legal action.[3]

Tokenization ensures enhanced security without hampering the customer journey/experience

For a customer there is no change in the way payment is made either in-store or online. However, no merchant will be able to store customer's original debit or credit card number. In place of the actual card number, a randomly generated token ID issued by customer's bank will be utilized. Furthermore, the 16-digit token which masks customer's actual card number, will be dynamic in nature. Due to the random assignation of tokens, it's almost impossible to reverse-engineer or compromise a token making the process of tokenization superior to other methods of encryption.



Decoding RBI Circular
& Understanding its impact for various Stakeholders

On 08 January 2019, the Reserve Bank of India (RBI) issued guidelines for card tokenization with an aim to further enhance the security of the payments ecosystem in India. It stated that banks, with the support of card networks, can offer tokenization services to holders of debit, credit and prepaid cards. This permission extends to all use cases/channels (NFC, MST, in app payments, QR code payments) or token storage mechanisms (cloud, secure element, trusted execution environment). For the first phase, this facility shall be offered through mobile phones/tablets only. Its extension to other devices will be leveraged later based on experience gained.

Role of Networks in Card Tokenization

- RBI has decided to permit only *authorized card payment networks* to offer card tokenization services to any token requestor i.e. by Visa's Visa Tokenization Service or MasterCard's MDES
- Card networks, need to define a process for *periodic system audits* at least annually, for all entities involved in the value chain for providing the card tokenization services to the customers.
- Additionally, networks must maintain request logs and make available when required. Card Network needs to take care for the process of certification for the token requestor.
- Card networks will have to introduce Additional Factor of Authentication (AFA) like OTP or PIN for card tokenized transaction. This will replace Customer Device Cardholder Verification Method through device biometric/ PIN and has been used by the customers to authenticate transactions. Card networks and token requestors have to ensure data security in compliance with PCI DSS guidelines and undertake certification and periodic audit of the systems.

Role of Issuing Bank in Card Tokenization

- Issuing Bank will be providing tokenization service to their cardholders *without any additional fees* on receiving the request from the customers
- Issuing Bank needs to provision that customer gets an *option for registering /deregistering* themselves for a particular bank specific tokenization use case which can be contactless/MST based, in-app payments.
- Customers will have to be given option to set and modify transaction limits for their tokens. Currently customers need to approach the issuer call center to manage token lifecycle. Issuers may look forward to make changes in their DCMS or bring in any other application to provide interface to the customers for token management and limit control.
- Keeping customer's security at the center RBI has asked issuing banks to put suitable velocity checks (i.e. how many transactions can be allowed by the customers in day/week/month). Banks can implement such checks over their existing risk management engines like Visa Risk Manager (VRM) & Mastercard's Expert Monitoring Solutions (EMS).

Thus with this circular RBI has defined roles & responsibilities of card networks & issuing bank w.r.t enhancement of tokenization acceptance as a service in India focusing simultaneously on customer's security & centricity.

The RBI guidelines will encourage card networks like VISA and Mastercard to expand card tokenization in the country in collaboration with other players like Apple, Google, Fitbit, Garmin etc. Networks like Discover, JCB and Union Pay who are trying to increase their footprint in the country can explore tie-up with National Payment Corporation of India (NPCI) to bring card tokenization to the country.

How can Bank's embrace for card tokenization?

Enhance systems like Switch, Card Management Systems, and Reconciliation System etc. to process token based transactions

Define rules in risk engines to accommodate transactional and environmental parameters based on which transactions will be processed.

Educate customers about the benefits, use cases of card tokenization

Sensitize call center agents to handle specific queries & dispute management

Participating **merchants**/ digital wallets will have to either directly integrate with card networks or token service providers to maintain card tokens in a secured environment. These token service providers have to be PCI DSS complaint and certified by card networks. Banks and card networks have to work together to encourage digital merchants to support tokenized transactions.

Acceptance of NFC based payments through mobile devices will form the largest use case as deployment of NFC capable PoS terminals increase in the country.

If **RBI** opens up **other use cases like e-commerce and card on file** over a period of time - online merchants in segments like food ordering, travel, online shopping etc., (who witness repeat purchase), will gain from card tokenization. Till such use case is allowed by RBI, applications like Samsung Pay, Jio Pay, PayTM, as and when they support card tokenization, will have to integrate with merchant apps.

Digital Wallets like Mobikwik, PhonePe, Amazon Pay, PayTM etc. may find in-app integrations as a use case where customer can make payments through the app without loading the wallet.

In India, as implementation of card tokenization gathers pace in retail payments space, we will see its usage extend to transit system on similar lines as in Singapore, Utah, and London etc.

In a nutshell, card tokenization can be seen as a change in the manner in which country will make payments for their purchases and transit fare. It further improves security in card transactions which will address the concerns of the consumers and thereby improving adoption of digital payments. RBI with its guidelines on Card Tokenization has defined the rules of the game for benefit of all the stakeholders i.e. Banks, card networks, merchants and customers

(With inputs from Mihir Gandhi, Neha Jaeel, Kanishk Sarkar, Raghav Saigal and Jaya Gupta)

Payments Technology Updates

RBI allows tokenization of card transactions, even for third party apps

Economic Times (Tech)

The Reserve Bank of India has allowed tokenization of debit, credit and prepaid card transactions to enhance the safety of the digital payments ecosystem in the country. By this means the regulator will allow the card details to be masked while a transaction is processed at point of sales, QR codes and other payment modes.

(Read More)

Understanding RBI's Big Move to Make Your Credit And Debit Card Transactions Safer

News18

The central bank is introducing a system called 'tokenization', which means you as a user will be able to create an alternate unique code that can replace the actual credit or debit card details while making a transaction or payment.

(Read More)

Bitcoin ATMs Now Number Over 4,000 Worldwide Despite Crypto Price Drop

valuewalk.com

Currently, the three most established systems are from Apple, Samsung and Google. Mobile payment systems use a method called tokenization to keep card details secure.

(Read More)

RBI Releases Guidelines for Electronic Card Payments

pymnts.com

The Reserve Bank of India has released guidelines for what it calls the "tokenization" of debit and credit card transactions, according to reports. The bank has offered permission for the process using all types of payment services and methods, including near-field communication (NFC), magnetic secure transmission (MST), in-app payment methods and cloud services.

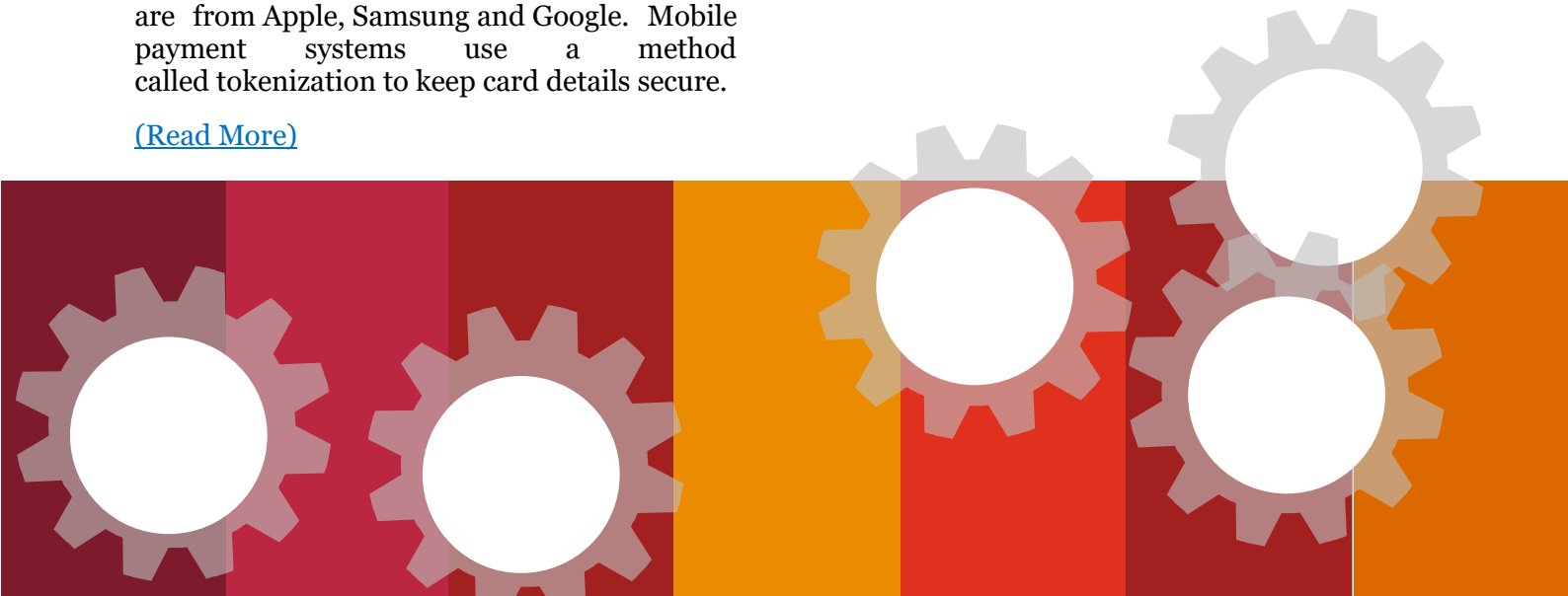
(Read More)

Tokenization Market Is Driven by the Increase in Cyberattacks and Data Breaches

Digital Journal

Need for payment card industry data security standard (PCI-DSS) compliance to secure cardholder data driving the global tokenization market

(Read More)



Please contact

For more information, please contact:

Vivek Belgavi
Partner & Leader – Financial Services Technology Consulting and India FinTech Leader

Tel: +91 9820280199
Email: vivek.belgavi@pwc.com

Mihir Gandhi
Partner & Leader – Payments Transformation

Tel: +91 9930944573
Email: mihir.ganhi@pwc.com