CAMSPay®

Payments Insider

Tokenization

A Triple S Factor!

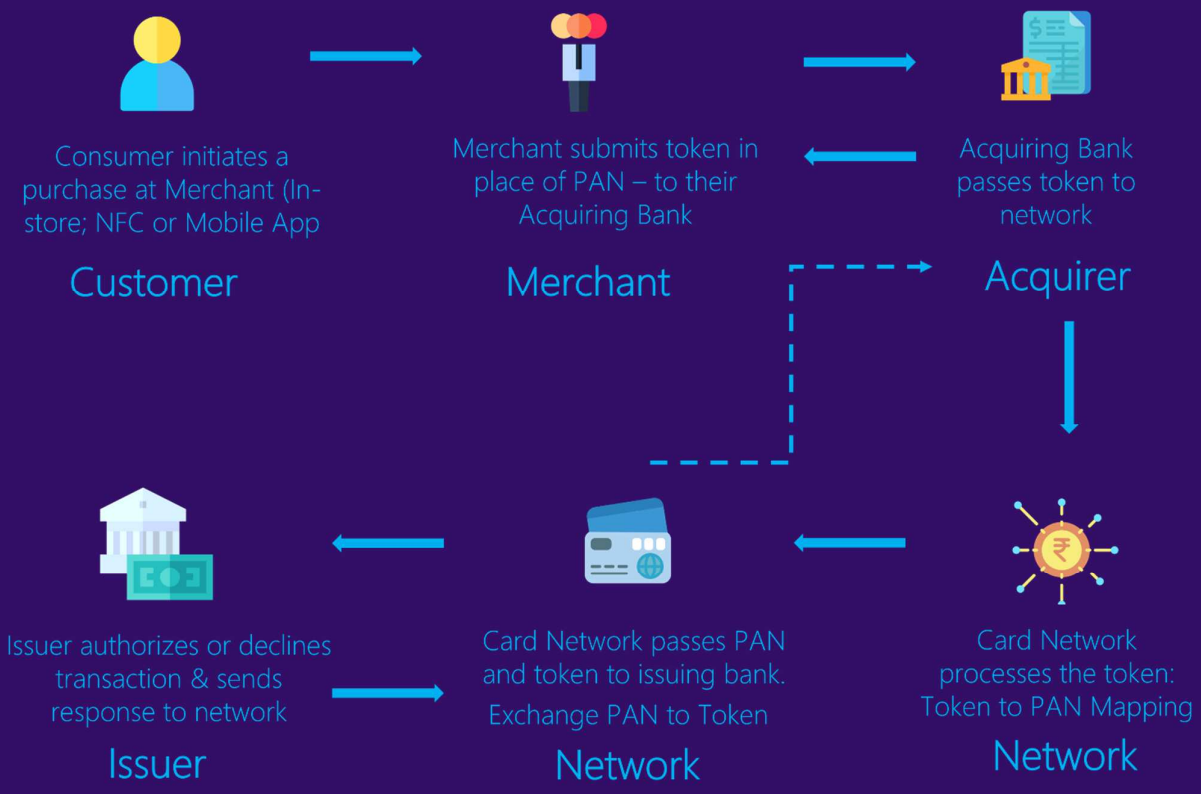
Substitution . Solution . Security

Tokenization is an industry-wide solution that ensures the cardholder's data is kept secure. This is performed by assigning a random string of characters to the receiver of the cardholder data and returning that string to the provider of the cardholder data. It's nearly impossible to reverse-engineer or compromise a token due to its random assignment.

A method of substituting a surrogate value for sensitive data.

In simple terms,

A merchant would send the credit card number to a trusted partner, such as your payment gateway, via encryption. In turn, the payment gateway will provide you with a reference number that reflects that credit card in their system. This is a random string associated with the payment card number you, the merchant, provided to the gateway.



- A credit card is swiped at a cash register or used to make an online purchase.
- The tokenization system receives the credit card number.
- To replace the original credit card number, the tokenization algorithm generates a string of 16 random characters.
- This system sends the newly created 16-digit random characters to the POS machine or e-commerce site, in place of the customer's credit card number.

Tokenization improves security without interfering with the customer's journey or experience.

Tokens are only useful if they are used in the correct gateway. What makes this system so safe is that no disgruntled employee or malicious attacker can use this token to steal our money, even if they have it. Even if this would-be attacker succeeded in stealing the token, the money would be in your bank account, which you would have complete control over.

It's also worth noting that, with the correct payment gateway, you may tokenize your bank account data. Tokenization is possible for both cards and accounts

Key Features of Tokenization

- It's efficient and cost-effective.
- Enables better cardholder experience while maintaining total data security
- Simple to set up.
- Global accessibility.
- A plug-and-play mobile solution that is particularly intended to protect card details while using digital wallets or in-app payments.

Who needs Tokenization?

- Mobile payment-focused independent sales groups.
- Any merchant who uses the "card on file" feature.
- Financial Institutions and Banks
- Retailers
- Ecommerce companies that offer digital wallets, mobile payments, and in-app purchases.
- Businesses that have a policy of not holding credit card information for security purposes.

Tokenization – Global Scenario?

North America was expected to have the largest tokenization market share in 2020, and APAC was expected to grow at the fastest CAGR over the forecast period. Any merchant who uses the "card on file" feature.

CAGR
19.5%

The global Tokenization market is expected to be worth USD 4.8 Billion by 2025, growing at a CAGR of 19.5% during the forecast period.

- The market growth can be attributed to the increased alignment of customers towards contactless payments and rising demand for cloud-based tokenization solutions and services.
- The global post-COVID-19 tokenization market is estimated grow from USD 1.9 billion in 2020 and reach USD 4.8 billion by 2025.
- The increasing need to stay compliant with regulations and growing need to ensure continuous customer experience and maintain fraud prevention levels are driving the tokenization market growth.
- Among verticals, the retails and eCommerce segment have great opportunities and is expected to grow at the highest CAGR during the forecast period.

Indian Scenario

Frauds involving INR 1 lakh or more increased at a CAGR of 34% between 2017 and 2020.

Visa Token Services, which have been in use in India since 2017, are aimed to facilitate safe payments across a wide range of connected devices, numerous digital wallet providers, and future payment innovations around the world.

The bank has granted permission to use all payment services and methods, including near-field communication (NFC), magnetic secure transmission (MST), in-app payment methods, and cloud services.

To guarantee the method is secure and protected, RBI recommends that tokenization and de-tokenization be performed only by an authorized card network, and that the request be recorded and retrievable if necessary.

According to the RBI, banks and card payment networks must be able to conduct a periodic system audit of all parties involved in the process of providing service to clients at least once a year.
The RBI also wants card issuers to make sure that users can simply report the loss of a "identified card," which might lead to unlawful access to personal information or funds.

For more latest industry news,
follow us on our socials

@camspay

www.camspay.com