cross river

Member FDIC

May 2023

Tokenization in Card Networks

Sensitive Information to Non-Sensitive Values

Over the past 20 years, the card payment system has seen data breaches exposing millions of customer records. One of the most massive breaches occurred in 2008, when hackers used a SQL injection to gain access to Heartland Payment Systems' corporate network and obtained six months of payment card data. Over 160 million credit and debit card accounts were compromised with an estimated monetary loss around $300 million.[1]

In response to the attack, additional protective measures including card data encryption and the PCI compliant standards were adopted. Unfortunately, a second hack occurred again in 2015 and 2,200 individual's personally identifiable information was stolen. The data breach indicated the need for data protection in the payment process.

Recently, card payment system has grown more sophisticated and has advanced to enable higher security and a better user experience. A leading innovation in the card payments system is the technology of tokenization.

The Traditional Card Transaction Flow

Before introducing the concept of tokenization, it is helpful to understand the traditional process of a card transaction.

A transaction typically includes three to four stakeholders depending on the transaction model.

Historically, Mastercard and Visa have been using a four-party model where the four parties include a cardholder, a merchant, an acquirer, and an issuer. American Express has operated a three-party model where the issuer and acquirer are the same. This means that it not only processes transactions but also issues its own cards. American Express began to transition to the four-party model to enable members who meet the model requirements to join the network.

Let us go into more details on the stakeholders:

*** Network**

The system that connects all stakeholders together, functioning as the backbone that facilitates a credit or debit card payment. Examples of card networks include Visa, Mastercard, American Express and Discover.

1. Cardholder

The person who wants to make a card payment to purchase goods or services.

2. Merchant

The seller of goods or services. The cardholder needs to pay the merchant for purchases.

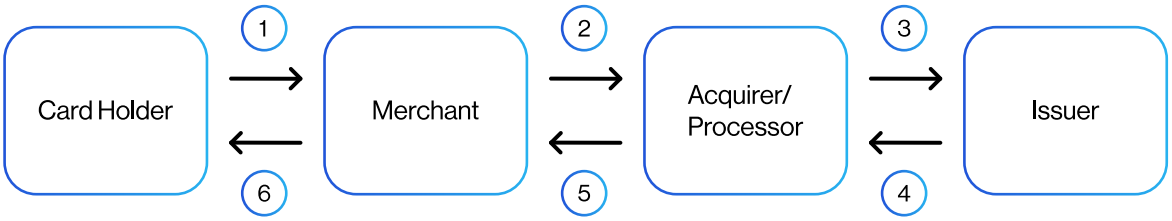
3. Acquirer/Processor

The provider of a varied combination of services to merchants, including supporting merchants with POS terminals, software, card processing, dispute management, and merchant-customer services. An acquirer may also serve as a gateway or processor which verifies or sends the card information to card networks or banks.

4. Issuer

The bank that is licensed by the Network to issue cards to the cardholder. Some

examples are Citi, Chase, and Bank of America.



Traditional Card Transaction Flow where Card Holder's sensitive details are passed

In this process, a cardholder provides card details to the merchant to initiate a transaction. The merchant then passes these details to the payment processor for authorization. The payment processor relays this information to the card network and sends it to the issuing bank for final approval. In the traditional card payment system, complete transaction details are shared with all the parties.

Transactional details include the following:

- Payment Card Information (Payment Account Number (PAN),[2] expiry date, CVX,[3] cardholder address information)
- Payment Amount
- Transaction Currency
- Merchant Name and Location

For users, the payment system poses several security risks to users' confidential information and can lead to identity theft and unauthorized use of cards. For merchants, payment data security is laborious and expensive to manage and secure user data. As a solution, tokenization becomes an important means of mitigating payment card risks.

An Introduction to Tokenization in Card Networks

The objective of tokenization is to replace sensitive information with non-sensitive values. A token value is considered non-sensitive when it does not have any value to an attacker or hacker. The Payment Card Industry (PCI) Security Standards Council defines card tokenization as "a process by which the primary account number (PAN) is replaced with a surrogate value called a token."[4]

Through tokenization, instead of using complete card information for transaction processing, the concerned parties transfer a token for payment processing. Since the respective card details of a token are saved in a secured vault, a hacker who manages to retrieve the token cannot fetch card details from it.

It should be noted that tokenization is not equivalent to encryption. Tokens are generated using a series of random numbers, so they are not mathematically reversible by design. To retrieve the underlying information that is tokenized, a user needs to access the original data from a secured vault and find the pairing. Encryption, on the other hand, uses a key to convert information to unintelligible strings. Encryption is mathematically reversible in that a hacker can, decrypt the unintelligible strings if he obtain the key.

The History of Tokenization

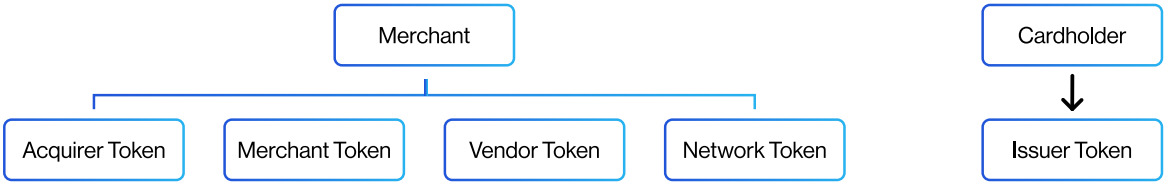
The concept of tokenization predates the digital payment era. Indeed, any object representing value can function as a token: a subway coin, a stack of casino chips, or even a pay toilet token. In the 1970s, value representation was replicated in the digital ecosystem to secure confidential data.[5]

Within the payment ecosystem, tokenization was first introduced in 2001 by TrustCommerce, a payment processor, to secure client-sensitive payment data. In 2005, during a Security Summit in Las Vegas, Nevada, Shift4 Corporation introduced tokenization for card payments.[6]

Since then, tokenization has evolved to give rise to five major types of tokens.

The Five Types of Tokens

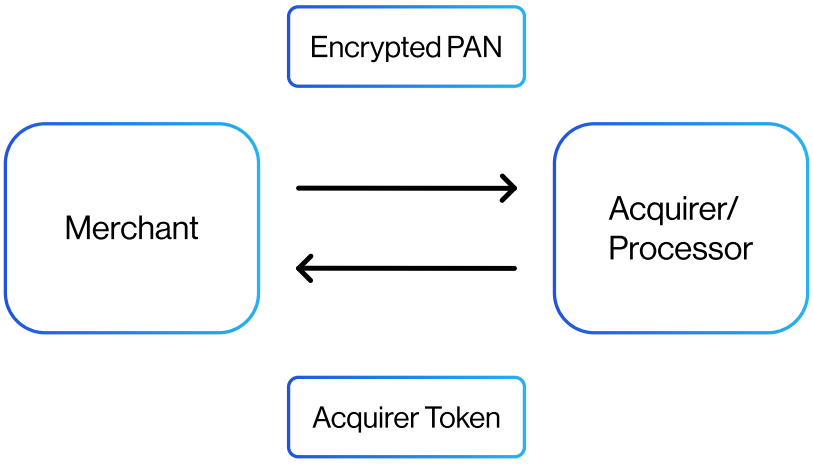
The evolution of tokenization has progressed from covering a part of the transaction to impacting the entire transaction flow. Tokens can be classified according to when they are generated in the payment process. The five types of tokens are acquirer tokens, merchant tokens, vendor tokens, network tokens, and issuer tokens.



Four of the token types – acquirer, merchant, vendor, and network – are designed to improve merchants' experience in managing payments. The fifth token type, issuer tokens, mainly benefit cardholders by enabling them to conduct digital payments.

These five types of tokens focus on merchants and cardholders, the two main stakeholders on the front-end of the transaction chain. While tokenization has the potential to benefit all stakeholders, including the back-end processors (acquirer, network, and issuer), the current development of tokenization has focused on front-end users.

Merchant-Specific Tokens



Acquirer tokens

Generated by the acquirer as part of the transaction process. The merchant transmits the cardholder's PAN to the acquirer to initiate the purchase process as described above. Before returning the issuer response to the merchant, the acquirer stores the PAN in their token vault and sends back the acquirer token to the merchant in place of the PAN. The tokenization step takes place as a one-way response from the acquirer to the merchant.[7] The merchant can store the token safely because the token can only be used when exchanged for the PAN in the acquirer's token vault. Merchants can continue to transact with the token if there are subsequent "card on file" transactions, or in the event a refund is needed.

The limitation of acquirer tokenization is that the token can only be used between the merchant and the acquirer who created it. If a merchant deals with multiple acquirers, the token issued by acquirer A cannot be used with acquirer B. This can become a problem when merchants use multiple acquirers for separate sales channels. For example, if the merchant works with different acquirers for online and in-store services, the merchant can't use the token created as part of an online purchase to issue an in-store refund, requiring the cardholder to re-present their card.

Merchant tokens

Generated by the merchant or a group of related merchants aiming to solve the limitations of acquirer tokens by managing tokens themselves.

At the time of the transaction, the merchant generates the token against cardholder details and stores the client's information in their own token vault. It then incorporates this merchant token in the other parts of the transaction flow. When a client returns, the merchant can fetch the client's token for payment processing.

This enables the merchant to manage one token for each client while working with multiple acquirers. However, these tokens are generally specific to a single merchant and not interoperable with other merchants.

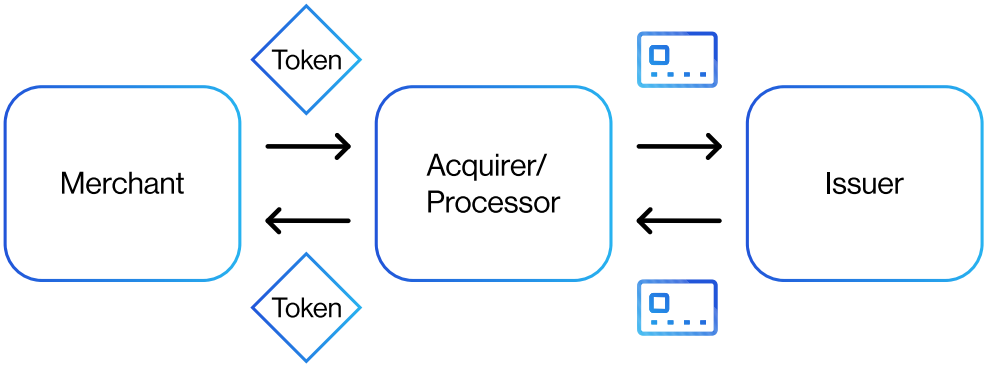
Vendor tokens

Generated by merchants' service providers. Vendor tokens can be shared by multiple unrelated merchants making them a more interoperable token. Vendor tokens also relieve a merchant from PCI DSS compliance, as the service provider is responsible for the compliance.

Network tokens

Generated by card networks such as Visa and Mastercard. At the time of token provisioning or generation, card details flow from cardholder to merchant to processor to card network to issuing bank. After validating card details, the issuing bank approves the registration of the card.

After approval from the issuing bank, the network generates and sends a token across to the merchant through the gateway. It should be noted that a merchant or gateway cannot store a user's card details. The merchant is only authorized to store the token generated by the network.



Network Tokenization Transaction Flow

At the time of the transaction, the merchant sends this token for approval along with the transaction amount. Users' card details would only be shared between the card network and the issuing bank.

Network Tokens are issued by card networks such as Visa, Mastercard, and American Express.

Cardholder-Specific Tokens

After discussing the four different tokens that improve merchants experience, let us turn to issuer tokens, specifically designed to enable digital payments for cardholders.

Issuer tokens

Generated by card issuers for use specific to digital wallets such as Apple Pay and Google Pay. In the case of Apple Pay, when a card is added to the Apple Pay wallet, Apple tokenizes the card information and generates an issuer token. The token is stored in the cardholders' phone and allows near-field communication (NFC) between the phone and a payments terminal. The issuer token is transmitted to the rest of the payment process pathway, where the card issuer connects to the Apple token vault to retrieve the PAN for processing.

The Current Tokenization Standard

While there are different types of tokens, a universal requirement framework to guide organizations to safeguard cardholder information was proposed in 2004 by the Payment Card Industry Security Standards Council (PCI-SSC). This framework is called the PCI Data Security Standards (PCI DSS).

The framework calls for protective measures around managing card data vaults where tokens and PANs are stored, securing cryptographic keys for encryptions, managing tokenization and de-tokenization processes, and defining tokenization scope to prevent external usages.[8] There is no legal requirement for organizations to meet the requirements, but most payment companies, including merchants, banks, processors, hardware and software developers, and point-of-sales vendors do participate.[9]

Conclusion

Tokenization in the card networks is an important technology to improve security and efficiency in the payment process. There are five types of tokens depending on when tokens are generated in the flow. Choosing the type of token to integrate depends on the objectives of the stakeholders involved.

Tokenization at Cross River

At Cross River, we embedded tokenization in our Push-to-Card disbursement (P2C) solution. P2C is a payment gateway that disburses funds in near-real-time to debit card accounts through participating debit card networks. P2C is faster and cheaper than wires and checks and allows for immediate reconciliation of books. Funds are debited as soon as the transaction completes.

The P2C process includes:

1. Merchant registers payee debit card numbers to P2C
2. Merchant funds disbursement requests to pay a registered card
3. The recipient receives funds immediately in their account

In this process, we use acquirer tokens to conduct transaction flow. When our merchants want to transact money to or from a card, they send us a card ID. We then find the corresponding card token and work with TokenEx to extrapolate PAN. By doing so, we alleviate merchants from managing data security and enhance efficiency of the payment process.

Citations & Resources

1 |
https://smartermsp.com/3-worst-data-breaches-time-learned/

2 |
PAN: Primary Account Number. It is the unique payment card number printed or embossed on the card.

3 |
CVX is a 3-digit security code printed on the back of a payment card. Visa refers them as CVC (Card Verification Code) and Mastercard refers them as CVV (Card Verification Value).

4 |
https://docs-prv.pcisecuritystandards.org/Guidance%20Document/Tokenization/Tokenization_Guidelines_Info_Supplement.pdf

5 |
https://en.wikipedia.org/wiki/Tokenization_(data_security)

6 |
https://www.pwc.in/industries/financial-services/fintech/dp/tokenization.html#:~:text=In%202001%2C%20Trust%20Commerce%20created,a%20client%2C%20Classmates.com.&text=Further%20the%20application%20of%20Tokenization,Las%20Vegas%2C%20Nevada%20in%202005.

7 |
https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-is-the-difference-between-acquiring-tokens-issuer-tokens-and-Payment-Tokens/

8 |
https://blog.rsisecurity.com/how-to-meet-tokenization-pci-dss-requirements/

9 |
https://www.pcisecuritystandards.org/get_involved/participating_organizations/

Skyflow.com

Aciworldwide.com

US Payments Forum

https://www.knowyourpayments.com/tokenization/

Authors

Jianing Wu

Sr. Product Research Associate, Strategy

Digant Chadha

Consultant

Contributors

Donald Apgar

Lead Product Manager, Card Payments & Merchant Acquiring

Andrew Lambert

Head of Product for Cards & BaaS

Disclosure

Cross River Bank and its affiliates do not provide tax, legal or accounting advice. This material has been prepared for informational purposes only, and is not intended to provide, and should not be relied on for, tax, legal or accounting advice. You should consult your own tax, legal and accounting advisors before engaging in any transaction.

Enable finance for *infinite* possibilities

Cross River's API-driven banking infrastructure embeds financial services across industries and provides the foundation for regulatory compliance upon which our partners grow.

Cross River merges the established safety and expertise of a bank with the innovation of a technology company. As experienced leaders firmly rooted in compliance, Cross River delivers streamlined end-to-end solutions propelling partner growth in an ever-evolving market.