International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V73I5P103

Volume 73 Issue 5, 14-18, May 2025

Original Article

A Technical Deep Dive into Tokenization

Kunal Nandi

Software Engineer in Test, TikTok USDS.

Corresponding Author : nandi.kunal@rediffmail.com

Received: 12 March 2025 Revised: 14 April 2025 Accepted: 30 April 2025 Published: 17 May 2025

Abstract *- Using card numbers in merchant terminals/e-commerce websites increases the risk of security breaches. In order to reduce this security breach and enhance the security of transactions, Tokenization replaces sensitive card numbers (debit/credit/prepaid) with unique, randomly generated tokens. This article provides a technical analysis of payment tokenization, covering token generation or provisioning, ID&V flow in token generation, payment transactions using Token, and a comparison among Encryption, Tokenization,3DS, Biometric Auth, TLCM and its role in the payment ecosystem.*

Keywords *- Tokenization, Digital payments, Payment security, Token Service Provider, Cryptographic validation.*

1. Introduction

The proliferation of digital payments, driven by the global adoption of e-commerce, mobile banking, and contactless technologies, has fundamentally transformed the financial landscape. Transactions are projected to reach $10.5 trillion annually by 2026 [1], intensifying the need for robust security mechanisms to protect sensitive cardholder data against escalating cyber threats such as data breaches and payment fraud. With the help of Tokenization, card numbers or PANs, i.e. Primary Account numbers, get replaced with tokens. Tokens are unique for the same device, app and card number combination. It is randomly generated. It has emerged as a cornerstone of payment security and compliance. It ensures PAN data is never exposed during transactions, unlike traditional encryption, which relies on reversible transformations, offering a paradigm shift in securing payments; as a result, unauthorized access and risk of fraud went down.

Tokenization addresses critical challenges in the payment ecosystem.

- Reduce fraud in online and in-store transactions: Tokens are useless outside their specific context.
- Prevent unauthorized access to cardholder data: Tokenization minimizes the risk of data exposure in breaches by replacing sensitive information with tokens.
- Enhancing security through cryptographic validation: Dynamic cryptograms and secure de-tokenization processes ensure transaction integrity.

Per Visa, 80% of global merchants will implement token-based payments by 2023 [2]. This article dives deep into token generation, token life cycle management and integration with digital wallet providers by providing a comprehensive technical analysis of Tokenization's mechanisms, ecosystem participants, and security benefits.

The objectives of this study are threefold:

1. To elucidate the end-to-end processes of Tokenization, from provisioning to payment flows.
2. To compare Tokenization with alternative security approaches, such as encryption and 3D Security.
3. To evaluate Tokenization's impact through empirical data on fraud reduction and adoption rates.

This article contributes to academic and industry understanding of payment security by addressing these objectives and offering insights for researchers, practitioners, and policymakers. The structure is as follows: Section2 reviews the literature, Section3 outlines the tokenization ecosystem, Section 4 details token generation, Section 5 describes payment flows, Section 6 covers lifecycle management, Section 7 compares Tokenization with existing approaches, Section 8 presents results and discussion, Section 9 discusses findings, and Section 10 concludes.

2. Literature Review

Tokenization has emerged as a critical payment security mechanism, surpassing traditional encryption in mitigating data breach risks (PCI Security Standards Council, 2018). Ulf T. Mattsson (2009) report a 30% fraud reduction for tokenized e-commerce transactions, while Visa (2023) notes an 80% global merchant adoption rate, reducing card-not-present (CNP) fraud by 25%. However, many challenges persist, such as TSP vulnerabilities (Dawoud, 2010) and cross-border interoperability (Mohanty et al., 2022). Recent studies explore Tokenization's integration with blockchain (Rani et al., 2023).

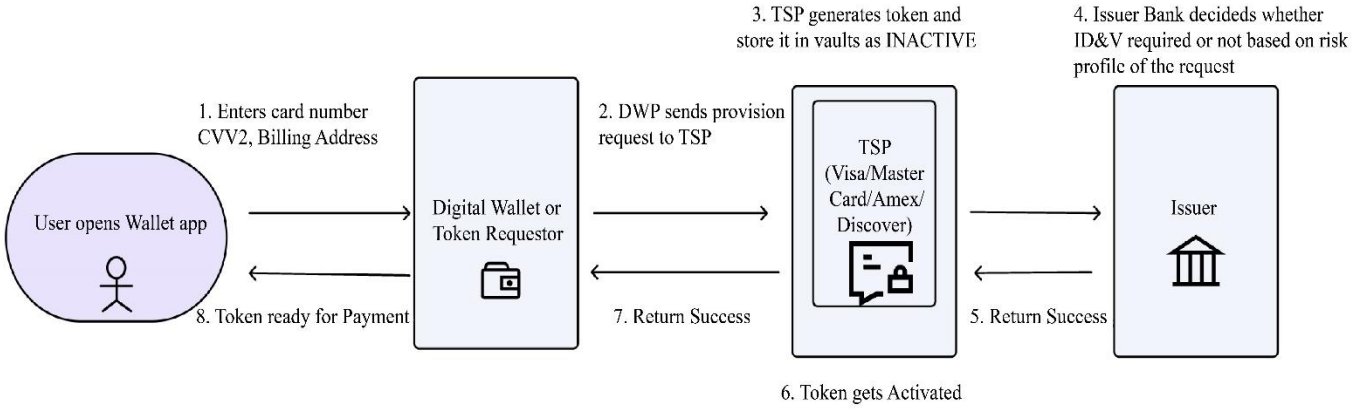


Fig. 1 Token Generation Flow

3. Tokenization Ecosystem and Participants

The key participants in the tokenization flow include:

- DWP: Digital Wallet Provider or Token Requestor. Examples: Apple Pay, Google Pay, Samsung Pay etc.
- Card Network: Visa / MasterCard/ Amex/ Discover, also known as TSP, i.e. Token Service Provider
- Issuer / Token Requestor: The entity requesting to generate a token. It can be a DWP or even an Issuer bank, such as JPMC, CITI Bank, BofA, etc.
- Merchant: Typical merchant store or e-comm website where the customer makes payments.

4. Token Generation Flow (Provisioning Flow)

Let us walk through an example of how a payment token is generated using Google Pay or Apple Pay. When a customer installs a digital wallet app on their phone, the first step is typically to scan or manually enter their card details.

Below is the one sample flow :

1. Card Entry: The user opens the digital wallet app and enters their card number, CVV2, expiration date, and other required details.
2. Device Registration: In the backend, the digital wallet registers the customer's phone with the Token Service Provider (TSP) (e.g., Visa, Mastercard) based on the entered card number. The TSP returns a unique device ID associated with the phone.
3. Eligibility Check: The app then sends an API request to the TSP with the unique device ID to verify two things:
   a. Whether the user is eligible to add their card to the wallet.
   b. Whether the user's issuing bank participates in Tokenization.
4. Bank Confirmation: If the Issuer bank confirms participation in Tokenization and the user's eligibility, the TSP returns the bank's Terms and conditions and card images to the digital wallet.
5. User Consent: The user accepts the Terms & Conditions, after which the app sends a token generation (provisioning) request to the TSP.
6. Token Creation: The TSP generates an inactive token and stores it securely in the vault. The TSP also informs the issuing bank about the new Token.
7. Issuer Authorization: Based on the bank's response:
   a) If no ID&V (Identity Verification) is required, the TSP activates the Token immediately and notifies the wallet.
   b) If ID&V is required, the Token remains inactive, and the TSP provides ID&V options (such as OTP app verification) to the digital wallet.
8. Identity Verification (ID&V): If the user selects OTP verification:
   a) The wallet sends an OTP generation request to the TSP.
   b) The TSP forwards this to the issuer bank, which sends the OTP to the customer by email, text, or phone. The TSP generates OTP.
   c) The user receives the OTP and enters it in the wallet app. Then, the wallet sends it back to the TSP to verify the OTP.
   d) Upon successful verification, the TSP activates the Token and notifies the issuer bank.

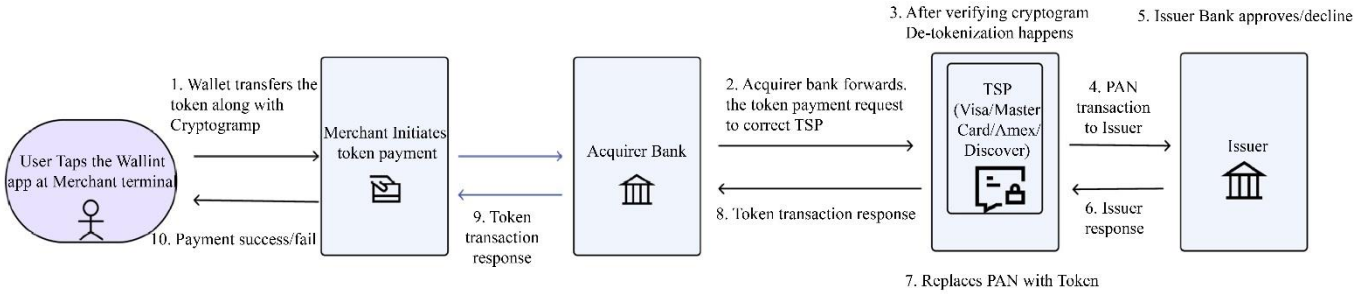
This end-to-end process ensures that the card is securely tokenized and linked to the user's device, enabling safe and seamless digital payments. Refer Figure 1.

5. Tokenized Payment Flow

Once the Token is generated, users can use it to make payments at the terminal or online. Below are the details of a typical tokenized payment transaction when a cardholder purchases something from a store and pays at a terminal :

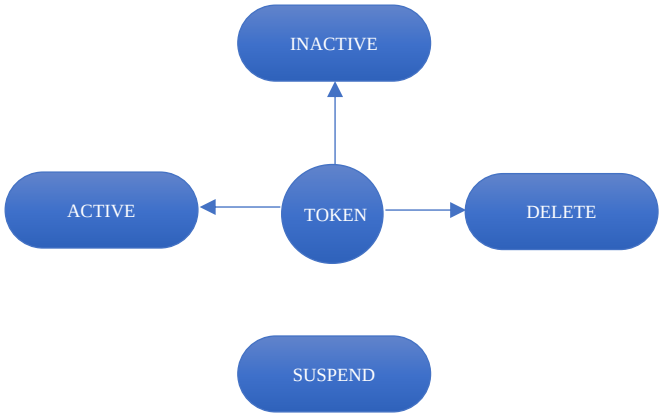
1. The customer taps their phone on the terminal (using NFC).
2. The Token and a dynamic cryptogram are sent to the merchant.
3. The merchant initiates a token-based payment request.
4. The request is routed to the Token Service Provider (TSP) based on the token type.
5. De-tokenization happens at the TSP, replacing the Token with the actual Primary Account Number (PAN).
6. The transaction is forwarded securely to the card issuer (e.g., the bank) for authorization.
7. Once authorized, the TSP replaces the PAN with the Token before sending the approval response to the merchant terminal.

This process ensures the merchant does not see or store the card number.



Token Based Payment Flow

Fig. 2 Tokenized Payment Flow



Token Life Cycle Management

Fig. 3 Token Lifecycle Management

6. Token Lifecycle Management

Once a Token is generated, it can have the below statuses -

- Inactive: Once a token is generated in a vault based on risk preference or Issuer bank choice, it will be inactive.
- Active: Once a card member performs the ID&V process with the Issuer bank, the Token is activated upon receiving a callback from the Issuer bank to TSP.
- Suspended: It can be initiated by DWP or Issuer based on customer request. Once suspended, payment will not work with the given Token.
- Resume: It can be initiated by DWP or Issuer based on customer request. Once resumed from the suspended state, payment will start working for the given Token.
- Delete: Deleting the Token from the ecosystem, i.e., TSP and DWP, upon customer request. It can be initiated from the DWP or the Issuer side.

7. Comparison with Existing Approaches

7.1. Comparison with Encryption

Tokenization replaces sensitive data with tokens; as a result, merchants do not need to store PAN with them, reducing the data breach. Encryption transforms sensitive data into unreadable formats using algorithms like AES-256, requiring secure key management (Anderson, 2018). Unlike Tokenization, encrypted data remains reversible, posing risks if keys are compromised.

This reduces PCI DSS compliance scope, as tokens are useless if intercepted. However, encryption is better suited for data in transit, while Tokenization excels in data at rest.

7.2. Comparison with 3D Secure

3D Secure (e.g., Verified by Visa) adds an authentication layer to online transactions. As part of 3DS, it requires cardholder additional OTP verification during the card, not present scenario. Though this verification is adequate, it also increases friction.

The study shows 3DS abandonment rates as high as 20% (Mastercard, 2022). Tokenization, by contrast, operates seamlessly in the background, enhancing security without impacting user experience.

However, 3D Secure provides stronger cardholder authentication, complementing Tokenization in high-risk scenarios.

7.3. Comparison with Biometric Authentication

Biometric authentication (e.g., fingerprint, facial recognition) verifies user identity at the point of transaction. While biometrics enhance device-level security, they do not protect card details during transmission. Tokenization secures the entire payment flow by replacing cards with tokens.

7.4. Summary

Table-1 summarizes the comparison, highlighting Tokenization's strengths in reducing compliance burdens and enhancing user experience, though it relies on TSP infrastructure, unlike decentralized biometric systems.

Table 1. Comparison of tokenization with existing payment security approach

Approach	Strengths	Weaknesses	Use Case
Tokenization	Reduces PCI DSS scope, seamless experience	TSP dependency, interoperability issues	Online and in-store payments
Encryption	Protects data in transit	Key management risks	Data transmission
3D Secure	Strong cardholder authentication	High abandonment rates	CNP transactions
Biometric Auth	Device-level security	Limited to user verification	Device-based payments

8. Results

8.1. Fraud Reduction

Per Visa (2023), there is a 25% reduction in fraud for CNP transactions due to merchants using token-based payment and dynamic cryptograms. Similarly, Mastercard (2022) showed a 30% reduction in fraud for in-store tokenized NFC-based payments.

8.2. Adoption Rates

Tokenization adoption has surged. In 2019, 15% of transactions were token-based, whereas in 2023, EMVCo reported that 40% of global digital payments were tokenization-based. This growth reflects merchant confidence in Tokenization's security and compliance benefits. In the U.S., 90% of top-tier merchants have adopted Tokenization, per Visa (2023).

8.3. Compliance Cost Savings

Tokenization reduces PCI DSS compliance costs by minimizing the storage of sensitive data. A survey by Ulf T. Mattsson (2009) found that merchants using tokenized systems saved an average of 35% on compliance audits, as tokens fall outside PCI DSS scope.

8.4. Limitations in Data

Although the results above demonstrate Tokenization's effectiveness, performance and adoption data for the following are limited:

- Tokenization impact on mult currency, international cross border scenario.
- Tokenization impacts SMB or small business onboarding growth.

9. Discussion and Future Directions

9.1. Novelty and Contribution

This article makes several novel contributions to the payment security literature:

- Technical Depth: It provides a granular analysis of token generation and lifecycle management, addressing a gap in prior work focused on outcomes (e.g., Ulf T. Mattsson, 2009).
- Comparative Analysis: The comparison with encryption, 3D Secure, and biometrics offers a holistic view of Tokenization's role in the security ecosystem. These contributions enhance the understanding of Tokenization's operational and testing aspects, benefiting researchers and practitioners.

9.2. Limitations and Challenges

Tokenization faces interoperability challenges in cross-border transactions and dependency on TSPs, which may introduce vulnerabilities (Dawoud, 2010). Small merchants may also face adoption barriers due to implementation costs.

10. Conclusion

Tokenization is a transformative payment security mechanism that reduces fraud and compliance burdens. This article comprehensively analyses its processes, compares with existing approaches, and empirical results. Continued research will further enhance its scalability and adoption

References

[1] Statista, Digital Payments – Worldwide, Statista Digital Market Outlook, 2023. [Online]. Available: https://www.statista.com/outlook/dmo/fintech/digital-payments/worldwide

[2] Visa, Visa Token Service: Enhancing Digital Payment Security, Visa Security Insights, 2023. [Online]. Available: https://usa.visa.com/solutions/visa-token-service.html

[3] PCI Security Standards Council, Information Supplement: PCI DSS Tokenization Guidelines, PCI DSS Documentation, 2011. [Online]. Available: https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

[4] Ulf T. Mattsson, "Analyzing the Security, Compliance and Cost Benefits of Tokenization," *Compliance and Cost Benefits of Tokenization*, pp. 1-7, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[5] Debasis Mohanty et al., "Blockchain Interoperability: Towards a Sustainable Payment System," *Sustainability*, vol. 14. no. 2, pp. 1-20, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Wesam Dawoud, Ibrahim Takouna, and Christoph Meinel, "Infrastructure as a Service Security: Challenges and Solutions," *2010 The 7th International Conference on Informatics and Systems (INFOS)*, Cairo, Egypt, pp. 1-8, 2010. [Google Scholar] [Publisher Link]

[7] Prity Rani, Rohit Kumar Sachan, and Sonal Kukreja, "Academic Payment Tokenization: An Online Payment System for Academia Utilizing Non-Fungible Tokens and Permissionless Blockchain," *Procedia Computer Science*, vol. 230, pp. 347-356, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed., John Wiley & Sons, pp. 1-1088, 2010. [Google Scholar] [Publisher Link]

[9] Mastercard, Mastercard Digital Payments Report, Mastercard Global Insights, 2022. [Online]. Available: https://www.mastercard.com/news/insights/

[10] EMVCo, EMV Payment Tokenisation: Adoption and Impact Report, EMVCo Technical Report, 2023. [Online]. Available: https://www.emvco.com/emv-technologies/payment-tokenisation/