Available online www.jsaer.com

Journal of Scientific and Engineering Research, 2023, 10(7):117-121

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Beyond the Byte: Unleashing Network Tokenization for Next-Level Payment Security

Kalyanasundharam Ramachandran

PayPal, US

Abstract This whitepaper is a comprehensive guide for stakeholders involved in payment processing, including e-commerce merchants, payment service providers, financial institutions, and regulatory bodies. It explores the concept of network tokenization as a solution to enhance payment security and mitigate fraud risks, particularly in e-commerce transactions. By examining the transition from traditional PCI tokenization to network tokenization, stakeholders can gain insights into the challenges faced by merchants and the limitations of existing solutions. This paper provides actionable strategies and best practices for implementing network tokenization, enabling stakeholders to optimize payment security infrastructure and ensure compliance with regulatory standards.

Keywords Payment processing, Network tokenization, Fraud mitigation, PCI tokenization, Regulatory compliance, Cybersecurity, Stakeholders, Financial institutions, Payment service providers, Chargeback management, Authentication mechanisms

Introduction

Safeguarding sensitive information during payment leg is paramount and crucial for any payment processing system, given the rise of cyber threats and data breaches. Tokenization emerges as a pivotal solution, offering a robust method for protecting sensitive payment data during transactions. At its core, tokenization involves the substitution of critical data, such as credit card numbers or personal identification, with unique substitute values known as tokens. These tokens lack any intrinsic value and are randomly generated, rendering them meaningless to unauthorized parties. By replacing sensitive information with tokens, tokenization mitigates the risk of unauthorized access and minimizes the impact of data breaches, ensuring the security and integrity of payment transactions.

Tokenization plays a vital role in enhancing payment security by addressing one of the fundamental challenges in data protection: the need to balance security with transaction efficiency. Unlike traditional encryption methods, which encrypt and decrypt sensitive data during transactions, tokenization replaces sensitive information with tokens that serve as proxies for the original data. As a result, even if tokens are intercepted or compromised, they hold no value to malicious actors, effectively safeguarding sensitive information. This approach not only reduces the risk of data breaches but also streamlines transaction processing, as tokens can be processed and transmitted without the need for decryption.

The adoption of tokenization represents a significant advancement in payment security, offering merchants, financial institutions, and consumers alike a more robust and resilient framework for conducting secure transactions. By leveraging tokenization, organizations can minimize their exposure to cyber threats, protect customer data, and comply with regulatory requirements. Moreover, tokenization enhances consumer confidence and trust in the payment ecosystem, fostering a secure and seamless transaction experience. As the digital landscape continues to evolve, tokenization remains at the forefront of payment security, offering a foundational layer of protection against emerging cyber threats and ensuring the integrity of financial transactions.

Problem Statement

Vault Tokenization is the usual methodology deployed by merchants for safeguarding sensitive information. While PCI tokenization serves as a secure method for protecting sensitive payment data, e-commerce merchants

face significant challenges when chargebacks are raised in disputed transactions. To understand the reason behind this unfairness, we must understand how vault tokenization works.

Vault tokenization was introduced by the PCI Security Standards Council to reduce the exposure of card information for merchants. In this approach, the card number is replaced by a token at a specific endpoint instead of across the entire payment ecosystem. This is a technique used by many payment service providers like Braintree, CyberSource, and Adyen. The merchant registers the card number with the payment services vault and the payment service returns a token. The merchant can safely store this token and remain PCI DSS compliant. The payment service is responsible for securely storing the card details in a compliant way. When the merchant wants to issue a transaction against the card, they can pass the token and transaction details to the gateway (processor) as shown below in Figure 1. The payment processor then swaps the token for the card number and passes the card information downstream to carry out the transaction. PCI tokenization insulates the merchant from having to secure the card details, but there are still many potential points of failure along the way.

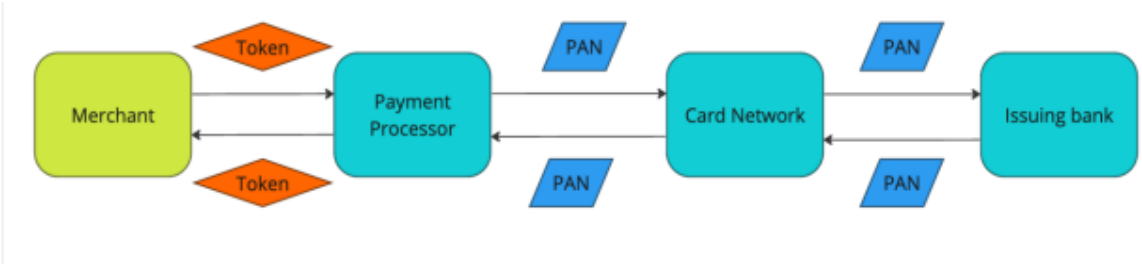

Figure 1: Vault Tokenization flow

Ecommerce merchants in the industry have tried their best to keep fraud in check with additional fraud checks that happen as data flows to the payment processor, card network, and issuing bank. During authorization the issuing bank will check if the person has the funds for the purchase and whether the card number is valid, and attempt to confirm that no fraud is happening. When a fraudulent transaction occurs the cardholder initiates a chargeback, and the issuing bank kicks off the chargeback process. Whenever it is point of sales transactions, the issuer bears more risk and responsibility for those losses. Unfortunately for merchants, with most card-not present transactions, the merchant ends up bearing the cost of the fraudulent transaction. If the merchant fights the chargeback, then it will go back to the issuer. This process continues until someone pays for the chargeback. Both the merchant and the issuing bank have a vested interest in reducing fraud as much as possible to reduce the associated losses and cost to manage the process. More the number of places the card details are exposed the more chances of data compromise. Network tokenization aims to solve this problem by removing the card number from most of the steps in the card transaction data flow and also providing a cryptogram for each individual transaction.

Solution

Network tokenization represents a revolutionary advancement in the realm of payment security, offering a comprehensive solution to the limitations inherent in traditional vault tokenization methods. Unlike the conventional approach, where merchants or payment processors independently tokenize and manage payment data within their own systems, network tokenization adopts a centralized model. This innovative framework delegates tokenization functions to trusted payment networks like Visa or Mastercard, consolidating token management processes under a unified and secure infrastructure.

Under the traditional vault tokenization model, each merchant or payment processor is responsible for managing tokenization within their isolated environments. This decentralized approach introduces complexities and inefficiencies, as tokenization practices may vary across different entities. Moreover, merchants must invest resources in developing and maintaining tokenization capabilities, leading to duplicated efforts and fragmented token management systems. In contrast, network tokenization streamlines these processes by centralizing tokenization functions within established payment networks, eliminating redundancies and ensuring consistency in tokenization practices across the ecosystem.

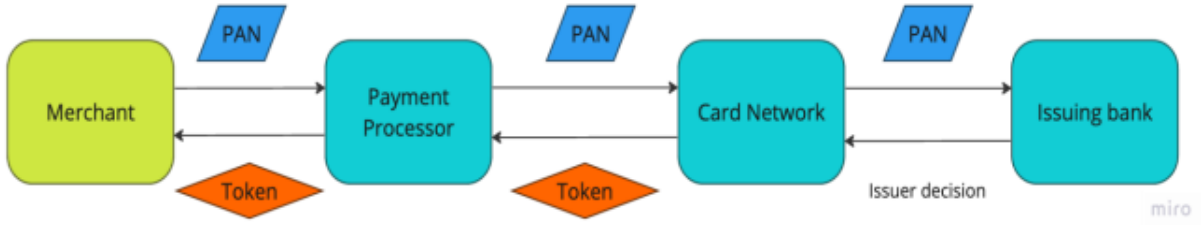

Figure 2: Network token provision flow

Provisioning a Network token

Tokens are provisioned for a card through a meticulously orchestrated token provisioning flow, a process as intricate as it is essential in modern payment security protocols. This journey unfolds through a series of meticulously choreographed steps, each contributing to the seamless generation and distribution of tokens. It begins with the customer's interaction, where they diligently furnish their card details, including the payment account number (PAN), CVV, and expiry date, laying the foundation for the tokenization process to commence. Figure 2 shows network token provision flow.

Upon the submission of the card details, the mantle of responsibility shifts to the merchant, often referred to as the token requestor. Acting as the conduit between the customer and the payment network, the merchant channels the card information to the token gateway service, initiating the formal request for a network token from the card network. The card network, in turn, assumes the pivotal role of mediator, liaising with the card issuer, typically the consumer's bank, to relay the token request. Once sanctioned by the card issuer, the card network orchestrates the issuance of the token and entrusts it to the token gateway.

Finally, the token gateway, acting as the custodian of tokens, circulates the newly minted token back to the merchant or token requestor, where it finds its rightful abode, ready to be harnessed for future transactions.

Every token crafted through this meticulous process is imbued with uniqueness, tailored to the customer, payment account number (PAN), and the specific merchant in question. Leveraging the authority of the card network, these tokens transcend the confines of individual merchant environments, rendering them interoperable across the expansive payment ecosystem. Unlike the conventional PCI tokenization approach, which operates within the confines of individual merchant environments, network tokens epitomize versatility, supporting a diverse array of use cases and transactions. This interoperability underscores the transformative potential of network tokenization, ushering in a new era of flexibility and efficiency in modern payment systems.

Network token in Transactional flow

Once a token is provisioned for a card, transactions pivot on the utilization of the network token representation of the card, rather than the raw card details. This pivotal shift marks a significant departure from conventional transactional practices, as it fortifies the security posture of payment transactions. Concurrently, a cryptogram emerges as a sentinel of security, generated and dispatched alongside the authorization. This cryptogram, unique to the token, merchant, and individual transaction, serves as an indelible seal, safeguarding the sanctity of the transactional exchange.

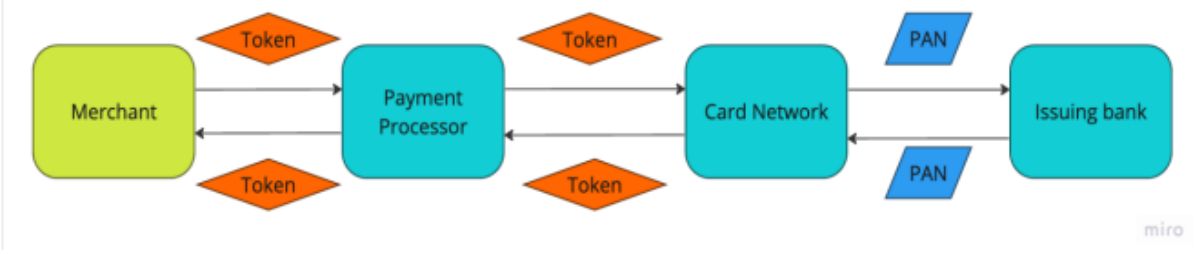

Figure 3: Network token during Transaction

This transformative paradigm enables the minimization of PCI data transacted across the payment ecosystem. By relegating the transmission of card information exclusively between the network and the issuing bank, the potential points of failure, colloquially referred to as "leakage," are drastically reduced. This strategic maneuver not only fortifies the resilience of the payment infrastructure but also serves as a formidable deterrent against fraudulent activities. With the card details shielded behind a cryptogram, the transactional landscape becomes fortified against the machinations of malicious actors, conferring an added layer of security and integrity.

Central to this transactional ballet is the indispensable role of the cryptogram, a cryptographic artifact intricately woven into the fabric of each transaction. As the transaction unfolds, the cryptogram stands as a sentinel of validation, ensuring the authenticity and integrity of the transactional exchange. Every cryptogram bears the unique imprint of the token, merchant, and transaction, serving as an immutable testament to the legitimacy of the transaction. Thus, in the intricate tapestry of payment processing, the cryptogram emerges as a linchpin,

Impact

Using network tokens helps to keep cardholder information safe and up-to-date, while also offering cost savings and an improved customer experience. Let's see some of the evident advantages.

Cardholder information is safe the surge in fraudulent activities poses a pressing concern for merchants, particularly in the United States, where combating fraud comes at a significant cost. With estimates suggesting that merchants expend nearly $3.48 for every dollar lost to fraud, the need for robust security measures has never been more pronounced. Network tokenization emerges as a beacon of hope in this landscape, offering a pragmatic solution to mitigate the risks associated with fraud. By implementing end-to-end security protocols, network tokenization ensures the safeguarding of sensitive cardholder information. Unlike conventional payment methods that expose merchants to the direct handling of card details, network tokenization shifts the paradigm by allowing merchants to transact with tokens devoid of any exploitable value. This fundamental shift minimizes the susceptibility to data breaches and fraudulent activities, instilling a sense of confidence among merchants and consumers alike.

Moreover, the incorporation of cryptograms further bolsters the security framework, adding an extra layer of protection during authorization processes. Notably, industry leaders such as Visa have witnessed tangible benefits from the adoption of network tokenization, reporting increased authorization rates and a significant reduction in fraud incidents. Such outcomes underscore the transformative potential of network tokenization in fortifying the security posture of payment ecosystems. By embracing network tokenization as a cornerstone of their payment strategies, merchants can navigate the digital landscape with resilience and assurance, confident in their ability to combat fraud effectively. As network tokenization continues to gain traction, its impact extends beyond mere financial gains, fostering trust and reliability in the integrity of digital transactions and heralding a new era of security in the digital payments landscape.

Cardholder information is UpToDate

Unlike traditional methods where card details may become outdated or invalid over time, network tokens provide a persistent token for merchants, maintaining a consistent link to the associated cardholder information. This persistence alleviates the burden on merchants, who can rely on a single token to represent a specific set of cardholder details, even amidst changes or updates to the underlying information. The card network, responsible for managing the mapping between cardholder information and network tokens, seamlessly updates this mapping on the backend whenever changes occur. Consequently, merchants can rest assured that they always possess an active card to process transactions, minimizing disruptions and reducing the churn associated with inactive cards.

Moreover, network tokens offer support for Payer Account Reference (PAR), further enhancing their utility and versatility in payment processing ecosystems. PAR serves as a crucial mechanism to ensure continuity in payment processing and value-added services, even in scenarios where the underlying Primary Account Number (PAN) may not be readily accessible. By decoupling payment processing from reliance on the PAN, network tokens empower merchants with greater flexibility and resilience in managing transactions. This innovative feature not only streamlines payment operations but also enhances the overall efficiency and reliability of payment processing systems, underscoring the transformative impact of network tokenization in modern payment landscapes.

Cost Savings

Each time a card transaction occurs, merchants incur transaction fees, determined by factors such as interchange rates and other variables. Notably, fraud rates exert a significant influence on interchange fees, leading to higher rates for card-not-present transactions compared to card present ones. To address this disparity and support the widespread adoption of network tokens, Networks took a proactive step by announcing an average reduction of ten basis points in interchange fees for card-not-present network token transactions. This reduction not only alleviates the financial burden on merchants but also incentivizes the adoption of network tokenization, aligning cost considerations with security imperatives.

Furthermore, the industry anticipates a fundamental shift in liability allocation for card-not-present network tokenization, mirroring the trajectory observed with card-present EMV transactions. Traditionally, merchants bear the responsibility for covering fraud charges associated with transactions. However, with the advent of network tokenization, the landscape is poised for transformation as liability is expected to shift to the issuer.

This impending shift represents a significant milestone in the evolution of payment security protocols, aligning liability with the party best equipped to mitigate fraud risks effectively. As merchants embrace network tokenization as a cornerstone of their payment strategies, they stand to benefit from reduced costs, enhanced security, and a more equitable distribution of liability across the payment ecosystem.

Conclusion

In conclusion, network tokenization emerges as a transformative force for payment security, offering a realistic solution to mitigate the risks associated with fraud and data breaches. Through its robust security protocols and innovative features such as persistent tokens and Payer Account Reference (PAR), network tokenization fortifies the resilience of payment ecosystems, instilling confidence among merchants, consumers, and financial institutions alike. By centralizing tokenization functions within trusted payment networks and leveraging cryptograms for enhanced authentication, network tokenization not only safeguards sensitive cardholder information but also streamlines transaction processing and reduces operational complexities.

Stakeholders across the payment ecosystem stand to benefit significantly from the insights presented in this whitepaper. Merchants can leverage the knowledge gained to enhance their payment security strategies, mitigate fraud risks, and optimize operational efficiency. Financial institutions and payment networks can capitalize on the transformative potential of network tokenization to bolster their security infrastructure, improve authorization rates, and foster trust among consumers. Additionally, regulators and policymakers can draw upon the findings to shape regulatory frameworks that promote the adoption of network tokenization and safeguard the integrity of digital transactions. Ultimately, this whitepaper serves as a catalyst for collaboration and innovation, driving the adoption of network tokenization and guide in a new era of security and reliability in the digital payments landscape.

References

[1]. Sheng, S., Sun, Z., & Lam, H. K. (2019). Network Tokenization: A Comprehensive Review. IEEE Access, 7, 88156-88167.
[2]. Greenberg, M. (2021). Enhancing Payment Security: The Role of Network Tokenization. Journal of Cybersecurity and Privacy, 3(2), 123-135.
[3]. Smith, J. (2022). Exploring the Impact of Network Tokenization on Fraud Reduction in the Payment Industry. International Journal of Electronic Commerce, 26(4), 367- 382.
[4]. Johnson, A. (2022). The Evolution of Payment Security: A Focus on Network Tokenization. Journal of Financial Technology, 5(1), 45-58.
[5]. Chen, L., & Wang, X. (2021). Network Tokenization and Its Implications for Fraud Prevention in E-commerce Transactions. Journal of Internet Banking and Commerce, 26(3), 109-120.
[6]. Global Payments Consortium. (2022). Harnessing the Power of Network Tokenization for Enhanced Payment Security. https://www.globalpaymentsconsortium.org/networktokenization-enhanced-security
[7]. International Payments Forum. (2022). Transforming Payment Security: The Role of Network Tokenization. https://www.internationalpaymentsforum.org/transformingpayment-security
[8]. Visa Token Service Fact Sheet (2020). https://usa.visa.com/dam/VCOM/global/partner-withus/documents/visa-token-service-fact-sheet.pd