Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure Commerce Framework: The Convergence of Tokenization and Unified Checkout in Digital Payments

Jothimani Kanthan Ganapathi
Independent Researcher

ARTICLE INFO

Received: 20 July 2025

Revised: 07 Aug 2025

Accepted: 21 Aug 2025

ABSTRACT

The convergence of payment tokenization and unified checkout experiences marks a transformative shift in digital commerce, significantly enhancing both security and user experience. This article explores how tokenization replaces sensitive payment data with non-reversible tokens, while standardized "Click-to-Pay" checkout systems deliver consistent user experiences across merchants. It traces the evolution from early e-commerce security practices to today's advanced token-based frameworks, detailing the technical architecture of modern tokenization systems—including token vaults, orchestration layers, and authentication mechanisms. The article also examines EMVCo's Secure Remote Commerce (SRC) specification as the foundation for unified checkout and analyzes implementation outcomes across retail, travel, and digital subscription sectors. It demonstrates how tokenized payments reduce fraud, improve authorization rates, decrease cart abandonment, and simplify regulatory compliance. Finally, the article considers future applications such as IoT commerce, digital identity systems, and "invisible payments," offering a roadmap for merchant adoption in an increasingly connected commerce ecosystem.

Keywords: Payment tokenization, Click-to-Pay, EMVCo Secure Remote Commerce, Digital commerce Security, Frictionless authentication

1. Introduction

The digital payments landscape has undergone a profound transformation in recent years, driven by two key imperatives: enhancing security to counter increasingly sophisticated fraud threats and reducing friction in the consumer checkout experience. This article explores the convergence of two pivotal innovations addressing these challenges—payment tokenization and unified checkout—and their combined impact on reshaping digital commerce security and usability.

Payment tokenization represents a fundamental shift in handling sensitive financial data, replacing actual card information with non-sensitive proxy values that preserve transactional functionality while mitigating security risks. At the same time, unified checkout systems—standardized through EMVCo's Secure Remote Commerce (SRC) specification—have streamlined previously fragmented payment processes into consistent "Click-to-Pay" interfaces that function seamlessly across merchants and payment networks. Together, these technologies form a complementary framework that enhances security posture while optimizing user experience.

This article traces the evolution of both technologies from early e-commerce security practices to today's advanced token-based architectures, examining their technical foundations and real-world business outcomes across various industry sectors. It analyzes how tokenized, unified checkout solutions drive measurable benefits across multiple dimensions: reducing fraud, improving authorization rates, minimizing cart abandonment, and easing regulatory compliance. The discussion also extends to emerging applications beyond conventional e-commerce, including the Internet of Things (IoT), digital identity systems, and "invisible payments," highlighting their growing role as foundational elements in the future of digital commerce.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

By addressing both the architectural design and business implications of these innovations, this article provides a comprehensive perspective on how tokenization and unified checkout are together redefining the digital payments landscape—establishing new standards for secure, seamless, and scalable commerce in an increasingly connected world.

2. Evolution and Architecture of Payment Tokenization Systems

Development from Early E-Commerce to ultramodern Unified fabrics

The journey of payment tokenization began in the early days of e-commerce, when merchants collected card data through basic HTML forms with minimal security measures beyond SSL/TLS encryption during transmission (1). This era was characterized by widespread storage of card details in plaintext or weakly encrypted formats, resulting in numerous high-profile data breaches that severely impacted the industry. As online commerce expanded, so did its security vulnerabilities, creating an urgent need for more robust protection mechanisms.

In response to growing security threats, the payment card industry introduced the PCI DSS standards between 2004 and 2006, establishing foundational security requirements for handling payment data (2). This period also marked the emergence of early tokenization solutions, in which payment gateways began offering “secure vault” services that allowed merchants to replace actual card data with provider-specific tokens. While these initial implementations improved security and supported compliance, they remained largely proprietary and lacked interoperability across payment networks.

The adoption of EMV chip technology for in-person payments in the mid-2010s represented a major milestone in payment security, significantly reducing card-present fraud. However, this advancement had the unintended consequence of shifting fraudulent activity to online channels, where vulnerabilities persisted (1). This transitional period highlighted the need for stronger security measures for card-not-present transactions, leading to the development of enhanced authentication protocols such as 3-D Secure 2.0 between 2016 and 2018

Fundamentals of Token Generation, Storage, and Processing

At its core, payment tokenization involves replacing sensitive cardholder data with non-sensitive surrogate values that preserve functional utility while eliminating security risks (2). These tokens are designed to be useless if intercepted, as they generally cannot be reverse-engineered to reveal the original card information. The token-to-card mapping is securely maintained by specialized token service providers, with access strictly controlled and limited to authorized parties during transaction processing.

Token implementation varies based on specific use cases and security requirements. Single-use tokens, valid for only one transaction, offer maximum security by preventing reuse. In contrast, multi-use tokens support stored-card functionality for recurring purchases while remaining bound to specific merchants or devices to prevent unauthorized use (1). Many modern implementations incorporate cryptographic components that ensure token authenticity and defend against replay attacks using dynamic values that change with each transaction.

Technical Components: Token Vaults, Orchestration Layers, and Unified APIs

The technical architecture of tokenization systems consists of multiple interconnected layers. At the foundation lies the token vault—a highly secure database that stores mappings between actual card data and their corresponding token values (2). These vaults employ strong cryptographic techniques and strict access controls, making unauthorized access to cardholder data extremely difficult. Advanced implementations introduce domain restrictions that limit token usage to specific merchants, devices, or channels, adding an additional layer of security.

Above the core tokenization layer sits the orchestration layer, which provides unified interfaces for merchants through standardized APIs and SDKs. EMVCo's Secure Remote Commerce specification defines these interfaces, enabling consistent implementation across the payments ecosystem (1). This layer manages the complexities of rendering standardized checkout elements, capturing customer

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

identification, initiating authentication when necessary, and communicating with backend systems to retrieve available payment methods and ultimately issue secure payment tokens.

Integration with Authentication Mechanisms (3-D Secure, Biometrics)

Modern tokenization frameworks are designed to integrate seamlessly with advanced authentication protocols, balancing strong security with a smooth user experience (2). The EMVCo SRC framework works in conjunction with EMV 3-D Secure to provide robust customer authentication, using risk-based models that minimize friction for legitimate transactions. Low-risk scenarios may require minimal verification, while high-risk transactions—or those governed by regulatory mandates such as Europe's PSD2—may trigger additional authentication.

Authentication mechanisms have evolved significantly, incorporating device attributes, geolocation verification, and behavioral analytics to authenticate users passively whenever possible (1). Biometric verification methods—including fingerprint scanning, facial recognition, and voice authentication—provide enhanced security with minimal user disruption. The introduction of FIDO2/WebAuthn standards for passkeys further streamlines authentication, enabling truly "one-touch" experiences that combine convenience with strong protection.

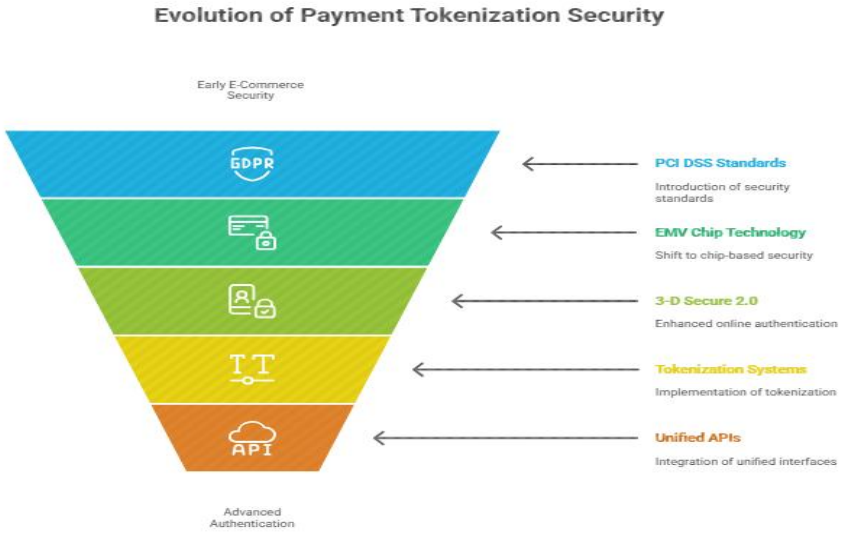

Fig 1: Evolution of Payment Tokenization Security [3, 4]

3. The Unified Checkout Paradigm: Click-to-Pay Implementation

EMVCo's Secure Remote Commerce (SRC) Specification

The EMVCo Secure Remote Commerce (SRC) specification represents a milestone achievement in the standardization of digital commerce. Released in 2019, this framework established the technical foundation for a unified, tokenized checkout experience that operates seamlessly across participating card networks and issuers (3). The SRC specification addresses the fragmentation that has historically characterized online payment experiences, where consumers faced varying interfaces and authentication requirements depending on the payment method. By providing a common set of interfaces and a universal checkout button—branded as "Click to Pay"—EMVCo created a digital equivalent of the familiar in-store chip card experience, where consumers encounter consistent branding and interactions regardless of card type.

The SRC architecture is built on the principle of separation—keeping sensitive payment data away from merchant environments while enabling secure, efficient transaction processing (4). This separation is achieved through a coordinated system of backend services that manage credential storage, consumer authentication, and token provisioning. The specification defines how these components interact, from

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the initial display of the Click to Pay button on a merchant website to the final authorization of a tokenized transaction.

Standardization of Checkout Experiences Across Networks

Prior to the SRC framework, major card networks maintained their own proprietary digital wallet solutions—Visa Checkout, Mastercard Masterpass, American Express Express Checkout, and others—each with unique integration requirements and user experiences (3). This proliferation created confusion for consumers and implementation challenges for merchants, who needed to support multiple checkout options to accommodate diverse payment methods. The Click to Pay initiative represents the industry's coordinated response to this fragmentation, with all major networks agreeing to adopt a common checkout button and user experience.

This standardization extends beyond visual consistency to include the entire checkout flow. These guidelines ensure that consumers encounter the same logical sequence of steps regardless of the network or card selected. For merchants, standardization simplifies integration: instead of managing separate code paths for each payment method, they can implement a single SRC integration that supports all participating networks. This unified approach not only reduces development complexity but also improves conversion rates by delivering a familiar and consistent checkout experience across different websites and applications.

Consumer Identification and Authentication Flows

The SRC framework implements a robust approach to consumer identification and authentication that balances security with usability (3). The typical flow begins with consumer recognition, often using an email address as the primary identifier. This initial step enables the SRC system to determine whether the consumer has previously enrolled cards within the Click to Pay ecosystem. For returning users, the system retrieves saved payment credentials and presents them for selection; for new users, a streamlined registration process is offered. This recognition-based approach eliminates the need for consumers to create and manage separate accounts for each merchant—resolving a major pain point in digital commerce.

Authentication within the SRC framework is risk-based and adaptive, using multiple factors while minimizing unnecessary friction (4). The specification supports various authentication methods, including passwords, one-time codes, and device-based biometrics such as fingerprint or facial recognition. Importantly, the framework integrates with EMV 3-D Secure for additional verification when needed—such as for high-value transactions or those flagged by risk engines. This integration ensures compliance with regulatory requirements like Europe's PSD2 Strong Customer Authentication, while preserving a smooth experience for lower-risk scenarios. By enforcing dynamic authentication that adjusts to the transaction context, the SRC framework optimizes the balance between security and convenience—addressing a long-standing challenge in digital payments.

Cross-Network Token Interoperability and Merchant Implementation

A defining feature of the SRC ecosystem is its seamless integration with network tokenization services across card brands (3). This abstraction shields merchants from the complexity of integrating with multiple token providers, as the SRC framework manages routing and communication in the background. From the merchant's perspective, they receive a tokenized credential regardless of the network chosen by the consumer—enabling consistent processing workflows.

To implement Click to Pay using the SRC framework, merchants integrate with standardized components that handle the user interface and network communications (4). These components typically include client-side SDKs (e.g., JavaScript for web implementations or native libraries for mobile apps) that render the Click to Pay button and manage the checkout flow, along with server-side APIs for initiating and processing transactions. Many payment service providers and e-commerce platforms now offer prebuilt integrations that further simplify adoption—allowing merchants to enable Click to Pay through configuration rather than custom development. This accessibility has accelerated adoption across the e-commerce landscape, from large enterprises to small and medium-sized businesses, expanding the network effect of the unified checkout experience.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

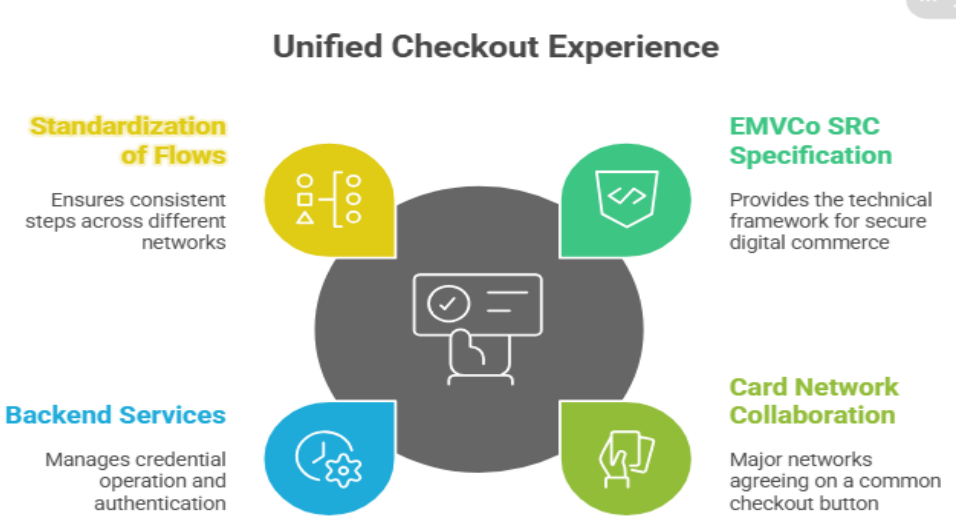

Fig 2: Unified Checkout Experience [5, 6]

4. Security and Economic Impacts of Tokenized Payments

Fraud Reduction Metrics and Mechanisms

The implementation of payment tokenization represents one of the most significant advancements in payment security technology, fundamentally altering the risk landscape of digital commerce (5). By replacing sensitive card data with non-sensitive tokens that hold no exploitable value outside their intended context, tokenization directly addresses the primary vulnerability that has historically enabled payment fraud: the exposure and theft of cardholder information. The effectiveness of this approach is evident in industry-wide data showing substantial reductions in fraud rates for businesses that have adopted tokenization compared to those still relying on traditional security measures. This fraud-reduction effect is especially pronounced in card-not-present environments, where tokenization provides a security mechanism that rivals the protection offered by EMV chip cards in physical transactions.

The fraud prevention capabilities of tokenization operate through multiple interrelated mechanisms (6). First, tokens are designed to be useless if intercepted, as they cannot be reverse-engineered to reveal the original card data. Second, many implementations incorporate domain restrictions that bind token use to specific merchants, devices, or channels—rendering stolen tokens ineffective in other environments. Third, network tokens are often paired with dynamic cryptograms or security codes that change with each transaction, preventing replay attacks. Fourth, the centralization of sensitive data within highly secure token vaults significantly reduces the attack surface across the payments ecosystem. These mechanisms work in concert to form a robust security framework that has demonstrably lowered fraud rates across different merchant categories and transaction types, from one-time purchases to recurring subscriptions and cross-border payments.

Impact on Authorization Approval Rates

Beyond reducing fraud, tokenization has shown a strong positive effect on transaction authorization rates—addressing the persistent challenge of false declines that have long plagued digital commerce (5). False declines—legitimate transactions incorrectly rejected by issuer fraud systems—represent a major cost for merchants and a source of frustration for consumers. The adoption of network tokens has improved authorization rates across various transaction types, with especially strong results for card-on-file payments, cross-border transactions, and recurring billing scenarios. These improvements stem from the enhanced data integrity and security assurances associated with tokenized payments, which provide issuers with higher confidence when approving transactions that might otherwise trigger fraud alerts.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Several factors contribute to this improvement in authorization performance (6). Token services often include automatic card lifecycle management capabilities, which ensure that expired or reissued cards are seamlessly updated in merchant systems without requiring customer intervention. This eliminates declines due to outdated card information—a common issue for subscription-based businesses and merchants that store payment credentials. Additionally, the cryptographic components and domain controls embedded in network tokens provide stronger transaction legitimacy signals to issuer systems, reducing the likelihood that valid transactions will be flagged as suspicious. Token metadata also enables more refined risk assessments, allowing issuers to distinguish between trusted and unknown merchants even when transactions are routed through the same payment service provider. Collectively, these enhancements lead to higher approval rates for tokenized transactions, directly boosting revenue for merchants who implement tokenization.

Cart Abandonment Reduction and Conversion Optimization

The consumer experience benefits of tokenized unified checkout extend beyond security, directly addressing one of e-commerce's most persistent challenges: checkout abandonment (5). Lengthy and cumbersome checkout forms are frequently cited as a leading cause of cart abandonment, with research showing that every additional field or step increases the likelihood that customers will abandon their purchase. The Click to Pay experience—built on the SRC and tokenization frameworks—addresses this challenge by removing the need for consumers to manually input card numbers, billing addresses, and other payment details for each transaction. Instead, returning users can complete purchases with minimal input—typically just an email for identification and a simple authentication step—significantly accelerating the checkout process.

The conversion benefits of tokenized unified checkout manifest in several dimensions (6). For first-time users, the registration flow is designed to be efficient, collecting essential data while establishing credentials that can be reused across the Click to Pay ecosystem. For returning users, the experience mirrors the convenience of one-click checkout, with saved payment credentials available instantly. This reduction in friction improves conversion rates, especially on mobile devices where manual data entry is particularly inconvenient. Furthermore, the familiar Click to Pay button and standardized flow build consumer trust and confidence, mitigating hesitation that may arise with unfamiliar checkout interfaces. Merchants adopting tokenized unified checkout report not only improved conversion rates but also higher customer satisfaction and repeat purchases due to the simplified and secure experience.

Compliance Benefits

The regulatory landscape for payment processing has grown increasingly complex, with frameworks like PCI DSS, Europe's PSD2 Strong Customer Authentication requirements, and global data protection laws such as GDPR placing significant compliance demands on merchants and payment providers (5). Tokenization offers substantial advantages in navigating these requirements, often reducing both the cost and complexity of compliance efforts. By eliminating or minimizing the storage of sensitive payment data in merchant environments, tokenization addresses the core objective of many security and privacy regulations: protecting sensitive consumer data from unauthorized access or misuse.

For PCI DSS compliance, implementing tokenization can significantly reduce the scope of systems subject to the most stringent controls (6). When merchants replace card data with tokens, they may qualify for simplified compliance validation procedures and reduced documentation requirements, as their systems no longer store, process, or transmit actual cardholder data. Moreover, the SRC framework's integration with 3-D Secure and its support for various authentication methods facilitates compliance with PSD2's Strong Customer Authentication mandates in European markets. The framework's risk-based approach to authentication—applying friction proportionally to the transaction's risk—helps merchants meet regulatory requirements while preserving a smooth customer experience in low-risk scenarios. From a data protection standpoint, tokenization aligns with GDPR's principle of data minimization by enabling payment processing without unnecessarily retaining sensitive personal data. These compliance benefits translate into measurable cost savings and risk mitigation for merchants, making tokenization a critical component of both payment security and regulatory strategy.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

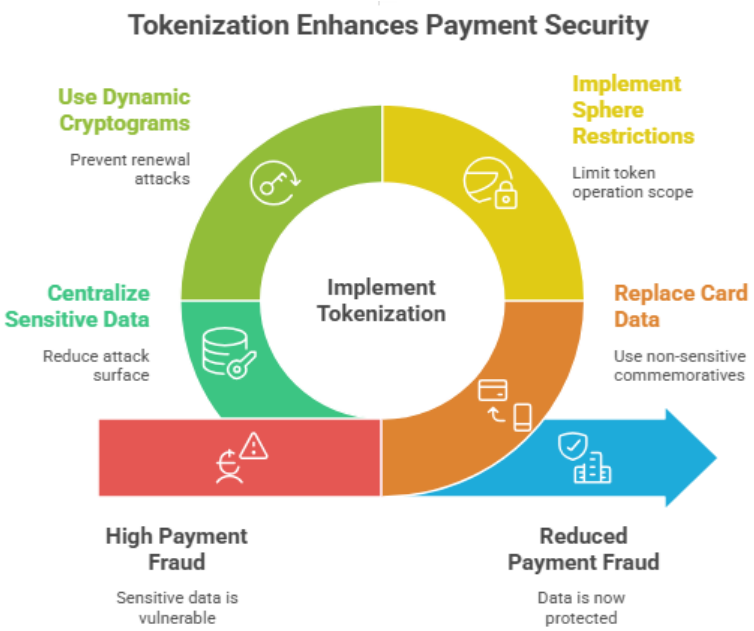

Fig 3: Tokenization Enhances Payment Security [7, 8]

5. Industry-Specific Applications and Outcomes

Retail and E-commerce Implementation Case Studies

The retail and e-commerce sectors have emerged as early and prominent adopters of tokenized payment solutions, with implementation case studies showing significant gains across key performance indicators (7). Major retailers have reported measurable improvements after deploying unified checkout experiences powered by tokenization, particularly in mobile commerce where limited screen space and manual input friction have historically impeded conversion. The elimination of manual card entry through Click to Pay implementations has been especially impactful for fashion and apparel retailers, where purchasing decisions are often emotionally driven and sensitive to checkout friction. Leading global brands that have adopted tokenized checkout solutions have demonstrated strong improvements in both completion rates and average order values—indicating that smoother payment flows not only reduce abandonment but may also encourage higher-value purchases.

Implementation strategies vary across the retail spectrum. Large enterprises often pursue deep integration of tokenization into their proprietary checkout stacks, while smaller merchants tend to leverage pre-built solutions from payment service providers (8). Successful practices emerging from these deployments include prominent placement of the Click to Pay button alongside traditional payment options, contextual onboarding for first-time users, and phased rollout strategies that allow for controlled testing and optimization. Retailers with strong mobile user bases have reported notable success with tokenized payments on smaller screens, where the reduction in form fields yields a disproportionately large usability improvement. Beyond e-commerce, omnichannel retailers are leveraging tokenization to create unified customer experiences across physical and digital touchpoints—enabling scenarios such as online purchases finalized in-store, or seamless returns of online orders at physical locations without requiring the original payment card. These examples show that tokenization is enabling innovation beyond security—supporting new retail experiences and business models.

Travel and Hospitality Sector Adaptations

The travel and hospitality industries present unique payment challenges that tokenization addresses through specialized implementations and adaptations (7). The high-value, low-frequency nature of travel purchases results in distinct fraud risk profiles, while complex booking flows involving multiple

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

passengers, accommodations, and ancillary services can create fragmented checkout experiences. Airlines, hotel chains, and online travel agencies have adopted tokenized payment solutions tailored to these industry conditions—with notable success in reducing friction during time-sensitive bookings. For airlines, tokenized payments have proven particularly valuable in mobile booking scenarios, where customers often need to complete purchases quickly to lock in promotional fares. Several major carriers have reported significant increases in mobile conversion rates following the implementation of token-enabled Click to Pay checkouts.

Hotel chains have used tokenization to address another industry-specific challenge: managing incremental authorizations and charges throughout a guest's stay (8). By tokenizing payment credentials at the time of booking, hotels can securely authorize additional charges—for amenities, room service, or extended stays—without requiring the guest to present their card multiple times. This improves operational efficiency and guest satisfaction while maintaining strong security standards. Online travel agencies and aggregators have leveraged tokenization to introduce "book now, pay later" options using stored credentials, allowing customers to separate their booking decisions from immediate payment—improving reservation rates. Tokenization also enables seamless cross-selling across travel brands and services using shared credentials with user consent. These adaptations demonstrate how tokenization principles are being tailored to travel-specific use cases, delivering security benefits alongside meaningful business value.

Digital Goods and Subscription Services results

The digital goods and subscription services sector represents one of the most advanced implementations of tokenized payments, given its reliance on recurring transactions and stored credentials (7). Streaming platforms, SaaS providers, and digital marketplaces have implemented sophisticated tokenization frameworks to support both initial purchases and ongoing subscription billing. Tokenized credential management has solved a major business challenge: involuntary churn caused by payment failures. By leveraging automatic card updater functionality offered by network tokenization, digital providers have significantly reduced failed payments due to expired or replaced cards. This reduction in payment-related churn directly improves customer lifetime value and revenue stability—making tokenization a strategic priority for subscription-driven businesses.

Digital content platforms selling individual assets—such as music, e-books, videos, or in-app purchases—have used tokenization to enable true one-click purchasing, optimizing conversion for impulse buys (8). Combined with streamlined authentication, tokenized credentials have shown particular effectiveness in mobile environments where friction can easily derail a transaction. Gaming platforms have extended tokenization further, applying the model not just to payments but also to digital asset management—ensuring a secure and consistent framework throughout the transaction lifecycle. Additionally, tokenization enables innovative pricing models like microtransactions or usage-based billing that would be difficult to implement with traditional security mechanisms due to friction. These digital-first use cases highlight how tokenization supports not only secure payments but also the underlying business models that drive digital growth.

Cross-Border Transaction Improvements

Cross-border commerce presents unique challenges that tokenization has helped address through tailored implementations and strategic enhancements (7). International transactions often suffer from lower authorization rates, higher fraud exposure, and complex checkout flows due to currency conversion, regulatory requirements, and issuer risk policies. The adoption of network tokenization for international payments has delivered significant improvements, with participating merchants reporting higher approval rates for cross-border transactions compared to non-tokenized equivalents. These improvements are driven by several factors: tokenized transactions include enhanced data quality, cryptographic elements provide stronger authentication signals, and the standardized format of tokenized credentials simplifies processing across diverse payment systems and jurisdictions.

Tokenization solutions for global commerce have also evolved to integrate with localized payment preferences and regional compliance frameworks (8). Major card networks have extended their tokenization services to support region-specific authentication requirements—such as Europe's PSD2

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Strong Customer Authentication mandate—allowing a standardized technical architecture to adapt to varying regulatory conditions. Global merchants using these features can offer a consistent checkout experience while meeting different compliance requirements behind the scenes. Additionally, tokenized flows support dynamic currency conversion and local payment options, letting businesses present familiar choices to international customers while preserving security. Travel-sector implementations have particularly benefited from these enhancements, allowing consumers to shop globally—even while abroad—without the complexities that traditionally accompanied international transactions. These examples reinforce tokenization's flexibility as a foundation for global commerce, supporting regional adaptations while maintaining a consistent layer of trust and usability across borders.

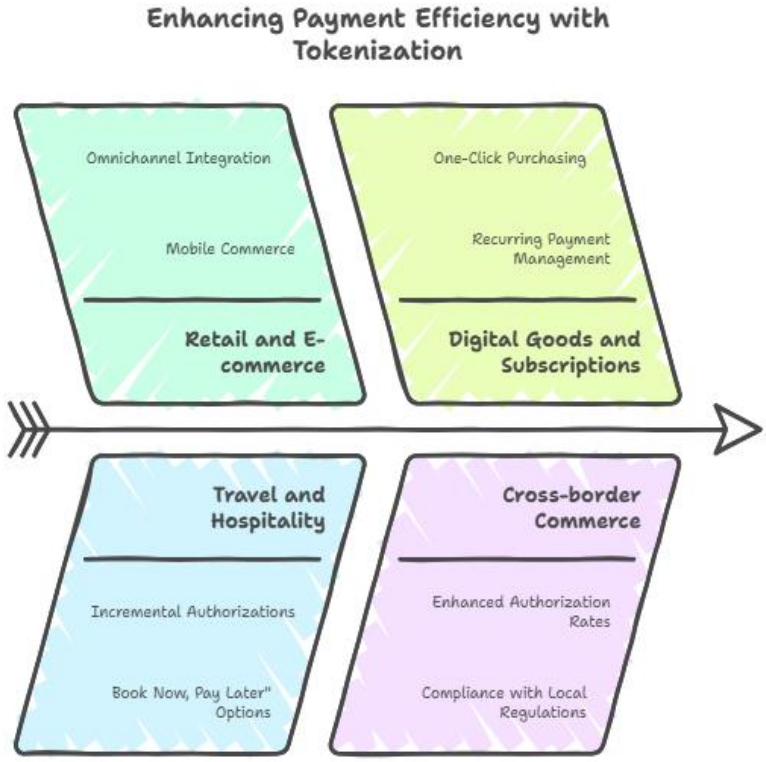

Fig 4: Enhancing Payment Efficiency with Tokenization [9, 10]

6. Future Trajectory and Emerging Applications

Integration with Emerging Commerce Channels (IoT, Voice, AR/VR)

The tokenization framework originally developed for traditional commerce is now expanding into emerging channels, enabling secure payments across the Internet of Things (IoT), voice assistants, augmented reality (AR), and virtual reality (VR) environments (9). These newer environments present unique challenges—payment credentials must be protected across a diverse ecosystem of connected devices with varying levels of security and differing user interfaces. Network tokenization provides an ideal foundation, enabling secure transactions without requiring sensitive data to be stored on potentially vulnerable edge devices. Industry projections forecast substantial growth in IoT payments in the coming years, with connected devices—from smart appliances and wearables to connected vehicles—increasingly embedded into commerce workflows. Early implementations show how tokenization can be adapted to these new environments while preserving consistent security standards. Connected vehicles represent one of the most advanced IoT commerce use cases enabled by tokenization (10). Automotive manufacturers and payment networks have collaborated to implement

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

in-vehicle payment solutions for use cases like fueling, tolls, parking, and drive-through purchases. These implementations often store tokenized credentials in the vehicle's secure element, with authentication handled via proximity to point-of-sale and driver verification—using biometrics, key fobs, or mobile devices. Similarly, voice commerce through smart speakers and digital assistants has benefited from tokenization, enabling secure purchases via conversational interfaces. Leading voice platforms now support tokenized payments authenticated through voice biometrics, companion devices, or challenge-response flows. These adaptations demonstrate how tokenization enables commerce in environments where traditional user interfaces are impractical, expanding secure digital payments beyond the screen to the broader connected ecosystem.

Extension of Tokenization Beyond Payments (Loyalty, Digital Identity)

The technical principles and architecture underlying payment tokenization are increasingly being applied to adjacent domains, including loyalty programs and digital identity—creating a unified approach to securing sensitive user data across digital ecosystems (9). Loyalty programs are a natural extension, as they face similar challenges to payment systems: identifying legitimate users, preventing fraud, and enabling seamless experiences. Retailers and hospitality providers have begun implementing tokenized loyalty identifiers that operate similarly to tokenized payment credentials, replacing sensitive loyalty account numbers with non-sensitive surrogates. This approach allows loyalty points and rewards to be securely used across multiple channels and partners without exposing the original account data, improving security and enabling more flexible loyalty experiences. Industry analysts forecast significant growth in loyalty tokenization as businesses recognize the parallel benefits it offers to payment tokenization.

Digital identity is perhaps the most transformative frontier for tokenization principles beyond payments (10). As users increasingly need to verify identity across a range of services, tokenization provides a secure and privacy-preserving model for identity verification—minimizing unnecessary data exposure. Several major financial institutions and technology providers have developed identity frameworks based on tokenization, where verified identity attributes (e.g., age, address) are represented by tokens that can be selectively shared with service providers. For example, a user could prove they are over 18 to access an age-restricted service without revealing their full birthdate, or verify their address to a merchant without disclosing other personal data. Adoption of tokenized digital identity is expected to accelerate as privacy regulations emphasize data minimization and purpose limitation. Applying lessons from payment tokenization, this approach lays the groundwork for more secure and user-centric digital interactions beyond commerce.

Passwordless Authentication and "Invisible" Payments

Advancements in authentication mechanisms are a critical complement to tokenization, enabling seamless, low-friction commerce experiences (9). Traditional password-based authentication has proven inadequate—offering poor security due to reuse and weak credentials, while increasing user friction. The payments industry is now leading the shift toward passwordless authentication, using biometrics, device signals, and cryptographic credentials to verify identity without passwords. The FIDO (Fast Identity Online) Alliance has established widely adopted standards for passwordless authentication, and major networks are now integrating FIDO-compliant methods with tokenized payment infrastructures. The combination of strong passwordless authentication and tokenization underpins what the industry refers to as "invisible payments"—transactions requiring little to no active involvement from the consumer beyond initial consent.

The concept of invisible payments has evolved from early implementations like ride-sharing apps—where payment occurs automatically at trip completion—into broader visions of ambient commerce (10). Leading payment and technology firms have built prototypes combining tokenization, passive authentication, and contextual signals to enable frictionless transactions. These systems might use a mix of facial recognition, device presence, behavioral signals, and risk scoring to authenticate and authorize transactions without explicit user input. For example, a retail store could recognize a returning customer via their smartphone, match facial recognition and historical purchase patterns, and automatically charge their tokenized payment credential when they exit with merchandise. The

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

elimination of checkout as a discrete action represents the culmination of efforts to minimize friction—with tokenization providing the secure foundation for such experiences. While mainstream adoption of invisible payments is still in its early stages, the convergence of tokenization and advanced authentication is already shaping next-generation commerce experiences.

Merchant Adoption and Implementation Roadmap

As tokenization and unified checkout capabilities mature, payment industry stakeholders have developed structured adoption roadmaps to help merchants implement these technologies effectively (9). These roadmaps typically recommend a phased approach that balances business needs with technical and compliance requirements—recognizing that tokenization represents both an infrastructure change and a strategic opportunity. The initial phase often focuses on enabling tokenization for newly stored cards (e.g., card-on-file for new customers), building a base of tokenized credentials without disrupting existing systems. Subsequent phases may involve migrating legacy stored cards to network tokens, deploying Click to Pay for guest checkout, and extending tokenization across all payment channels. Industry best practices emphasize measuring key performance indicators throughout the journey—such as fraud rates, authorization approvals, and checkout conversion—to demonstrate business value beyond compliance.

Modern implementation roadmaps increasingly position tokenization as a pillar of digital customer experience and unified commerce strategies (10). Forward-looking merchants are leveraging tokenization not only for security, but also to enable cohesive customer journeys across devices, channels, and experiences. This includes use cases like seamless handoffs from online browsing to in-store purchasing, single-click reordering across devices, and subscription billing models powered by secure stored credentials. The roadmap also highlights the need for cross-functional collaboration—bringing together teams from payments, security, marketing, and product to align on business goals and technical execution. As adoption grows, implementation guidance is becoming more tailored to merchant segments—recognizing that the optimal approach for a subscription-based SaaS provider differs from that of a global retailer or cross-border marketplace. This evolution reflects tokenization's transition from an emerging technology to a foundational element of modern digital commerce infrastructure.

7. Conclusion: The Future of Tokenized, Unified Commerce

Tokenization and unified checkout mark the culmination of the payment industry's strategic response to the twin challenges of digital commerce: securing sensitive data and reducing user friction. By replacing vulnerable payment credentials with secure, domain-limited tokens and standardizing checkout across card networks, these technologies have delivered measurable benefits across the ecosystem. Merchants experience higher conversion rates and reduced fraud losses, consumers benefit from faster and safer experiences, and payment providers see improved transaction security and authorization performance.

As tokenized, unified commerce extends into emerging channels—including IoT, voice-enabled transactions, and immersive AR/VR environments—it sets the stage for a future in which payments become increasingly ambient and seamless, while remaining anchored in strong security. The application of tokenization frameworks to domains beyond payments, such as loyalty programs and digital identity, signals its growing role as a foundational model for privacy-preserving data exchange.

For the digital payments industry, this is not just an incremental evolution but a fundamental redesign of how digital transactions are conducted. Tokenization and unified checkout redefine the standard for secure, scalable, and user-friendly commerce—creating a future where digital interactions are both trusted and frictionless by default.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

References

[1] EMVCo, "EMV® Secure Remote Commerce," 2025. [Online]. Available: https://www.emvco.com/emv-technologies/secure-remote-commerce/
[2] Adyen, "Payment Tokenization Guide," 2023. [Online]. Available: https://www.adyen.com/knowledge-hub/payment-tokenization-guide
[3] Theodore Sterling, "EMV SRC Explained for Beginners," 2024. [Online]. Available: https://www.chargeback.io/blog/emv-src-explained
[4] Merchant Support, "Click to Pay integration guide," [Online]. Available: https://support.every-pay.com/merchant-support/click-to-pay-integration-guide/
[5] Lorien Carter, "Network Tokenisation Market Report 2025-29," 2025. [Online]. Available: https://www.juniperresearch.com/research/fintech-payments/fraud-security/network-tokenisation-market-research-report/
[6] CyberSource, "Discover the latest payment methods, AI innovations, and fraud trends for merchants," [Online]. Available: https://www.cybersource.com/en/solutions/fraud-and-risk-management/fraud-report.html
[7] BIS, "Leveraging tokenisation for payments and financial transactions," 2025. [Online]. Available: https://www.bis.org/publ/othp92.pdf
[8] Debut Infotech, "Diverse Tokenization Use Cases Across Industries,". [Online]. Available: https://www.debutinfotech.com/use-cases/tokenization-use-cases-across-industries
[9] Getnet, "The Future of Payments Today," 2023. [Online]. Available: https://www.getnetworld.com/content/dam/getnetworld/documents/The%20future%20of%20Payments,%20Today23.pdf
[10] NIC, "Digital Payments driving the growth of Digital Economy" 2023. [Online]. Available: https://www.nic.gov.in/digital-payments-driving-the-growth-of-digital-economy/

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.