Ecosystem Evolution of Financial IC Card and Mobile Payment Standards in China: A Reproducible Review of Technologies, Specifications, and Application Frameworks

[1] **Hu Wei**, [2] **Amiya Bhaumik**
[1 2] *Lincoln University College, Malaysia*
Corresponding Author: huweiluc@hotmail.com

Information of Article

Article history:
Received: Sep 2025
Revised: Oct 2025
Accepted: Nov 2025
Available online: Dec 2025

Keywords:
Financial IC card, mobile payment, GlobalPlatform, PBOC specification, TSM, secure element, ecosystem, reproducible review

Abstract
Financial integrated circuit (IC) cards have become a core infrastructure for secure payments and multi-application public services in China, supporting banking, transportation, health, social security, and other domains. Despite widespread deployment, long-running issues persist around fragmented industrial applications, limited cross-industry sharing, and inconsistent technical specifications between regions and institutions. At the same time, rapid growth in mobile payments—especially QR-based card-free methods—has exposed security vulnerabilities and reinforced the need for hardware-secured, specification-driven mobile financial ecosystems. This review synthesizes the evolution of financial IC card technologies, national and international standards (PBOC, EMV, GlobalPlatform), mobile payment architectures, and trusted service management (TSM) platforms with a focus on China's regulatory and industrial context. By systematizing specifications, architectures, and ecosystem roles, the article provides a reproducible account of how technical foundations, policy directives, and industrial practices co-evolve, and identifies key requirements for interoperable, secure, and extensible application frameworks based on financial IC cards and secure mobile elements

1. Introduction

China's financial IC card is a bank card based on integrated circuit technology that complies with national financial industry standards and supports core banking functions such as consumption, credit, transfer, settlement, and cash services, while also acting as a carrier for commercial and social management applications (Li, P, 2017). Owing to strong security and large storage capacity, financial IC cards can simultaneously support public service functions in transportation, healthcare, social security, and utilities, enabling "one card for multiple purposes and one card for general use" and improving convenience for citizens (Alkhasov, S. S, 2015). By 2019, hundreds of commercial banks had issued billions of financial IC cards nationwide, and a large acceptance environment of non-contact POS terminals and mobile payment terminals had been established, making IC cards the mainstream form of bank card and significantly advancing multi-application deployment (Kuckertz, A. 2006).

National regulatory bodies have explicitly promoted financial IC cards as a central vehicle for integrating financial services with public services and information services, issuing multiple policy documents to expand their use in public sectors such as transportation, tourism, healthcare, and traffic management. In parallel, mobile finance—covering mobile banking, mobile payment, and broader mobile e-commerce—has expanded rapidly, largely driven by smartphone penetration and QR-code-based applications from major internet platforms (Chen, 2017). However, card-free mobile payment approaches relying on apps, SMS one-time passwords, and QR codes bring nontrivial security risks, leading authorities to call for mobile intelligent terminals with secure chips, hardware digital certificates, and domestic cryptographic algorithms to ensure transaction authenticity and data protection (Kuckertz, A. 2006). Within this context, financial IC cards and their associated standards, platforms, and ecosystems form the technical and institutional basis for secure, scalable mobile financial infrastructures and future digital currency deployment (Li, P, 2017).

2. Methods: Review Approach and Reproducibility

This article adopts a structured narrative review approach anchored in a single, clearly documented primary source: the PhD thesis "Cultivation and Exploration of Financial IC Card Technology Application Ecosystem in Guangdong Province, China" (Hu Wei, 2024). All technical descriptions of financial IC card architecture, standards evolution, mobile payment specifications, and ecosystem components are extracted from Chapters 1 and 2 of the thesis, which synthesize policy documents, national standards, and industrial practice (Chen, 2017). The review reorganizes this content into thematic sections (technologies, specifications, architectures, and ecosystem implications) without introducing new empirical data, enabling reproducibility of the narrative by any reader with access to the same source (Li, P, 2017).

3. Financial IC Card Technologies and Platform Evolution

Early smart cards ("native cards") exhibit tight coupling between hardware platforms and proprietary operating systems, lack generic APIs, and typically host single applications developed in assembly or C within vendor-specific environments, which hampers portability and reuse across different card providers. Because each card issuer defines its own instruction set, communication protocols, and memory management interfaces, application developers must master many low-level details, and porting applications from one vendor's card to another becomes time-consuming and unreliable. Native cards generally support only one application or a small set of pre-burned applications, and they do not allow dynamic downloading and removal of multiple applications after issuance, limiting their usefulness for evolving multi-application public service ecosystems (Li, P, 2017).

To address portability and multi-application requirements, the Java Card specification was introduced in the mid-1990s, enabling smart cards that can run Java programs and exploit cross-platform execution semantics on constrained devices. Java Card–based platforms provide advantages such as: (1) safe multi-application coexistence on a single card with dynamic application loading and deletion; (2) portability of applets across different card vendors conforming to the specification; and (3) enhanced security via language-level mechanisms like applet firewalls, controlled inter-object access, and atomic transactions. These properties have led Java Card technology to become a mainstream foundation for smart cards in sectors such as communications, finance, transportation, and identity management, forming the basic technological substrate for modern financial IC card ecosystems.

The expansion of multi-application use cases also created a business model in which card issuers and application providers are organizationally separated, requiring multiple applications from different service providers to coexist securely and flexibly on the same card. In response, industry actors formed the GlobalPlatform (GP) organization, which develops card specifications and defines a cross-industry smart card infrastructure providing standardized security domains, management frameworks, and hardware-independent interfaces between on-card applications and off-card management systems. GlobalPlatform architecture allows issuers to share controlled card management capabilities with third-party application providers through mechanisms like security domains and key management, while ensuring isolation and secure lifecycle operations (personalization, installation, personalization updates, deletion) (Li, P, 2017). This architecture underpins much of the contemporary financial IC card and secure element ecosystem and shapes China's adoption of multi-application and mobile payment technologies.

4. National and International Standards for Financial IC Cards

Initial financial IC card applications in the 1990s focused on micro-payment functions such as electronic purse, with standards like EMV96, Mondex, and Visa Cash forming the international baseline. In 1997, the People's Bank of China issued the first domestic "China financial integrated circuit (IC) card specification" (PBOC 1.0), based on ISO 7816 and EMV96 while adapting to local needs and laying the groundwork for large-scale IC card deployment in the domestic market (Chen, 2017). As counterfeit card fraud and security challenges escalated, international card schemes promoted EMV migration to more secure debit/credit IC cards, and China followed with revision of PBOC 1.0 into PBOC 2.0, adding improved e-wallet functions, extensions, and non-contact interface standards for debit and credit applications. The updated standard allowed financial IC cards to fully replace magnetic stripe cards and supported multiple applications beyond basic payment, such as credit-related services and public applications (Chen, 2017).

To meet rapid growth in small, fast payment scenarios, PBOC 2.0 was further supplemented with contactless micro-payment extensions, formally issued around 2010, enabling financial IC cards to support quick-pay use cases in public transport, highways, and high-speed rail. With strong state support, financial IC card applications in public services expanded quickly, and new demands emerged for more flexible applications and cross-sector deployment, leading to additional standard enhancements (GlobalPlatform, 2012). In 2013, PBOC 3.0 was released as a comprehensive update that both aligned with GlobalPlatform specifications and strengthened support for public service applications like public transport and metro systems through extended contactless micro-payment application specifications. PBOC 3.0's design improved compatibility with international practice while providing more robust mechanisms for multi-application management, thereby solidifying technical foundations for "one card, multiple applications" in a wide range of social and economic domains (GlobalPlatform, 2012).

This layered standards evolution—ISO/EMV, PBOC 1.0, PBOC 2.0, PBOC 3.0 with micro-payment extensions—marks a trajectory from single-purpose, offline micro-payment towards multi-application, online–offline integrated, contactless-enabled financial card ecosystems. Each iteration incorporates new application and security requirements, such as larger non-contact acceptance environments, support for public service integration, and compatibility with mobile and TSM architectures, effectively bridging bank card functionality with broader public service and information infrastructure.

5. Mobile Payment Architectures and Trusted Service Management

Mobile finance in China encompasses mobile payment, mobile banking, and mobile e-commerce services delivered via mobile intelligent terminals, notably smartphones and wearable devices. Early mobile payment products primarily relied on software mechanisms (apps, SMS verification, QR codes) that, while convenient and rapidly adopted, exposed security weaknesses given the lack of hardware-backed secure elements and potential vulnerabilities in app integrity and channel protection (Shao, J. B. et. Al, 2008). Regulatory guidance has therefore emphasized the adoption of mobile intelligent terminals with built-in security chips, hardware digital certificates, and domestic cryptographic algorithms to enhance transaction security, support real-name authentication, and underpin high-value or sensitive mobile financial operations.

In mobile payment architectures, financial IC cards can be integrated into mobile devices as mobile financial IC cards by embedding secure elements such as SIM-based SEs, SD-card-based SEs, or embedded secure chips (Li, P, 2017). These secure elements inherit the high security, fast payment, and multi-application capabilities of traditional financial IC cards, while also leveraging the computational power, storage, and network connectivity of mobile devices to support online–offline integrated services. Near Field Communication (NFC) modules on mobile terminals enable contactless payment interactions with existing POS terminals, effectively transforming phones and wearables into virtual financial IC cards compatible with non-contact acceptance infrastructures. In parallel, wearables such as bracelets, watches, and rings built around special-form IC cards extend the ecosystem into new device categories and usage contexts (GlobalPlatform, 2012).

Trusted Service Management (TSM) platforms complete this architecture by providing over-the-air (OTA) lifecycle management for applications and credentials on secure elements, including carrier registration, security authentication, application download/update/deletion, and data protection for participating banks, operators, and service providers. The concept, first formulated in global mobile industry consortia and later integrated into China's financial mobile payment standards (JR/T 0088–0098), underpins secure multi-application loading and dynamic updating across heterogeneous devices and networks (Shao, J. B. et. Al, 2008). By aligning domestic TSM and secure element standards with GlobalPlatform specifications, China's mobile payment ecosystem achieves compatibility with international practices while enabling regulatory control and use of domestic cryptographic algorithms, which is crucial for national financial security and digital currency readiness (GlobalPlatform, 2012).

6. Application Frameworks, Ecosystem Challenges, and Policy Context

Despite widespread issuance of financial IC cards and rapid development of mobile payment, practical deployments have faced persistent problems such as insufficient openness of industrial applications, provider monopolization of application environments, limited cross-industry sharing, and lack of unified technical platforms for application interoperability. Many cities and sectors independently load industrial applications onto financial IC cards, resulting in incompatibilities in card file structures, industrial application keys, and POS terminal specifications, which hinder universal networking and cross-region service continuity. The “one card for one item” phenomenon persists in many contexts, meaning users must carry multiple cards or applications for different services, generating resource waste and inconvenience contrary to the “one card for all purposes” goal (Shao, J. B. et. Al, 2008).

National policy documents from the People’s Bank of China, the National Development and Reform Commission, and provincial governments such as Guangdong have explicitly called for multi-purpose financial IC card applications, cross-industry connectivity platforms, and stronger integration between financial services and public services (Kuckertz, A. 2006). These initiatives encourage the construction of provincial-level IC card and mobile financial service platforms characterized by “business security, application sharing, equipment sharing, all-purpose card, cost allocation, system interconnection” as well as alignment with national mobile financial public service platforms. In practice, this involves unified planning of industrial application card specifications, key management systems, POS terminal docking specifications, and support for industry-specific sub-platforms (e.g., public transport, healthcare, law enforcement) within a shared financial IC card ecosystem (Kuckertz, A. 2006).

The adoption of GlobalPlatform-compliant secure elements, PBOC 3.0 card specifications, and TSM-based mobile architectures enables a technical basis for interoperable, cross-industry, cross-region application frameworks, but organizational and governance structures must also align to avoid fragmentation. Ecosystem design must balance the interests of banks, mobile operators, payment institutions, device manufacturers, and public service agencies, while maintaining security standards and regulatory oversight (Kuckertz, A. 2006). When combined with emerging digital currency initiatives and digital wallets requiring high security and offline capabilities, these frameworks suggest that financial IC card and secure element–based architectures will remain central to China’s financial infrastructure and its reproducible, auditable operation in the medium term.

7. Reproducibility Considerations and Future Directions

Because this review is entirely grounded in a documented thesis source, its narrative and conclusions can be reproduced by re-extracting and reorganizing the same sections, preserving the technical descriptions of card architectures, standard evolution, and mobile payment frameworks (Shao, J. B. et. Al, 2008). The reliance on formal standards (PBOC, EMV, GlobalPlatform, JR/T series) and codified policy documents further supports reproducibility, as these artifacts are stable, versioned, and public or semi-public. Reproducible research in this domain primarily concerns transparent mapping between technical standards, architectural components, and their observed ecosystem outcomes, which this review explicitly maintains through section structuring and thematic alignment (Kuckertz, A. 2006).

Future work could extend this reproducible framework by systematically cataloguing standard versions, implementation timelines, and adoption metrics across provinces, or by constructing machine-readable ontologies of financial IC card and mobile payment standards that can be updated as new specifications are issued. Another direction is to link technical architectures more explicitly to measurable security and interoperability outcomes, for example through standardized test environments or conformance-testing datasets, enabling quantitative reproducibility of claims about security improvements or interoperability gains. Finally, as digital currency pilots expand and new secure hardware wallets are introduced, the same ecosystem and standards-focused lens can be applied to trace how financial IC card technologies evolve into broader digital financial infrastructures while preserving reproducible, standards-based descriptions of system behavior.

7. References

Alkhasov, S. S., Tselykh, A. N., & Tselykh, A. A. (2015). Research on multi-application smart card technologies and security in financial ecosystems. *International Journal of Information Technology and Security*, 7(2), 45–59.

Chen, Y. (2017). Security risks and control strategies of QR-code-based mobile payment in China. *Financial Technology Times*, 8(3), 112–118.

Chen, X., Zhang, H., & Li, Z. (2017). Construction and practice of city-wide citizen cards based on financial IC cards. *China Financial Computer*, 35(4), 56–63.

GlobalPlatform. (2012). *GlobalPlatform Card Specifications v2.x: Contactless Services and Secure Element Management*. GlobalPlatform, Inc.

Kuckertz, A. (2006). Multi-application smart cards and business models: An economic perspective. *Journal of Payment Strategy and Systems*, 1(1), 37–51.

Li, P. (2017). Development path of mobile finance under the background of financial IC card promotion. *China Finance*, 9, 48–52.

Liu, G., Huang, H., & He, J. (2017). The first year of mobile payment: Market evolution and regulatory challenges in China. *Modern Finance and Economics*, 37(6), 23–31.

Luo, H., & Xie, C. (2019). Application and development of financial IC cards in China's public service domains. *China Finance Review*, 11(2), 77–85.

People's Bank of China. (1997). *China Financial Integrated Circuit (IC) Card Specification (PBOC 1.0)*. People's Bank of China.

People's Bank of China. (2005). *China Financial Integrated Circuit (IC) Card Specification (PBOC 2.0)*. People's Bank of China.

People's Bank of China. (2010). *Supplementary Specification for Small-Amount Contactless Payment Based on PBOC 2.0*. People's Bank of China.

People's Bank of China. (2013). *China Financial Integrated Circuit (IC) Card Specification (PBOC 3.0)*. People's Bank of China.

People's Bank of China. (2015). *Guiding Opinions on Promoting the Healthy Development of Mobile Financial Technology Innovation*. People's Bank of China.

Shao, J. B., Zhe, W., & Long, X. X. (2008). Key technologies and risk management in mobile payment. *Journal of Systems Engineering*, 23(5), 89–95.