Payment Strategies Brief | February 1, 2021

Coming Soon to the U.S.: A National Standard for Mobile Financial Services[1]

Susan Pandy, Ph.D., Director, Payment Strategies

[1] X9.134 defines mobile financial services (MFS) as mobile payments (including retail) and other mobile banking services.

Contents

Introduction

The use of mobile devices for mobile banking and payments at the point of sale (POS) or remotely (e.g., mobile application, in-application, browser) continues to grow. Juniper Research reports that global mobile commerce (m-commerce)[2] payments will reach $3.1 trillion in 2025, from $2.1 trillion in 2020.[3] Both e-commerce and m-commerce sales volume continues to expand rapidly in the U.S. The Census Bureau estimates that U.S. retail e-commerce sales for the second quarter of 2020 increased 44.5 percent over the second quarter of 2019. Business Insider Intelligence forecasts that by 2024, 44 percent of all retail e-commerce will be generated via m-commerce.[4] Smartphones are now a driving force behind m-commerce growth, with notable increases in both digital buyers and average spending per buyer due to the global pandemic.[5] In spite of these projected growth trends, the market remains highly fragmented, with many different solutions available to consumers, financial institutions (FIs), and non-FI mobile service providers.

The U.S. does not have an open standard specific to Mobile Financial Services (MFS) that mirrors the international version, *ISO 12812: Core Banking – Mobile Financial Services,*[6] published in 2017. To address this gap, the Accredited Standards Committee (ASC) X9, Inc.,[7] launched a workgroup to develop American National Standard X9.134 in 2019 modeled after ISO 12812. X9.134 recognizes industry changes since 2017 and reflects the U.S. perspective. The X9.134 standards framework will support: (1) interoperability[8] between MFS components and functions; (2) a better consumer experience when choosing among mobile devices or products;[9] and (3) a secure environment to ensure trust in the mobile financial service provider (MFSP)[10] and enable FIs and payment processors to manage risks.

This brief describes the purpose and scope of the X9.134 standard work effort, current adoption status, and future expectations for U.S. industry adoption. X9.134 consists of five parts: (1) a general framework (adopted as a standard in January 2020); (2) security requirements (adoption scheduled for Q1 2021); (3) application lifecycle management,

---

[2] M- commerce invoices shopping through a mobile device (i.e., smartphone), while e-commerce invoices shopping online using a PC or tablet.
[3] Juniper Research (2020, Dec. 14). *Alternative payments and the evolving ecommerce landscape*. Retrieved from https://www.juniperresearch.com/document-library/white-papers/alternative-payments-and-the-evolving-ecommerce.
[4] Meola, A. (2019, Dec. 17). Rise of m-commerce: Mobile ecommerce shopping stats & trends in 2020. *Business Insider*. Retrieved from https://www.businessinsider.com/mobile-commerce-shopping-trends-stats.
[5] Samet, A. (2020, July 2). US ecommerce will rise 18% in 2020 amid the pandemic. *eMarketer*. Retrieved from https://www.emarketer.com/content/us-ecommerce-will-rise-18-2020-amid-pandemic.
[6] ISO 12812 is a five-part standard that includes: Part 1 - general framework, adopted as an international standard, and Parts 2-5 adopted as technical specifications. Part 2 addresses security requirements, Part 3 mobile financial application management, Part 4 payments-to-persons, and Part 5 payments-to-businesses. For more information, see https://www.iso.org/news/2016/05/Ref2083.html and https://www.iso.org/standard/59844.html.
[7] For more information, see https://x9.org.
[8] Interoperability is the ability for systems and organizations to work together, or to inter-operate.
[9] Including the ability to transfer MFS from one device to another (i.e., portability).
[10] A mobile financial service provider (MFSP) is an entity that has created an MFS offering accessed by its customers via a mobile device. For example, Apple, Google, PayPal, Samsung, financial institutions, and other third-party mobile wallet providers may be MFSPs.

including authentication and credentialing (anticipated adoption in Q1 2021); (4) payments between persons (under development with anticipated adoption in Q2 2021); and (5) payments to a retail business (work scheduled to begin in early 2021).

The Need for Standardization of Mobile Financial Services (MFS)

Interoperability is a central tenet of the X9.134 standard because multiple entities comprised of technical components are often involved in the payments value chain. For example, FIs are bound by network rules in a payment network, which allow payments to flow from one FI customer to another FI customer over the same network. Examples of payment networks include organizations handling check, automated clearing house (ACH), and electronic funds transfer (EFT). In addition, the X9.134 standard covers how non-bank MFS issuers are able to interoperate in the same system, whether using the same networks or different networks. The X9.134 standard addresses the role of the mobile device in the payments value chain and its impact on newly created components and/or interfaces.

Mobile payments occur at the POS or remotely via the online channel and can be made by a consumer to a business or to another person (e.g., payments-to-a-person). The underlying process may include near field communications (NFC) technology to transmit data from the mobile device, a mobile application (app) installed on the mobile device, quick-response (QR) codes, and other forms of digital tokens. Current and future mobile technologies will need to coexist. This ecosystem creates complex supply chains, emphasizing the need for standards that support the technology and process and help to minimize risk within the components.

X9.134-1 – General Framework

A critical aspect of building the U.S. version is developing common terminology and basic principles for implementation of MFSs X9.134 that: 1) define the components, related interfaces and roles necessary to operate MFS for specific use cases; 2) identify existing standards that address MFSs; and 3) ascertain possible gaps. Part 1 provides a general framework for mobile banking and payments, including terms and definitions that apply to the entire standard. Part 1 does not include any requirements but presents general principles for how Parts 2 through 5 interact. It also provides guidance on how an MFS should operate.[11]

[11] This X9 work effort does not reinvent existing X9 or other national/international standards for processing payments (e.g., ISO 8583, ISO 20022). Other relevant existing X9 standards have been leveraged to address the mobile secure environment (e.g., X9.112-Part 4, X9.117, X9.122). Finally, X9.134 will not address specific communications protocols or mobile devices, where several existing standards by different standards bodies (e.g., ITU) have already been developed and are being utilized in the marketplace. This standard will not drive or promote any specific mobile application technology, nor will it stifle innovation.

The purpose of Part 1 is to facilitate the interoperability, security, and quality of MFS solutions under development by U.S. entities. It also aids in the efficient development of MFS products and solutions by leveraging various mobile environment features and supporting resolution of identified standardization challenges. These challenges include navigating complex ecosystems and regulations, adapting MFS to fast-evolving technology, meeting consumer expectations for access to MFSs, and managing risk in the mobile environment.

A national standard offers clear requirements to MFSPs for implementing mobile banking and payments functionality. First, an MFSP must support multiple implementations and different mobile devices to offer MFS to a wide range of consumers. Second, an MFSP must accommodate the needs of other, different MFSPs operating MFS solutions on the same device. Finally, security is critical to building systemic trust with consumers and merchants alike. An MFSP has little control over the mobile devices used or the vulnerabilities presented by access to the Internet or use of Wi-Fi networks, leaving devices susceptible to malware. An MFSP must conduct an assessment to identify risks, define proper countermeasures, and implement security mechanisms (e.g., secure environment) to prevent and mitigate the identified risks and minimize fraud.

Part 1 also addresses technology components, such as the mobile device, mobile apps, user interface, and mobile wallet. Supporting technologies need to utilize a secure environment (see Part 2), which can be achieved using a trusted execution environment (TEE),[12] secured server, secure element (SE),[13] or supplemental software security controls. A secure environment includes controls such as: (1) separation of applications (e.g., identity, banking, and retail payments), (2) supervision of application management, and (3) control of application access rules. A secure environment for an MFS application should provide the basic trusted services: strong customer authentication, integrity, end-to-end confidentiality, non-repudiation of transactions, and consumer privacy.

X9.134-2 – Data Protection and Security

The proliferation of mobile devices, as well as the vulnerability of mobile communication networks and mobile apps, creates security challenges for mobile payment technology. Security is the central requirement for every MFS. The risks associated with a consumer payment experience differ when using a wireless mobile device instead of a physical payment card at the point of purchase and require a different assessment of risk management practices. Industry stakeholders need to mitigate fraud risk and protect their customers and businesses by identifying threats against the integrity and confidentiality of data prior to implementing an MFS solution.

---

[12] A trusted execution environment (TEE) comprises hardware and/or software (usually both) in the mobile device and provides security services to the mobile device computing environment, protects data against general software attacks, and isolates hardware and software security resources from the operating system.
[13] A secure element is a tamper-resistant platform in the mobile device capable of securely hosting and executing applications and associated confidential and cryptographic data (e.g., key management).

Part 2 explains the risks inherent in the ecosystem and the suitability of existing security standards (architecture, devices, and mechanisms) to assist MFS developers and MFSPs when evaluating and selecting security mechanisms that meet an established security policy. It is important for all MFSPs and MFS users to understand how security requirements and other considerations factor into the mobile environment.

Mobile devices and mobile apps leverage various technologies (e.g., NFC, QR codes) in conjunction with an appropriate secure environment (e.g., SE, TEE, and software with supplemental security controls) resident in the device or accessible from a remote/cloud-based server. These technologies offer different ways to secure financial data, financial applications, and personal information. Part 2 differentiates security requirements between a proximate[14] mode of operation and a remote mode of operation. Proximate payments occur when the consumer's mobile device communicates with another mobile device (i.e., payee mobile device) or a merchant payment terminal to initiate a transaction.

Part 2 also analyzes security issues related to platforms and technologies used to operate an MFS solution and identifies malware vulnerabilities (e.g., worms, viruses, trojans) specific to mobile devices. Part 2, along with a number of other payment security-oriented American National Standards developed by ASC X9, Inc., outlines the requirements for a safe and secure MFS.

X9.134-3 – Financial Application Lifecycle Management

Part 3 outlines the basic principles and requirements for application lifecycle management. Part 3 defines an application as one that includes software modules and associated data to provide functionality for an MFS. The application software and associated data, including payment credentials, may be located, accessed, and processed within a mobile device or on a server. Portions of the required software may be stored inside or outside of the secured environment (e.g., SE, TEE). Alternatively, when the app is located on a secured server, the user must be able to access it through the mobile device.

Part 3 also describes the application lifecycle activities and principles from service activation to termination. The phases include subscribing to the MFS, installing the application on a mobile device, ongoing usage of the application, termination of the MFS, and deletion of the application. The MFSP assumes the underlying responsibility to ensure that all entities involved in the application lifecycle comply with the MFS functional and security requirements. Such activities include establishing a security policy, application development, application user interface development, personalization, and activation of the application.

---

[14] X9.134 defines proximate payments as those that occur when the payer and the payee are and must be physically present in the same location and use a wireless communication channel to initiate the transaction.

There are nine technical requirements related to lifecycle management: service management, MFS portability, security and privacy, risk assessment, user interface and branding, customer relationship management (CRM), terms of service, storage of payment credentials, and access to credentials.

Service level agreements (SLAs) between entities that manage the MFS establish the requirements for service management. SLA requirements should address CRM, scalability, and operational aspects (e.g., technical processes, security, fraud reporting). If a customer changes mobile devices, the MFSP should be able to support portability of the MFS from the original mobile device to a new mobile device.

Security and privacy requirements enable the secure deployment and operation of MFS applications. While this requirement references X9.134-2, the requirements are specific to the MFS application and its configuration. The application must have a secure environment (e.g., SE, TEE, or secured server), user interface (display and entry on the keyboard), mobile devices, and lifecycle management with associated cryptographic key management. Part 3 requires the MFSP to document and retain the risk assessments used to configure an MFS.

User interface and branding features require the MFSP to create a data structure that provides information to the mobile OS: MFSP name, application name, version, and brands/logos. For CRM, the MFSP must provide customers with their contact information to provide technical support and resolve incidents of loss or theft of a mobile device. The terms of service should include the rights and obligations to both parties regarding application lifecycle management and applicable regulations.

Part 3 requires that payment credentials (e.g., primary account number, demand deposit account information, stored value, or tokenized references to credentials) be stored securely in a secure environment on the mobile device or on a remote server. The MFSP must also ensure that the user has easy access to payment credentials to update or modify them.

X9.134-4 – Payments to Persons

In recent years, the U.S. has experienced significant growth in mobile solutions in the payments-to-persons space (e.g., Venmo and Zelle).[15] The workgroup is improving ISO 12812 – Part 4 to reflect current industry models. The ISO-12812 – Part 4 specification describes similar FI-centric or proprietary-based models but concentrates on Single European Payments Area card-based models. Therefore, the X9 standard differs materially from ISO-12812 to reflect the U.S. market and changes in user experience over the last few years. Part 4 categorizes industry models for payments-to-persons as

[15] This reference is not intended to be exclusive of other market payments-to-persons solutions and products.

bank-centric (e.g., Zelle) or non-bank centric (e.g., Venmo) and addresses how a payer interacts with a person to initiate and complete a mobile payment.[16]

Clause 5 of Part 4 describes the principles of mobile payments-to-persons, while Clause 6 describes specific requirements. The requirements seek to facilitate the interoperability of mobile payments-to-persons. Part 4 also provides MFSPs with technical provisions to enable development of interoperable mobile services, where the payer or the payee uses a mobile device to send and receive payments.

Part 4 provides comprehensive requirements and recommendations for implementation of interoperable mobile payments-to-persons. It emphasizes principles governing the operations of mobile systems and processes, and the underlying technical, organizational, business, legal, and policy issues, recognizing the need to address legacy systems.

X9.134-5 – Payments to Businesses

A key component of the MFS environment is being able to make mobile payments to merchants and other businesses. There are several ways a retail or business customer can pay a merchant. Part 5 focuses on mechanisms by which a person ("consumer," "payer," or "business") uses a mobile device to initiate a payment to a business entity ("merchant" or "payee"), including remittances. It provides a comprehensive standard for using mechanisms to initiate the transfer of funds between the various parties to the transaction. Part 5 also applies to potential implementers of mobile retail payment solutions.

Work will begin on X9.134 - Part 5 in early 2021 after the completion of X9.134 - Part 4 and should require minimal changes to become a U.S. standard

Summary

The complete X9.134 standard is expected to be fully adopted by mid- to late 2021. Interested parties are encouraged to consider X9 membership to participate in the workgroup effort for Parts 4 and 5. The workgroup welcomes participation by industry experts who can help accurately develop the U.S. requirements. This underscores the importance of generating industry awareness of this effort and encouraging broader participation.

[16] A "person" can be either a natural individual or a small business entity legally recognized as a "person," but where the payment is casual in nature (e.g., where the purpose is to transfer funds between people who know each other, such as family members, friends, or neighbors, or where the relationship between two people is casual, such as to pay the babysitter, nanny, handyman, etc.).