Mobile and Contactless Payments Standards Glossary

Version 1.0

Publication Date: November 2019

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

About the Mobile and Contactless Payments Working Committee

The goal of the Mobile and Contactless Payments Working Committee is for all interested parties to work collaboratively to explore the opportunities and challenges associated with implementation of mobile and contactless payments in the U.S. market, identify possible solutions to challenges, and facilitate the sharing of best practices with all industry stakeholders.

Table of Contents

1. Purpose of the Document

The U.S. Payments Forum Mobile and Contactless Payments Working Committee developed this glossary to provide the U.S. payments community with an accessible resource that lists and provides a high-level explanation of the various standards and standards bodies that are applicable to mobile or contactless payments.

For the purpose of this document, mobile and contactless payments consist of all non-contact payment approaches that facilitate convenient, fast and secure payment transactions for consumers. This includes all mobile payments approaches (e.g., bar code, QR code, Near Field Communication (NFC), Samsung Magnetic Secure Transmission (MST), EMV/Magnetic Stripe Data (MSD) contactless, Bluetooth, in-app, m-commerce browser transactions, and other mobile technologies that can be used to enable payment), all form factors (e.g., dual-interface EMV chip cards, mobile devices, wearables and cards on file), and both card and non-card (e.g., faster payments) approaches.

2. References

This document assumes understanding of key terms and definitions specific to mobile payments with point-of-sale (POS) interactions, including loyalty/reward cards. Terms and definitions can be found in the U.S. Payments Forum Mobile and Contactless Payments Glossary.

This document also describes the various stakeholder groups involved with mobile and contactless payments. Refer to the U.S. Payments Forum Mobile and Contactless Requirements and Interactions guide for descriptions of stakeholders.

3. Purpose and Usefulness of Standards

According to the International Standards Organization, standards ensure that products and services are safe, reliable and of good quality. For businesses, they can be strategic that reduce costs by minimizing waste and errors and increasing productivity. Standards may help companies to access new markets, level the playing field for developing countries and facilitate free and fair global trade.

In addition, standards provide organizations with a basis for mutual understanding, and can facilitate business interactions and speed the delivery of new products to the market. Use of standards also helps provide interoperability between new and existing products.

Standards can establish a base for the introduction of new technologies and help to ensure that products or services supplied by different companies will be compatible.

Standardization often results from a voluntary collaboration among industry and other interested parties to develop technical specifications that are created and approved by consensus.

Not all standards are free to view and/or implement. Standards organizations may charge for the rights to acquire, rights to view and/or rights to implement a standard. Some standards may be acquired individually, others through an organizational membership. For any particular standard, visit the organization's website for their policies and terms of use. As with all third-party materials, consult with legal counsel on terms and conditions.

4. Stakeholder Groups

In preparing this paper, the Mobile and Contactless Payments Working Committee identified and solicited input from the industry stakeholder groups listed in this section. A summary description of each stakeholder group is below.

For more detailed information on Stakeholder Groups and their interactions, refer to the Mobile and Contactless Payments Requirements and Interactions white paper.

- **Issuer** – The financial institution that issues payment cards and holds the account or credit line behind the card.
- **Acquirer/Processor** – A company (often a third party) appointed by a merchant to handle card transactions for merchant acquiring banks.
- **Retail Merchant** – The entity that accepts payments from customers (i.e., consumers/cardholders) in exchange for goods and/or services and connects to a payment network through an acquirer. There are both overlapping and unique requirements across merchant industries, including retail, petroleum, transit, and unattended systems operators (e.g., ATM, vending).
- **Payment Network** – A payment network provides POS and ATM services for credit, debit, ATM and prepaid card issuers and corresponding transaction acquirers. It establishes participation requirements, operating rules and technical specifications for the purpose of receiving, routing, securing authorization for, settling and reporting domestic and international payment transactions. Each payment network determines the types of transactions, payment devices and terminals that are permitted in its respective network.
- **Consumer/Cardholder** – The end users purchasing goods and services.
- **Mobile Payment Application (MPA) Provider** – The entity that provides the applications that run on the mobile device and tie the mobile device to the site system (e.g., retail POS).
- **Wallet Provider** – The provider of software and services that represent a physical wallet, putting debit and credit cards into an application that holds payment credentials through which someone can pay, using the digital version of the debit or credit cards in that person's physical wallet, and linking to the same account, to pay.
- **Mobile Device and Operating System Provider** – The entity that provides/manufactures mobile devices and/or the operating systems on those devices.
- **Mobile Network Operator** – The wireless communications services provider that owns or controls all of the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure, back haul infrastructure, billing, customer care, provisioning computer systems and marketing and repair organizations.
- **Token Service Provider (TSP)** – The entity within the payments ecosystem that provides registered token requestors with 'surrogate' PAN values, otherwise known as payment tokens by managing the operation and maintenance of the token vault, deployment of security measures and controls, and the registration process of allowed token requestors.
- **Token Requestor –** The token requestor is a payment tokenization specific role. Token requestors register with one or more TSPs in order to request payment tokens.
- **Terminal/POS Vendor** – The entity that provides the site systems to a merchant.

5. Listing of Standards

This section includes a compilation of standards relevant to mobile or contactless payments. Each section includes a description of the relevant standards body, a summary of its most relevant standards, a list of stakeholder groups for which the standard likely holds the most relevance, a link to the standards documents, and a link to the standard organization's homepage.

Standards noted as "Draft" are works in various stages of progress and have not been released for final publication. As producing and releasing a published standard is often a lengthy undertaking, draft standards are included in this document to inform readers of their existence.

Not all standards organizations are alike. Some develop standards through voluntary efforts of industry stakeholders. Others develop specifications that may incorporate industry input. Both types of organizations are represented below, to provide the reader with a comprehensive selection of relevant specifications.

5.1 EMVCo

Per the EMVCo website[1], "EMVCo exists to facilitate worldwide interoperability and acceptance of secure payment transactions. It accomplishes this by managing and evolving the EMV® specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Today there are EMV specifications based on contact chip, contactless chip, EMV 2nd Generation, Common Payment Application (CPA), card personalisation, Payment Tokenization, and 3-D Secure. EMVCo's work is overseen by EMVCo's six member organisations—American Express, Discover, JCB, Mastercard, UnionPay, and Visa—and supported by dozens of banks, merchants, processors, vendors and other industry stakeholders who participate as EMVCo Associates."

5.1.1 EMV[2] Contactless Mobile Payment – Application Activation User Interface

The EMVCo Contactless Mobile Payment – Application Activation User Interface specification:

- Describes the components necessary to enable application activation from within an Application Activation User Interface (AAUI) application
- Provides guidelines for interacting with components outside the purview of EMVCo
- Defines the requirements for PPSE[3] behavior on a mobile device

This specification explains how the different components that make application activation possible are connected. It specifies functionality of the AAUI, defining the interaction with the contactless applications and contactless management entities on the secure element, and with the contactless module. The document does not detail the functionality of the contactless management services of a secure element or of the contactless module but covers the interaction between the AAUI and those components.

---

1 See https://www.emvco.com/about/overview/

2 EMVCo facilitates global interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues.

3 The Proximity Payment Service Environment (PPSE) is the first contactless application selected by a merchant terminal presenting the contactless applications available for conducting a transaction.

Stakeholders: Mobile Payment Application Providers, Mobile Device and Operating System Providers

Website: https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/AAUI_V1.0_Dec2010_20111123125448314.pdf

Organization Homepage: https://www.emvco.com/

5.1.2 EMV® QR Code Specification for Payment Systems: Merchant-Presented Mode

This specification provides:

- A brief description of merchant-presented EMV QR code payment and the entities involved
- Requirements for the merchant-displayed QR code, including format and content

How the mobile application processes the QR code and resulting network messages are out of scope of this document. The cardholder initiates payment by scanning a QR code displayed by the merchant on a POS terminal screen or a static poster. The cardholder uses the mobile device to transmit this information to the issuer for a push payment transaction.

Stakeholders: Issuers, Acquirers/Processors, Retail Merchants, Payment Networks, Consumers/Cardholders, Mobile Payment Application Providers, Wallet Providers, Terminal/POS Vendors

Website: https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMVCo-Merchant-Presented-QR-Specification-v1-1.pdf

Organization Homepage: https://www.emvco.com/

5.1.3 EMV® QR Code Specification for Payment Systems: Consumer-Presented Mode

This specification defines the format, encoding, and decoding of the data "payload" of the consumer-presented QR code used to perform EMV-based QR code transactions. The cardholder displays a QR code on the mobile device to make a payment to the merchant. The merchant uses a QR code reader to scan and process this information as an EMV transaction.

Stakeholders: Issuers, Acquirers/Processors, Retail Merchants, Payment Networks, Consumers/Cardholders, Mobile Payment Application Providers, Wallet Providers, Token Service Providers, Token Requestors, Terminal/POS Vendors

Website: https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMVCo-Consumer-Presented-QR-Specification-v1-1.pdf

Organization Homepage: https://www.emvco.com/

5.1.4 EMV® Contactless Specifications

This specification refers to transactions initiated from proximity NFC payment devices by waving or tapping on an EMV contactless-enabled terminal. Similar to contact chip cards, contactless payment devices also support cryptographic functions for more secure transactions than with traditional magnetic-stripe cards. With the goal of realizing universal acceptance of contactless payments, EMVCo has developed a design for contactless payments that is compatible with existing payment system solutions, while offering the opportunity for the eventual development of a common EMV contactless acceptance solution.

The specification defines a generalized POS system environment that includes:

- Reader functionality
- Terminal functionality
- Entry point software that performs the initial analysis of a contactless transaction and invokes appropriate kernel software
- Several kernels, each of which provides processing appropriate to specific contactless transactions

This specification has nine parts:

- Book A: Architecture and General Requirements
- Book B: Entry Point Specification
- Book C-2: Kernel 2 Specification
- Book C-3: Kernel 3 Specification
- Book C-4: Kernel 4 Specification
- Book C-5: Kernel 5 Specification
- Book C-6: Kernel 6 Specification
- Book C-7: Kernel 7 Specification
- Level 1 Specifications for Payment Systems, EMV Contactless Interface Specification

  Stakeholders: Issuers, Acquirers/Processors, Retail Merchants, Payment Networks, Consumers/Cardholders, Mobile Payment Application Providers, Wallet Providers, Mobile Device and Operating System Providers, Mobile Network Operators, Token Service Providers, Token Requestors, Terminal/POS Vendors

  Website: https://www.emvco.com/emv-technologies/contactless/

  Organization Homepage: https://www.emvco.com

5.1.5 EMV® PPSE and Application Management for Secure Element

This specification contains content specific to *GlobalPlatform Card Contactless Services*, which has been extracted from the original Application Activation User Interface document and combined with an overview of managing applications on secure elements.

Additionally, EMVCo has refined the test cases applying to secure element hosted PPSE applications, and included the requirements matching these test cases.

Stakeholders: Issuers, Mobile Payment Application Providers, Wallet Providers, Mobile Device and Operating System Providers, Mobile Network Operators, Token Service Providers, Token Requestors, Terminal/POS Vendors

Website: https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMVCo_PPSE_and_Application_Mgmt_for_SE_v1.0-1.pdf

Organization Homepage: https://www.emvco.com/

5.2 ISO – International Organization for Standardization

Per the ISO website[4], "ISO is an independent, non-governmental international organization with a membership of 161 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant International Standards that support innovation and provide solutions to global challenges."

5.2.1 ISO 8583-1:2003 - Financial transaction card originated messages – Interchange message specifications – Part 1: Messages, data elements and code values

ISO 8583-1:2003 specifies a common interface by which financial transaction card-originated messages may be interchanged between acquirers and card issuers.

It specifies message structure, format and content, data elements and values for data elements. How settlement occurs is not within the scope of this part of ISO 8583.

Stakeholders: Issuers, Acquirers/Processors, Retail Merchants, Payment Networks, Wallet Providers, Token Service Providers, Token Requestors, Terminal/POS Vendors

Website: https://www.iso.org/standard/31628.html

Organization Homepage: https://www.iso.org

5.2.2 ISO 12812-1:2017 Core banking – Mobile financial services – Part 1: General framework

ISO 12812-1:2017 defines the general framework of mobile financial services (MFS - payment and banking services involving a mobile device), with a focus on:

- A set of definitions commonly agreed by the international financial industry
- The opportunities offered by mobile devices for the development of such services
- The promotion of an environment that reduces or minimizes obstacles for mobile financial service providers who wish to provide a sustainable and reliable service to a wide range of customers (persons and businesses), while ensuring that customers' interests are protected
- The different types of mobile financial services accessed through a mobile device including mobile proximity payments, mobile remote payments and mobile banking, which are detailed in other parts of ISO 12812
- The mobile financial services supporting technologies
- The stakeholders involved in the mobile payment ecosystems

ISO 12812-1:2017 includes the following informative annexes:

- Annex A: Overview of other standardization initiatives in mobile financial services
- Annex B: Description of possible mobile payment business models
- Annex C: Description of typical payment instruments which may be used

Stakeholders: Issuers, Acquirers/Processors, Retail Merchants, Payment Networks, Mobile Payment Application Providers, Wallet Providers, Mobile Device and Operating System Providers, Mobile Network Operators, Token Service Providers, Token Requestors, Terminal/POS Vendors

[4] https://www.iso.org/about-us.html

Website: https://www.iso.org/standard/59844.html

Organization Homepage: https://www.iso.org

5.2.3 ISO/TS 12812-2:2017 Core banking – Mobile financial services – Part 2: Security and data protection for mobile financial services

ISO 12812-2:2017 describes and specifies a framework for the management of the security of mobile financial services (MFS). It includes:

- A generic model for the design of the security policy
- A minimum set of security requirements
- Recommended cryptographic protocols and mechanisms for mobile device authentication, financial message secure exchange and external authentication, including the following to consider for MFS:
  - Point-to-point
  - End-to-end
  - Security certification
  - Generation of mobile digital signatures
- Interoperability issues for the secure certification of MFS
- Recommendations for the protection of sensitive data
- Guidelines for the implementation of national laws and regulations (e.g. anti-money laundering and combating the funding of terrorism (AML/CFT))
- Security management considerations

In order to avoid the duplication of standardization work already performed by other organizations, this document references other international standards as required. Users of this document are directed to materials developed and published by ISO/TC 68/SC 2 and ISO/IEC JTC 1/SC 27.

Stakeholders: Issuers, Acquirers/Processors, Retail Merchants, Payment Networks, Mobile Payment Application Providers, Wallet Providers, Mobile Device and Operating System Providers, Mobile Network Operators, Token Service Providers, Token Requestors

Website: https://www.iso.org/standard/59845.html

Organization Homepage: https://www.iso.org

5.2.4 ISO/TS 12812-5:2017 Core banking – Mobile financial services – Part 5: Mobile payments to businesses

ISO/TS 12812-5:2017 focuses on mechanisms by which a consumer, payer or business uses a mobile device to initiate a payment to a merchant or other payee. Mobile payments to merchants for goods and services process over the traditional merchant point of service (POS) system, where settlement follows well-established merchant services paradigms. Additionally, a consumer may make a payment to a merchant, using the mobile device to initiate, authorize and process transactions outside of traditional payment networks. This document supports both push and pull payments (i.e., transactions that are pushed or transmitted from a mobile device to a POS or pulled/received into a mobile device or POS), which are initiated and/or confirmed by a consumer to purchase goods and or services, including proximity payments, remote secure server payments, and mobile payments that leverage other technologies (e.g., cloud, QR codes, biometrics, geo-location).

ISO 12812 provides a comprehensive standard for using the mechanisms involved in mobilizing the transfer of funds regardless of who is involved in the process. This document is intended to be used by potential implementers of mobile retail payment solutions (consumer to business), while ISO 12812-4 is

intended for potential implementers of solutions for mobile payments to persons (person to person). However, some of the payment terms for parties to the payment and methods of payment are not applicable in the U.S. X9 is developing a U.S. version of ISO 12812 that should be referenced as well.

ISO 12812 seeks to support all possible technologies and is not designed to highlight or endorse specific technologies in the competitive marketplace.

> **Stakeholders**: Issuers, Acquirers/Processors, Retail Merchants, Payment Networks, Consumers/Cardholders, Mobile Payment Application Providers, Wallet Providers, Mobile Device and Operating System Providers, Mobile Network Operators, Token Service Providers, Token Requestors, Terminal/POS Vendors
>
> **Website**: https://www.iso.org/standard/59848.html
>
> **Organization Homepage**: https://www.iso.org

5.2.5 ISO 20022 – Universal financial industry message scheme

This standard (previously named "UNIFI") is the international standard that defines the ISO platform for the development of financial message standards. Its business modelling approach allows users and developers to represent financial business processes and underlying transactions in a formal but syntax-independent notation. These business transaction models are the "real" business standards because they can be converted into physical messages in the desired syntax. When ISO 20022 was developed, XML (eXtensible Mark-up Language) was the preferred syntax for e-communication. Therefore, the first edition of ISO 20022, published in December 2004, proposed a standardized XML-based syntax for messages. The second edition of the standard, published in May 2013, included the possibility to use ASN.1 (Abstract Syntax Notation One) as well. The standard was developed within the Technical Committee TC68 - Financial Services of ISO.

> **Stakeholders**: Issuers, Acquirers/Processors, Retail Merchants, Payment Networks, Wallet Providers, Token Service Providers, Token Requestors, Terminal/POS Vendors
>
> **Website**: https://www.iso20022.org/
>
> **Organization Homepage**: https://www.iso20022.org/

5.3 ISO/IEC – International Electrotechnical Commission

Per its website[5], "The International Electrotechnical Commission (IEC) is a not-for-profit, quasi-governmental organization, founded in 1906." It is the "world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies." "IEC publications serve as a basis for national standardization and as references when drafting international tenders and contracts." "When appropriate, IEC cooperates with ISO or ITU (International Telecommunication Union) to ensure that International Standards fit together seamlessly and complement each other. Joint committees ensure that International Standards combine all relevant knowledge of experts working in related areas."

[5] See https://iectest.iec.ch/about/

5.3.1 ISO/IEC 14443-1:2018 Cards and security devices for personal identification – Contactless proximity objects – Part 1: Physical characteristics.

Contactless card standards encompass a variety of device types as embodied in the ISO/IEC 10536 series of standards (close-coupled cards), the ISO/IEC 14443 series of standards (contactless proximity objects) and the ISO/IEC 15693 series of standards (contactless vicinity objects). These device types are intended, respectively, for operation when very near, nearby and at a longer distance from associated coupling devices.

The ISO/IEC 14443 series of standards defines the technology-specific requirements for identification cards conforming to ISO/IEC 7810, thin flexible cards conforming to ISO/IEC 15457-1 and the use of such cards to facilitate international interchange. It also recognizes that the technology offers the possibility that proximity objects may be provided in forms other than that of the ISO card formats. Furthermore, it does not preclude the incorporation of other standard technologies on the card, such as those referenced in the standard's bibliography.

The ISO/IEC 14443 series of standards accommodates the operation of proximity cards in the presence of other contactless cards conforming to the ISO/IEC 10536 series of standards and the ISO/IEC 15693 series of standards. Part 1 of 14443 is intended to be used in conjunction with other parts of ISO/IEC 14443.

Stakeholders: Issuers, Terminal/POS Vendors

Website: https://www.iso.org/standard/73596.html

Organization Homepage: https://www.iso.org/home.html

5.3.2 ISO/IEC 14443-2:2016 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface

ISO/IEC 14443-2:2016 describes the characteristics of the fields used for power and bi-directional communication between proximity coupling devices (PCDs) and proximity cards or objects (e.g., proximity integrated circuit cards (PICCs)).

It does not specify the means of generating coupling fields, nor the means of compliance with electromagnetic radiation and human exposure regulations, which can vary according to country.

Stakeholders: Issuers, Terminal/POS Vendors

Website: https://www.iso.org/standard/66288.html

Organization Homepage: https://www.iso.org/home.html

5.3.3 ISO/IEC 14443-3:2018 Cards and security devices for personal identification – Contactless proximity objects – Part 3: Initialization and anti-collision

This standard describes the following:

- Polling for proximity cards or objects (PICCs) entering the field of a proximity coupling device (PCD)
- The byte format, the frames and timing used during the initial phase of communication between PCDs and PICCs
- The initial Request and Answer to Request command content
- Methods to detect and communicate with one PICC among several PICCs (anti-collision)
- Other parameters required to initialize communications between a PICC and PCD

- Optional means to ease and speed up the selection of one PICC among several PICCs based on application criteria
- PXD device capability, which is the capability to alternate between the functions of a PICC and a PCD to communicate with a PCD or a PICC, respectively.

Stakeholders: Issuers, Mobile Payment Application Providers, Mobile Device and Operating System Providers, Terminal/POS Vendors

Website: https://www.iso.org/standard/73598.html

Organization Homepage: https://www.iso.org

5.3.4 ISO/IEC 14443-4:2018 Cards and security devices for personal identification – Contactless proximity objects – Part 4: Transmission protocol

This standard specifies a half-duplex block transmission protocol featuring the special needs of a contactless environment and defines the activation and deactivation sequence of the protocol.

This document is intended to be used in conjunction with other parts of ISO/IEC 14443.

Stakeholders: Issuers, Mobile Payment Application Providers, Wallet Providers, Mobile Device and Operating System Providers, Terminal/POS Vendors

Website: https://www.iso.org/standard/73599.html

Organization Homepage: https://www.iso.org

5.4 ASC X9 – Accredited Standards Committee X9

The Accredited Standards Committee X9 (ASC X9) in support of the financial services industry has the mission to create and maintain U.S. and international standards that improve payments and securities transactions, protect data and facilitate information exchange.

5.4.1 X9.112-3 Wireless Management and Security Part 3: Mobile

ANSI X9.112 Wireless Management and Security is a multipart standard addressing different technologies and application environments using wireless communications. Part 3: Mobile, addresses the management and security requirements for implementations applicable to manufacturers, application developers, and mobile financial service providers.

Stakeholders: Mobile Payment Application Providers, Wallet Providers, Mobile Device and Operating System Providers, Mobile Network Operators, Token Service Providers, Token Requestors

Website: https://webstore.ansi.org/standards/ascx9/ansix91122018

Organization Homepage: https://x9.org/

5.4.2 X9.119 – Retail Financial Services Requirements for Protection of Sensitive Payment Card Data – Part 1 Using Encryption Method

Theft of sensitive card data during a retail payment transaction is increasingly becoming a major source of financial fraud. Besides an optional encrypted PIN, this data includes magnetic stripe track 2 data: primary account number (PAN), expiration date, card verification value, and issuer private data. While thefts of this data at all segments of the transaction processing system have been reported, the most vulnerable segments are between the point of transaction device that captures the magnetic stripe data

and the acquirer processing systems. This document standardizes the security requirements and implementation methods to protect sensitive card data over these segments. Several implementation methods exist to address the situation and this document provides guidance for evaluating them. For support of the automated fuel dispenser industry, clarification based on card brand guidance for the encryption of the middle digits has been added to this document.

Website: https://webstore.ansi.org/Search/Find?in=1&st=x9.119

Organization Homepage: https://x9.org/

5.4.3 X9.119 Retail Financial Services Requirements for Protection of Sensitive Payment Card Data – Part 2: Implementing Post-Authorization Tokenization Systems

This standard defines the minimum security requirements for implementing tokenization with post-authorization systems to protect sensitive payment card data. It provides requirements and guidance about the tokenization environment, including:

- Review of the evolving uses of tokens and tokenization to protect sensitive payment card data
- Description of use of a tokenization service securely distributing a token to a tokenization request interface on the behalf of a requesting entity
- Description of acceptable token generation methods for use in a tokenization service
- Security requirements about establishment and maintenance of a tokenization service by a TSP

Stakeholders: Issuers, Acquirers/Processors, Payment Networks, Mobile Payment Application Providers, Wallet Providers, Mobile Device and Operating System Providers, Token Service Providers, Token Requestors, Terminal/POS Vendors

Website: https://webstore.ansi.org/Search/Find?in=1&st=x9.119

Organization Homepage: https://x9.org/

5.4.4 X9.122 – Secure Customer Authentication for Internet Payments (Draft)

This standard defines the requirements for secure customer authentication in order to support electronic payment transactions, via Internet, mobile or voice channels initiated through the interchange system (debit/credit network).

Stakeholders: Acquirers/Processors, Payment Networks, Mobile Payment Application Providers, Wallet Providers, Token Service Providers, Token Requestors

Website: Not available

Organization Homepage: https://x9.org/

5.4.5 X9.134 – Core Banking: Mobile Financial Services – General Framework (Draft)

Note: This will become the U.S. version of ISO 12812 parts 1-5

X9.134 is a domestic mobile financial services (MFS) standard modeled after the *ISO 12812: Core Banking – Mobile Financial Services* standard and technical specifications published in 2017. This standard will: 1) define the components and related interfaces as well as the roles necessary to operate MFS according to recognized use cases; 2) identify existing standards that address MFS; and 3) ascertain possible gaps. X9.134 consists of five parts. Part 1 provides a general framework for mobile banking and payments, including a comprehensive list of terms and definitions that apply throughout the entire

standard. The framework provides an overview that applies to any type of mobile app or other mobile features developed or used operationally. Part 1 does not include any requirements, but presents general principles for how the other four parts of the standard interact with one another, and it provides guidance on how MFSs should operate. X9.134 will leverage other applicable standards. X9.134 Part 1 does not include technical requirements; however, parts 2-5 will. For example, *X9.134 Part 2 – Security and Data Protection for Mobile Financial Services* will include requirements for mobile financial service providers (MFSPs) that detail what a mobile financial application must do to protect personal data and secure transactions, such as using mutual authentication, protecting sensitive data from unauthorized disclosure, modification, or substitution, and authenticating credentials (e.g., mobile passwords, PINs) and account numbers.

Stakeholders: Issuers, Acquirers/Processors, Retail Merchants, Payment Networks, Consumers/Cardholders, Mobile Payment Application Providers, Wallet Providers, Mobile Device and Operating System Providers, Mobile Network Operators, Token Service Providers, Token Requestors, Terminal/POS Vendors

Website: https://webstore.ansi.org/

Organization Homepage: https://x9.org/

5.5 Conexxus

Per its website[6], "Conexxus is a non-profit, member-driven technology organization dedicated to the development and implementation of standards, technologies innovation and advocacy for the convenience store and petroleum market. Conexxus membership collaborates on key present and future industry challenges and innovations."

5.5.1 Conexxus Mobile Payment Specification

"The Conexxus Mobile Payment Specification provides a standard message interface between existing on-site fuel industry systems (e.g., point of sale, electronic payment server, forecourt device controller) and a mobile payment processing application. This enables transactions both in-store (with or without fuel) and forecourt (fueling area) purchases through a mobile device (e.g., smartphone, tablet, connected car). It provides a solution for common use cases (e.g., pay for merchandise inside, pre-pay for fuel inside (with or without additional merchandise), pay at the pump, buy a car wash outside). The specification also supports loyalty functionality.

The Conexxus Mobile Payment Specification allows for site-level processing (i.e., using existing payment and/or loyalty rails) or above-site processing (i.e., the mobile payment processor interfaces directly with the payment and/or loyalty host). In either case, the specification provides messages into the site systems to control site-specific functionality (e.g., pump authorization, car wash code generation). To provide flexibility, the way payment and loyalty are processed may be different. For example, loyalty may be processed above-site while payment is processed at site-level.

Standard interfaces between mobile devices, mobile payment applications, and site equipment/networks foster innovation and promote interoperability for vendors and manufacturers."[7]

[6] https://www.conexxus.org/content/about

[7] https://www.conexxus.org/ourwork/mobile-payment-standard

Stakeholders: Acquirers/Processors, Retail Merchants, Mobile Payment Application Providers, Terminal/POS Vendors

Website: https://www.conexxus.org/content/retail-financial-transactions-rft-standards#Mobile

Organization Homepage: https://www.conexxus.org/

5.6 IFSF – International Forecourt Standards Forum

Per its website[8], "The IFSF is a forum of international petroleum retailers with the common objective of harmonisation of equipment interconnectivity and communication standards for use in the Petroleum Retail Business. The IFSF's approach is to work with established professional bodies such as the Committee of European Manufacturers of Petroleum Measuring and Distributing Equipment (CECOD), the pump/dispenser manufacturer's trade association, and financial institutions, to achieve common standards and where possible adopt existing ones."

5.6.1 International Forecourt Standards Forum (IFSF) Part 3-60 Mobile Payment to Site Interface Specification

This specification covers the various architectures present in the fuel payment industry and includes all functional requirements currently available for making mobile payments inside and outside.

The document follows the IFSF POS to Electronic Payment Server version 3 standard and other IFSF standards where appropriate.

Stakeholders: Acquirers/Processors, Retail Merchants, Mobile Payment Application Providers, Terminal/POS Vendors

Website: https://ifsf.org/document/part-3-60-ifsf-mobile-payment-to-site-interface-specification-v1-11/

Organization Homepage: https://ifsf.org/

5.7 nexo standards

According to its website[9], "nexo standards enables fast, interoperable and borderless payments acceptance by standardizing the exchange of payment acceptance data between merchants, acquirers, payment service providers and other payment stakeholders. nexo's messaging protocols and specifications adhere to ISO20022 standards, are universally applicable and are freely available globally.

nexo standards is an open, global association dedicated to removing the barriers present in today's fragmented global card payment acceptance ecosystem. Headquartered in Brussels, its members represent the full spectrum of card payments stakeholders, including acceptors, processors, card schemes, payment service providers and vendors."

5.7.1 nexo Acquirer Protocol

The protocol offers a next generation international card payment standard that replaces ISO 8583 and its national derivatives. The standard allows the use of real-time or batch submission as well as supporting direct connections from merchant to acquirer or via a payment service provider (PSP)

[8] https://ifsf.org/about/
[9] https://www.nexo-standards.org/about-us

intermediary. nexo acquirer protocols are ISO 20022 acceptor-to-acquirer card transactions. The protocol addresses the interface between an acceptor and an acquirer.

Stakeholders: Issuers, Acquirers/Processors, Payment Networks, Token Service Providers

Website: https://www.nexo-standards.org/standards/nexo-acquirer-protocol

Organization Homepage: https://www.nexo-standards.org/

5.7.2 nexo Retailer Protocol

The nexo Retailer protocol defines a set of interfaces between a card payment application and a retail POS system. It offers new innovative features such as a clear separation between sale and payment, the provision of a complete series of payment and loyalty services, as well as a common approach for all types of architectures and environments.

Stakeholders: Acquirers/Processors, Retail Merchants, Mobile Payment Application Providers, Wallet Providers, Terminal/POS Vendors

Website: https://www.nexo-standards.org/standards/nexo-retailer-protocol

Organization Homepage: https://www.nexo-standards.org/

6. Legal Notice

This document is provided solely as a convenience to its readers. While great effort has been made to ensure that the information and materials in or referenced in this document is accurate and current as of the publication date, the list of materials referenced herein is not necessarily exhaustive, and does not necessarily reflect all specifications and standards (or any laws, statutes, regulations, rules or requirements) that may be relevant to mobile or contactless payments, or to a particular implementation thereof. Accordingly, this document does not constitute legal or technical advice, should not be relied upon for any legal or technical purpose, and all warranties of any kind, whether express or implied, relating to this document, the information or materials set forth or otherwise referenced herein, or the use thereof are expressly disclaimed, including but not limited to all warranties as to the accuracy, completeness or adequacy of such information or materials, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. All third party materials referenced herein are the property of their respective owners, and neither the U.S. Payments Forum nor any of its members is or shall be responsible or liable for the content thereof.

All registered trademarks, trade names, or service marks are the property of their respective owners.