Testing & Certification Terminology

Version 1.0

Date: May 2017

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, formerly the EMV Migration 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.

EMV is a trademark owned by EMVCo LLC.

Table of Contents

1. Introduction

This document defines field descriptions used commonly in acquirer testing and certification forms.

2. Terms

Term Used	Description/Comment
Combined Reader	The combined reader has a single slot used to insert both chip and magnetic stripe-only cards. Combined readers can select chip or magnetic stripe technology without the cardholder or merchant taking any action.
Session Management Supported	The process of keeping track of activity across the entire transaction – potentially from the point at which the POS 'wakes up' and knows a purchase is being made until a final receipt is generated. Using sessions has some implications for the way technical fallback transactions are processed.
External PIN Pad	The POS terminal interfaces with a PIN pad that is not integrated. The external PIN pad may provide some, all, or none of the EMV functionality.
PCI Approval Class	As declared in the PCI-PTS Letter of Approval. The PCI Approval Class is used to ensure that payment security device approvals accurately describe today's ever-evolving designs.
Tag 9F35 (Terminal Type)	Indicates the environment of the terminal, its communications capability, and operational control (e.g., 21 - merchant attended online only, 22 - merchant attended offline with online capability)
Tag 9F33 (Terminal Capabilities)	Indicates the card data input, Cardholder Verification Method (CVM), and security capabilities of the terminal. If quick service/express-type transactions (no CVM required) are supported, the type-approved configuration must be listed.
Tag 9F1A (Terminal Country Code - ISO 3166)	Identifies the country of the terminal, represented in accordance with ISO standards. Country code for the U.S. is 840
Tag 5F2A (Transaction Currency Code)	Identifies the currency of the transaction, represented in accordance with ISO standards. Currency code for U.S. dollars is 840
CDA Mode (This may be set hardcoded in the software.)	Identifies the type of offline Card Authentication Method (CAM), specifically for Combined Dynamic Data Authentication, that the terminal supports. Value is 1, 2, 3 or 4. Terminals operating in Mode 1 have the most secure configuration.

Term Used	Description/Comment
PIN Management Transaction Supported	Support for functions such as changing PINs.
Cumulative Transaction Checking	Cumulative transaction checking (amount) is performed through card risk management. The card compares the accumulation of transactions performed offline, including the current transaction, to determine if the transaction should go online for authorization.
Fixed Amounts (i.e., $5, $10, $25)	Fixed amounts indicate a terminal can only perform transactions for certain set amounts, such as at an ATM.
Contactless Interface Maximum Keyed-In Amount Value	Maximum of 12 digits with no comma, or dots. Last two digits are considered as decimals.
Floor Limit Value (9F1B)	Indicates the floor limit in the terminal in conjunction with the AID. The same value is used for contactless and contact transactions.
CDA	Combined Dynamic Data Authentication. A card authentication technique used in online and offline chip transactions that combines dynamic data authentication (DDA) functionality with the application cryptogram used by the issuer to authenticate the card. CDA is mandatory for offline-capable contactless terminals.
Terminal Risk Management Data (Tag 9F1D - Hex 8 Bytes)	Application-specific value used by the contactless card or payment device for risk management purposes.
Integrated Data Storage Supported	Enables the reading and writing of data to be integrated with the commands associated with a normal payment transaction. It might be used with functions such as loyalty or ticketing which are linked to the completion of the transaction.
Consumer Device Cardholder Verification Supported	A mobile payment device may also support Consumer Device Cardholder Verification Method (CDCVM) where a PIN or biometric is validated by the device before a transaction is completed.
Transaction Limit (CDCVM) Value	Maximum of 12 digits with no comma, or dots. Last two digits are considered as decimals.
Mobile Confirmation Code Supported	Terminal allows confirmation code as CVM and the application is embedded in a mobile phone.
Receipt Printing Requests	Some contactless devices are capable of printing receipts. By selecting 'Yes,' it will include receipt requirements for tests that have the option. If the device does not support receipts, then select 'No.'

3. Legal Notice

While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any legal purpose, whether statutory, regulatory, contractual or otherwise. All warranties of any kind are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

Without limiting the foregoing, it is important to note that the information provided in this document is limited to the payment networks specifically identified, and that applicable rules, processing, liability and/or results may be impacted by specific facts or circumstances.

Additionally, each payment network determines its own rules, requirements, policies and procedures, all of which are subject to change.

Merchants, issuers, acquirers, processors and others implementing EMV chip technology in the U.S. are therefore strongly encouraged to consult with all applicable stakeholders regarding applicable rules, requirements, policies and procedures for transaction receipts, including but not limited to their respective payment networks, testing and certification entities, and state and local requirements.