EMV Migration Forum: Communications & Education Working Committee Standardization of Terminology

Version 2.1

Date: January 2014

About the EMV Migration Forum

The EMV Migration Forum is a cross-industry body focused on supporting the coordination of EMV implementation across global and regional payment networks, issuers, processors, merchants, and consumers to help ensure a successful introduction of more secure EMV contact and contactless technology in the United States. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV technology in the United States. For more information on the EMV Migration Forum, please visit http://www.smartcardalliance.org/pages/activities-emv-migration-forum.

Purpose of this Document

The goal of this document is to define a set of standard terminology to enable clear recognition and understanding of information for industry stakeholders and consumers. The document includes recommendations for common EMV and EMV migration terms that would be used in stakeholder communications. While all U.S. market stakeholder groups were considered in the development of this list of terms, technical terms have been limited to those that would be used in educational and marketing communications.

The document includes four columns: Industry Recommended Term (and acronym if indicated), Also Known As (AKA) terms, Industry Stakeholder Definition and Cardholder/Customer Definition.

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Acquirer	• Merchant acquirer Third-Party Examples: • Bank of America Merchant Services (BAMS) • First Data • SHAZAM/ITS, Inc. • Vantiv (formerly Fifth Third Processing Solutions) • Wells Fargo • The Bancorp Bank	The party recognized by the network as the financial sponsor for a merchant (typically a regulated financial institution like a bank). The network holds the acquirer responsible financially for transactions processed by the merchant and that the merchant operates under the rules laid out by the network.	Not required
Acquiring Processor	Examples: • Chase Paymentech • Elavon (US Bank) • First Data • Global Payment Systems • Heartland Payment Systems • TSYS Acquiring Solutions • Vantiv • WorldPay	Third-party service provider that acquires and processes payment transactions for merchants, manages the relationship with the global and regional payment networks on the merchant's behalf (including interchange qualifying, chargeback disputes and fees to networks and issuers), and manages the transaction database. The acquirer connects merchant transactions to payment networks by (1) providing the point-of-sale (POS)/ATM terminal; and/or (2) securely routing transactions from the POS/ATM terminal or from the POS/ATM payment gateway to the payment network; and/or (3) managing transactions from authorization to clearing to settlement.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Application Authentication Cryptogram (AAC)		A cryptogram generated by the card at the end of offline and online declined contact transactions. It can be used to validate the risk management activities for a given transaction.	Not required
Application Cryptogram (AC)	• AAC • ARQC • TC • Cryptogram	A cryptogram generated by the card in response to a GENERATE AC command, providing the card decision on the transaction. The AC is used to validate that the card has genuinely generated the response. The three types of cryptograms are Transaction Certificate (TC), Authorization Request Cryptogram (ARQC), and Application Authentication Cryptogram (AAC). The creation and validation of the cryptogram enables dynamic authentication.	Not required
Application Identifier (AID)		An alpha numeric representation of the application defined within ISO 7816. A data label that differentiates payment systems and products. The card issuer uses the data label to identify an application on the card or terminal. Cards and terminals use AIDs to determine which applications are mutually supported, as both the card and the terminal must support the same AID to initiate a transaction. Both cards and terminals may support multiple AIDs. An	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
		AID consists of two components, a registered application identifier (RID) and a propriety application identifier extension (PIX).	
Application Transaction Counter (ATC)		A counter, maintained by the chip card application (incremented by the chip), that provides a sequential reference to each transaction. Each payment application has its own ATC.	Not required
Authorization Response Cryptogram (ARPC)		A cryptogram generated by the issuer and sent in the authorization response back to the terminal. The terminal provides this cryptogram back to the card which allows the card to verify the validity of the issuer response.	Not required
Authorization Request Cryptogram (ARQC)		A cryptogram generated by the card at the end of the first round of card action analysis, which is included in the authorization request sent to the card issuer and which allows the issuer to verify the validity of the card and message.	Not required
Card Manufacturer	Examples: • ABnote • CPI Card Group • Gemalto • Giesecke & Devrient • Oberthur Technologies • Perfect Plastic Printing	Entity that converts raw materials into payment chip cards on behalf of the issuer; includes application loading, quality testing, and distribution to a personalization bureau.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Card Reader	• Chip card reader • Dip reader • Manual reader • Motorized reader	The part of a chip payment terminal where the chip card is inserted or tapped to initiate a chip transaction. There are three types of card readers; motorized contact and manual contact and contactless. A motorized reader has a mechanism that transports the card into, and ejects the card from, the reader. A manual reader requires the card to be manually inserted into, and removed from, the reader. A contactless reader requires the cardholder tap the card near the device.	
Card Risk Management	• Offline risk parameters • Authorization controls	Issuer defined risk parameters and authorization controls programmed into the chip application enabling the card to act on the issuer's behalf at the point of transaction to determine if the transaction should be sent online, approved offline or declined offline. These controls aid issuers in managing their below-floor limit exposure to fraud and credit losses. They may be tailored to the risk level of individual cardholders or groups of cardholders.	Not required
Card Security Code (CSC)	Examples: • CSC—Card Security Code (American Express) • CID—Card Identification	3 or 5 digit numeric codes either written on the payment card magnetic stripe or printed on the card that are used by the financial payment brands for credit, debit, and prepaid	Codes used by MasterCard, Visa, and other payment networks to protect against fraudulent transactions on credit, debit, and prepaid cards.

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
	Data (Discover) • CVC or CVC 2—Card Validation Code (MasterCard) • CVV or CVV2—Card Verification Value (Visa)	transactions to protect against card fraud for swipe or online transactions.	
Card Sequence Number	• PAN sequence number	A value encoded on the chip and provided to the issuer in authorization and clearing messages that uniquely identifies each card when two or more cards are associated with a single account.	Not required
Card Verification Results (CVR)		The chip card internal registers that store information concerning the chip card functions performed during a payment transaction. The major chip card functions reflected in these registers are the personal identification number (PIN) verification, the card risk management checks, and the status of the previous transaction. The CVR is signed in the application cryptogram (AC) created at the end of a payment transaction.	Not required
Cardholder	• Customer • Client • Card member • Subscriber	End product user. One who possesses a payment card.	Customer to whom the card is issued.

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Cardholder Verification Method (CVM)		In the context of a transaction, the method used to authenticate that the person presenting the card is the valid cardholder. EMV supports four CVMs: offline personal identification number (PIN) (offline enciphered & plain text), online encrypted PIN, signature verification, and no CVM. The issuer decides which CVM methods are supported by the card and the merchant chooses which CVMs are supported by the terminal. The issuer sets a prioritized list of methods on the chip for verification of the cardholder.	Not required
Certificate	• Digital certificate	An electronic document binding some pieces of information together, such as a user's identity and public encryption key. The digital certificate is used to prove to the data recipient the origin and integrity of the data.	Not required
Certificate Authority (CA)		A trusted central administration that issues and revokes certificates and is willing to act as a guarantor for the identities of those to whom it issues certificates and their association with a given key.	Not required
Certificate Authority Public Key (CAPK)		In order to support data authentication or offline enciphered personal identification number (PIN), the terminal must store one or more public keys for each	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
		supported Registered Application. When required, the card will supply a CAPK index that is used to identify which of these keys should be used for that transaction.	
Chip Capable Terminal	• Chip card reader • EMV device • Manual reader • Motorized reader • Dip reader	A payment terminal that has a chip card reader and is able to accept an EMV application. While the terminal is capable, the EMV functionality may or may not be enabled.	
Chip Card	• EMV chip card • Smart card • ICC—Integrated Circuit Card • Contact chip card • Contactless chip card	A device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory, or a secure memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, chip cards have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication), and interact intelligently with a card reader. All EMV cards are chip cards.	A plastic card with a chip in it that communicates information to a payment or ATM terminal. Chip cards offer increased security. All EMV cards are chip cards.
Chip Card Security Code	Examples: • iCVV—Visa • Chip CVC—MasterCard • iCSC—American Express	The chip equivalent data for the CSC written on the track used to prevent fraud. All chip cards are issued with the card security code on the track data stored on the magnetic stripe and chip card	

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
		security code stored on the chip, and are calculated with the same Data Encryption Standard (DES) key but with a '999' service code.	
Chip Compatible Terminal	• Device	A terminal that does not have a chip card reader but can be connected to a peripheral reader and can accept an EMV application in the device.	
Chip Enabled Terminal	• Chip card reader • EMV device	A terminal that has, or is connected to, a chip card reader, an EMV application, and is able to process EMV transactions.	
Chip Manufacturer		Entity that designs, manufactures, and supplies EMV compliant integrated circuits to card manufacturers to be used in the production of chip cards.	
CDA	• Combined DDA/Application (CDA) Cryptogram generation	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.	Not required
Common Core Definition (CCD)		A definition of the minimal card application implementation options, card application behaviors, and data element definitions sufficient to accomplish an EMV transaction.	

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Contact Chip Card		A chip card that communicates with an EMV capable terminal into which the card is inserted. Communication is defined by ISO 7816.	A chip card that communicates with an EMV capable terminal into which the card is inserted.
Contactless Chip Card	• Contactless card • Proximity card • NFC card	A chip card that communicates with a reader through a radio frequency interface. Communication is defined by ISO 14443.	A chip card that communicates with a reader through a radio frequency interface, usually through a wave or tap of the card on the designated area on the terminal.
Contactless Payments	• Contactless • Contactless transaction	Payment transactions that require no physical contact between the consumer payment device and the physical terminal. In a contactless payment transaction, the consumer holds the contactless card, device, or mobile phone in close proximity (less than 2-4 inches) to the terminal and the payment account information is communicated wirelessly (via radio frequency [RF]).	In a contactless payment transaction, the consumer holds the contactless card, device, or mobile phone in close proximity (less than 2-4 inches) to the terminal and the payment account information is communicated wirelessly (via radio frequency [RF]).
Cryptogram	Examples: ARQC ARPC TC AAC	An alphanumeric value that is the result of data elements entered into an algorithm and then encrypted, commonly used to validate data integrity. The creation and validation of the cryptogram enables dynamic authentication.	Not required
CVM Fallback		The term used for the scenario when the preferred cardholder verification method (CVM) for a	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
		transaction is bypassed by the cardholder or merchant and the transaction is completed with another CVM.	
CVM List		The list of cardholder verification methods supported on the card, their relative priority, their permitted use and CVM fallback behaviors.	
Data Preparation		The activities involved in preparing the chip specific tags and cryptographic keys needed to personalize a chip card.	Not required
Debit Payment Network	• Regional network • Debit network • Domestic network	A debit payment network provides POS and ATM services principally for debit, ATM and prepaid card issuers and corresponding transaction acquirers. It establishes participation requirements, operating rules and technical specifications under a common brand(s) for the purpose of receiving, routing, securing authorization for, settling and reporting domestic payment transactions. Each debit payment network determines the types of transactions, payment devices and terminals that are permitted in its respective network.	
Dual Interface Chip Card	• Dual interface card • Dual chip card • Contactless card	A chip card that has both contact and contactless interfaces, enabling a payment transaction with either interface.	A chip card that can be either tapped or inserted into the terminal to make a payment.

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Dual Interface Terminal	• Chip terminal	A terminal that has both contact and contactless functionality, enabling a payment transaction with either interface.	A terminal that can process both contact and contactless transactions.
Dynamic Authentication Data		Information that is used during a transaction to generate the cryptogram used to verify the card participating in the trans-action and that changes from transaction to transaction.	Not required
Dynamic Card Security Code	Examples: • DCID • dCVC • dCVC3 • DCVV	A security code which changes for each transaction, replacing the static magnetic stripe-based card security code for a contactless transaction.	Not required
DDA	Dynamic Data Authentication	A card authentication technique used in offline chip transactions that requires the card to digitally sign unique data sent to it from the terminal. DDA protects against card skimming and counterfeiting.	Not required
EEPROM	• Electronically Erasable Programmable Read-Only Memory • E^2	Memory that can be erased and reused, but does not require electrical power to maintain data. It is used to store information that will change, such as transaction counters or cardholder unique data like the account number. It is possible to load new data elements and applications into EEPROM after a card has been issued.	Not required
EMF	• EMV Migration Forum	The EMV Migration Forum is an independent, cross-industry body created by the Smart Card Alliance to	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
		address issues that require broad cooperation and coordination across many constituents in the payments space to promote the efficient, timely, and effective migration to EMV-enabled cards, devices, and terminals in the United States.	
EMV®	• Note: EMV stands for Europay, MasterCard, Visa	Specifications developed by Europay, MasterCard, and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.	
EMV Application	• App <u>Major Brand EMV Applications:</u> • American Express—AEIPS • Discover—D-PAS • MasterCard—M/Chip • Visa—VSDC	A computer program and associated data that reside on an integrated circuit chip and payment terminal and satisfy a business or risk management function; i.e., a set of defined parameters, for transaction processing. A payment system application is comprised of the following: 1. A set of files in the ICC providing data customized by the issuer 2. Data in the terminal provided by the acquirer or the merchant 3. An application protocol agreed upon by both the ICC and the terminal	Programs on a card chip that allow the card to be used for payment, to store value, and to receive loyalty rewards.
EMV Compliant		Cards and terminals that meet security, interoperability, and functionality requirements outlined by EMVCo.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
EMV Liability Shift Date		The date on which a party that has made investment in EMV deployment is protected from financial liability for card-present fraud losses. If neither or both parties are EMV compliant, the fraud liability remains the same as it is today.	Not required
EMV Terminal	• Chip terminal • EMV ATM terminal • EMV POS terminal • Chip/EMV card reader • Chip reader • EMV compliant terminal • EMV device • EMV payment terminal	Point-of-sale (POS) device or ATM that is able to process chip transactions.	Point-of-sale (POS) device or ATM that is able to process chip transactions.
EMVCo		The organization formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications for Payment Systems. EMVCo is currently owned by American Express, Discover Financial Services, JCB, MasterCard Worldwide, UnionPay, and Visa, Inc.	Not required
Enciphered PIN		Personal identification number (PIN) processing in which the PIN entered by the cardholder is encrypted using public key cryptography at the PIN pad and then sent to the chip card where it is decrypted inside the chip and verified.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
GlobalPlatform		A cross-industry membership organization created to advance standards for multiple application smart card growth. A major goal of GlobalPlatform is the definition of specifications and infrastructure for multi-application smart cards, including cards, terminals, and back-end host systems. The GlobalPlatform Specifications are based on the Open Platform Specifications, which were donated to the consortium by Visa.	Not required
Hardware Security Module	• HSM	A hardware device used to securely generate and store encryption keys and perform cryptographic processes.	Not required
Host		Centralized computer systems for aggregating and processing transactions. The host would typically be operated by the acquiring processor but may be operated by the merchant. Payment terminals connect to and are "hosted by" these systems. The issuing processor's back-end transaction-processing systems are sometimes included in the definition of "host."	Not required
Hybrid Card		A card that utilizes more than one technology, such as chip combined with physical access or other customizable features.	

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Hybrid Terminal		A terminal that utilizes more than one technology, such as chip and loyalty based payment or features specific to customized programs such as electronic benefits or healthcare.	
Independent Sales Organizations (ISOs)	• Merchant service providers • MSPs	Third-party organizations that partner with acquiring banks to find, open, and manage merchant accounts on behalf of such businesses in exchange for a higher fee, or for a percentage of the merchant's sales.	Not required
Industry Organization	Examples: • ATMIA • EMV Migration Forum • ETA • MAG • NRF • Smart Card Alliance • SRPC	An association of organizations or entity which facilitates industry-wide communication around the U.S. EMV migration including: • Stakeholder communication • Government advocacy • Industry conferences and networking	Not required
International Standards Organization (ISO)		A global institution that maintains more than 13,000 international standards for business, government, and society.	Not required
Issuer	• Card issuer	Entity that issues payment data devices (cards) to customers and performs many activities that could include, but are not limited to: • Performs the task of authorizing or declining transactions • Cardholder customer service	The financial institution that issues payment cards and holds the account or credit line behind the card.

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
		• Data preparation • Configuration set-up • Fulfillment of personalized chip card, with all paper inserts; preparation for mailing to customer • Define card profile, including risk parameters • Receive and manage card records and keys to form a personalization record • Generate personalization script • Key management activities for EMV, card verification values (CVVs)/card validation codes (CVCs), and personal identification numbers (PINs) between card manufacturer and personalization bureau and between issuer and personalization bureau.	
Issuer Action Codes (IACs)	• Parameters	Codes placed on the card by the issuer during card personalization. These codes indicate the issuer's rules for approving transactions offline, declining transactions offline, and sending transactions online to the issuer based on the risk management performed.	Not required
Issuer Script	• Dynamic data update • Post issuance update	A process by which an issuer can update securely the contents digitally stored on chip cards without reissuing the cards. Examples of issuer scripts include blocking and unblocking an account, blocking the entire card,	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
		changing and unblocking the cardholder's personal identification number (PIN), and changing the cardholder's offline authorization controls (ACs).	
Issuing Processor	Examples: • Elan • First Data • FIS • Fiserv • SHAZAM/ITS, Inc. • TSYS • Vantiv • Self-processing issuers	An entity that facilitates card issuance activities on behalf of an issuer such as processing payment transactions, card enrollment, preparing and sending the card personalization information to the card vendor, and maintaining the cardholder database. The issuer processor may provide only card issuing activities or may provide other ancillary services as well (e.g., web front-end administrative and cardholder account management applications, customer service, settlement and clearing, chargeback processing).	Not required
ISO 7816		The ISO standard for contact chip cards. The EMVCo standards are built on ISO 7816.	Not required
ISO 14443		The ISO standard for communicating with contactless devices. ISO 14443 recognizes Type A (NXP MIFARE) and Type B (Motorola) standards. Type C (Sony) is also widely used in Asia Pacific, but has not yet been formally adopted by ISO.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
ISO 18092		An ISO standard for contactless devices. This standard allows bi-directional communication between the data source and the point-of-sale (POS). Although this can be used on cards, the primary advantage is expected to be on mobile devices that are sending contactless chip data. This allows for non-payment type messages, such as coupons, loyalty offers, to be delivered to the consumer's phone.	Not required
Kernel		The set of functions required to be present on every terminal (or card reader) implementing a specific interpreter. The kernel contains device drivers, interface routines, security and control functions, and the software for translating from the virtual machine language to the language used by the real machine. In other words, the kernel is the implementation of the virtual machine on a specific real machine.	Not required
Magnetic Stripe Card	• Mag stripe card	A plastic card that uses a band of magnetic material to store data. Data is read by a mag stripe reader.	A payment card that does not have a chip and uses the magnetic stripe on the back only.
Merchant	• Retailers	Entity that accepts payments from customers in exchange for goods and/or services and connects to a payment network through an acquirer.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Multi-application Card	• Combo card • Combi card	The presence of multiple applications on a single chip card, such as payment, loyalty and identification.	Not required
Multi-function Card		A card that has more than one function, though not necessarily more than one application, such as photo identification and logical access (similar to a corporate ID badge that is used to get through doors/turnstiles).	
NFC	• Near Field Communication • ISO 18092	A standards-based wireless communication technology that allows data to be exchanged two-ways between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate smart chips (called secure elements) that allow the phones to securely store the payment application and consumer account information and to use the information as a "virtual payment card." NFC is an extension of RFID.	Near Field Communication (NFC) is a set of standards for smartphones and similar devices used to establish communication with each other by touching them together or bringing them close.
Offline Authorization	• Offline approval	Authorizing or declining a payment transaction through card-to-terminal communication, using issuer-defined risk parameters that are set in the card to determine whether the transaction can be authorized without going online to the issuer host system.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Offline Card Authentication Method (CAM)	• Online card authentication • Card authentication • Offline data authentication (ODA)	A typically asymmetric cryptographic process in which a payment terminal is able to validate the authenticity of a payment card, without communication to the issuer of the payment card. The three methods used are SDA, DDA and CDA.	Not required
Offline Data Authentication	• ODA	A process whereby the card is validated at the point of transaction, using RSA public key technology to protect against counterfeit or skimming. Three forms of offline data authentication are defined by EMV: Static (SDA), Dynamic (DDA) and Combined DDA/Application Cryptogram (CDA).	Not required
Offline Only Terminal		A chip terminal that is not capable of sending an online authorization request and where all transactions have to be approved or declined offline.	Not required
Offline Preferring Terminal		A chip terminal that typically processes low value transactions offline and may defer or decline transactions that require online authorization.	Not required
Offline PIN		The personal identification number (PIN) stored on the chip card (versus a PIN stored at the host). In a chip transaction using offline PIN, the PIN entered at the terminal is compared with the PIN stored securely on the chip card without going online to the issuer host for	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
		the comparison. Only the result of the comparison is passed to the issuer host system. Two types of offline PIN are enciphered and plaintext.	
Online Authorization		Authorizing or declining a payment transaction by sending transaction information to the issuer and requesting an authorization response from the issuer usually in real time.	Not required
Online CAM	• Dynamic authentication • Online authentication	A typically symmetric cryptographic process in which an issuer host is able to validate the authenticity of a payment card, and a payment card is optionally able to validate the issuer host. The cryptographic process follows a variety of cryptograms defined by EMV or the payment brand.	
Online Capable Terminal		A chip terminal that supports both offline and online processing.	Not required
Online Card Authentication		Validation of a chip card by the issuer during online authorization to protect against data manipulation and skimming. See also Authorization Request Cryptogram (ARQC).	Not required
Online EMV	• Online only EMV • Streamlined EMV	A streamlined imple-mentation of EMV that uses online card authentication and online transaction authorization together and requires 100 percent online authentication/authoriza-	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
		tion. Online EMV may be appropriate for countries with a fast, reliable telecommunications infrastructure, such as the U.S.	
Online Issuer Authentication	• Issuer authentication • Host authentication	Validation of the issuer by the card to ensure the integrity of the issuer. See also ARPC (Authorization Response Cryptogram).	Not required
Online Only Terminal		A chip terminal that only supports online processing of transactions.	Not required
Online PIN	• Online enciphered PIN	In a chip transaction, the process of comparing the cardholder's entered personal identification number (PIN) with the PIN stored on the issuer host system. The PIN is encrypted by the terminal PIN pad before being passed to the acquirer system. The PIN is then decrypted and re-encrypted as it passes between each party on its way to the issuer. This is supported today with mag-stripe.	Not required
Payment Card Industry Data Security Standard (PCI DSS)		A framework developed by the PCI Security Standards Council (SSC) for developing a robust payment card data security process – including prevention, detection, and appropriate reaction to security incidents.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Payment Network	• Global brand Examples: • American Express • Discover • MasterCard • Visa	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 under a common brand(s) 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.	Card brand
PIN	• Personal Identification Number • Offline PIN • Online PIN • Secret code	A numeric code of 4 to 12 digits that is used to identify cardholders at a customer-activated PIN pad. PINs can be verified online by the issuer or sent to the chip card for offline PIN verification. See also offline PIN.	A secret code or number that an individual memorizes and uses to authenticate his or her identity for card use.
Personalization	Data preparation	Process by which the elements specific to the issuer and cardholder are added to the plastic card, magnetic stripe and/or chip.	Not required
Personalization Bureau	Examples: • CPI Card Group • EFT Source • First Data • FIS • Fiserv • Giesecke & Devrient	An entity that provides some of the following personalization services to issuers: • Data preparation (can also be done by issuing bank) • Configuration set-up • Fulfillment of personalized chip card, with all paper	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
	• Oberthur Technologies • Shoreline • TSYS • Self-processing issuers • In-house issuers	inserts; preparation for mailing to customer • Define card profile, including risk parameters (with issuing bank's approval) • Receive and manage card records and keys to form a personalization record • Generate personalization script • Perform key management activities for EMV, CVV/CVC, and PINs between card manufacturer and personalization bureau and between issuer and personalization bureau	
Personalization Validation	• Card Personalization Validation (CPV) • Personalization Validation Tool (PVT)	A process used to validate that a card has been personalized correctly based on a particular card brand's personalization specification.	Not required
PIN Management		The process of using issuer scripts to securely update personal identification number (PIN) data stored on the card. PIN management includes PIN change and PIN unblock.	
Plaintext PIN	• Offline plaintext PIN	Offline personal identification number (PIN) processing in which the PIN entered by the cardholder is sent unencrypted, in plaintext, from the PIN pad to the chip card for verification.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Point-of-Sale (POS)/ATM Terminal Manufacturers/ Suppliers	Examples: • Diebold • Ingenico • NCR • VeriFone	An entity that manufactures and supplies point-of-sale (POS)/ATM terminals to POS/ATM terminal operators/owners.	Not required
Point-of-Sale (POS)/ATM Terminal Operators/ Owners	Examples: • Acquirer • IAD (Independent ATM Deployer) • ISO (Independent Sales Organization) • Merchant • VARs (Value Added Resellers)	An entity that drives or operates some or all parts of payments through terminals or ATMs.	Not required
Private Key		The secret component of an asymmetric key pair. The private key is always kept secret by its owner. It may be used to digitally sign messages for authentication purposes and it may be used to decrypt messages encrypted with the matching public key.	Not required
PIX	• Proprietary Application Identifier Extension	The last digits of the application ID that enables the application provider to differentiate between the different products they offer.	Not required
Public Key		The public component of an asymmetric key pair. The public key is usually publicly exposed and available to users. A certificate to prove its origin often accompanies it. It may be used to validate a message signed by the matching private key, and it can be used to encrypt messages to be sent to the private key holder.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Public Key Certificate (PKC)	• IPKC (Issuer PKC) • ICC public key certificate	A digitally signed document that serves to validate the sender's authorization and name. The document consists of a specially formatted block of data that contains the name of the certificate holder (which may be either a user or a system name) and the holder's public key, as well as the digital signature of a certification authority for authentication. The certification authority attests that the sender's name is the one associated with the public key in the document.	
Public Key Cryptography		An encryption method that is used to verify an identity or to encrypt data or messages. It consists of two keys, one public and one private. The public key is in the public domain and available to all users and the private key is kept secret. Public key cryptography may also be used to verify digital signatures to authenticate the message sender.	Not required
Public Key Infrastructure (PKI)		The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.	Not required
ROM	• Read Only Memory	Permanent memory that cannot be changed once it is programmed. It is used to store chip operating systems and permanent data.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
RID	• Registered Application Provider Identifier	The first part of the application ID, used to identify a payment system (card scheme) or network, e.g., MasterCard, Visa, or Interac.	Not required
RSA	• Rivest, Shamir, and Adelman	A widely used public key algorithm, developed by Rivest, Shamir and Adelman. The RSA algorithm is used, for example, in offline data authentication.	Not required
SAM	• Secure application module • Secure access module	A logical device used to provide security for insecure environments. It is protected against tampering and stores secret and/or critical information. SAMs are often inserted into point-of-sale terminals to store keys, especially for chip card applications.	Not required
Standards Body	Examples: • EMVCo • GlobalPlatform • ISO	An entity that ensures physical and logical global interoperability of contact and contactless capable devices and systems: e.g., cards, mobile devices, point-of-sale (POS) systems, ATMs, acquiring networks, issuer host systems. • ISO – ISO/IEC 7816 - primary standard for smart cards, ISO/IEC 14443 for contactless smart cards. • EMVCo – payment specifications (security, messaging, interoperability). • GlobalPlatform – messaging specifications, key management.	Entity which creates standards for all companies to work well together

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
SDA	• Static Data Authentication	A card authentication technique used in offline chip transactions that uses signed static data elements. With SDA, the data used for authentication is static—the same data is used at the start of every transaction. This prevents modification of data, but does not prevent the data in an offline transaction from being replicated.	Not required
Symmetric Key Technology		In a symmetric cryptographic system, the same secret key is used to perform both the cryptographic operation and its inverse (for example to encrypt and decrypt, or to create a message authentication code and to verify the code). The secret key is shared between the sender and the receiver or the card and the issuer.	Not required
Tag	• EMV tag • TLV	Values involved in an EMV transaction (which result from the issuer's implementation choices) are transported and identified by a tag which defines the meaning of the value, the format, and the length. The "tag" is simply a number that identifies the meaning of each piece of data transmitted between the ICC and the terminal.	Not required
TLV	• Tag, Length, Value • BER-TLV (Basic Encoding Rules – TLV)	Represents the format and order of information in an EMV data field (EMV tag).	

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Technical Fallback	• Fallback transaction	The term used for the scenario when a transaction is initiated between a chip card and a chip terminal but chip technology is not used and the transaction is completed via magnetic stripe or key entry.	Not required
TACs	• Terminal action codes	Codes placed in the terminal software by the acquirer. These codes indicate the acquirer's instructions for approving transactions offline, declining transactions offline, and sending transactions online to the issuer based on risk management performed.	Not required
Terminal Verification Results (TVR)		The result of the risk management checks performed by the terminal during the transaction.	Not required
TC	• Transaction certificate	A cryptogram generated by the card at the end of all offline and online approved transactions. The cryptogram is the result of card, terminal, and transaction data encrypted by a Data Encryption Standard (DES) key. The TC provides information about the actual steps and processes executed by the card, terminal, and merchant during a given transaction and can be used during dispute processing.	Not required

Industry Recommended Term	Also Known As (AKA)	Industry Stakeholder Definition	Cardholder/Customer Definition
Triple DES	• Data Encryption Standard • TDES • 3DES	A sophisticated implementation of Data Encryption Standard (DES), in which the procedure for encryption is the same but repeated three times. First, the DES key is broken into three sub keys. Then the data is encrypted with the first key, decrypted with the second key and encrypted again with the third key. Triple DES offers much stronger encryption than DES.	Not Required

This document will be updated periodically based on EMV Migration Forum member and industry feedback and experience. The most up-to-date version will be located on the EMV Connection website at http://www.emv-connection.com. Recommendations for edits or additions to this document should be submitted to terminology-feedback@us-emvforum.org.