EMV: A to Z (Terms and Definitions)

First Data participates in many industry forums, including the EMV Migration Forum (EMF). The EMF is a cross-industry body focused on supporting an alignment of the EMV implementation steps required for global and regional payment networks, issuers, processors, merchants, and consumers. The goal of the EMV is to ensure a successful move from magnetic stripe technology to more secure EMV contact and contactless technology in the United States.

As part of the EMV Migration Forum, this common set of EMV-related terms and definitions were developed to enable clear recognition and understanding of information for industry stakeholders and consumers. For more information on the EMV Migration Forum, please visit smartcardalliance.org/pages/activities-emv-migration-forum

TERM	DEFINITION
Acquirer	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 POS device; and/or (2) securely routing transaction from POS device or from POS payment gateway to payment network; (3) managing transactions from authorization to clearing to settlement.
Acquiring Processor	Entities that process transactions on behalf of acquirers by connecting merchant transactions to payment networks.
Application	A computer program and associated data that reside on an integrated circuit chip and satisfy a business or risk management function; i.e., a set of defined parameters, for transaction processing. Examples of applications include payment, terminal behavior, CVM preferences, security keys, rules, risk policies, stored value, and loyalty. Programs on card chip that allow card to be used for payment, to store value and to get loyalty rewards.
Application Authentication Cryptogram (AAC)	A cryptogram generated by the card at the end of offline and online declined transactions. It can be used to validate the risk management activities for a given transaction.
Application Cryptogram	A cryptogram generated by the card in response to a GENERATE AC command.
Application Identifier (AID)	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 AID consists of two components, an RID (alpha and numeric) and a PIX (numeric only).
Application Transaction Counter (ATC)	A counter, maintained by the chip card application (incremented by the chip), that provides a sequential reference to each transaction. A duplicate ATC, a decrease in ATC or a large jump in ATC values may indicate data copying or other fraud to the issuer.
Authorization Controls **Also known as:** **• offline risk parameters**	Information programmed into the chip application enabling the card to act on the issuer's behalf at the point of transaction. 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.
Authorization Response Cryptogram (ARPC)	A cryptogram used for a process called Online Issuer Authentication. This cryptogram is the result of the Authorization Request Cryptogram (ARQC) and the issuer's authorization response encrypted by a DES key. It is sent to the card in the authorization response. The card validates the ARPC to ensure that it is communicating with the valid issuer.

TERM	DEFINITION
Authorization Request Cryptogram (ARQC)	A cryptogram used for a process called Online Card Authentication. This cryptogram is generated by the card for transactions requiring online authorization. It is the result of card, terminal, and transaction data encrypted by a DES key. It is sent to the issuer in the authorization or full financial request. The issuer validates the ARQC to ensure that the card is authentic and card data was not copied from a skimmed card.
Card Authentication Method (CAM) **Also known as:** **• Online Card Authentication** **• Card Authentication**	In the context of a payment transaction, the method used by the terminal and/or issuer host system to determine that the payment card being used is not counterfeit.
Card Manufacturer	Entity which converts raw materials into payment chip cards on behalf of the Issuer; includes application loading, quality testing, and distribution to a personalization bureau.
Card Security Code	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 transactions to protect against card fraud. Codes used by MasterCard, Visa and other payment networks to protect against fraudulent transactions on credit, debit and prepaid cards. Examples: • CSC – Card Security Code (American Express) • CID - Card Identification Data (Discover) • CVC or CVC2 - Card Verification Code (MasterCard) • CVV or CVV2– Card Verification Value (Visa)
Card 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.
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 PIN verification, the card risk management checks and the status of the previous transaction.
Cardholder **Also known as:** **• Customer** **• Client** **• Card member**	End product user. One who possesses a payment card. Customer to whom the card is issued.
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 PIN (offline enciphered & plain text), online PIN, signature verification and no CVM. All CVMs can be available on all payment types (credit, debit and prepaid) as defined by the issuer. The merchant chooses which CVMs they will support. The issuer sets a prioritized list of methods on the chip for verification of the cardholder.
Certificate **Also known as:** **• Digital Certificate**	An electronic document binding some pieces of information together, such as a user's identity and public key. The digital certificate is used to prove to the data recipient the origin and integrity of the data.
Certificate Authority (CA)	A trusted central administration that issues and revokes certificates and is willing to vouch for the identities of those to whom it issues certificates and their association with a given key.
Certificate Authority Public Key (CAPK)	In order to support data authentication or offline enciphered PIN, the terminal must store one or more public keys for each RID. When required, the card will supply a CAPK index which is used to identify which of these keys should be used for that transaction.
Chip Card **Also known as:** **• EMV Chip Card** **• Smart Card** **• ICC – Integrated Circuit Card** **• Contact 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	Codes written on the track with equivalent data stored on the chip 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 security code stored on the chip. Calculated with the same DES key but with a '999' service code. Examples: • iCVV - Visa • Chip CVC - MasterCard • iCSC – American Express

TERM	DEFINITION
Combined DDA/Application (CDA) Cryptogram Generation	An authentication technique used in offline chip transactions that combines DDA functionality with the application cryptogram used by the issuer to authenticate the card. The application cryptogram is used to assure that the data in the transaction maintain integrity even after the transaction is completed.
Contact Chip Card	A chip card that communicates with a reader through a contact plate. The plate must come into contact with a terminal, usually through a dip reader into which the card is inserted. A chip card that communicates with a reader through a contact plate. The plate must come into contact with a terminal, usually through a dip reader into which the card is inserted.
Contactless Chip Card **Also known as:** **• Contactless card** **• Proximity card** **• NFC card**	A chip card that communicates with a reader through a radio frequency interface. 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 Magnetic Stripe Data (MSD)	An approach for implementing contactless payments. With contactless MSD, the message layout for Track 1 and Track 2 magnetic stripe data remains intact, with one notable difference. The chip on the card allows for the calculation of a dynamic card verification value (DCVV) based on a card-unique key and a simple application transaction counter (ATC). The dynamic card verification value is passed in the message in the same field that was used for the original card verification value. The ATC is passed in the area reserved on the track layout for issuer discretionary data.
Contactless Payments **Also known as:** **• Contactless** **• Contactless transaction**	Payment transactions that require no physical contact between the consumer payment device and the physical point- of-sale (POS) 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 merchant POS 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 merchant POS terminal and the payment account information is communicated wirelessly (via radio frequency (RF)).
Cryptogram	An alphanumeric value that is the result of data elements entered into an algorithm and then encrypted commonly used to validate data integrity. Commonly used cryptograms are Authorization Request Cryptogram (ARQC), Authorization Response Cryptogram (ARPC), Transaction Certificate (TC), and Application Authorization Cryptogram (AAC).
Cryptography	The science of protecting information by using mathematics to transform it (encrypt it) into an unreadable format. Cryptography is often used to secure assets like PINs or to authenticate an entity such as an issuer or cardholder. See also Cryptogram.
Dual Interface Chip Card **Also known as:** **• Dual Interface Card** **• Dual Chip 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 payment terminal to make a payment.
Dynamic Authentication Data	Information that is used during a transaction to verify the card or the cardholder participating in the transaction and that changes from transaction to transaction.
Dynamic Data Authentication (DDA)	An authentication technique used in offline chip transactions that calculates a cryptogram for each transaction that is unique to the specific card and transaction. DDA protects against card skimming and counterfeiting.
Dynamic Card Security Code	A security code which changes for each transaction, replacing the static magnetic stripe-based card security code for a contactless transaction. • DCID • DCVC • DCVC3 • DCVV
EEPROM **Also known as:** **• Electronically Erasable Programmable Read-Only Memory** **• E2**	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. Generally, after personalization and issuance few application data could be updated. This is linked to card security requirements.
EMF **Also known as:** **• EMV Migration Forum**	The EMV Migration Forum is an independent, cross-industry body created by the Smart Card Alliance to 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.

TERM	DEFINITION
EMV	Specifications that define a set of requirements to ensure interoperability between payment chip cards and terminals. Formally known as the EMV Integrated Circuit Card Specifications for Payment Systems and owned by EMVCo. A set of standards developed to ensure payment chip cards and terminals operate successfully together. Note: EMV formerly stood for Europay, MasterCard, Visa
EMV Compliant	Cards and terminals that meet security, interoperability, and functionality requirements outlined by EMVCo.
EMV tags	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.
EMV Terminal **Also known as:** **• Chip Terminal** **• EMV ATM Terminal** **• EMV POS Terminal** **• Chip/EMV Card Reader** **• Chip Reader**	Point of sale 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, JCB, MasterCard Worldwide, and Visa, Inc.
Enciphered PIN	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.
Fallback or 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. There are multiple reasons this could occur such as an inoperative or malfunctioning chip/chip reader, improper use or a counterfeit card.
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.
Hardware Security Module (HSM)	A hardware device resident at the association, an acquirer, an issuer, or a vendor used to securely generate and store encryption keys and perform cryptographic processes.
Hybrid Card	A card that utilizes more than one technology, such as chip and magnetic stripe.
Independent Sales Organizations (ISO) Also known as: • Merchant Service Providers • MSP	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.
Industry Organization	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 Examples: • ATMIA • EMV Migration Forum • ETA • MAG • NRF • Smart Card Alliance
International Standards Organization (ISO)	A global institution that maintains over 13,000 international standards for business, government and society.

TERM	DEFINITION
Issuer	Entity that issues payment data devices (cards) to customers and performs many activities that could include, but are not limited to: • Cardholder customer service • 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, CVV/CVC, and PINs between card manufacturer and personalization bureau and between issuer and personalization bureau The financial institution which issued the card to the cardholder and holds the account or credit line behind the card.
Issuer Action Codes (IAC) **Also known as:** **• Parameters**	Codes placed on the card by the issuer during card personalization. These codes indicate the issuer's preferences for approving transactions offline, declining transactions offline, and sending transactions online to the issuer based on the risk management performed.
Issuer Script **Also known as:** **• 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, changing the cardholder's PIN, and changing the cardholder's Authorization Controls.
Issuing Processor	An entity that facilitates card issuance activities on behalf of an issuer such as process 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)
ISO 7816	The ISO standard for chip cards with contacts. The EMVCo standards are built on ISO 7816.
ISO 14443	The ISO standard for contactless chip cards. 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.
ISO 18092	A new ISO standard for contactless chip cards and contactless payment data. This standard allows bi-directional communication between the data source and the 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.
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.
Liability Shift	The process of determining where the liability resides for a particular transaction/situation. Each brand defines the rules around their liability structure.
Magnetic Stripe Card **Also known as:** **• Mag stripe card**	A plastic card that uses a band of magnetic material to store data. Data is stored by modifying the magnetism of magnetic particles on the magnetic material and is read by "swiping" the magnetic stripe through a mag stripe reader. A payment card that does not have a chip and uses the magnetic stripe on the back only.
Merchant **Also known as:** **• Retailers**	Entity which accepts payments from customers in exchange for goods and/or services and connects to a payment network through an acquirer.
Multi-application Card	The presence of multiple applications on a single chip card, such as payment, loyalty and identification.
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 or Near Field Communication	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". 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	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.
Offline Data Authentication	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: SDA, DDA and CDA.

TERM	DEFINITION
Offline PIN	The 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 the comparison. Only the result of the comparison is passed to the issuer host system. Two types of offline PIN are enciphered and plaintext.
Offline Only Terminal	A chip terminal that is not capable of sending an online authorization request and where all transactions have to be approved offline.
Online Authorization	Authorizing or declining a payment transaction by sending transaction information to the issuer and requesting a response real-time.
Online Capable Terminal	A chip terminal that supports both offline and online processing.
Online Card Authentication	Validation of a chip card by the issuer during online authorization to protect against data manipulation and skimming. See also ARQC (Authorization Request Cryptogram).
Online EMV	A streamlined implementation of EMV that uses online card authentication and online transaction authorization together and requires 100 percent online authentication / authorization. Online EMV may be appropriate for countries with a fast, reliable telecommunications infrastructure, such as the U.S.
Online Issuer Authentication	Validation of the issuer by the card to ensure the integrity of the issuer. Also known as Issuer Authentication and Host Authentication. See also ARPC (Authorization Response Cryptogram).
Online PIN	In a chip transaction, the process of comparing the cardholder's entered PIN with the PIN stored on the issuer host system. The PIN is encrypted by the POS 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.
Payment Card Industry Data Security Standard (PCI DSS)	A framework developed by the Payment Card Industry Security Standards Council for developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents.
Payment Network	Organization which defines specifications and rules of the network, routes transactions between issuers and acquirers, and ensures security and interoperability. Also known as a card brand.
Personalization	Process by which the elements specific to the issuer and cardholder are added to the plastic card, magnetic stripe and/or chip.
Personalization Bureau	An entity which 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 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
PIN **Also known as** **• Personal Identification Number** **• Offline PIN** **• Online PIN**	An alphanumeric code of 4 to 12 characters 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.
PIX **Also known as:** **• Proprietary Application Identifier Extension**	The last four digits of the Application ID
Plaintext PIN **Also known as:** **• Offline Plaintext PIN**	Offline 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.
POS/ATM Terminal Manufacturers/ Suppliers	An entity which manufactures and supplies POS/ATM terminals to POS/ATM terminal operators/owners
POS/ATM Terminal Operators/ Owners	An entity which drives or operates some or all parts of payments through terminals or ATMs. Examples: • Acquirer • IAD (Independent ATM Deployer) • ISO (Independent Selling Organization) • Merchant • VARs (Value Added Resellers)

TERM	DEFINITION
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.
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.
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.
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.
Regional Debit Network **Also known as:** **• Regional network**	Organization which defines specifications and rules for a debit-only payment network, routes debit transactions between issuers and acquirers, merchants and ATMs, and ensures security and interoperability. A debit network supports debit transactions (withdrawals, balance inquiries, transfers, and cash advances).
RID (Registered Application Provider identifier)	The first part of the Application ID, starting with a letter and containing nine numbers, used to identify a payment system (card scheme) or network, e.g., MasterCard, Visa, Interac.
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.
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.
SAM (Secure Application 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.
Standards Body	An entity which ensures physical and logical global interoperability of contact and contactless capable devices and systems: e.g., cards, mobile devices, 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.
Static Data Authentication (SDA)	An authentication technique used in offline chip transactions that uses a cryptogram using a static public key certificate and static data elements. With SDA, the data used for authentication is static—the same data is used at the start of every transaction.
Symmetric Key Technology	Keys that are used for symmetric (secret) key cryptography. 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.
TACs (Terminal Action Codes)	Codes placed in the terminal software by the acquirer. These codes indicate the acquirer's preferences for approving transactions offline, declining transactions offline, and sending transactions online to the issuer based on risk management performed.
Terminal Verification Results (TVR)	The result of the checks performed by the terminal during the transaction.
Transaction Certificate (TC)	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 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.
Triple DES **Also known as:** **• Data Encryption Standard** **• TDES** **• 3DES**	A sophisticated implementation of 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.