Chip Terms Explained

A Guide to Smart Card Terminology

Contents

6 Issuer Authentication Service
Issuer Public Key
Issuer Public Key Certificate
Issuer Script
Java™
JCOP10, 20, 30 – Java Card Open Platform 10, 20, 30
Key
Key Management

7 Key Revocation
MAC – Message Authentication Code
MSI – Magnetic Stripe Image
Multi-application Card
Multi-function Card
Offline Data Authentication
Offline Enciphered PIN
Offline PIN

8 Offline PIN Verification
Offline Plaintext PIN
Online Card Authentication
Online Issuer Authentication
Open Platform (now GlobalPlatform)
PED – PIN Entry Device
Personalization
PIN – Personal Identification Number
Post-Issuance Update
Private Key
Public Key

9 Public Key Cryptography
PKI – Public Key Infrastructure
ROM – Read-Only Memory
RSA – Rivest, Shamir and Adelman
SAM – Secure Application Module
Security Levels 1, 2, 3
SDA – Static Data Authentication
SPA – Simple Power Analysis
Skimming
Smart Card

10 SVC – Stored Value Card
TACs – Terminal Action Codes
TC – Transaction Certificate
TDES – Triple DES
UKIS – United Kingdom Integrated Circuit Specification
VEE – Visa Easy Entry
VIS – Visa Integrated Circuit Card Specification
Visa Cash

11 Visa Private Key
Visa Public Key
VOP – Visa Open Platform
VSDC – Visa Smart Debit/Credit

February 2002. Version 1.0.

A – C

AAC – Application Authentication Cryptogram
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.

AID – Application Identifier
A data label that identifies an application on the card or terminal. For example, the AID for **VSDC** is 1010, Visa Electron is 2010, and PLUS is 8010. 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.

Applet
An application written in the **Java™** programming language. The current **Visa Smart Credit/Debit (VSDC)** applications, as well as increasingly more value-added applications such as loyalty are written in **Java™**.

ARQC – Authorization Request Cryptogram
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.

ARPC – Authorization Response Cryptogram
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.

Authorization Controls
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.

CA – Certificate Authority
A certificate authority is 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**. For **VSDC**, Visa acts as the CA by issuing certificates to issuers (comprised of the **Issuer Public Key** signed by the **Visa Private Key**).

C

CAD – Card Acceptance Device
A device (usually a point-of-sale terminal) that is cable of reading and processing data from magnetic stripe and **chip card**s.

CAM – Card Authentication Method
Validation of the card by the issuer to protect against data manipulation and **skimming**. Also referred to as **Online Card Authentication**. See also **Authorization Request Cryptogram** (**ARQC**).

CVM – Cardholder Verification Method
A method used to confirm the identity of a cardholder and to signify cardholder acceptance of a transaction, such as signature, **Offline PIN** and Online **PIN**.

Card Mask
The method used to permanently burn data into the **ROM** of a chip. For **VSDC** cards, the operating system and the bulk of the functionality of the **VSDC** application are usually 'masked' into **ROM**.

Certificate
See **Digital Certificate**.

CCPS – Chip Card Payment System
A Visa product term now referred to as **Visa Smart Debit/Credit** (**VSDC**).

Chip Card
A plastic card embedded with an integrated circuit, or chip, that communicates information to a point of transaction terminal. Chip cards offer increased functionality (and security) through the combination of significant computing power and substantial data storage. Also referred to as **ICC** or **smart card**.

Combi/Dual Interface Card
A card that has a single chip and two interfaces – usually a contact interface and a **contactless** interface. The main advantages of having one chip with two interfaces (versus two chips with two interfaces – e.g. **hybrid card**) are lower card costs and the ability to access the same application and its associated data from either the contact or the contactless interface. For example, Visa has a combi card with a **VSDC** application that uses the contact interface and an **ePurse** application that uses both the contact and **contactless** interfaces.

Contactless Card
The use of either radio frequency or infrared technology to allow the card and the terminal to communicate or transact without physically touching. Contactless technology is popular with mass transit, road toll and physical security access applications which require fast transaction speeds. The contactless technology most applicable to Visa is based on the **ISO 14443** standard.

Cryptogram
A numeric value that is the result of data elements entered into an algorithm and then encrypted, commonly used to validate data integrity. Cryptograms used for **VSDC** 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. In **VSDC**, cryptography is often used to secure sensitive information like PINs or to authenticate an entity such as an issuer or cardholder. See also **Cryptogram**.

DES – Data Encryption Standard
A cryptographic algorithm in which two users share the same secret **key**. This algorithm is used in **VSDC** transactions for various functions, such as **Online Card Authentication**.

DDA – Dynamic Data Authentication
A type of **Offline Data Authentication** in which the card uses **public key** technology to generate a cryptographic value, which includes transaction-specific data elements, that is validated by the terminal to protect against **skimming**.

DPA – Differential Power Analysis
A type of attack on a smart card which attempts to compromise the data on the card by monitoring the electrical activity on the chip (**Simple Power Analysis – SPA**) and then using advanced statistical methods to determine secret information (such as secret **key**s and user **PIN**s) stored in the chip.

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. Visa issues digital certificates (via the **Certificate Authority**) to issuing banks that then load the digital certificate onto **VSDC** cards. This certificate can be used to authenticate data on the card via **SDA** or **DDA**.

Dynamic Data Update
See **Issuer Script**.

Early Data Option
A **VSDC** implementation in which the issuer or acquirer makes minimal host system changes at the beginning of their program and migrates to **Full data option** changes at a later time.

E – F

EEPROM – Electronically Erasable Programmable Read-Only Memory
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.

eCash – Electronic Cash
See **ePurse**.

ePurse – Electronic Purse
A chip application designed to mimic the use of cash. ePurse cards are sometimes referred to as **eCash** or **Stored Value Cards** (**SVC**), and can be either reloadable or disposable. They are popular for use with mass transit and road tolling systems. See also **Visa Cash**.

EMV – Europay, MasterCard, Visa Specifications (EMV)
Technical specifications developed jointly by Europay International, MasterCard International and Visa International outlining the interaction between **chip card**s and terminals/**CADs** to ensure global interoperability.

EMV/VIS Compliant
Cards and terminals that meet security, interoperability, and functionality requirements outlined in **EMV** and **VIS**.

EMVCo
Europay International, MasterCard International and Visa International formed EMVCo. EMVCo's role is to manage, maintain and enhance the EMV Integrated Circuit Card Specifications for payment systems.

Fallback
The term used for the scenario when an **EMV chip card** transaction is initiated via its magnetic stripe at an **EMV** chip terminal. This may be the result of an inoperative chip on the card or a malfunction of the terminal chip reader.

Full Data Option
Visa's recommended **VSDC** host implementation in which the issuer and/or acquirer makes all of the required host system changes to transmit and receive full chip data. The Full Data Option ensures Members are able to maximize the additional risk management benefits of chip data processing and make advantage of additional features including **online card authentication** and **post-issuance** card updates (see **Issuer Script**).

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 Visa, a Member, 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. The term hybrid card has also been used to describe a card combining two chips and two interfaces (contact and **contactless**), as opposed to a card combining a single chip with two interfaces (contact and **contactless**), which is known as a **combi card**.

ICC – Integrated Circuit Card
See **Chip Card**.

iCVV – Card Verification Value for Integrated Circuit Cards
An alternate Card Verification Value defined for storage on a Visa **EMV chip card**, and uses "999" instead of the service code encoded on the magnetic stripe image of the chip for the iCVV calculation. iCVV enables issuers to identify fraudulent use of chip data in magnetic-stripe read transaction processing.

ISO – International Organization for Standardization
An institution that maintains over 13,000 International Standards for business, government and society.

ISO 7816
The ISO standard for **chip cards** with contacts. The **EMV** standards are built on ISO 7816.

ISO 14443
The ISO standard for **contactless chip cards**. **ISO 14443** recognizes Type A (Philips 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**.

IACs – Issuer Action Codes
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.

I – K

Issuer Authentication Service
A VisaNet service in which Visa generates the **Authorization Response Cryptogram** (**ARPC**) on behalf of an issuer and forwards it to the card in the authorization response.

Issuer Public Key
The **public key** part of an issuer's **public/private key** pair, which is to be used with a specific Visa product or service. The Issuer Public Key is contained in an **Issuer Public Key Certificate** issued by the **CA**.

Issuer Public Key Certificate
An **Issuer Public Key** signed by the **Visa Private Key**. This information must be unique to each application on the card. The **certificate** is loaded on the card during **personalization** and used by the card and terminal during **Offline Data Authentication** to validate that the card comes from a valid issuer.

Issuer Script
A process by which an issuer can update the electronically stored contents of **chip card**s without reissuing the cards. Issuer Scripts include blocking and unblocking an account, blocking the entire card, changing the cardholder's **PIN**, and changing the cardholder's **Authorization Controls**. Also known as **Dynamic Data Updates** and **Post-Issuance Update**.

Java™
A programming language used for developing applications. In smart cards, one of the major benefits of Java™ is that an application (**applet**) can be written once in Java™ and used on several **chip card** platforms.

JCOP10, 20, 30 – Java Card Open Platform 10, 20, 30
A term that refers to the **chip card**s currently available in the Visa Low Cost Card Program. Visa has negotiated special pricing with **chip card** vendors for Visa branded chip programs. The name refers to the name of the operating system (from IBM), and the number refers to an increase in memory size and/or functionality: JCOP10 is a non-**public key** card, JCOP20 adds **public key**, JCOP30 is a **combi card** and adds **public key** and a **contactless** interface.

Key
The numerical value entered into a cryptographic algorithm that allows the algorithm to encrypt or decrypt a message. Also referred to as a cryptographic key. See **DES**, **Private Key**, and **Public Key**.

Key Management
The various processes that deal with the creation, distribution, authentication, and storage of **key**s.

Key Revocation
The withdrawal of a scheme **public key** (for example **Visa Public Key**) from the acceptance infrastructure, and card certificates (for example **Issuer Public Key Certificate**) created under the scheme's **private key** (for example **Visa Private Key**). Key revocation can be required on a planned, accelerated or emergency basis to ensure the integrity and security of the payment scheme. The first planned key revocation of a **Visa Public Key** is the Visa **CA** 768-bit key on 31 December 2002.

MAC – Message Authentication Code
A digital code generated by passing data through a cryptographic algorithm. A MAC ensures that a message has not been altered during transmission.

MSI – Magnetic Stripe Image
A duplicate of the data on the magnetic stripe loaded onto the chip as the baseline feature of any **VSDC** card that represents the fundamental information needed for transaction processing and account access. MSI is the minimum chip payment service data required to process a transaction that is **EMV** compliant. See **Quick Start**.

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). This term is sometimes considered synonymous with **Multi-application Card**.

Offline Data Authentication
The use of **public key** technology to validate the card and/or card's data at the point of transaction. Offline Data Authentication protects data on the card against alteration and manipulation – ultimately to detect counterfeit cards. See **SDA** and **DDA**.

Offline Enciphered PIN
Offline **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.

Offline PIN
A **PIN** value stored on the card that is validated at the point of transaction between the card and the terminal. Two methodologies are used: **Offline Plaintext** or **Offline Enciphered PIN**.

O – P

Offline PIN Verification
The process in which the **chip card** compares the **PIN** entered by the cardholder into the terminal to a Reference PIN securely stored on the chip.

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.

Online Card Authentication
Validation of a **chip card** by the issuer during online authorisation to protect against data manipulation and **skimming**. Also known as **CAM** (**Card Authentication Method**). See also **ARQC** (**Authorization Request Cryptogram**).

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**).

Open Platform (now GlobalPlatform)
The Visa preferred technology and architecture for multi-application chip cards (including terminals, personalization systems, data preparation systems and card management systems). See **GlobalPlatform**.

PED – PIN Entry Device
A secure device that allows a consumer to enter their **PIN**.

Personalization
The process of populating persistent memory (**EEPROM**) with cardholder data, uniquely identifying the card with a given cardholder and account. For **VSDC**, this includes encoding the magnetic stripe, embossing the card (if applicable) and loading data onto the chip.

PIN – Personal Identification Number
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**.

Post-Issuance Update
See **Issuer Script**.

Private Key
As part of a public key cryptographic system, the key that is kept secret and known only to the owner, and typically stored in a **HSM**.

Public Key
As part of a public key cryptographic system, the key known to all parties.

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.

PKI – Public Key Infrastructure
The infrastructure needed to support **public key** encryption, decryption and **key management**. It requires a **Certificate Authority** to issue and verify the **keys**.

ROM – Read-Only Memory
Permanent memory that cannot be changed once it is created. 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. In **VSDC**, 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 **ePurse** applications.

Security Levels 1, 2, 3
Visa defined **chip card** security testing & approval levels. Level 1 is no longer permitted, Level 2 is the minimum requirement for **VSDC** and Level 3 is the minimum requirement for **Open Platform** and **Stored Value Cards**.

SDA – Static Data Authentication
A type of **Offline Data Authentication** in which the terminal validates a cryptographic value placed on the card during **personalization**. This validation is similar to CVV and protects against some types of counterfeit fraud, but does not protect against **skimming**.

SPA – Simple Power Analysis
An attack on a smart card that attempts to compromise the data on the card by directly observing the chip's power consumption.

Skimming
A type of counterfeit in which the data from a genuine card (including magnetic stripe and CVV) is copied onto a counterfeit card. In **VSDC**, skimming is combated by **Online Card Authentication** and **Offline Data Authentication** (such as **DDA**).

Smart Card
See **Chip Card**.

S – V

SVC – Stored Value Card
See **ePurse**.

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.

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 **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.

TDES – Triple DES
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**, and as a consequence will shortly be adopted as the encryption standard for all Visa **PED**s.

UKIS – United Kingdom Integrated Circuit Specification
An **EMV** compliant **chip card** and terminal implementation by the UK banking organization APACS (Association Payment And Clearing Services).

VEE – Visa Easy Entry
A Visa product term used to describe a pre-**EMV** Visa chip credit program in which the chip stores a replication of the magnetic stripe contents (track data). VEE is not compliant with **EMV** and is therefore being phased out based on Visa International Board approved dates: all existing VEE programs must be converted to **EMV** compliant programs by 31 December 2003, and no new Easy Entry programs are allowed after 31 December 2000.

VIS – Visa Integrated Circuit Card Specification
Visa's implementation of the **EMV** specifications to aid vendors in developing **VSDC** cards and terminals.

Visa Cash
The Visa Cash service description describing the product requirements and Visa Operating Regulations surrounding the use of a Visa branded **ePurse** program.

Visa Private Key

The **private key** component of the Visa **RSA** key pair. The Visa Private Key is managed in a secure environment by Visa and is used to sign the **Issuer Public Key** to create an **Issuer Public Key Certificate** that is loaded onto a Visa chip card by a participating Visa issuer. Typically, a Visa public/private key pair will be unique to a Visa product or service.

Visa Public Key

The **public key** component of the Visa **RSA** key pair. The Visa Public Key may be stored in a terminal/**CAD**, and is used at the merchant end of a Visa transaction to decrypt the **Issuer Public Key** from the **Issuer Public Key Certificate** in the process of validating a transaction. Typically, a Visa public/private key pair will be unique to a Visa product or service.

VOP – Visa Open Platform

See **Open Platform** & **GlobalPlatform**.

VSDC – Visa Smart Debit/Credit

The Visa service offerings for chip-based debit and credit programs. These services, based on **EMV** and **VIS** specifications, are supported by VisaNet processing, as well as by Visa rules and regulations. The term VSDC is also used to refer to the actual payment application/**applet** that resides on the card.