EMV Key Management

Karthick Chandrasekar
Product and Payments Leader | Digital Transformation | Banking | Fintech
Veröffentlicht: 6. Jan. 2019
+ Folgen

What is EMV?

The technology move from magnetic stripe based payment cards to chip cards has now been underway for more than a decade. It was originally initiated by Europay (now part of MasterCard), MasterCard and Visa, and abbreviated as EMV. The move has largely been regionally driven by security due to fraud, liability shift, and technology – e.g. contactless,and more recently mobile.

EMV Chip

During the past decade chips have evolved with regards to capabilities,while the price has gone down, so acquiring cards with cryptographic co-processors and dual interfaces for contact and contactless payment is quite inexpensive. The combination of security and functionality, particularly through the contactless interface, has opened the door to themobile market space, which is here to stay.

The main tasks related to the process of issuing EMV cards are to extract customer information from a bank's database, feed it into a data preparation system (which adds additional data including digital certificates and cryptographic keys) and finally write that data onto the chip. The last step is termed personalization.

EMV Keys and EMV Certificates

EMV introduces a well-structured security design. The proven security mechanisms of RSA and 3DES are deployed across a six-entity issuing model.

Secure Usage – Cryptography in EMV

All EMV cards have a mandated minimum requirement for using one card unique 3DES key and have a choice between three increasingly secure usages of RSA signatures and keys, termed SDA (Static Data Authentication), DDA (Dynamic Data Authentication), and CDA (Combined Data Authentication).

SDA – Static Data Authentication

The initial and most basic layer of crypto is RSA signatures authenticating the payment card itself when it is used at the ATM and POS terminal. For SDA, the smart card contains application data which is signed by the private key of the issuer's RSA key pair. When a card with an SDA application is inserted into a terminal, the card sends this signed static application data, the CA index, and the issuer certificate to the terminal.

The terminal verifies the issuer certificate and the digital signature by comparing these to the actual application data present on the card. In short, an RSA signature gives the assurance that the data is in fact original and created by the authorised issuer.

DDA – Dynamic Data Authentication

SDA does not prevent replay attacks as it is the same static data that is presented in every transaction. This is improved with DDA where the smart card has its own card-unique RSA key that signs dynamic data, i.e. unpredictable and transaction-dependent data, and sends this to the terminal. When a card with a DDA application is inserted into a terminal, the card sends the signed dynamic application data, the CA index, the issuer certificate and the card certificate to the terminal. The terminal then verifies the issuer certificate, the smart card certificate and the signed dynamic application data.

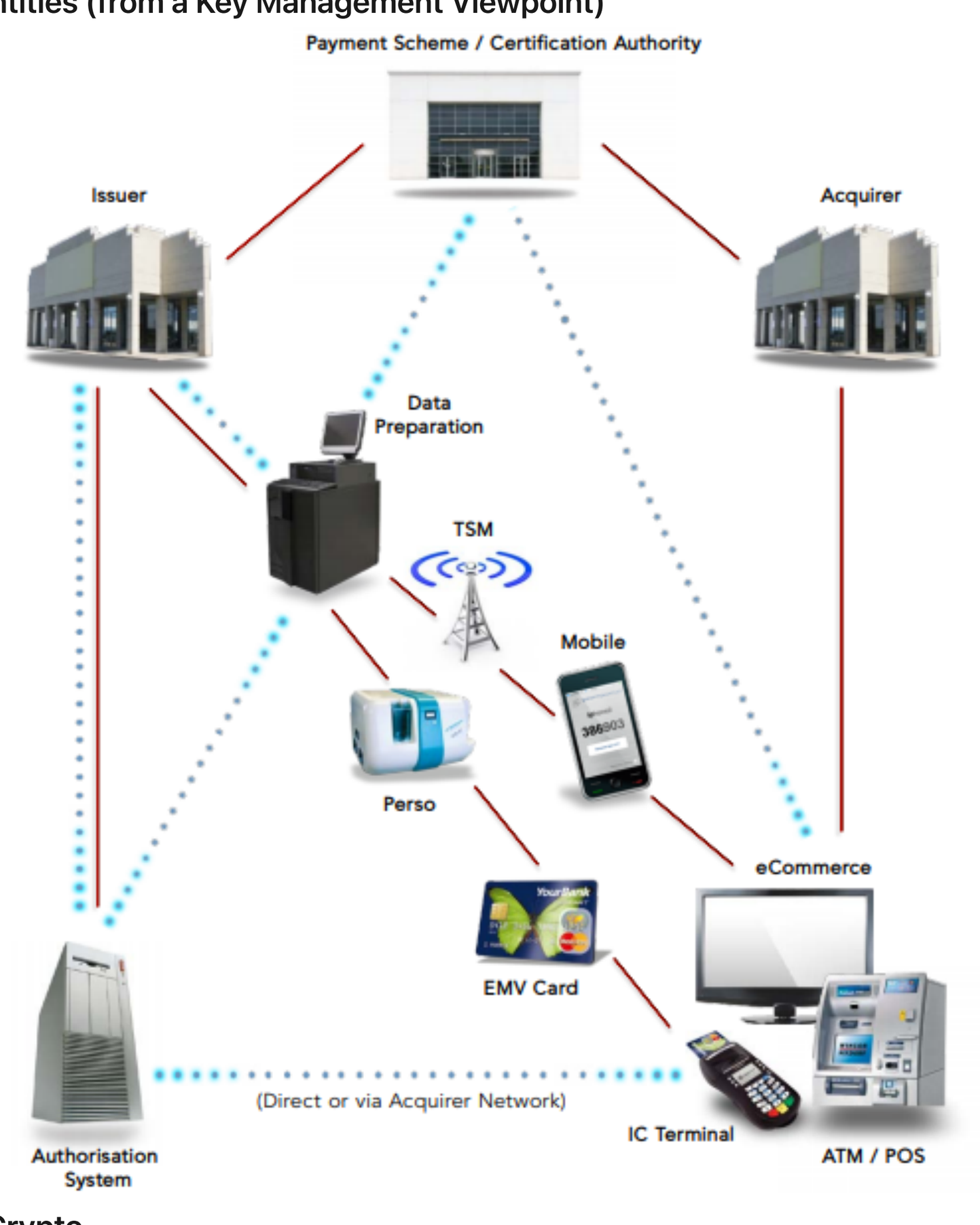
CDA – Combined Dynamic Data Authentication Application Cryptogram Generation

The SDA and DDA schemes both suffer from protocol weaknesses that may be exploited for criminal purposes. The security mechanism in SDA is there to compare what is on the actual card (PAN, expiry date etc.) with signed data generated at the time of personalization. The digital certificate is a static certificate, i.e. independent of the actual transaction, and hence could be subject to replay attacks. DDA is stronger and makes use of a card resident unique RSA key to dynamically sign unpredictable and transaction unique data. This, however, is only for the purpose of authenticating the card.

The EMV protocol for transaction approval or denial does contain more logical processing, and there is a potential weakness between the steps of verifying the card (using SDA or DDA) and the step comprising of approving the actual transaction. Once the card has been approved a subsequent step is for the card to validate whether the actual transaction shall be denied, approved, or sent online for issuer decision. The card makes that decision based on other card parameters, and it is possible to first go through the SDA/DDA process and then change the message from the card with the verdict on the transaction, although the latter does use card-generated cryptograms.

A scheme has been devised that combines both the card authentication and the transaction approval decision in one step. The scheme is termed 'Combined Dynamic Data Authentication-Application Cryptogram Generation' and is abbreviated to CDA. Essentially, it consists of including the card decision among the data being signed by the card's RSA key.

EMV Entities (from a Key Management Viewpoint)



3DES Crypto

Whereas SDA, DDA and CDA are based on the RSA public key infrastructure, 3DES is used for evaluating the actual transaction request.The evaluation is done jointly by parameter logic in the card, ATM/POS, and if need be, the issuer through online communication. A 3DES key is used for encrypting the card's part of the decision and to verify a response from the issuer. Further, the issuer may choose to use the opportunity to send additional commands to the card, such as parameter updates, which necessitates two more 3DES keys to be present in the card for secure command verification.

The latter process is termed scripting. In the issuing scenario the mathematical security perspective of the RSA scheme is the most complex, as it is a multi-layer RSA public key certificate structure. The 3DES scheme is simply for the issuer's data preparation system and authorisation system to share a set of master keys.

Issuer

The issuer supplies card holder data from its card management or host system to a data preparation system. There is a data set for each individual cardholder including the brand of card to produce, account number, card parameters, such as spending limits, plus 'profile' information. A profile defines which cryptographic keys are to be used, settings for PINs, and fixed card type specifics, e.g. risk parameters. In essence an issuer must have the complete overview of all security aspects and cryptographic keys.

The CA – Certificate Authority

In preparation for issuing EMV cards an issuer must establish a relationship with a payment scheme and exchange cryptographic keys and digital certificates. This occurs via a secure exchange between the bank's data preparation system (be it in-house or outsourced) and the payment scheme's certificate authority – the CA.

Issuer and CA Interaction

It is an initial task for the issuer to interact with the CA. Files with digital certificates and files with corresponding hash-values are exchanged; the exchange method varies slightly for each scheme, but in all cases it is a well defined sequence of easy steps. Aside from file extension differences the logical content exchanged is identical.

First the issuer sends a 'certificate-request'; the data preparation system generates an RSA key pair, embeds the public key in a self-signed certificate, and sends it to the scheme CA. The CA evaluates the key and returns a certificate on the key. This is called an issuer certificate.

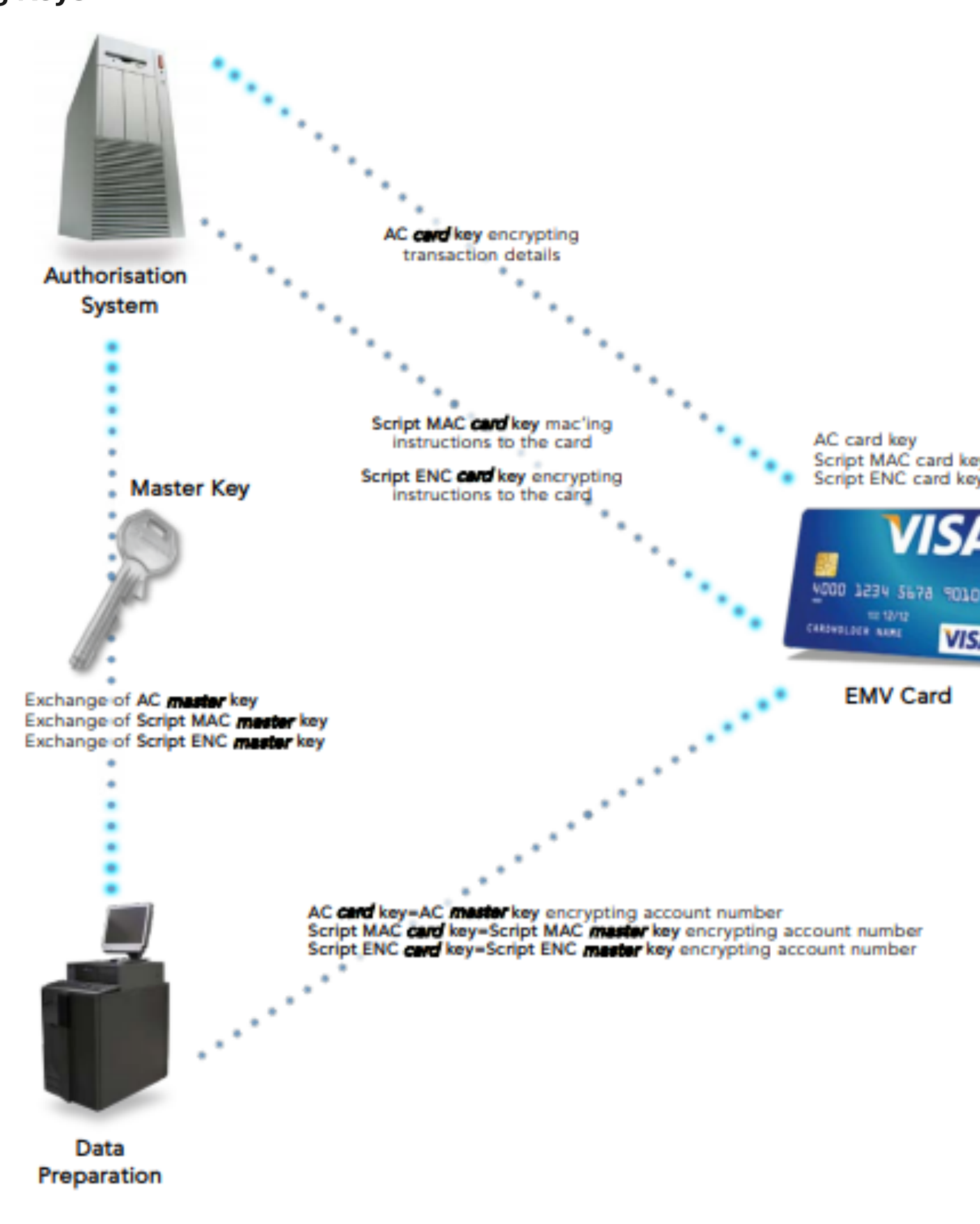
The issuer certificate is a data block containing the issuer's original public key and related data, all signed by a private key belonging to a CA RSA key pair. The CA also sends its own self-signed certificate on its corresponding CA public key, so that the data preparation system can verify the issuer certificate. For security purposes, a separate file is finally sent with a hash of the certificate. It is a simple procedure that is exactly the same for SDA, DDA, CDA and contactless cards.

Authorisation System

In preparation for EMV issuing, a bank must establish a technological infrastructure with an authorisation system and exchange cryptographic keys.The keys are all 3DES keys which are used for encrypting transaction data.

Interacting with a CA

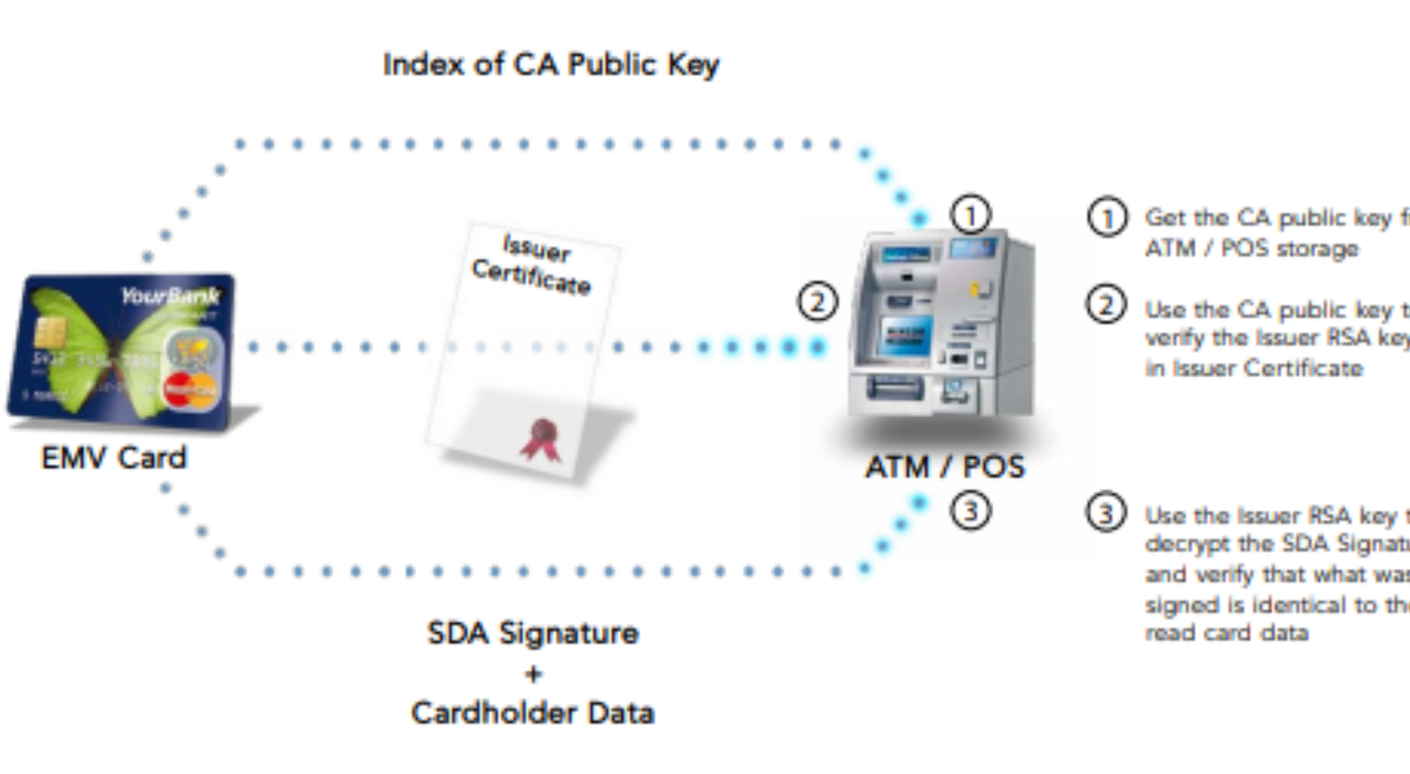
Sharing Keys



PINs

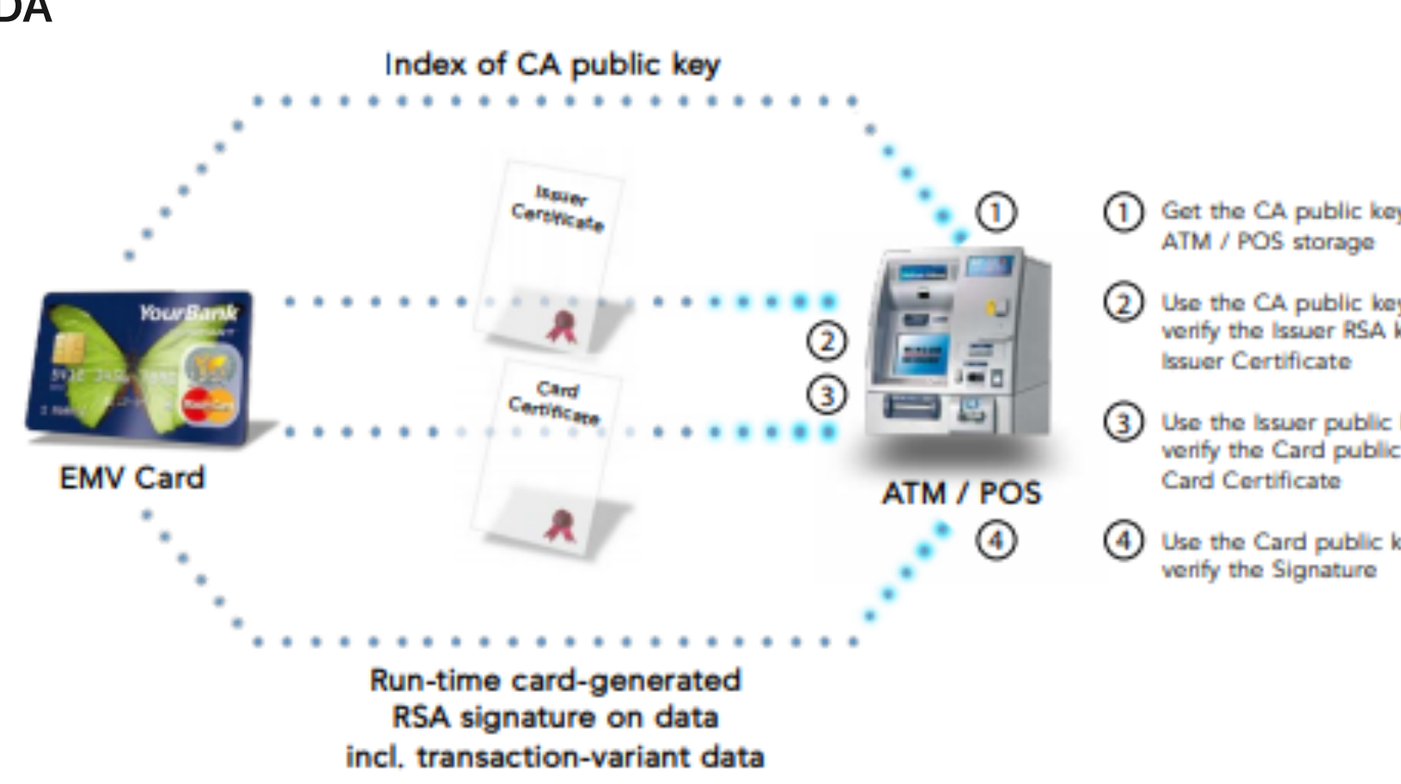
PINs require special management: for online PIN verification the authorisation system may need it; for offline PIN verification the card, and hence the data preparation system may need it; for cards supporting both options, all systems need it. Many non-EMV issuers may already be generating PINs and can re-use them also for EMV. Care should be taken that the PIN formats used at the various points are synchronised; ISO-0, ISO-1, and ISO-2 formats are all in play

SDA



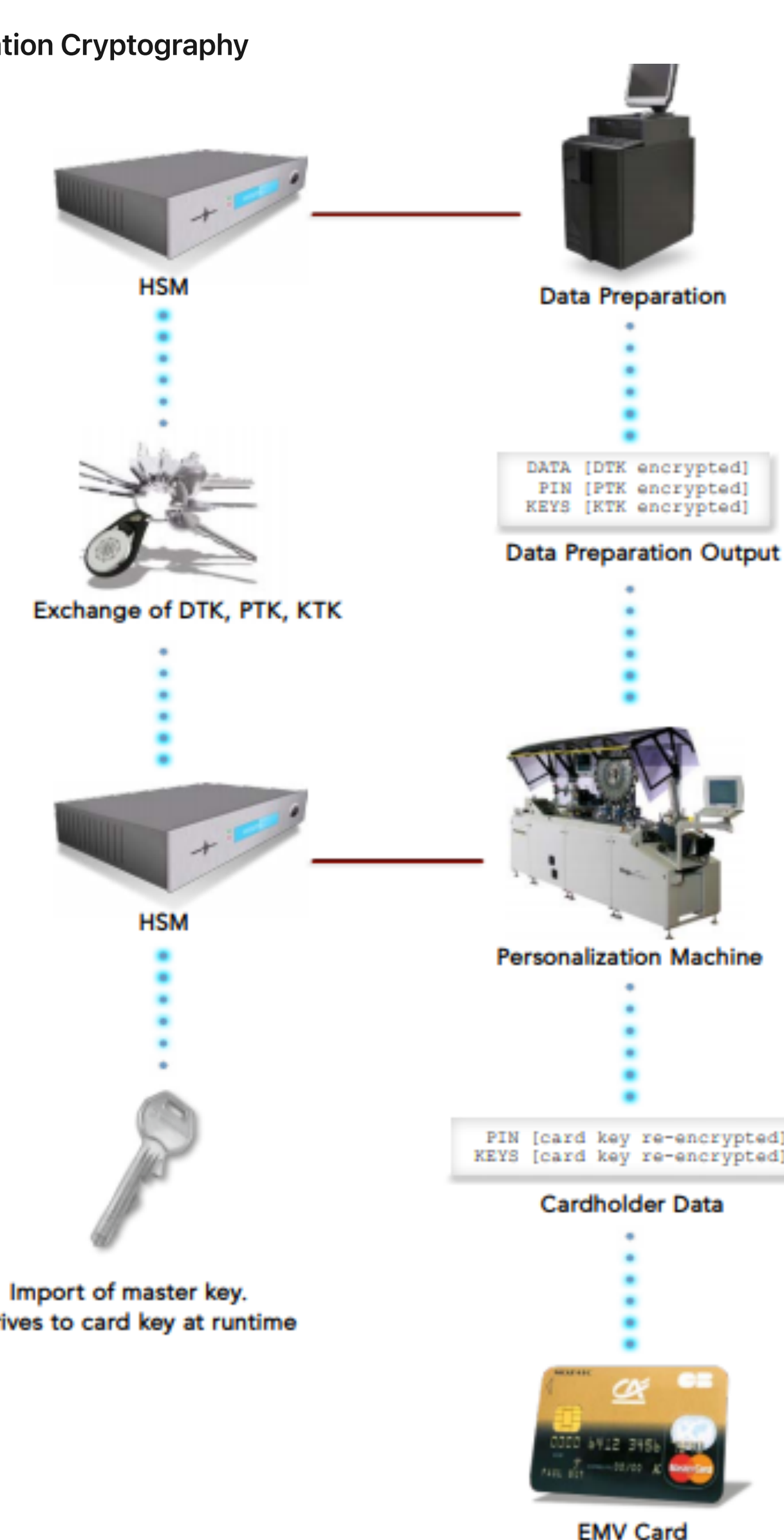
For SDA cards, the data preparation system uses an issuer's RSA key to generate a digital signature on the card data. It then puts this digital signature and the imported CA-signed issuer certificate onto the card. Each ATM/POS has the actual scheme CA RSA public key available, and hence can verify that the issuer certificate was properly CA signed, and that the signature was correct. It compares the signed data with the actual data stored on the card to see that it is identical.

DDA/CDA



For DDA and CDA cards, the data preparation system also makes an RSA key for each card. The system puts the public part of this RSA key into a card certificate and signs the certificate with the issuer RSA private key. The card certificate is put onto the card together with the issuer certificate that was previously imported from the scheme CA

Personalization Cryptography



At run-time, the data preparation system encrypts its output with these keys, hands over the data to the machine, which then decrypts the data using the same keys. Immediately after, the machine re-encrypts the data under a card specific storing key. It then stores the data on the chip which finally decrypts the data using the same card specific card storing key. Variations occur regarding the data encryption key as certain machines cannot handle a dedicated key for the data part, and instead uses whole-file encryption. Keys and PINs are, however, always encrypted using dedicated keys and a Hardware Security Module (HSM) must be deployed for this

Conclusion

We covered the basic of EMV key management, i strongly suggest to read more about the key management and explore yourself. Payment systems basics will never change no matter whether it's core baking or crypto etc... First learn the basic and dream/innovate.Whatever your imagination if it cover buy,sell,charge and recon you have whitepaper in your hand.Please remember Innovation key will open always by simple imagination key. Keep dream,innovate and achieve