A brief overview of the challenges involved in key management for EMV personalization

Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

EMV personalization relates to the process of writing specific information to the chip of a payment card. These data are most often of cryptographic nature and involve extreme security and confidentiality data transmission between the personalization devices and the chip of the cards. EMV personalization is ruled by a global document named the CPS, for 'Common Personalization Specifications' or alternatively for 'Card Personalization Specifications' (see [1]) which contains the main guidelines for personalising a payment card. Additionally, card schemes often have their own specifications requirements. For instance, Visa maintains the VISA Global Personalisation Requirements (GPR).

—--------------------------------------

The EMV personalization data processing in itself is not the topic of the present article but rather we wish to focus on the cryptographic schemes involved in EMV personalization as well as the key management involved, which is both complex and mandatory.

The main actors of EMV personalization

Introduction

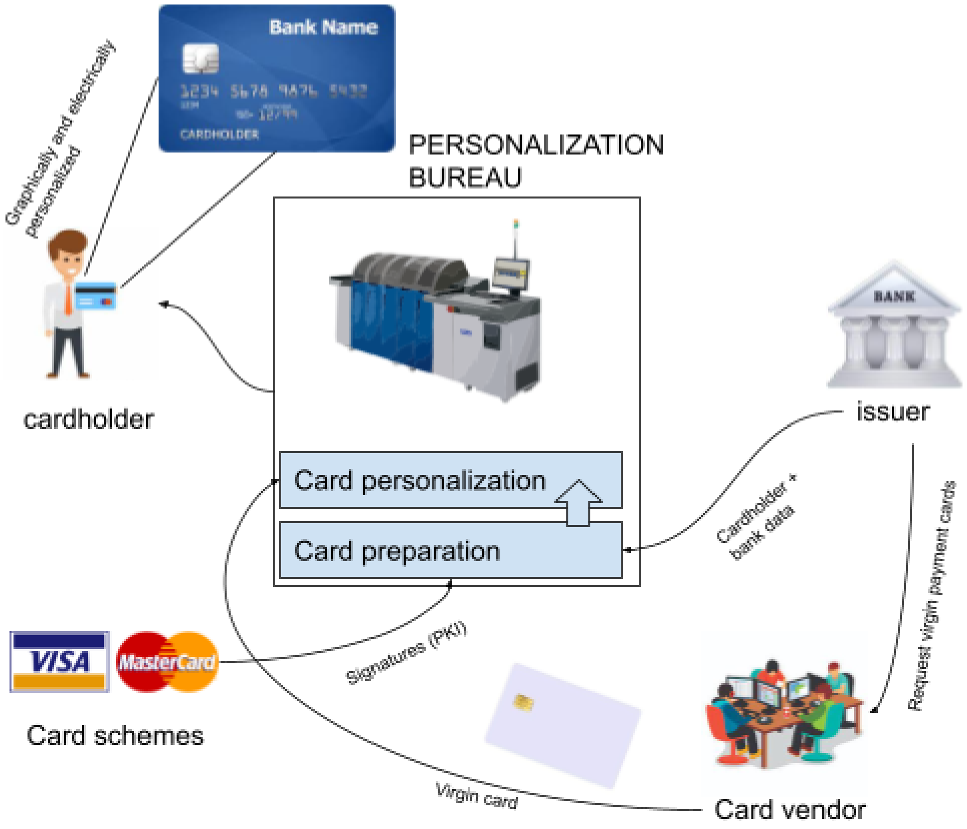
First we need to introduce briefly the main actors involved in a typical EMV personalization process:

- The cardholder.
  This is the person who is authorised to use a payment card delivered by the issuer. This is generally a client of the issuer bank.
- The issuer.
  As described in the four-corner model, an issuer is a financial organisation that produces ('issues') EMV payment cards.
- The personalization bureau
  This is the entity that defines the data that will be used to personalise a payment card profile. Typically they also act as a data preparation centre and a personalization centre but not always.
- The data preparation centre
  This is where the data is collected and prepared. A file produced by the personalization bureau (card personalization data file) is processed together with a card profile by an EMV data preparation system.
- The personalization centre
  This is where the personalization physically takes place. E.g the environment where payment cards are inserted into couplers and where data is written to the memory. (only for contact cards)
- The card integrator (or card vendor)
  This is a trusted third party that manufactures and programs the chip of the payment cards on behalf of the issuer.
- The card scheme
  This is also known as a card brand, e.g. Visa, Mastercard etc …

In a contactless personalization, also known as Over-the-air (OTA) personalization we must also consider the additional following actors:

- The token services providers (TSP)
  This is a trusted third party that provides tokenization
- The trusted service managers (TSM)
  This is a trusted third party that provides OTA personalization services, e.g connecting remotely a personalization centre to a secure element.

There are in fact more actors but as we can see the ecosystem is already quite complex. It is also worth noting that some entities may play several roles. For example issuers may also be the ones who do the data preparation etc …



Let us look in more details at the role of each parties:

Personalization Bureau

There are two aspects in a card personalization: the most obvious is 'feeding' the data (cardholder data, bank data, keys…) and formatting them , securing them and getting them written to the virgin payment card but there is a second aspect which is less obvious.

With the EMV card, a card issuer must define the configuration of the EMV parameter settings. In other the 'profile' of a card product. There are more than a hundreds of such parameters which will define the 'rules' of a transaction and how the card should behave: if a transaction should be authorised online or offline, how many PIN tries there can be, how the card should handle risk management and so on. Because of the great complexity involved in the combinations of all these parameters, card profiles can be very different, even if the same payment applications are used.

The definition of a card profile is highly important for an issuer and it's often a delicate and difficult matter. The issuer is usually totally involved in the decision process which is conducted with experts from the personalization bureau. Such a personalization bureau can be run by the card vendor or by the issuer itself.

Data Preparation Process

The data preparation process consists in generating a specific EMV personalization file from the issuer’s card personalization data file . The output has to be transferred securely to the card personalization centre, either because an HSM containing the data is directly attached to the machines of the card personalization centre, or via a secure channel using both encryption and authentication. The CPS ([1]) makes a difference between the direct or indirect personalization methods. In the indirect cases, two distinct zone keys are involved meaning two secure channels transporting the data from the data preparation to the personalization device (e.g a coupler) and from that personalization device to the IC card. This means that transport keys have to be involved.

The card personalization centre

The card personalization centre is a highly-secured area usually protected by conditional access video monitoring and security guards. The card personalization centre continuously receives the order from issuers and processes them automatically into batches. They maintain warehouses with all the necessary material to ship the cards once they are personalised. The centre must respect a very strict policy and follow specific security rules. Without such rules malevolent people could access the cards and perform some manipulations or access secret data. For instance it must be strictly impossible for an intruder to insert spy devices between the electronic personalization device (‘coupler’) and the chip itself. However even if such devices were installed, the sensitive data would still be protected because they are ciphered between the coupler and the chip.

EMV Personalization cryptographic requirements

overview

There are several secrets that must be protected during a EMV personalization:

1) The ‘offline’ PIN;
2) The private keys of the cards used for offline authentication (SDA[1],DDA,CDA);
3) The secure channel keysets (Global Platform secure channel);
4) Keys used for cryptogram computations and verifications (GENERATE AC).

All these secrets need to be both obtained and transported securely to the IC. In what follows we will detail what are these secrets and how they are generated and crypted for EMV personalization.

Direct and indirect methods

[1] SDA is deprecated and considered as broken and unsecure however, so generally not to be used

An EMV personalization can be performed using two techniques: the direct and the indirect method.

The simplest is the direct method, where the data preparation system is directly integrated to the coupler that will interface the ICC. In such a case there is no need for transport keys since there is only one zone separating the data preparation and the ICC.

The indirect method is more complex. It implies that the data preparation is separated from the personalization device and therefore there are two key zones. From the data preparation system to the personalization device(‘coupler’) , transport keys must be used. In general they are defined as follows:

- DTK, the data transport key, used for genetic data;
- PTK, the PIN transport key, used for PINs;
- KTK , the Key transport key, used for keys.

These transport keys must be unique each time. Each of these transport keys must be exchanged, either as split components or encrypted under a zone master key. It has to be note that the payment scheme regulations for key distribution are very formal and detailed procedures extend all the way down to typing in individual key digits for import into an HSM

The Secure Channel protocol (Global Platform) used for EMV personalization

The notion of an EMV compliant secure channel is fundamental when it comes to EMV personalization. In general , these secure channels are implemented in such a way that they follow the Global Platform secure channels specifications ([2]). There are different types of such channels: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, and SCP81.

SCP02, using triple DES encryption is deprecated but still in use in various personalization centres because it had been historically the dominant algorithm for a long time while SCP03 and the other schemes, using AES encryption or Elliptic Curves are still being introduced at a slow pace. Such channels come with various security levels : data encryption, mac-based authentication, response-mac-encryptions etc… and they are also available in different modes.

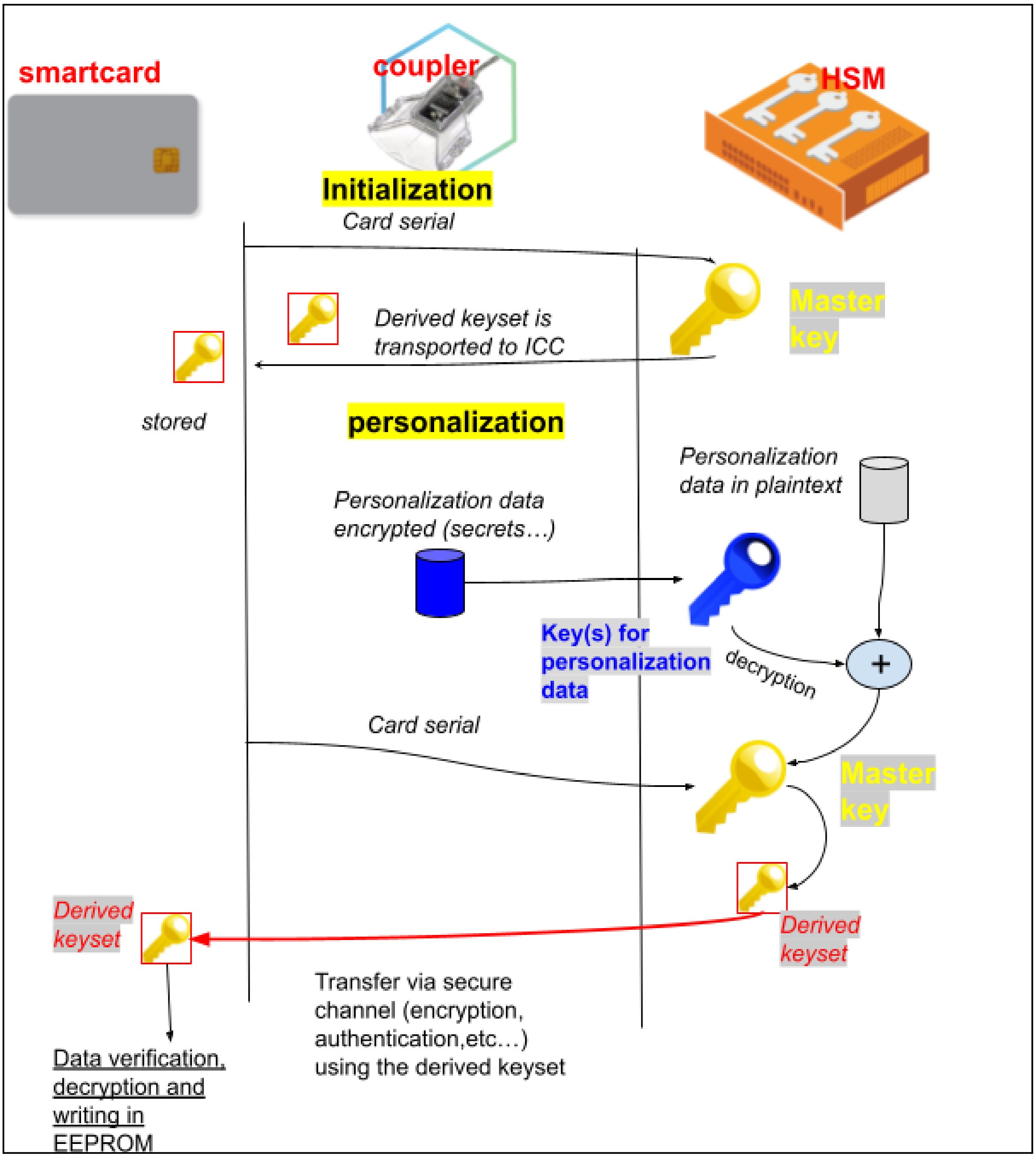
These secure channels can use symmetric or asymmetric cryptography and key exchange protocols.In general, they are derived from a masterkey located inside an HSM during an *initialization* phase (pre-personalization). For example SCP02, the simplest of all, uses a 3DES keyset based on 3 keys of 16 bytes each: the data encryption key, the mac key and key encryption key.

Once the initialization phase has been performed, the IC personalization can start using the secure channel between the coupler and the IC.The initialization phase must be mandatorily separated from the personalization phase, because of security considerations.

In the following diagram, we represent the flow of a typical EMV personalization: Firstly the card is queried for its serial number, which allows to derive the cards keys from a master key stored in an HSM. Once the keys are derived, they are transported to the ICC and stored there. This ends the initialization phase. The ICC is loaded with a specific, individual keyset.

During the personalization, data will be received from a database of encrypted secrets and from another database of plain text. The secret data will be securely decrypted by the HSM and the card will be required to provide its serial number, which allows the HSM to compute the card keyset and use that can keyset to open a secure channel with the card and send the data. The card will eventually verify and decrypt the data and write them on its EEPROM.

This is a very simplified version of an EMV personalization but EMV personalization centres usually do not disclose their methods and the exact algorithms that they use and therefore there is not a universal system which can be described.


smartcard
coupler
HSM
Initialization
Card serial
Derived keyset is transported to ICC
Master key
stored
personalization
Personalization data in plaintext
Personalization data encrypted (secrets…)
Key(s) for personalization data
decryption
+
Card serial
Master key
Derived keyset
Derived keyset
Transfer via secure channel (encryption, authentication,etc…) using the derived keyset
Data verification, decryption and writing in EEPROM

Key management in EMV personalization

In an EMV personalization, the way the keys are generated and transported is done in a very rigorous way.

Generation of keys

Here is a list of the main cryptographic secrets that must be generated during the personalization of a payment card:

- A 4 to 12 digit PIN. There are several algorithms permitted by payment networks, for example the 3624 IBM PIN generation method of the Interbank PIN generation algorithm;
- Generation of PIN blocks;
- Computation of IVCVC3;
- Computation of the DAC (Data Authentication Code);
- Generation of the derived master personalization key and EMV issuer keys (depending on the secure channel version used);
- Generation of signature for EMV data (offline verification methods);
- RSA key pair generation (for the smartcard);
- certification of smart card public keys;
- Encryption of EMV data groups (DGI);
- Generation of MAC values.

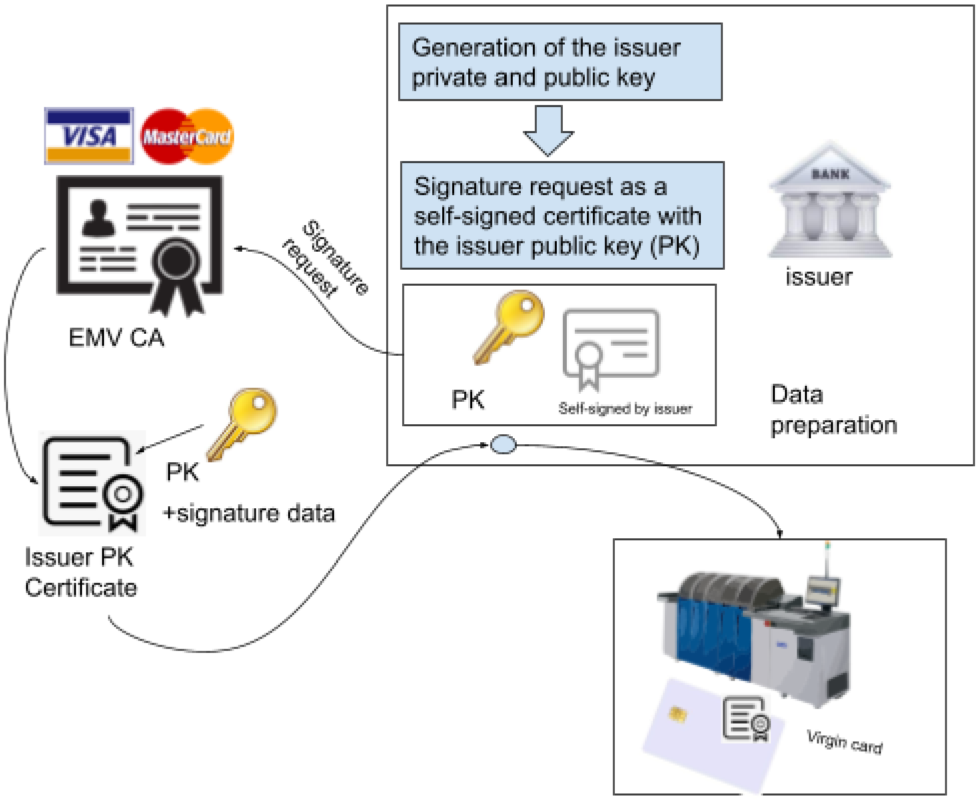
PKI structure of a EMV personalization (The EMV CA)

In an EMV personalization, a PKI structure is needed. This PKI structure is formed by the issue, a Certification Authority (CA) which is authorised by EMVco and the ICC card.

The certification authority maintains their key pair that they use for signature of issuer public keys (Issuer PK). The issuer must submit a signature request to the EMV CA during the personalization process. After verification, the CA will return the Issuer PK Certificate. This certificate will then be loaded into the ICC as part of the confidential data.

The selection of the right CA is done using the RID of the payment application (the issuer PK Certificate is per payment application) and an RID index.

During a transaction, after personalization and in the active phase of the card life cycle, a terminal can verify the signature by using the adequate CA public key (these keys are publicly available)


Generation of the issuer private and public key
Signature request as a self-signed certificate with the issuer public key (PK)
issuer
PK
Self-signed by issuer
Data preparation
Signature request
EMV CA
PK
+signature data
Issuer PK Certificate
Virgin card

Overview of the cryptographic process between the actors

The complete EMV personalization process is complex because it involves a lot of keys, generated and shared between some of the parties.

Card issuers may or may not choose to perform their own data preparation. There are pros and cons to this.Data preparation involves costly and complex processes but offers more security to an issuer. However the data preparation is often outsourced by the issuer.

The starting point is to generate and manage LMK and ZMK keys. They are respectively the local master keys and the zone master keys. Keys for transports must also be shared with the relevant other parties (PTK, KEK etc …)

As we saw previously, the issuer PK certificate must be obtained from the relevant EMV CA.

ICC PK pairs and ICC PK Certificate used for DDA (Dynamic Data Authentication) must also be generated and stored. They are used in addition to the issuer PK certificate by the card during the offline authentication methods (generally DDA or CDA)

The AC keys which are used for cryptogram verification by the card and issuer must also be generated by the EMV MDK key for AC keys.

Finally the secure messaging keys must also be generated from EMV MDK keys and CMK (card master keys) keys. These keys will be put on the card and in the possible various additional security domains as per the Global Platform specifications ([2]). The final three card manager derived keys will replace the original transport keys of the card as sent by the card manufacturer to the personalization centre.

The issue must keep a copy of these keys (or be able to regenerate them) because they will be needed for online verification (AC keys) and issuer scripting (secure messaging keys)

The cryptographic relationships between the parties : issuer, card preparation, personalization bureau, EMV CA, personalization centre are really complex and what's more they have to follow extremely strict guidelines dictated by the card schemes.

Necessity of a key management system

Using a key management system is not an option, in fact it's mandatory. The payment scheme mandates it (see [4] for instance). There is a strict paperwork which is required for EMV personalization and which describes very precisely how keys are generated, with what entities they are shared, who can access them etc …

Key ceremonies are needed as well as signed documents with employees (keys custodians) who have performed the ceremony.

A dedicated key management software is required to keep track of all the keys and follow in 'real-time' if possible the progress of a personalization flow.

Conclusion

We have seen the challenges that must solve a key management system in a typical EMV personalization: they are huge. We did not even describe the whole process and most of it is usually secret and depends on the culture and usages of local actors and personalization centres. The key management of an EMV card personalization is vital and any security breach could lead to a catastrophe.

References and Further Reading

- [1] EMVco. Card Personalisation Specification Version 2.0, August 2021
- [2] GlobalPlatform Technology. Card Specification. Version 2.3.1. Public Release, March 2018
- [3] EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management Version 4.3 November 2011
- [4] VISA Global **Personalisation Requirement** (GPR)