**Part II - PIN Block... first take-off and first stop.**

We started the PINBlock journey by explaining how PINblock is created, please refer to the below link for the previous article **The Journey Of a PINBlock [PIN Block... What and How??]:**

<https://www.linkedin.com/pulse/journey-pinblock-ahmed-hemdan-farghaly/>

The next step is to ship the created PINBlock safe and secure to the acquirer.

To do this is simple, we need to encrypt the PINBlock with a key before being transmitted from the PED to the acquirer.

The not so simple part is how we are going to manage the encryption key so that it won't be compromised.

For that, acquirer needs to follow one of the common key management schemes, which are:

**1- Master/Session**

**2- DUKPT**

**[Master/Session]**

With master/session scheme, the acquirer generates a TMK [terminal master key] and a TPK [terminal PIN key] which is derived from TMK (this is sometimes called session key or working key).

The steps for Master/Session process are as follows:

- TMK is injected into PED and hardly changed, while TPK is dynamically exchanged between PED and acquirer [where TPK is always encrypted under TMK].

- When PED creates a PINBlock and want to send a transaction to the acquirer, the PED will first decrypt TPK under TMK to get the clear TPK, then using the clear TPK, PED will encrypt PINBlock (usually using triple DES encryption algorithm).

- PINBlock is transmitted encrypted to the acquirer [making the first Stop in its journey].

- having TMK & TPK, the acquirer will be able to translate PINBlock.

**[DUKPT] or [Derived Unique Key Per Transaction]**

While master/session sounds good, yet a compromised TPK [session key] will compromise all subsequent transactions which use this key.

In this case, the strength of DUKPT appears, The strength of DUKPT as an algorithm is its ability to generate unique keys for every transaction, so if an encryption key [session key] is compromised, all subsequent transactions will be safe as it uses a different key.

The steps for DUKPT process are as follows:

- The algorithm starts with an initial single key or base derivation key BDK. BDK is saved inside Tamper-Resistant security module or HSM at the acquirer side.

- Then a key is derived from the DBK along with the PED’s own unique Key Serial Number (KSN), this key will be known as initial pin encryption key [IPEK].

- IPEK is injected into the PED.

- IPEK creates another set of keys [pool of future keys], then IPEK itself is discarded.

- At this point we have three levels of keys.

- DBK, the one and only [inside acquirer HSM].

- IPEK, one per device [initially injected to device then discarded after generating future keys].

- Future keys [session keys], up to 21 key generated from IPEK which will actually be used for encryption.

- One of the future keys are used to encrypt the PINBlock [one can argue that this is currently the TPK or the session key] (usually using triple DES encryption algorithm).

- The process of encryption will also involve creating a key serial number [KSN] which is formed from PED unique id [terminal ID] and PED transaction counter.

- PED then increment the transaction counter, discard the key just used, and generate more future keys.

- PINBlock is transmitted encrypted to the acquirer along with the new KSN [making the first Stop in its journey].

- having DBK & KSN, the acquirer will be able regenerate the IPEK and goes through a similar process as PED to regenerate the session key.

- Finally, the acquirer will be able to translate PINBlock.

The first stop in our journey is now completed, our next and final article will talk about moving the PINBlock between institutions [zones] all the way to the card issuer.

Stay tuned...

Link to the next article:

<https://www.linkedin.com/pulse/journey-pinblock-arrival-ahmed-hemdan-farghaly/>

**Abbreviations**

**PIN**: personal identification number

**PED**: pin entry device

**Acquirer**: bank or payment institution which accept card payment

**Issuer**: bank or payment institution which manage the cardholder account

**DUKPT**: Derived Unique Key Per Transaction

**TMK**: Terminal Master Key

**TPK**: Terminal PIN Key

**BDK**: Base Derivation Key

**HSM**: Host Security Module

**KSN**: Key Serial Number

**IPEK**: Initial Pin Encryption Key