Sunmi Key Loading Device Key Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Content** | **Write** | **Review** |
| V1.0.0 | Jun 23 | Create Doc | Ack | Bruce |
| V1.0.1 | Aug 18 | 1．Add Transport Key on USB | Bruce | Ack |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1. Key Descriptions on RKEK 3](#_Toc48839936)

[2. Key Descriptions on MKEK 3](#_Toc48839937)

[3. Key Descriptions on KEK 3](#_Toc48839938)

[4. Transport Key on USB 3](#_Toc48839939)

[5. Device Transport 4](#_Toc48839940)

[6. Diagrams 5](#_Toc48839941)

# 1. Key Descriptions on RKEK

1.1 Root KEK is created by HSM in factory based on random number, key value is stored in HSM.

1.2 Root KEK will not be outside HSM, it can be derived, derived value injected to master POS with secure messaging within KIF.

1.3 Root KEK can be updated and relocated in secure messaging, authenticated and with integrity, protected by HSM management key.

# 2. Key Descriptions on MKEK

2.1 MKEK is derived on HSM by the customer ID and injected into terminals in production.

2.2 Each customer has its unique MKEK.

2.3 MKEK is encrypted by the public key of the Master POS and downloaded to the Master POS via local area network in secure room.

2.4 MKEK stored in hex with 128 bits.

2.5 MKEK in Master POS is protected by tamper proof area which is PCI-PTS certified.

# 3. Key Descriptions on KEK

3.1 KEK is derived on the Master POS by MKEK and the Target POS SN and random number.

3.2 Each Target POS has its unique KEK.

3.3 KEK is encrypted by the public key of the Target POS and download to the Target POS via USB.

3.4 KEK length is 128 bits, stored in hex with index and checksum, resided in terminal's tamper detected area which is PCI-PTS certified.

# 4. Transport Key on USB

For data privacy between Master POS and Target POS, each Target POS will create a pair of 2048-bit RSA key at production floor, at start session of LKI, Target POS will send public key to Master POS, and the data packets from Master POS will be encrypted using this public key, and Target POS will decrypt the data packets using its private key accordingly.

# 5. Device Transport

5.1 Master POS is delivered to customer with tamper evidence package with trace number.

5.2 Key injection dual control cards are shipped by separate package from Master POS package.

# 6. Diagrams

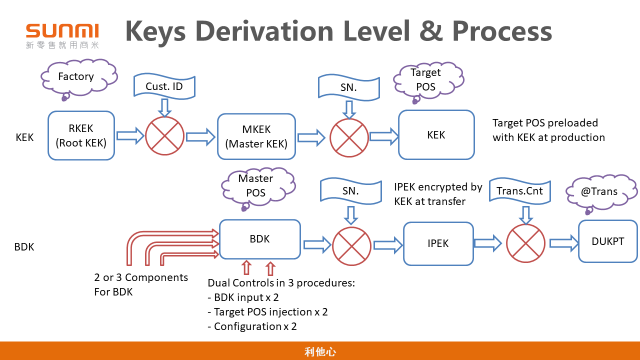
****

Diagram 1, Key Layers-1

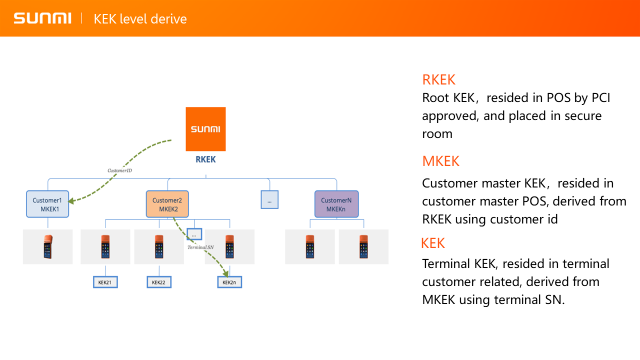
****

Diagram 2, Key Layers-2

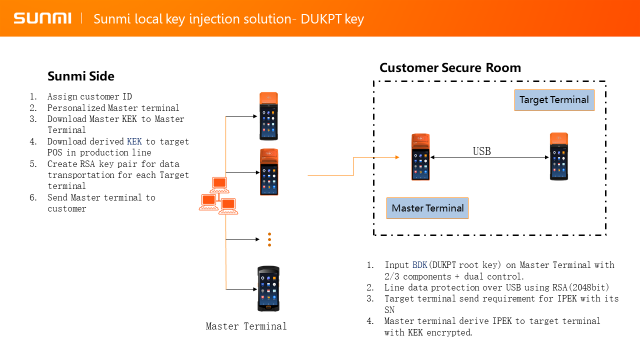
****

Diagram 3, Facilities and Roles