E-wallet CPU card and PSAM card consumption key loading analysis

原创 There is no love in life, but you can ... Posted on 2016-12-20 11:26:29 Reading: 4.6k Collection 10 Likes

Category Column: Financial terminal applications

1. Distinguish the consumption key under an ADF in the PSAM card

Different consumer keys are installed based on the key version number, and the key version of the consumer key in the CPU card must be the same as that in the PSAM card

There is also the algorithm logo

00-3DES

01-DES

02-255 reserved

Note: The key version of a consumption key identifies the key version during consumption, and the key versions of other keys are used as key identifiers.

2. Set the purpose of the key in the PSAM card

The upper 3 bits are the dispersed secret level, and the lower 5 bits are the key type

The primary dispersion is 0x01<<5 = 0x20 and the consumption key is 0x02, so the key purpose should be

0x20|0x02 = 0x22

The key purpose of the second-level decentralized consumption key should be 0x40|0x02 = 0x42

The key usage of the third-level decentralized consumption key should be 0x60|0x20 = 0x62

Note:1At least once key dispersion is required in the PSAM card when consumption, and I have always wanted to ..... unsuccessfully without dispersion

2. The secret level of the consumer key should correspond to the LC in the MAC1 command

Secret level=1, Lc=0x14 + 1*8

Secret level=2, Lc=0x14 + 2*8

Secret level=3, Lc=0x14 + 3*8

Of course, in order to obtain the data fields in the MAC1 command, the corresponding dispersion factors should be added in order

3. Load the consumption key in the PSAM card

When the consumer key is loaded on the PSAM card, the consumer key under the current application should be used to encrypt the consumer key and calculate the MAC address

Eg:

84 D4 0000 1C

CLA INS P1 P2 Lc

All the data behind the LC is encrypted by DES, and then the encrypted data is spliced with the command

Perform MAC address calculation on the concatenated command, where the length of Lc is the length of the encrypted data + 4

DATA field data: 22 00 00001122334455667788 99aabbccddeeff

Encrypt DATA with 3DES, process it a little before encrypting, add the plaintext length, and make up 80 00 for less than 8 bytes in chunks...

Command line encryption protection calculation:

3DES-ECB mode

Processed data:

13 22 0000 00112233445566778899aabbccddeeff 80 00 00 00

0x13 is the length of data to be encrypted in the plaintext of 62-FF, 19 pieces

80 00 00 00 is a supplement to the data to be encrypted, as it is less than 8 bytes after the chunk

22 is the key usage, 6 is the decentralized series, and 2 is the key type-consumption

00 00 is the key version and algorithm identifier

00112233445566778899aabbccddeeff The clear text of the key to add

Key: 00112233445566778899aabbccddeeff (Master Key under the current application)

Result: DCC0BB5793ABFCA2CA8C1624822F6E01A86A0B5CBED191DD (data after data domain encryption)

MAC-CBC Mode-DES

Initial vector**:** 5d 72 b3 fd 000000000 (5d 72 b3 fd 4-byte random number obtained from the card).

Processing data: 84D400001CDCC0BB5793ABFCA2CA8C1624822F6E01A86A0B5CBED191DD

Key: 00112233445566778899aabbccddeeff (Master Key under the current application)

Result: 8A9D4ADB

Full command

84D400001CDCC0BB5793ABFCA2CA8C1624822F6E01A86A0B5CBED191DD8A9D4ADB

4. The key in the CPU card

In this case, the key in the CPU card should be the key after dispersion

Key Dispersion Algorithm:

Note: The key loaded in the PSAM card is dispersed one by one to the dispersion factor, and the specific number of dispersions is determined according to the dispersion level when the key is loaded in the PSAM card

1. The key (the key loaded in the PSAM card or the key after the last dispersion) is used as the left 8 bytes of the new dispersion key by 3DES encryption of the 8-byte dispersion factor

2. The key (the key loaded in the PSAM card or the key after the last dispersion) is used as the right 8 bytes of the new dispersion key after the 8-byte dispersion factor is inverted by 3DES encryption

3. Splice the left and right 8 bytes obtained in the above two steps to form a new 16-byte dispersed key

4. If there is a lower level of dispersion, use the newly obtained dispersion key as the key to encrypt the dispersion factor

Repeat the above three steps.

Eg:

Purpose: Load the consumption key into the PSAM card and disperse the serial number of the user card at the first level during consumption

It can be consumed with the CPU card that is equipped with the corresponding key

The consumption key in the PSAM card is: 00112233445566778899aabbccddeeff

Dispersion factor: 8-byte card application serial number 122334455667788

DPK left half

Card application serial number: 1122334455667788

Key: 00112233445566778899aabbccddeeff

Result: 496BD7A351364453

Right half of the DPK

Card application serial number negation: eeddccbbaa998877

Key: 00112233445566778899aabbccddeeff

Result: 3100B54E71196528

Final result: 496BD7A3513644533100B54E71196528

LOAD COMMAND: 80D40000153EF0F20000496BD7A3513644533100B54E71196528

Note: Whether other verification is done before the key is loaded depends on the added permissions when the key file is created

At this time

The consumption key in the PSAM card is: 00112233445566778899aabbccddeeff

The consumption key in the CPU card is: 496BD7A3513644533100B54E71196528