Set up a simple test PBOC payment environment on the FMCOS CPU card

原创 robur 于 2024-04-11 22:36:28 发布 阅读量1k 收藏 18 点赞数 17 版权
分类专栏： RFID 文章标签： FMCOS CPU卡 PBOC 电子钱包 圈存

The purpose of this article is to quickly build a simple payment environment to facilitate the storage and consumption test of e-wallets. As a result, many data files and security mechanisms are omitted.

Do not use this test payment environment in a production system, as it may pose a significant security risk.

Establish an easy test PBOC payment environment

at the root（3F00）下建立应用目录3F01

```
80 E0 3F 01 0D 38 08 00 F0 F0 95 FF FF 11 22 33 44 55
```

Select Application Catalog 3F01

```
00 A4 00 00 02 3F 01 00
```

Create a key file

```
80 E0 00 00 07 3F 01 8F 95 F0 FF FF
```

Add an external authentication key

```
80 D4 01 00 0D 39 F0 F0 AA FF 11 22 33 44 55 66 77 88
```

Add a consumption key

```
80 D4 01 00 15 3E F0 F0 00 01 3E 3E 3E 3E 3E 3E 3E 3E 11 22 33 44 55 66 77 88
```

Add a captive key

```
80 D4 01 00 15 3F F0 F0 00 01 3F 3F 3F 3F 3F 3F 3F 3F 11 22 33 44 55 66 77 88
```

Add a DTK/TAC key

```
80 D4 01 00 15 34 F0 F0 00 01 34 34 34 34 34 34 34 34 11 22 33 44 55 66 77 88
```

Add a password key（PIN）

```
80 D4 01 00 07 3A F0 EF AA FF 12 34
```

Create transaction record file 0018

```
80 E0 00 18 07 2E 0A 17 F0 EF FF FF
```

Create e-wallet file 0002

```
80 E0 00 02 07 2F 02 08 F0 00 FF 18
```

A simple test payment environment has been set up.

Deposit the e-wallet

Read the balance

> Rdr: 80 5C 00 02 04
> Tag: 00 00 00 00 [90 00] The command was executed successfully

It can be seen that the current balance is 0.

Verification Password (PIN)

> Rdr: 00 20 00 00 02 12 34
> Tag: [90 00] The command was executed successfully

For e-wallets, the lapping operation enforces the verification of the PIN. You can read the balance and spend without verifying the PIN.

Trap initialization

> Rdr: 80 50 00 02 0B 【00】【00 00 00 10】【66 66 66 66 66 66】10
> Tags: 【00 00 00 00】【00 00】【00】【01】【4E 06 65 48】【0D 39 AD BB】[90 00] The command was executed successfully

The valid data sent by the card reader is as follows: the key identification, the transaction amount, and the terminal number

The valid data of the card reply are: old balance, online transaction serial number, key version, algorithm identification, random number, and MAC1

Computation of the process key

will be a random number（4E 06 65 48）、The online transaction serial number（00 00）and padding bytes（80 00）The complete data of the composition4E 06 65 48 00 00 80 00，Encrypt with a captive key to get a "process key"：3B 75 C7 9C FA 8C 23 27

MAC1 COMPUTE

The old balance（00 00 00 00）、The amount of the transaction（00 00 00 10）、The type of transaction（02）and the terminal number（66 66 66 66 66 66）The complete data of the composition00 00 00 00 00 00 00 10 02 66 66 66 66 66 66，Calculated using the Process KeyMAC，getMAC1：0D 39 AD BB。

Note: Transaction type 02 indicates e-wallet; 01 indicates an electronic passbook.

Captivity

> Rdr: 80 52 00 00 0B 【20 24 04 11】【21 21 21】【09 7E 98 FE】04
> Tag: 【A8 02 86 3E】[90 00] 命令执行成功

The valid data sent by the card reader is in order: transaction date, transaction time, and MAC2

Valid data for card response is: Transaction Verification Code (TAC)

MAC2 COMPUTE

The amount of the transaction（00 00 00 10）、The type of transaction（02）、Terminal number（66 66 66 66 66 66）、The date of the transaction（20 24 04 11）and trading hours（21 21 21）The complete data of the composition，00 00 00 10 02 66 66 66 66 66 66 20 24 04 11 21 21 21，Calculated using the Process KeyMAC，getMAC2：09 7E 98 FE

Calculation of Transaction Verification Code (TAC).

Replace the new balance (old balance00 00 00 00 + The amount of the transaction00 00 00 10 = 00 00 00 10）、The online transaction serial number（00 00）、The amount of the transaction（00 00 00 10）、The type of transaction（02）、Terminal number（66 66 66 66 66 66）、The date of the transaction（20 24 04 11）and trading hours（21 21 21）Composition of complete data：00 00 00 10 00 00 00 00 00 10 02 66 66 66 66 66 66 20 24 04 11 21 21 21。

XOR the left and right (high and low) 8 bytes of the DTK/TAC key, ie34 34 34 34 34 34 34 34 XOR 11 22 33 44 55 66 77 88. XOR is performed to obtain the key used to calculate TAC：25160770615243BC。Use this key to pair the full data obtained earlier（00 00 00 10 00 00 00 00 00 10 02 66 66 66 66 66 66 20 24 04 11 21 21 21）The MAC is computed to obtain the TAC：A8 02 86 3E

Read the balance again

> Rdr: 80 5C 00 02 04
> Tag: 00 00 00 10 [90 00] 命令执行成功

Read the transaction history

> Rdr: 00 B2 01 C4 00
> Tag: 00 01 00 00 00 00 00 00 10 02 66 66 66 66 66 66 20 24 04 11 21 21 21 [90 00] 命令执行成功