FIRST TECH®

Construindo relações duradouras

Smartcards Autorization Oficcer

MATRIZ: Av. Angélica, 2248 - 4º andar
Higienópolis · São Paulo · SP
Fone: **11 3024-3200**

FILIAL: Rua da Quitanda, 60
12º andar - Centro - RJ
Fone: **21 3543-1650**

first-tech.com
ACOMPANHE A FIRST
company/first-tech/

FIRST TECH®
Construindo relações duradouras

Índice

1. LMK

O exemplo abaixo mostra o processo de criação e gravação dos componentes de uma LMK do tipo Key Block AES. A aglutinação desses componentes forma a LMK.

1.1. Formatar

Formatação dos smartcards para receber a LMK.

```
Online>fc

Insert card and press ENTER:
Card already formatted; continue? [Y/N]: y
Format card for HSM SETTINGS/LMKs/KTKs? [H/L/K]: l
    Erasing card
    Formatting card...
Enter new PIN for smartcard: *****
Re-enter new PIN: *****
Enter time [hhmmss]: 104010
Enter date [DDMMYY]: 130421
Enter User ID: ft
Enter Issuer ID: ft

Format complete
```

```
Online>fc

Insert card and press ENTER:
Card already formatted; continue? [Y/N]: y
Format card for HSM SETTINGS/LMKs/KTKs? [H/L/K]: l
    Erasing card
    Formatting card...
Enter new PIN for smartcard: *****
Re-enter new PIN: *****
Enter time [hhmmss]: 104210
Enter date [DDMMYY]: 130421
Enter User ID: ft
Enter Issuer ID: ft

Format complete
```

```
Online>fc

Insert card and press ENTER:
Format card for HSM SETTINGS/LMKs/KTKs? [H/L/K]: l
    Erasing card
    Formatting card...
Enter new PIN for smartcard: *****
Re-enter new PIN: *****
Enter time [hhmmss]: 105810
Enter date [DDMMYY]: 130421
Enter User ID: ft
Enter Issuer ID: ft

Format complete
```

1.2. Criar

Processo de criação dos componentes da LMK. Os componentes são criados e gravados nos smartcards.

```
Secure>gk

Variant scheme or keyblock scheme? [V/K]: k
Enter algorithm type [D=DES, A=AES]: a
Enter the number of components to generate: [2-9]: 3
Enter the number of components required to reconstitute the LMK: [2-3]: 2
Key status? [L/T]: l

Check value for the LMK: 185FC6
Insert blank card and enter PIN: *****
    Writing keys...
    Checking keys...
Device write complete, check: 18958D

Insert blank card and enter PIN: *****
    Writing keys...
    Checking keys...
Device write complete, check: DE6FAF

Insert blank card and enter PIN: *****
    Writing keys...
    Checking keys...
Device write complete, check: 6D9B85
```

1.3. Carregar

Depois de criados os smartcards com os componentes da LMK, o próximo passo é o processo de carregamento da LMK no HSM.

```
Secure>lk

Enter LMK id [0-1]: 0
Enter comments: key block

Load LMK from components or shares
Insert card and press ENTER:

Enter PIN: *****
Check: 18958D

Insert card and enter PIN: *****
Check: DE6FAF

LMK Check:      185FC6
LMK id:         00
LMK key scheme: KeyBlock
LMK algorithm:  AES-256
LMK status:     Live
Comments:       key block

Confirm Details? [Y/N]: y

Use the LO/LN command to load LMKs into key change storage.
```

2. Autorization Oficcer - Console

2.1. Formatar

Processo de formatação dos dois smartcards que serão utilizados como Authorization Office.

```
Secure>fc

Insert card and press ENTER:
Format card for HSM SETTINGS/LMKs/KTKs? [H/L/K]: l
    Erasing card
    Formatting card...
Enter new PIN for smartcard: *****
Re-enter new PIN: *****
Enter time [hhmmss]: 133513
Enter date [DDMMYY]: 130421
Enter User ID: ft
Enter Issuer ID: ft

Format complete
```

```
Secure>fc

Insert card and press ENTER:
Card already formatted; continue? [Y/N]: y
Format card for HSM SETTINGS/LMKs/KTKs? [H/L/K]: l
    Erasing card
    Formatting card...
Enter new PIN for smartcard: *****
Re-enter new PIN: *****
Enter time [hhmmss]: 133613
Enter date [DDMMYY]: 130421
Enter User ID: ft
Enter Issuer ID: ft

Format complete
```

2.2. Criar

Use o Comando: CO cuja função é copiar a senha de um authorizing officer para outro smartcard de HSM comum (os RLMKs (Smartcards payShield manager com componentes LMK) são suportados) são usados para colocar o HSM no estado autorizado. Observe que apenas LMK dos smartcards de componentes 1 e 2 contêm a senha, portanto para cópia deve ser copiado dos componentes 1 e 2.

```
Secure>co

Insert card for component or share set 1 or 2 and press ENTER:
Enter PIN: *****
Insert card for authorizing officer and enter PIN: *****

Copy complete
```

```
Secure>co

Insert card for component or share set 1 or 2 and press ENTER:
Enter PIN: *****
Insert card for authorizing officer and enter PIN: *****

Copy complete
```

2.3. Autorizar

Exemplo da utilização dos smartcards do Autorization Office no processo de autorizar a utilização dos comandos de “admin”.

```
Secure>a

Enter LMK id [0-1]: 0

No activities are authorized for LMK id 00.

List of authorizable activities:
generate   genprint   component  import
export     pin        audit      admin
diagnostic misc       command

Select category: admin

host       console

Select interface or <Return> for all:

Enter time limit for admin, or <Return> for permanent:

Console authorizations will expire in 720 minutes (12 hours).

Make host activity persistent? [Y/N]: y

Enter additional activities to authorize? [Y/N]: n

The following activities are pending authorization for LMK id 00:

admin..console:720
admin..host:persistent

First officer:
Insert card and press ENTER:
Enter PIN: *****

Second officer:
Insert card and press ENTER:
Enter PIN: *****

The following activities are authorized for LMK id 00:

admin..console:720  (720 mins remaining)
admin..host:persistent
```

3. Autorization Oficcer via payShield Manager

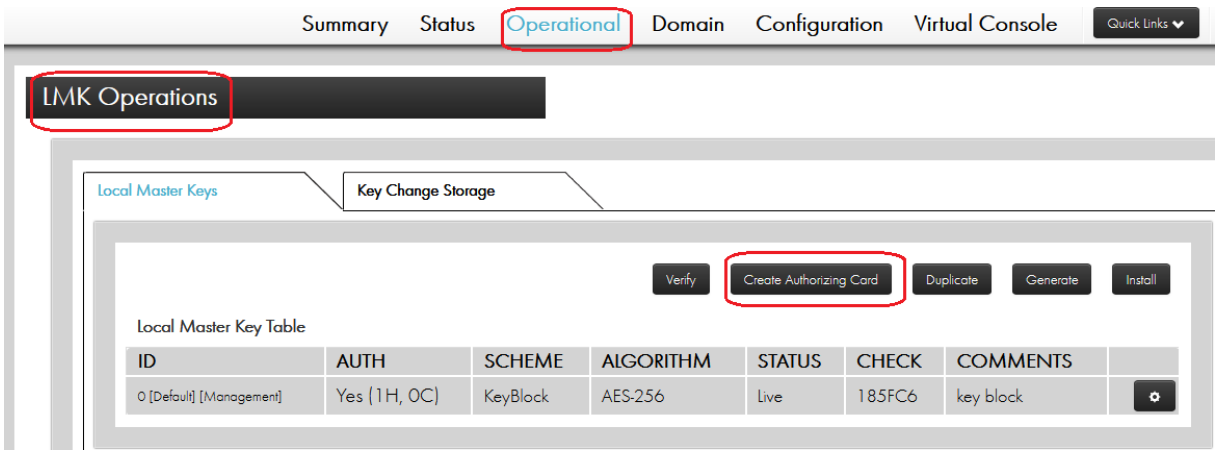
3.1. Pré Requisitos

Ter os smartcards novos comissionados para transformar em autorization Oficcer pelo payshild manager.

Ter a RLMK que são os componentes da LMK divididos em smartcard do payShield manager.

3.2. Criar

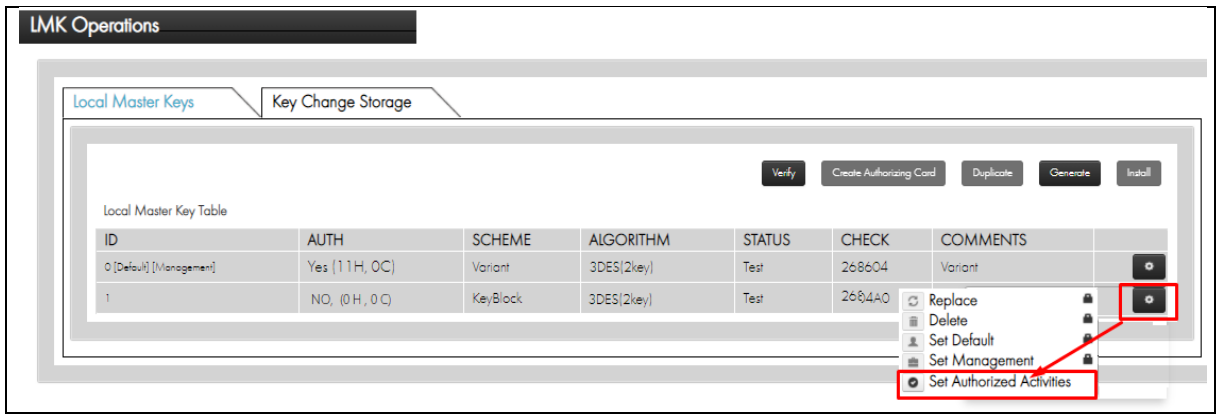
Após acionar o Create Autorizing Card coloque o Smartcard payShield manager RLMK com componente 1 após carregar retire o Smartcard.

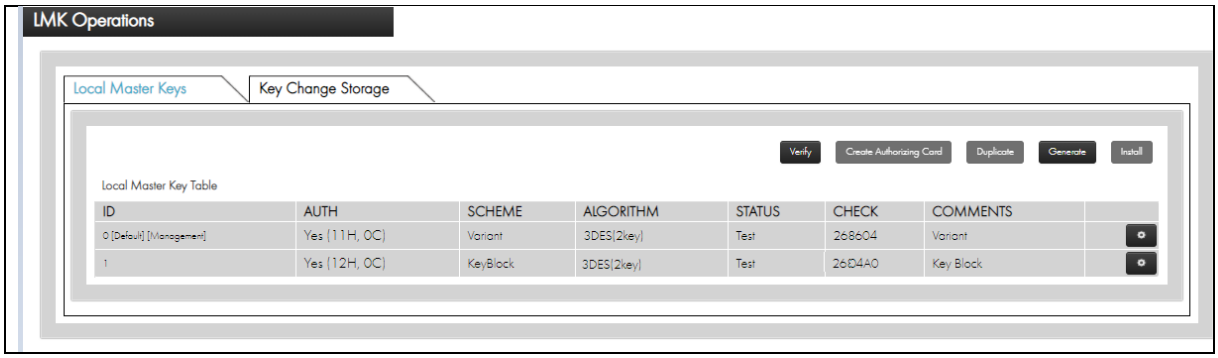


Coloque o smartcard payShield Manager comissionado para receber o componente 1. Repetir o processo para o componente 2.

3.3. Autorizar

Estado autorizado é um modo de operação do HSM que permite um ou mais funções sensíveis possam ser executados. São necessários dois Authorizing Officers para confirmar a atividade usando seus smartcards e PINs.




LMK Operations
Local Master Keys
Key Change Storage
Verify
Create Authorizing Card
Duplicate
Generate
Install
Local Master Key Table
ID
AUTH
SCHEME
ALGORITHM
STATUS
CHECK
COMMENTS
0 [Default] [Management]
Yes (11H, 0C)
Variant
3DES(2key)
Test
268604
Variant
1
Yes (12H, 0C)
KeyBlock
3DES(2key)
Test
261D4A0
Key Block

4. Release Notes

Autor	Descrição	Data
Caio Ferreira	Primeira versão	13/04/2021
Bruno Araujo	Inclusão de texto e revisão	14/04/2021