.

**payShield Manager - GETNET**

Índice

[1. Arquitetura de Smartcards 3](#_Toc69198912)

[1.1. Comando FC (Format Card) para LMK 3](#_Toc69198913)

[2. Criar LMK Key Block 3DES 4](#_Toc69198914)

[3. Decommission (formatar smartcards payShield manager) 5](#_Toc69198915)

[4. Comission (comissionamento de smartcard payShield manager) 5](#_Toc69198916)

[5. Transfeir a LMK dos smartcards de HSM para os smartcards do payShield manage 6](#_Toc69198917)

[6. Adicionar os novos smartcards na whitelist de todos os equipamentos 7](#_Toc69198918)

[7. Adicionar SmartCard via payShield Manager 8](#_Toc69198919)

[8. Remoção de LMK 10](#_Toc69198920)

[9. Instalação de uma nova LMK 11](#_Toc69198921)

[10. Autorização da nova LMK 13](#_Toc69198922)

[11. Release Notes 13](#_Toc69198923)

# Arquitetura de Smartcards

A arquitetura de smartcards aqui apresentada visa a segmentação de funções bem como a hierarquização das permissões de uso do equipamento.

## Comando FC (Format Card) para LMK

Nesta etapa, os smartcards serão formatados. O processo abaixo deve ser executado com 04 smartcards para criação da LMK Key Block 3DES nos smartcards HSM.

* 2 principais
* 2 copias

|  |
| --- |
| ***SMARTCARD HSM 1 – COMPONENTE 1***  Secure-AUTH>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]: [000000]  Enter date [DDMMYY]: [110421]  Enter User ID: [LMK COMPONENTE 1]  Enter Issuer ID: [GETNET] |

|  |
| --- |
| ***SMARTCARD HSM 2 – COMPONENTE 1 COPIA***  Secure-AUTH>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]: [000200]  Enter date [DDMMYY]: [110421]  Enter User ID: [LMK COMPONENTE 1 COPIA]  Enter Issuer ID: [GETNET] |

|  |
| --- |
| ***SMARTCARD HSM 3 – COMPONENTE 2***  Secure-AUTH>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]: [000400]  Enter date [DDMMYY]: [110421]  Enter User ID: [LMK COMPONENTE 2]  Enter Issuer ID: [GETNET] |

|  |
| --- |
| ***SMARTCARD HSM 4 – COMPONENTE 2 COPIA***    Secure-AUTH>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]: [000000]  Enter date [DDMMYY]: [110421]  Enter User ID: [LMK COMPONENTE 2 COPIA]  Enter Issuer ID: [GETNET] |

# Criar LMK Key Block 3DES

O exemplo abaixo mostra a criação de componentes de uma LMK Key Block 3DES e a gravação dos componentes no respectivos smartcards, processo de cópia por componente.

A aglutinação desses componentes forma a LMK Key Block 3DES.

|  |
| --- |
| Secure> **GK** *<Return>*  Variant scheme or key block scheme? [V/K]: **K** *<Return>*  Enter algorithm type [D=DES,A=AES]: **D**  Key status? [L/T]: **L** *<Return>*  LMK component set [1-9]: **1** *<Return>*  Enter secret value A: *<Return>*  Enter secret value B: *<Return>*  Enter secret value C: *<Return>*  ***SMARTCARD HSM 1 – COMPONENTE 1***  Insert blank card and enter PIN: **\*\*\*\*\*\*\*\*** *<Return>*  Writing keys...  Checking keys...  Device write complete, check: ZZZZZZ  Remova o Smartcard e armazene-o com segurança.  Make another copy? [Y/N]: Y *<Return>*  1 copies made.  ***SMARTCARD HSM 2 – COMPONENTE 1 COPIA***  Insert blank card and enter PIN: **\*\*\*\*\*\*\*\*** *<Return>*  Writing keys...  Checking keys...  Device write complete, check: ZZZZZZ  Repita o procedimento para gerar os demais componentes.  Secure> **GK** *<Return>*  Variant scheme or key block scheme? [V/K]: **K** *<Return>*  Enter algorithm type [D=DES,A=AES]: **D**  Key status? [L/T]: **L** *<Return>*  LMK component set [1-9]: **2** *<Return>*  Enter secret value A: *<Return>*  Enter secret value B: *<Return>*  Enter secret value C: *<Return>*  ***SMARTCARD HSM 3 – COMPONENTE 2***  Insert blank card and enter PIN: **\*\*\*\*\*\*\*\*** *<Return>*  Writing keys...  Checking keys...  Device write complete, check: ZZZZZZ  Make another copy? [Y/N]: Y *<Return>*  1 copies made.  ***SMARTCARD HSM 4 – COMPONENTE 2 - COPIA***  Insert blank card and enter PIN: **\*\*\*\*\*\*\*\*** *<Return>*  Writing keys...  Checking keys...  Device write complete, check: ZZZZZZ |

# Decommission (formatar smartcards payShield manager)

Essa etapa consiste em descomissionar os 04 smartcards para limpeza de algum possível conteúdo (usar se o Smartcard estiver sendo reutilizado)

* 2 principais
* 2 copias

|  |
| --- |
| Secure> XX <Return>  Please insert card to decommission and press ENTER: <Return>  Warning: Resetting a payShield Manager Smartcard to its original state  will erase all key material from the card.  Are you sure? [Y/N]: Y <Return>  payShield Manager Smartcard successfully decommissioned  Would you like to decommission another card? [Y/N]: N <Return>  Secure>  ***Repita o procedimento para os demais smartcards.*** |

# Comission (comissionamento de smartcard payShield manager)

Essa etapa consiste em comissionar os 4 smartcards payshield Manager.

Será utilizado o conjunto de CTA’s que compõe o grupo que representa a Confiança do Cliente. Estes smartcards também funcionam como certificados e permitem a inclusão de mais smartcards no domínio criptográfico operacional (domínio do payShield Manager).

* 2 principais
* 2 copias

|  |
| --- |
| Secure-AUTH>xr  Please have all Customer Trust Anchor (CTA) payShield Manager smartcards available  Insert first **CTA payShield Manager** Smartcard and press ENTER:  Enter PIN: \*\*\*\*\*\*  Insert **CTA payShield Manager** Smartcard 2 of 3 and press ENTER:  Enter PIN: \*\*\*\*\*\*  Insert **CTA payShield Manager** Smartcard 3 of 3 and press ENTER:  Enter PIN: \*\*\*\*\*\*  ***# LEFT – 1 - smartcard payShield manager 1***  Enforce a PIN change on first use? [Y/N]: n  Insert a payShield Manager Smartcard to be commissioned and press ENTER:  Enter new PIN for smartcard: \*\*\*\*\*\*  Re-enter new PIN: \*\*\*\*\*\*  Do you wish to add the smartcard 7356006342073196 to the HSM whitelist [Y/N]: y  Assign smartcard as a Left or Right Key RACC? [L/R/N]: L  Would you like to commission another card? [Y/N]: y  ***# RIGHT – 2 smartcard payShield manager 2***  Enforce a PIN change on first use? [Y/N]: n  Insert a payShield Manager Smartcard to be commissioned and press ENTER:  Enter new PIN for smartcard: \*\*\*\*\*\*  Re-enter new PIN: \*\*\*\*\*\*  Do you wish to add the smartcard 7356006350073196 to the HSM whitelist [Y/N]: y  Assign smartcard as a Left or Right Key RACC? [L/R/N]: R  Would you like to commission another card? [Y/N]: y  ***# LEFT – 1 - smartcard payShield manager 3***  Enforce a PIN change on first use? [Y/N]: n  Insert a payShield Manager Smartcard to be commissioned and press ENTER:  Enter new PIN for smartcard: \*\*\*\*\*\*  Re-enter new PIN: \*\*\*\*\*\*  Do you wish to add the smartcard 7356006327073196 to the HSM whitelist [Y/N]: y  Assign smartcard as a Left or Right Key RACC? [L/R/N]: L  Would you like to commission another card? [Y/N]: y  ***# RIGHT – 2 - smartcard payShield manager 4***  Enforce a PIN change on first use? [Y/N]: n  Insert a payShield Manager Smartcard to be commissioned and press ENTER:  Enter new PIN for smartcard: \*\*\*\*\*\*  Re-enter new PIN: \*\*\*\*\*\*  Do you wish to add the smartcard 7356006360073196 to the HSM whitelist [Y/N]: y  Assign smartcard as a Left or Right Key RACC? [L/R/N]: R  Would you like to commission another card? [Y/N]: N |

# Transfeir a LMK dos smartcards de HSM para os smartcards do payShield manage

|  |
| --- |
| Secure>xt  Please have all the local LMK components and enough commissioned RACCs to receive the LMK ready.  Insert card and press ENTER:  ***SMARTCARD 1 – COMPONENTE 1***  ***SMARTCARD 3 – COMPONENTE 2***  **Ou as copias**  Enter PIN: [**\*\*\*\*\***]  Check: ZZZZZZ  Load more components? [Y/N]: [**n**]  LMK Check: ZZZZZZ  LMK key scheme: Keyblock  LMK algorithm: 3DES(2key)  LMK status: Test  Is this the LMK you wish to transfer? [Y/N]: [**y**]  Enter the number of shares to split the LMK into: [2-9]: [4]  Enter the number of shares required to reconstitute the LMK: [4-2]: [**2**]  ***smartcard payShield manager 1***  Insert a commissioned card 1 of 4 and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Card Check: 14A6E8  LMK share written to smartcard.  ***smartcard payShield manager 2***  Insert a commissioned card 2 of 4 and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Card Check: A895E9  LMK share written to smartcard.  ***smartcard payShield manager 3***  Insert a commissioned card 3 of 4 and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Card Check: B855E3  LMK share written to smartcard.  ***smartcard payShield manager 4***  Insert a commissioned card 4 of 4 and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Card Check: C855B9  LMK share written to smartcard  Want to test the reassembly of the LMK? [Y/N]: [**n**] |

Será iniciado o processo de divisão da LMK local nos smartcards de PayShield Manager, assim criando nos smartcards de acesso o carregamento da LMK remota, use o comando XT (Transfer Existing LMK to RLMK).

# Adicionar os novos smartcards na whitelist de todos os equipamentos

A *whitelist* dos smartcards de acesso é a lista que enumera e indica quais os smartcards estão permitidos a acessar determinado equipamento.

Cada smartcard tem seu próprio serial number e após comissionado recebe a numeração de certificado. O comissionamento dos smartcards de acesso é feito pelo conjunto de smartcards CTA.

Os smartcards na whitelist podem ser removidos ou inseridos mediante a presença dos custódios dos smartcards chave esquerda e chave direita colocando o HSM no modo Secure. Cada HSM tem sua própria whitelist, ou seja, cada uma deve ser configurada individualmente em cada equipamento.

Use o comando XY para obter lista com serial number e a numeração de certificado, salve essa lista para adicionar os smartcards na whitelist individualmente em cada equipamento.

|  |
| --- |
| Secure>xy  Thales Trust installed : Yes  1 - Issued to: B4665310361O, Issued by: HSMKEY  Validity : Aug 18 11:50:28 2020 GMT to Aug 12 11:50:28 2045 GMT  Unique ID: DD50CD57E5F5602CFC500D839A49ECB6 - 5DDD8FCB  Customer Trust Anchor Installed : Yes  2 - Issued to: ft, Issued by: ft  Validity : Aug 18 10:16:33 2020 GMT to Aug 12 10:16:33 2045 GMT  Unique ID: F1D8033575B1DF91AF94A1F7E8BBFC9A - E22398C5 (Root)  HSM Public Key Certificate Installed : Yes  3 - Issued to: B4665310361O, Issued by: ft  Validity : Aug 18 11:58:18 2020 GMT to Aug 12 11:58:18 2045 GMT  Unique ID: ACCE079E52272AB28CD3B09173F9289C - E22398C5  Is HRK passphrase user defined : Yes  Is HRK available for use : Yes  Authorized RACCs : 4  Serial Number Certificate Number RACC Type  7307004059072979 1210C4CD0F312F52 right key  7307004132072979 27C7D56A28670A93 left key  7307004059172979 1210C4CD0F312F52 right key  7307004132172979 17C7D56A28670A91 left key |

# Adicionar SmartCard via payShield Manager

Acessar o payShield Manager com os smartcards Left e Right comissionados pelo comando XH Observação: O HSM deverá estar em modo on line para realizar o acesso:

Interface gráfica do usuário

Descrição gerada automaticamente

Acesso com os 2 smartcards left e Rigth (RACCs) que fazem parte do domínio criptográfico existente para poder incluir os novos na whitelist.

Utilize o boneco (login) do rodapé na imagem para confirmar os smarcards conectados modo online.

Interface gráfica do usuário

Descrição gerada automaticamente

Acessar a Aba Domain e depois em payShield Security Group.

Interface gráfica do usuário

Descrição gerada automaticamente com confiança média

Ao acessar irá apresentar a tela abaixo, primeiro adicione a informação do smartcard, para depois clicar no sinal “+” e logo em seguida clique em “Apply”, para adicionar novos smartcards:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

# Remoção de LMK

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamenteAcesso o payShield Manager e vá em Operational e LMK Operations.

A LMK a ser removida deverá estar em modo autorizado e o HSM em modo SEGURO: Clique na engrenagem da LMK a ser deletada e clique para deletar:

Interface gráfica do usuário

Descrição gerada automaticamente

Confirme a exclusão:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

# Instalação de uma nova LMK

Para instalar uma nova LMK clique em Install:

Interface gráfica do usuário

Descrição gerada automaticamente com confiança baixa

Escolha o ID a ser instalado e digite os comentários da LMK e clique em Next:

Interface gráfica do usuário

Descrição gerada automaticamente

Será solicitado o primeiro smartcard, insira e digite a senha quando necessários:

Uma imagem contendo Teams

Descrição gerada automaticamente

Se necessário será solicitado o segundo smartcard:

Interface gráfica do usuário

Descrição gerada automaticamente

Remova o smartcard e clique em OK.

Interface gráfica do usuário

Descrição gerada automaticamente com confiança média

# Autorização da nova LMK

* Entrar Estado Autorizado.

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

Em qualquer estado, você pode entrar no estado Autorizado clicando no botão próximo ao LMK que deseja autorizar e selecione “set authorized activities”.

Interface gráfica do usuário

Descrição gerada automaticamente

Dependendo do modo de autorização selecionado (autorização única ou multi-autorização) do configurações iniciais de segurança, você começará a entrar no estado autorizado (em uma única modo de autorização) ou ser apresentado com um menu de atividades autorizadas (no modo de multiautorização)..

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Bruno Araujo | Primeira versão | 11/04/2021 |
|  |  |  |