.

**payShield Manager - Cielo**

Índice

[1. Arquitetura de Cartões 3](#_Toc53129507)

[1.1. Domain Authority (DA) 3](#_Toc53129508)

[1.2. Customer Trust Anchor (CTA) 3](#_Toc53129509)

[1.3. Cartões de Acesso 3](#_Toc53129510)

[1.4. Whitelist 3](#_Toc53129511)

[2. Novo HSM 4](#_Toc53129512)

[2.1. Passphrase 4](#_Toc53129513)

[2.2. Certificado 4](#_Toc53129514)

[2.3. Reboot 4](#_Toc53129515)

[2.4. Comissionar o HSM 5](#_Toc53129516)

[2.5. Cartão Guest 5](#_Toc53129517)

[2.6. Resultado Final 6](#_Toc53129518)

[3. LMK e Clone 7](#_Toc53129519)

[3.1. LMK 7](#_Toc53129520)

[3.2. Clone 8](#_Toc53129521)

[3.2.1. Comissionar 8](#_Toc53129522)

[3.2.2. Clonar 10](#_Toc53129523)

[4. HSM de Produção 11](#_Toc53129524)

[4.1. Whitelist 12](#_Toc53129525)

[4.2. Guest para Direito/Esquerdo 13](#_Toc53129526)

[5. Release Notes 15](#_Toc53129527)

# Arquitetura de Cartões

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

## Domain Authority (DA)

Serão utilizados seis cartões que compõe o grupo que representa a Confiança pré Depositada do fabricante. Estes cartões funcionam como certificados e permitem a inclusão de mais equipamentos no domínio criptográfico operacional, ou seja, o domínio do payShield Manager.

## Customer Trust Anchor (CTA)

Serão utilizados seis cartões que compõe o grupo que representa a Confiança do Cliente. Estes cartões também funcionam como certificados e permitem a inclusão de mais equipamentos no domínio criptográfico operacional (domínio do payShield Manager) em conjunto com os cartões **DA**.

## Cartões de Acesso

Os cartões de acesso são criados durante o processo de inicialização do domínio criptográfico operacional e, após comissionados, permitem o acesso remoto nos equipamentos determinados. Existem 3 tipos de cartões de acesso:

* Chave Esquerda (LK)
* Chave Direita (RK)
* Guest (G)

Além das funções inerentes estes cartões podem ser portadores de componente de LMK.

## Whitelist

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

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

Os cartões na *whitelist* podem ser removidos ou inseridos mediante a presença dos custódios dos cartões 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.

# Novo HSM

## Passphrase

|  |
| --- |
| Secure>sk  \*\*\*\* NOTE \*\*\*\*  Passphrase rules as follows:  1 - Must be between 8 and 30 characters long.  2 - Can contain spaces  3 - Must be comprised of (at a minimum):  2 digits  2 uppercase characters  2 lowercase characters  2 symbols (e.g. !/?.#:')  Enter administrator 1 passphrase: \*\*\*\*\*\*\*\*  Re-enter administrator 1 passphrase: \*\*\*\*\*\*\*\*  Enter administrator 2 passphrase: \*\*\*\*\*\*\*\*  Re-enter administrator 2 passphrase: \*\*\*\*\*\*\*\*  Creating HRK. Please, wait ...  Successfully generated an HRK |

## Certificado

|  |
| --- |
| Secure>rh  Insert Domain Authority private key card and enter PIN: \*\*\*\*\*  Insert another Domain Authority private key card and enter PIN: \*\*\*\*\*  Insert another Domain Authority private key card and enter PIN: \*\*\*\*\*  Domain Authority parameters as follows  Issuer name: CertAuth  Signature algorithm: RSA  Hash algorithm: SHA-256  CA RSA key length: 2048  HSM RSA key length: 2048  CARD RSA key length: 2048  Public Exponent: 65537  Continue generating HSM Certificate using the above Domain Authority parameters [Y/N]:y  Generating HSM key pair ...  HSM certificate generated and stored  Reboot unit to complete installation of Thales Trust |

## Reboot

O HSM deve ser reinicializado utilizando o botão **vermelho** localizado na frente do HSM.

## Comissionar o HSM

|  |
| --- |
| Secure>xh  Please have all Customer Trust Anchor (CTA) payShield Manager  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 - A**  Starting the commissioning of the HSM process...  Please insert left key card and press ENTER:  Enter PIN: \*\*\*\*\*\*  **# RIGHT – A**  Please insert right key card and press ENTER:  Enter PIN: \*\*\*\*\*\*  Successfully commissioned HSM |

## Cartão Guest

|  |
| --- |
| Secure>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: \*\*\*\*\*\*  **# GUEST - A**  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 7356006465073196 to the HSM whitelist [Y/N]: y  Assign smartcard as a Left or Right Key RACC? [L/R/N]: n  Would you like to commission another card? [Y/N]: n |

## Resultado Final

|  |
| --- |
| Secure>xy  Thales Trust installed : Yes  1 - Issued to: B4665303299K, Issued by: HSMKEY  Validity : Sep 30 18:34:37 2020 GMT to Sep 24 18:34:37 2045 GMT  Unique ID: CAD47AB5EF5182BA0B9936C835CCA201 - 5DDD8FCB  Customer Trust Anchor Installed : Yes  2 - Issued to: ft.local, Issued by: ft.local  Validity : Sep 28 19:06:40 2020 GMT to Sep 22 19:06:40 2045 GMT  Unique ID: C057B4251B7BE792E4CD66FD12E4F3C3 - B58BF759 (Root)  HSM Public Key Certificate Installed : Yes  3 - Issued to: B4665303299K, Issued by: ft.local  Validity : Sep 30 18:36:32 2020 GMT to Sep 24 18:36:32 2045 GMT  Unique ID: DE24F7384451CDEC21C5BE2227FF7F7F - B58BF759  Is HRK passphrase user defined : Yes  Is HRK available for use : Yes  Authorized RACCs : 3  Serial Number Certificate Number RACC Type  7356006472073196 95B3331C7DE2B562 left key  7356006321073196 62C8CBE52FF0187F right key  7356006465073196 70D99B9FC7B64A3C guest |

# LMK e Clone

## LMK

Essa etapa consiste em inserir a LMK nos cartões Left/Hight/Guest previamente definidos nos comandos anteriores.

|  |
| --- |
| Secure>xt  Please have all the local LMK components and enough commissioned RACCs to receive the LMK ready.  Insert card and press ENTER:  Enter PIN: \*\*\*\*\*  Check: 516398  Load more components? [Y/N]: y  Enter PIN: \*\*\*\*\*  Check: 764074  Load more components? [Y/N]: y  Enter PIN: \*\*\*\*\*  Check: 330219  Load more components? [Y/N]: n  LMK Check: 602636  LMK key scheme: Variant  LMK algorithm: 3DES(2key)  LMK status: Live  Is this the LMK you wish to transfer? [Y/N]: y  Enter the number of shares to split the LMK into: [2-9]: 3  Enter the number of shares required to reconstitute the LMK: [2-9]: 3  Insert a commissioned card 1 of 3 and press ENTER:  Enter PIN: \*\*\*\*\*\*  Card Check: 94C627  LMK share written to smartcard.  Insert a commissioned card 2 of 3 and press ENTER:  Enter PIN: \*\*\*\*\*\*  Card Check: 1CFCC0  LMK share written to smartcard.  Insert a commissioned card 3 of 3 and press ENTER:  Enter PIN: \*\*\*\*\*\*  LMK share written to smartcard.  Want to test the reassembly of the LMK? [Y/N]: n |

## Clone

### Comissionar

Essa etapa consiste em comissionar os novos cartões Left/Hight/Guest.

|  |
| --- |
| 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 - B**  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 - B**  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  **# GUEST - B**  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]: n  Would you like to commission another card? [Y/N]: y  **# LEFT - C**  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]: l  Would you like to commission another card? [Y/N]: y  **# RIGHT - C**  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 7356006375073196 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  **# GUEST - C**  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 7351011479073174 to the HSM whitelist [Y/N]: y  Assign smartcard as a Left or Right Key RACC? [L/R/N]: n  Would you like to commission another card? [Y/N]: y  **# GUEST - 01**  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 8234051237074283 to the HSM whitelist [Y/N]: y  Assign smartcard as a Left or Right Key RACC? [L/R/N]: n  Would you like to commission another card? [Y/N]: y  **# GUEST - 02**  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 7351010261073174 to the HSM whitelist [Y/N]: y  Assign smartcard as a Left or Right Key RACC? [L/R/N]: n  Would you like to commission another card? [Y/N]: n |

### Clonar

Essa etapa consiste em clonar os 03 primeiros cartões Left/Hight/Guest que contém a LMK para outros dois conjuntos de cartões Left/Hight/Guest.

|  |  |
| --- | --- |
| Clone do cartão **Hight** para outros dois cartões **Hight** comissionados anteriormente. | Secure-AUTH>dc  Insert card to be duplicated and press ENTER:  Enter PIN: \*\*\*\*\*\*  Insert commissioned RACC to store RLMK share and press ENTER:  Enter PIN: \*\*\*\*\*\*  Secure-AUTH>dc  Insert card to be duplicated and press ENTER:  Enter PIN: \*\*\*\*\*\*  Insert commissioned RACC to store RLMK share and press ENTER:  Enter PIN: \*\*\*\*\*\* |
| Clone do cartão **Left** para outros dois cartões **Left** comissionados anteriormente. | Secure-AUTH>dc  Insert card to be duplicated and press ENTER:  Enter PIN: \*\*\*\*\*\*  Insert commissioned RACC to store RLMK share and press ENTER:  Enter PIN: \*\*\*\*\*\*  Secure-AUTH>dc  Insert card to be duplicated and press ENTER:  Enter PIN: \*\*\*\*\*\*  Insert commissioned RACC to store RLMK share and press ENTER:  Enter PIN: \*\*\*\*\*\* |
| Clone do cartão **Guest** para outros dois cartões **Guest** comissionados anteriormente. | Secure-AUTH>dc  Insert card to be duplicated and press ENTER:  Enter PIN: \*\*\*\*\*\*  Insert commissioned RACC to store RLMK share and press ENTER:  Enter PIN: \*\*\*\*\*\*  Secure-AUTH>dc  Insert card to be duplicated and press ENTER:  Enter PIN: \*\*\*\*\*\*  Insert commissioned RACC to store RLMK share and press ENTER:  Enter PIN: \*\*\*\*\*\* |

# HSM de Produção

Nesta situação, O HSM de produção já está inserido no Domínio Criptográfico da Cielo. Desta forma, o Thales Trust (DA), o Customer Trust Anchor da Cielo (CTA), o HSM Public Key Certificate estão instalados e as duas Passphrase já estão definidas. Além disso, já foram inseridos os cartões Left/Right/Guest na whitelist.

|  |
| --- |
| Secure>xy  Thales Trust installed : Yes  1 - Issued to: B4665303299K, Issued by: HSMKEY  Validity : Sep 30 18:34:37 2020 GMT to Sep 24 18:34:37 2045 GMT  Unique ID: CAD47AB5EF5182BA0B9936C835CCA201 - 5DDD8FCB  Customer Trust Anchor Installed : Yes  2 - Issued to: ft.local, Issued by: ft.local  Validity : Sep 28 19:06:40 2020 GMT to Sep 22 19:06:40 2045 GMT  Unique ID: C057B4251B7BE792E4CD66FD12E4F3C3 - B58BF759 (Root)  HSM Public Key Certificate Installed : Yes  3 - Issued to: B4665303299K, Issued by: ft.local  Validity : Sep 30 18:36:32 2020 GMT to Sep 24 18:36:32 2045 GMT  Unique ID: DE24F7384451CDEC21C5BE2227FF7F7F - B58BF759  Is HRK passphrase user defined : Yes  Is HRK available for use : Yes  Authorized RACCs : 3  Serial Number Certificate Number RACC Type  7356006321073196 62C8CBE52FF0187F right key  7356006465073196 70D99B9FC7B64A3C guest  7356006472073196 95B3331C7DE2B562 left key |

## Whitelist e Redifinição

Nesta etapa, serão inseridos na Whitelist os novos 02 conjutos de cartões Left/Right/Guest e os 02 cartões Guest. O comando XA será executado 08 vezes.

Quando os cartões são inseridos na Whitelist, ele são inseridos como um cartão Guest. Desta fora, será necessário converter o cartão Guest para Left/Right. Para fazer essa conversão, será utilizado o comando XK. Desta forma, o comando XK será executado 04 vezes

|  |
| --- |
| Secure>xa  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to add card 7356006342073196 to the whitelist? [Y/N] y  Card 7356006342073196 added to whitelist.  Secure>xa  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to add card 7356006350073196 to the whitelist? [Y/N] y  Card 7356006350073196 added to whitelist.  Secure>xa  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to add card 7356006327073196 to the whitelist? [Y/N] y  Card 7356006327073196 added to whitelist.  Secure>xa  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to add card 7356006360073196 to the whitelist? [Y/N] y  Card 7356006360073196 added to whitelist.  Secure>xa  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to add card 7356006375073196 to the whitelist? [Y/N] y  Card 7356006375073196 added to whitelist.  Secure>xa  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to add card 7351011479073174 to the whitelist? [Y/N] y  Card 7351011479073174 added to whitelist.  Secure>xa  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to add card 7356006472073196 to the whitelist? [Y/N] y  Card 7356006472073196 added to whitelist.  Secure>xa  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to add card 8234051237074283 to the whitelist? [Y/N] y  Card 8234051237074283 added to whitelist. |

|  |
| --- |
| Secure>xy  Authorized RACCs : 9  Serial Number Certificate Number RACC Type  7356006472073196 95B3331C7DE2B562 left key  7356006321073196 62C8CBE52FF0187F right key  7351011479073174 B35E2DE89428FA17 guest  7356006327073196 86298FA45DEB777A guest  7356006342073196 BA54119A5547F31A guest  7356006350073196 054018CF750AF394 guest  7356006360073196 6A5DA10F69B12E81 guest  7356006375073196 C9571D2C7A0DD902 guest  7356006465073196 70D99B9FC7B64A3C guest  7356006472073196 95B3331C7DE2B562 guest  8234051237074283 090332AE42876082 guest |

## Guest para Direito/Esquerdo

|  |
| --- |
| Secure>xy  Authorized RACCs : 9  Serial Number Certificate Number RACC Type  7356006472073196 95B3331C7DE2B562 left key  7356006321073196 62C8CBE52FF0187F right key  7351011479073174 B35E2DE89428FA17 guest  7356006327073196 86298FA45DEB777A guest  7356006342073196 BA54119A5547F31A guest  7356006350073196 054018CF750AF394 guest  7356006360073196 6A5DA10F69B12E81 guest  7356006375073196 C9571D2C7A0DD902 guest  7356006465073196 70D99B9FC7B64A3C guest  7356006472073196 95B3331C7DE2B562 guest  8234051237074283 090332AE42876082 guest |

Comando XK.

|  |
| --- |
| Secure>xk  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to make 7356006342073196 a [L]eft or [R]ight key? l  Card 7356006342073196 is now a left key.  Secure>xk  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to make 7356006350073196 a [L]eft or [R]ight key? r  Card 7356006350073196 is now a right key.  Secure>xk  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to make 7356006360073196 a [L]eft or [R]ight key? l  Card 7356006360073196 is now a left key.  Secure>xk  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: \*\*\*\*\*\*  Do you want to make 7356006375073196 a [L]eft or [R]ight key? r  Card 7356006375073196 is now a right key. |

Resultado final.

|  |  |
| --- | --- |
| Secure>xy  Authorized RACCs : 9  Serial Number Certificate Number RACC Type  7356006472073196 95B3331C7DE2B562 left key  7356006321073196 62C8CBE52FF0187F right key  7351011479073174 B35E2DE89428FA17 guest  **7356006327073196 86298FA45DEB777A left key**  **7356006342073196 BA54119A5547F31A right key**  7356006350073196 054018CF750AF394 guest  **7356006360073196 6A5DA10F69B12E81 left key**  **7356006375073196 C9571D2C7A0DD902 right key**  7356006465073196 70D99B9FC7B64A3C guest  7356006472073196 95B3331C7DE2B562 guest  8234051237074283 090332AE42876082 guest |  |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 29/09/2020 |
|  |  |  |