.

**payShield Manager**

Índice

[1. Novo Domínio Criptográfico 3](#_Toc53124852)

[1.1. Comando FC (Format Card) 3](#_Toc53124853)

[1.2. Comando SK (Generate HRK Passphrases) 3](#_Toc53124854)

[1.3. Comando RI (Initialize Domain Authority) 4](#_Toc53124855)

[1.4. Comando RH (Generate an HSM certificate) 4](#_Toc53124856)

[1.5. Reboot 5](#_Toc53124857)

[1.6. Comando XI (Generate Customer Trust Anchor) 5](#_Toc53124858)

[1.7. Comando XH (Comission the HSM) 6](#_Toc53124859)

[1.8. Comando XR (comission the smartcards) 7](#_Toc53124860)

[1.9. Comando XT (Transfer Existing LMK to RLMK) 8](#_Toc53124861)

[2. Domínio Criptográfico já existente 9](#_Toc53124862)

[2.1. Comando SK (Generate HRK) 9](#_Toc53124863)

[2.2. Comando RH (Generate an HSM certificate) 9](#_Toc53124864)

[2.3. Reboot 10](#_Toc53124865)

[2.4. Comando XH (Comission the HSM) 10](#_Toc53124866)

[2.5. Comando XA (To add a RACC to the whitelist on the HSM) 11](#_Toc53124867)

[3. Release Notes 12](#_Toc53124868)

# Novo Domínio Criptográfico

Nesta situação, não existe um Domínio Criptográfico criado e o payShield Manager não está comissionado.

## Comando FC (Format Card)

Nesta etapa, os futuros cartões DA serão formatados. O processo abaixo deve ser executado nos 03 cartões DA.

|  |
| --- |
| 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]: [**k**]  Erasing card  Formatting card...  Enter new PIN for smartcard: [**\*\*\*\*\***]  Re-enter new PIN: [**\*\*\*\*\***]  Enter time [hhmmss]: [**093609**]  Enter date [DDMMYY]: [**180820**]  Enter User ID: [**ft**]  Enter Issuer ID: [**ft**] |

## Comando SK (Generate HRK Passphrases)

Nesta etapa, será definido 2 passphrases de administração para configuração de certificado de HSM Recovery Key (HRK).

|  |
| --- |
| Secure-AUTH>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 |

## Comando RI (Initialize Domain Authority)

Nesta etapa, será efetuada a configuração dos cartões DA, além da geração do certificado que serão armazenados nos cartões DA.

|  |
| --- |
| Secure-AUTH>ri  Issuer name: [default = CertAuth]:  Signature algorithm: [RSA]: (press enter)  Hash Algorithm: [SHA-1, SHA-256 (default = SHA-256)]:  CA RSA key length: [1024-2048 (default = 2048)]:  HSM RSA key length: [1024-2048 (default = 2048)]:  Card RSA key length: [1024-2048 (default = 2048)]:  Public exponent: [3, 65537 (default = 65537)]:  Enter number of Domain Authority private key shares: [3-9]:[**3**]  Enter number of shares to recover the Domain Authority private key: [3-3]:[**3**]  Enter 9 character alpha-numeric CA serial number : [**123456789**]  Generating Domain Authority key pair ...  Insert first Domain Authority private key card and enter PIN:[**\*\*\*\*\***]  Insert second Domain Authority private key card and enter PIN: [**\*\*\*\*\***]  Insert third Domain Authority private key card and enter PIN: [**\*\*\*\*\***]  Domain Authority generation complete 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  Number of CA private key shares: 3  Number of shares to recover private key: 3 |

## Comando RH (Generate an HSM certificate)

Nesta etapa, será gerado o certificado do par de chaves privadas/públicas para o gerenciamento do HSM remoto. Cartões CTA. Para poder executar essa etapa, serão utilizado os cartões DA.

|  |
| --- |
| Secure-AUTH>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

Apertar o botão vermelho REBOOT localizado na parte da frente do HSM para que o equipamento seja reinicializado.

## Comando XI (Generate Customer Trust Anchor)

Nesta etapa, serão gerados os cartões CTA e gravado nos smartcards. Nesta etapa, serão utilizados os cartões de PayShield Manager.

|  |
| --- |
| Secure>xi  Please enter the certificate Subject information:  Country Name (2 letter code) []: [**br**]  State or Province Name (full name) []: [**sao paulo**]  Locality Name (eg, city) []: [**sao paulo**]  Organization Name (eg, company) []: [**ft**]  Organizational Unit Name (eg, section) []: [**ft**]  Common Name (e.g. server FQDN or YOUR name) []: [**ft**]  Email Address []: [**ft@ft.local**]  Enter number of **Customer Trust Authority** private key shares [3-9]: [**3**]  Enter number of shares to recover the **Customer Trust Authority** private key [3-3]: [**3**]  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)  Insert payShield Manager Smartcard 1 of 3 and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Enter new PIN for smartcard: [**\*\*\*\*\*\***]  Re-enter new PIN: [**\*\*\*\*\*\***]  Working....  CTA share written to smartcard.  Insert payShield Manager Smartcard 2 of 3 and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Enter new PIN for smartcard: [**\*\*\*\*\*\***]  Re-enter new PIN: [**\*\*\*\*\*\***]  Working....  CTA share written to smartcard.  Insert payShield Manager Smartcard 3 of 3 and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Enter new PIN for smartcard: [**\*\*\*\*\*\***]  Re-enter new PIN: [**\*\*\*\*\*\***]  Working....  CTA share written to smartcard.  Successfully generated a **Customer Trust Anchor** |

## Comando XH (Comission the HSM)

Nesta etapa, será iniciado o processo de comissionamento do HSM.

|  |
| --- |
| Secure>xh  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: [**\*\*\*\*\*\***]  Starting the commissioning of the HSM process...  Please insert **left** key card and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Enter new PIN for smartcard: [**\*\*\*\*\*\***]  Re-enter new PIN: [**\*\*\*\*\*\***]  Working...  Please insert **right** key card and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Enter new PIN for smartcard: [**\*\*\*\*\*\***]  Re-enter new PIN: [**\*\*\*\*\*\***]  Working...  Successfully commissioned HSM |

## Comando XR (comission the smartcards)

Nesta etapa, será iniciado o processo para configuração dos cartões de backup (Left, Right) além de caso necessário os cartões de acesso 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: [**\*\*\*\*\*\***]  Enforce a PIN change on first use? [Y/N]: [**n**]  Insert a payShield Manager Smartcard to be commissioned and press ENTER:  PIN is currently set. Must verify current PIN before continuing.  Enter PIN: [**\*\*\*\*\*\***]  Enter new PIN for smartcard: [**\*\*\*\*\*\***]  Re-enter new PIN: [**\*\*\*\*\*\***]  Do you wish to add the smartcard 7307003927072979 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**]  Enforce a PIN change on first use? [Y/N]: [**n**]  Insert a payShield Manager Smartcard to be commissioned and press ENTER:  PIN is currently set. Must verify current PIN before continuing.  Enter PIN: [**\*\*\*\*\*\***]  Enter new PIN for smartcard: [**\*\*\*\*\*\***]  Re-enter new PIN: [**\*\*\*\*\*\***]  Do you wish to add the smartcard 7307003627072979 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**] |

## Comando XT (Transfer Existing LMK to RLMK)

Nesta etapa, será iniciado o processo de divisão da LMK local nos cartões de PayShield Manager, assim criando nos cartões de acesso o carregamento da LMK remota.

|  |
| --- |
| Secure>vt  LMK table:  ID Authorized Scheme Algorithm Status Check Comments  **00 No Variant 3DES(2key) Test 268604 variant**  01 No KeyBlock AES-256 Test 9D04A0 keyblock  Key change storage table:No keys loaded in key change storage  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: 268604  Load more components? [Y/N]: [**n**]  LMK Check: 268604  LMK key scheme: Variant  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]: [**2**]  Enter the number of shares required to reconstitute the LMK: [2-2]: [**2**]  Insert a commissioned card 1 of 2 and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Card Check: 14A6E8  LMK share written to smartcard.  Insert a commissioned card 2 of 2 and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Card Check: A895E9  LMK share written to smartcard.  Want to test the reassembly of the LMK? [Y/N]: [**n**] |

# Domínio Criptográfico já existente

Nesta situação, o cliente já possui um Domínio Criptográfico e ele deseja adicionar um novo HSM payShield a este Domínio Criptográfico.

## Comando SK (Generate HRK)

Nesta etapa, será definido 2 passphrases de administração para configuração de certificado de HSM Recovery Key (HRK).

|  |
| --- |
| 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 |

## Comando RH (Generate an HSM certificate)

Nesta etapa, será gerado o certificado do par de chaves privadas/públicas para o gerenciamento do HSM remoto.

|  |
| --- |
| 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

Apertar o botão vermelho REBOOT do HSM para reiniciar o mesmo

## Comando XH (Comission the HSM)

Nesta etapa, será iniciado o processo de comissionamento do HSM (definição dos cartões de acesso Right, Left).

|  |
| --- |
| Secure>xh  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: [**\*\*\*\*\*\***]  Starting the commissioning of the HSM process...  Please insert **left** key card and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Please insert **right** key card and press ENTER:  Enter PIN: [**\*\*\*\*\*\***]  Successfully commissioned HSM |

## Comando XA (To add a RACC to the whitelist on the HSM)

Nesta etapa, será adicionado cartão Guest ao Domínio Criptográfico.

|  |
| --- |
| Secure>xa  Insert payShield Manager Smartcard and Press ENTER:  Enter PIN: [\*\*\*\*\*\*]  Do you want to add card **7307003927072979** to the whitelist? [Y/N] [y]  Card 7307003927072979 added to whitelist.  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  **7307003927072979** 90DDDCA684FA75F5 guest  7307004059072979 1210C4CD0F312F52 right key  7307004132072979 87C7D56A28670A92 left key |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 18/08/2020 |
|  |  |  |