

**Ceremonial de Chaves**

Índice

[1. Smartcards 3](#_Toc46583966)

[1.1. Formatação dos Smartcards 3](#_Toc46583967)

[2. LMK 4](#_Toc46583968)

[2.1. Criação da chave LMK 4](#_Toc46583969)

[2.2. Leitura da chave LMK 5](#_Toc46583970)

[2.3. Exibição da chave LMK 5](#_Toc46583971)

[3. ZMK (000) 6](#_Toc46583972)

[3.1. Criação dos componentes da chave ZMK 6](#_Toc46583973)

[3.2. Geração da chave ZMK a partir dos componentes 7](#_Toc46583974)

[4. ZPK (001) 8](#_Toc46583975)

[4.1. Criação dos componentes da chave ZPK 8](#_Toc46583976)

[4.2. Geração da chave ZPK a partir dos componentes 8](#_Toc46583977)

[5. Resumo das Chaves 10](#_Toc46583978)

[6. Exportando Chaves 11](#_Toc46583979)

[6.1. Exportando a chave ZPK 11](#_Toc46583980)

[7. Importando Chaves 12](#_Toc46583981)

[7.1. Importando a chave ZPK 12](#_Toc46583982)

[8. Release Notes 13](#_Toc46583983)

# Smartcards

## Formatação dos Smartcards

**- Cartão 01**

|  |
| --- |
| 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]: [**161216**]  Enter date [DDMMYY]: [**311019**]  Enter User ID: [**FT**]  Enter Issuer ID: [**FT**]  Format complete |

**- Cartão 02**

|  |
| --- |
| 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]: [**161216**]  Enter date [DDMMYY]: [**311019**]  Enter User ID: [**FT**]  Enter Issuer ID: [**FT**]  Format complete |

**- Cartão 03**

|  |
| --- |
| 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]: [**161216**]  Enter date [DDMMYY]: [**311019**]  Enter User ID: [**FT**]  Enter Issuer ID: [**FT**]  Format complete |

# LMK

## Criação da chave LMK

**- Cartão 01**

|  |
| --- |
| Secure>GK  Variant scheme or keyblock scheme? [V/K]: [**V**]  Enter algorithm type [2=2DES, 3=3DES]: [**2**]  Key status? [L/T]: [**L**]  LMK component set [1-9]: [**1**]  Enter secret value A:  Enter secret value B:  Enter value C:  Insert blank card and enter PIN: [**\*\*\*\*\***]  Writing keys...  Checking keys...  Device write complete, check: 616380  Make another copy? [Y/N]: [**N**] |

**- Cartão 02**

|  |
| --- |
| Secure>GK  Variant scheme or keyblock scheme? [V/K]: [**V**]  Enter algorithm type [2=2DES, 3=3DES]: [**2**]  Key status? [L/T]: [**L**]  LMK component set [1-9]: [**2**]  Enter secret value A:  Enter secret value B:  Enter value C:  Insert blank card and enter PIN: [**\*\*\*\*\***]  Writing keys...  Checking keys...  Device write complete, check: 784663  Make another copy? [Y/N]: [**N**] |

**Cartão 03**

|  |
| --- |
| Secure>GK  Variant scheme or keyblock scheme? [V/K]: [**V**]  Enter algorithm type [2=2DES, 3=3DES]: [**2**]  Key status? [L/T]: [**L**]  LMK component set [1-9]: [**3**]  Enter secret value A:  Enter secret value B:  Enter value C:  Insert blank card and enter PIN: [**\*\*\*\*\***]  Writing keys...  Checking keys...  Device write complete, check: 649844  Make another copy? [Y/N]: [**N**] |

## Leitura da chave LMK

**- Cartão 01**

|  |
| --- |
| Secure>LK  Enter LMK id [0-1]: [**0**]  Enter comments: [**VARIANT**]  Load LMK from components or shares  Insert card and press ENTER:  Enter PIN: [**\*\*\*\*\***]  Check: 616380  Load more components? [Y/N]: [**Y**] |

**- Cartão 02**

|  |
| --- |
| Enter PIN: [**\*\*\*\*\***]  Check: 784663  Load more components? [Y/N]: [**Y**] |

**- Cartão 03**

|  |
| --- |
| Enter PIN: [**\*\*\*\*\***]  Check: 649844  Load more components? [Y/N]: [**N**]  LMK Check: 169467  LMK id: 00  LMK key scheme: Variant  LMK algorithm: 3DES(2key)  LMK status: Live  Comments: variant  Confirm details? [Y/N]: [**Y**]  Use the LO/LN command to load LMKs into key change storage.  Do you want to make this LMK the default LMK? [Y/N]: y  Do you want to make this LMK the management LMK? [Y/N]: y |

## Exibição da chave LMK

|  |
| --- |
| Secure>VT  LMK table:  ID Authorized Scheme Algorithm Status Check Comments  00 No Variant 3DES(2key) Live 169467 variant  Key change storage table:No keys loaded in key change storage |

# ZMK (000)

## Criação dos componentes da chave ZMK

**- Componente 01**

|  |
| --- |
| Online-AUTH>GC  Enter LMK id [0-1]: [**0**]  Enter key length [1,2,3]: [**2**]  Enter key type: [**000**]  Enter key scheme: [**U**]  Clear component: **C10D 8008 6E4A BCFB 7A6D 51A4 7A68 C494**  Encrypted component: **U3C99 6B78 61E5 2BB6 2C50 F3F5 E105 179F**  Key check value: **F9E3BD** |

**- Componente 02**

|  |
| --- |
| Online-AUTH>GC  Enter LMK id [0-1]: [0]  Enter key length [1,2,3]: [2]  Enter key type: [000]  Enter key scheme: [u]  Clear component: **E616 B051 EAF7 79E0 156D 2045 6EB0 B58A**  Encrypted component: **U88C8 74A8 6FCD FE91 3EC0 9A2D A59E E853**  Key check value: **F918FB** |

**- Componente 03**

|  |
| --- |
| Online-AUTH>GC  Enter LMK id [0-1]: [**0**]  Enter key length [1,2,3]: [**2**]  Enter key type: [**000**]  Enter key scheme: [**U**]  Clear component: **9797 4502 4A13 92A7 43D5 DF45 D379 46F4**  Encrypted component: **UB8CB ED41 727E F386 6BC6 46FC 15A2 868D**  Key check value: **B50C38** |

## Geração da chave ZMK a partir dos componentes

|  |
| --- |
| Online-AUTH>FK  Enter LMK id [0-1]: [**0**]  Enter key length [1,2,3]: [**2**]  Enter key type: [**000**]  Enter key scheme: [**U**]  Enter component type [X,H,T,E,S]: [**X**]  Enter number of components [2-9]: [**3**]  Enter component 1: [**C10D 8008 6E4A BCFB 7A6D 51A4 7A68 C494**]  Component 1 check value: **F9E3BD**  Continue? [Y/N]: [**Y**]  Enter component 2: [**E616 B051 EAF7 79E0 156D 2045 6EB0 B58A**]  Component 2 check value: **F918FB**  Continue? [Y/N]: [**Y**]  Enter component 3: [**9797 4502 4A13 92A7 43D5 DF45 D379 46F4**]  Component 3 check value: **B50C38**  Continue? [Y/N]: [**Y**] |

**- Chave ZMK**

Encrypted key: **U2C8C FD85 7D51 C070 5FAB 260F 766E ECC5**

Key check value: **6A2537**

# ZPK (001)

## Criação dos componentes da chave ZPK

**- Componente 01**

|  |
| --- |
| Secure-AUTH>GC  Enter LMK id [0-1]: [**0**]  Enter key length [1,2,3]: [**2**]  Enter key type: [**001**]  Enter key scheme: [**U**]  Clear component: **38B3 54CE 76DA ABD6 B973 8543 BC02 B664**  Encrypted component: **UE5FC B44F 150A 0D44 A28B 7EE6 FCD2 E3D6**  Key check value: **D414D4** |

**- Componente 02**

|  |
| --- |
| Secure-AUTH>GC  Enter LMK id [0-1]: [**0**]  Enter key length [1,2,3]: [**2**]  Enter key type: [**001**]  Enter key scheme: [**U**]  Clear component: **F737 CDF8 E570 8F29 8A86 CD2C 4354 8CEF**  Encrypted component: **U2C2D C1EA C9EF 4AC1 747E 8CA9 388C F6D8**  Key check value: **CEF972** |

**- Componente 03**

|  |
| --- |
| Secure-AUTH>GC  Enter LMK id [0-1]: [**0**]  Enter key length [1,2,3]: [**2**]  Enter key type: [**001**]  Enter key scheme: [**U**]  Clear component: **B634 EF2C 8A67 389B 7561 6B45 9E6B 3137**  Encrypted component: **UFE6E FCE5 DC8C 0847 0394 207D F4B8 4BA6**  Key check value: **C72B55** |

## Geração da chave ZPK a partir dos componentes

|  |
| --- |
| Secure-AUTH>FK  Enter LMK id [0-1]: [**0**]  Enter key length [1,2,3]: [**2**]  Enter key type: [**001**]  Enter key scheme: [**U**]  Enter component type [X,H,T,E,S]: [**X**]  Enter number of components [2-9]: [**3**]  Enter component 1:[ **38B3 54CE 76DA ABD6 B973 8543 BC02 B664**]  Component 1 check value: **D414D4**  Continue? [Y/N]: [**Y**]  Enter component 2: [**B634 EF2C 8A67 389B 7561 6B45 9E6B 3137**]  Component 2 check value: **C72B55**  Continue? [Y/N]: [**Y**]  Enter component 3: [**F737 CDF8 E570 8F29 8A86 CD2C 4354 8CE**]  Component 3 check value: **CEF972**  Continue? [Y/N]: [**Y**] |

**- Chave ZPK**

Encrypted key**: UFD06 BC18 0FA2 8517 1DD3 4352 5565 CADC**

Key check value: **A19B7E**

# Resumo das Chaves

**- Chave ZMK (000)**

Encrypted key: **U2C8C FD85 7D51 C070 5FAB 260F 766E ECC5**

Key check value: **6A2537**

**- Chave ZPK (001)**

Encrypted key: **UFD06 BC18 0FA2 8517 1DD3 4352 5565 CADC**

Key check value: **A19B7E**

# Exportando Chaves

## Exportando a chave ZPK

|  |
| --- |
| Secure-AUTH>KE  Enter LMK id [0-1]: [0]  Enter key type: [001]  Enter key scheme: [X]  Enter ZMK: **U[2C8CFD857D51C0705FAB260F766EECC5]**  Enter key under LMK: **U[FD06BC180FA285171DD343525565CADC]**  Key under ZMK: **X[FB81 5F3E CBFC EEE6 829C 0905 5218 CE78]**  Key check value: **A19B7E** |

# Importando Chaves

## Importando a chave ZPK

|  |
| --- |
| Secure-AUTH>IK  Enter LMK id [0-1]: [**0**]  Enter key type: [**001**]  Enter key scheme: [**U**]  Enter ZMK**: U[2C8CFD857D51C0705FAB260F766EECC5]**  Enter key: **U[FD06BC180FA285171DD343525565CADC]**  Warning: key parity corrected  Encrypted key: **U[6AB8 76C4 2AA5 D2D3 CCCB F840 732A 39FF]**  Key check value: **66E07D** |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 11/11/2019 |
| Caio Ferreira | Utilização de tabela | 25/07/2020 |