

**Ceremonial de Chaves**

Índice

[1. HSM A 3](#_Toc46353628)

[1.1. ZMK – Componentes 3](#_Toc46353629)

[1.2. ZMK – Chave 3](#_Toc46353630)

[1.3. BDK – Componentes 4](#_Toc46353631)

[1.4. BDK – Chave 4](#_Toc46353632)

[1.5. KE 5](#_Toc46353633)

[2. HSM B 6](#_Toc46353634)

[2.1. FK 6](#_Toc46353635)

[2.2. IK 7](#_Toc46353636)

[3. Release Notes 8](#_Toc46353637)

# HSM A

## ZMK – Componentes

Componentes de uma chave do tipo ZMK

|  |  |
| --- | --- |
| Secure-AUTH>gc  Clear component: B07F 15C4 6702 FB46 1629 2AA2 68D0 31AB  Encrypted component: U66F1 3C87 F9F4 D52D 926C 2E5A 76DF 301F  Key check value: 07A7D1  Secure-AUTH>gc  Clear component: 1086 3B16 2967 5B25 AB6D C120 49F4 CEB6  Encrypted component: U655F 91EB 2A8D 156F 8A47 8B91 1954 C215  Key check value: EE4F33 | |
|  | |
|  |  |
|  |  |
|  |  |

## ZMK – Chave

Chave de criptografia do tipo ZMK criptografada pela LMK\_A do HSM\_A

|  |  |
| --- | --- |
| Secure-AUTH>fk  **Encrypted key: UAF9B 072F 4B24 BA4A 79B1 D73D 589C 4426**  **Key check value: 684DF7** | |
|  |  |
|  |  |

## BDK – Componentes

Componentes de uma chave do tipo BDK.

|  |
| --- |
| Secure-AUTH>gc Clear component: F45D DFF8 8CCD 836B 4F10 19C1 B583 5EC2  Encrypted component: UFDE7 E021 9D98 AA58 C094 60BC 055C 825B  Key check value: 230F38  Secure-AUTH>gc Clear component: 1A8A 529E 86E6 011C 5D76 6B68 FEA2 3EF7  Encrypted component: UDCA0 FB9C 9502 DBFA 6D03 6717 2D64 FA2C  Key check value: 4D4847 |

|  |  |
| --- | --- |
|  |  |
|  |  |

## BDK – Chave

Chave de criptografia do tipo BDK criptografada pela LMK\_A do HSM\_A.

|  |
| --- |
| Secure-AUTH>fk **Encrypted key: U3E4B 7470 2DAD 2390 8EBD 6AF5 7B4B BE99  Key check value: 498634** |

|  |  |
| --- | --- |
|  |  |
|  |  |

## KE

O comando KE é utilizado para traduzir a chave criptografada sobre uma determinada LMK para uma outra chave. No exemplo abaixo, uma chave do tipo BDK que está criptografado pela LMK\_A será criptografada pela chave ZMK. O processo de exportação da chave está sendo feito no formato X9.17.

|  |
| --- |
| Online-AUTH>ke    Enter LMK id [0-1]: 1  Enter key type: 009  Enter key scheme: X  Enter ZMK: UAF9B 072F 4B24 BA4A 79B1 D73D 589C 4426  Enter key under LMK: U3E4B 7470 2DAD 2390 8EBD 6AF5 7B4B BE99    **Key under ZMK: X23E9 0874 5E34 D596 8C9D A0AA 9F41 A372**  **Key check value: 498634** |

|  |  |
| --- | --- |
|  |  |

# HSM B

## FK

Reconstruindo a chave de criptografia do tipo ZMK criada no HSM\_A e agora criptografada pela LMK\_B.

|  |
| --- |
| Online-AUTH>fk    Enter LMK id [0-1]: 1  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 [1-9]: 2    Enter component 1: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Component 1 check value: 07A7D1  Continue? [Y/N]: y    Enter component 2: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Component 2 check value: EE4F33  Continue? [Y/N]: y    Encrypted key: **UAF9B 072F 4B24 BA4A 79B1 D73D 589C 4426**  Key check value: **684DF7** |

|  |  |
| --- | --- |
|  |  |
|  |  |

## IK

O comando IK é utilizado para traduzir uma chave, no exemplo abaixo, uma chave do tipo BDK que está criptografada sobre uma ZMK para uma chave LMK\_B do HSM B. O processo de importação está sendo feito no formato X9.17.

|  |
| --- |
| Online-AUTH>ik    Enter LMK id [0-1]: 1  Enter key type: 009  Enter key scheme: u  Enter ZMK: **UAF9B 072F 4B24 BA4A 79B1 D73D 589C 4426**  Enter key: **X23E9 0874 5E34 D596 8C9D A0AA 9F41 A372**    Encrypted key: **U3E4B 7470 2DAD 2390 8EBD 6AF5 7B4B BE99**  Key check value: **498634** |

|  |  |
| --- | --- |
|  |  |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 18/02/2020 |
| Caio Ferreira | Foi trocado a chave do tipo ZPK para o tipo BDK | 22/07/2020 |
| Caio Ferreira | Foram adicionados diagramas no texto. | 22/07/2020 |