

**Ceremonial de Chaves – keyblock 2 variant**

Índice

[1. Objetivo 3](#_Toc49522980)

[2. Origem 3](#_Toc49522981)

[2.1. LMK Keyblock 3](#_Toc49522982)

[2.2. ZMK 3](#_Toc49522983)

[2.3. ZPK 4](#_Toc49522984)

[2.4. ZAK 5](#_Toc49522985)

[2.5. EXPORT ZMK(ZPK) 5](#_Toc49522986)

[2.6. EXPORT ZMK(ZAK) 5](#_Toc49522987)

[3. Destino 6](#_Toc49522988)

[3.1. LMK Variant 6](#_Toc49522989)

[3.2. ZMK 6](#_Toc49522990)

[3.3. IMPORT ZMK(ZPK) 6](#_Toc49522991)

[3.4. IMPORT ZMK(ZAK) 6](#_Toc49522992)

[4. Release Notes 7](#_Toc49522993)

# Objetivo

Processo de cerimonial cujo HSM de origem utiliza uma LMK do tipo Keyblock e o HSM de destino possui uma LMK do tipo Variant.

# Origem

## LMK Keyblock

|  |
| --- |
| LMK table:  ID Authorized Scheme Algorithm Status Check Comments  01 Yes(H,C) KeyBlock AES-256 Test 9D04A0 keyblock |

## ZMK

Gerando os componentes da chave ZMK.

|  |
| --- |
| Online-AUTH>gc  Enter LMK id [0-1]: 1  Enter algorithm type [D=DES, A=AES]: d  Enter key length [2,3]: 2  Enter key scheme: s  Enter Key Usage: k0  Enter Mode of Use: n  Enter component number [1-9]: 1  Enter Exportability: s  Enter Optional Blocks? [Y/N]: n    Clear component: 0108 37F8 297C 6B08 853E A4A2 3846 0DC2  Encrypted component: S10096K0TNc1S0001C7AD5A40F719C81B31B9C7D81BA20D5B2760FE838284D146E69E0C425E7DAAD8390F8F8ACA3BC02F  Key check value: 868D91  Clear component: 8FFE 383B A120 4CEF A107 79CD 2A4C 8F20  Encrypted component: S10096K0TNc2S0001C5BFF203F205F548CE8A942622CEB018DCAD3A144D34A27439169A483751D62483093FA1535521EA  Key check value: A1F3DE  Clear component: EF08 B613 0292 9867 348A 6210 2C2A F14F  Encrypted component: S10096K0TNc3S00015C7BD083F2C185AB670AD399D0D08F057EEE8DD6024864DB1F3A7901E893A8D26F2763767A24383D  Key check value: 742D47 |

Baseado nos componentes gerados anteriormente, foi gerado a chave do tipo ZMK.

|  |
| --- |
| Online-AUTH>fk  Enter LMK id [0-1]: 1  Enter algorithm type [D=DES, A=AES]: d  Enter key length [2,3]: 2  Enter key scheme: s  Enter component type [X,E,S]: x  Enter number of components [2-9]: 3  Enter Key Usage: k0  Enter Mode of Use: n  Enter Key Version Number: 00  Enter Exportability: s  Enter Optional Blocks? [Y/N]: n    Encrypted key: S10096K0TN00S0001E74CEFEE0DC383183F2DDD78AD96DE95EA472449B7EA97BD6924B01254E55C9AAD08BCDD80E7906C  Key check value: AC7E1D |

## ZPK

|  |
| --- |
| Online-AUTH>kg  Enter LMK id [0-1]: 1  Enter algorithm type [D=DES, A=AES]: d  Enter key length [2,3]: 2  Enter key scheme (LMK): s  Enter key scheme (ZMK):  Enter ZMK:  Enter Key Usage: p0  Enter Mode of Use: n  Enter Key Version Number: 00  Enter Exportability: s  Enter Optional Blocks? [Y/N]: n    Key under LMK: S10096P0TN00S00019771AD01C59B1978C6C1DD3D760B9A59888ECA5C8F646D6963D0B47F4287AA8DE105EC8957702E3C  Key check value: CAD50D |

## ZAK

|  |
| --- |
| Online-AUTH>kg  Enter LMK id [0-1]: 1  Enter algorithm type [D=DES, A=AES]: d  Enter key length [2,3]: 2  Enter key scheme (LMK): s  Enter key scheme (ZMK):  Enter ZMK:  Enter Key Usage: m3  Enter Mode of Use: n  Enter Key Version Number: 00  Enter Exportability: s  Enter Optional Blocks? [Y/N]: n    Key under LMK: S10096M3TN00S0001B8DB3831DCBFD9B4AB8181302755846CE8BBA2E3682FE255A75ACE46217901C8BD0289319A57A1E5  Key check value: 1D12B2 |

## EXPORT ZMK(ZPK)

|  |
| --- |
| Online-AUTH>ke  Enter LMK id [0-1]: 1  Enter key scheme: x  Enter ZMK: S10096K0TN00S0001E74CEFEE0DC383183F2DDD78AD96DE95EA472449B7EA97BD6924B01254E55C9AAD08BCDD80E7906C  Enter key under LMK: S10096P0TN00S00019771AD01C59B1978C6C1DD3D760B9A59888ECA5C8F646D6963D0B47F4287AA8DE105EC8957702E3C    Key under ZMK: X4E00 1ED1 B9D7 21FC DA3A F5D7 61B7 FD8D  Key check value: CAD50D |

## EXPORT ZMK(ZAK)

|  |
| --- |
| Online-AUTH>ke  Enter LMK id [0-1]: 1  Enter key scheme: x  Enter ZMK: S10096K0TN00S0001E74CEFEE0DC383183F2DDD78AD96DE95EA472449B7EA97BD6924B01254E55C9AAD08BCDD80E7906C  Enter key under LMK: S10096M3TN00S0001B8DB3831DCBFD9B4AB8181302755846CE8BBA2E3682FE255A75ACE46217901C8BD0289319A57A1E5    Key under ZMK: X89D0 7553 8081 D3F0 127E 4639 679D 19A5  Key check value: 1D12B2 |

# Destino

## LMK Variant

|  |
| --- |
| LMK table:  ID Authorized Scheme Algorithm Status Check Comments  00 Yes(H,C) Variant 3DES(2key) Test 268604 variant |

## ZMK

|  |
| --- |
| 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    Encrypted key: U94FC 1E17 AD05 A047 DD0F 571F 584C C4C6  Key check value: AC7E1D |

## IMPORT ZMK(ZPK)

|  |
| --- |
| Online-AUTH>ik  Enter LMK id [0-1]: 0  Enter key type: 001  Enter key scheme: u  Enter ZMK: U94FC 1E17 AD05 A047 DD0F 571F 584C C4C6  Enter key: X4E00 1ED1 B9D7 21FC DA3A F5D7 61B7 FD8D    Encrypted key: U8D42 7510 DCE7 914F 4F08 7C99 CD6E 9C5A  Key check value: CAD50D |

## IMPORT ZMK(ZAK)

|  |
| --- |
| Online-AUTH>ik  Enter LMK id [0-1]: 0  Enter key type: 008  Enter key scheme: u  Enter ZMK: U94FC 1E17 AD05 A047 DD0F 571F 584C C4C6  Enter key: X89D0 7553 8081 D3F0 127E 4639 679D 19A5    Encrypted key: U0D10 314F 2978 4B27 3E77 2DD2 5545 E311  Key check value: 1D12B2 |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 28/08/2020 |
|  |  |  |