

**LMK - Migração**

Índice

[1. Introdução 3](#_Toc67309072)

[2. Configuração de Segurança 3](#_Toc67309073)

[3. LMK 3](#_Toc67309074)

[4. BDK 3](#_Toc67309075)

[4.1. Chave Criptografica 3](#_Toc67309076)

[5. Importação da LMK 4](#_Toc67309077)

[5.1. Console 4](#_Toc67309078)

[5.2. payShield Manager 5](#_Toc67309079)

[5.3. LMK 6](#_Toc67309080)

[6. Migração da chave de criptografia 7](#_Toc67309081)

[7. Resumo das Chaves 7](#_Toc67309082)

[8. Simulação 8](#_Toc67309083)

[8.1. M0 – criptografar dados 8](#_Toc67309084)

[8.2. M2 – descriptografar dados 9](#_Toc67309085)

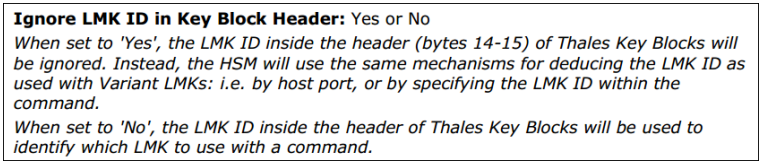
[9. Release Notes 10](#_Toc67309086)

# Introdução

Migrar uma chave de criptografia que esta criptografada por uma LMK do tipo Variant 3DES (2key) para uma LMK do tipo Key Block AES-256.

# Configuração de Segurança

As chaves sob o formato de LMK Key Block carregam em seu cabeçalho a identificação do slot da LMK sob as quais foram criadas. Dependendo do método de migração utilizado, haverá a necessidade de definir a configuração de segurança abaixo para YES.



Isto significa que o HSM não levará em consideração esta informação durante o uso das chaves migradas.

# LMK

A LMK do tipo Variant está armazenada no HSM e está sendo utilizada para criptografar as outras chaves.

|  |
| --- |
| 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 key block  Key change storage table:No keys loaded in key change storage |

# BDK

## Chave Criptografica

Criação de uma chave do tipo BDK.

|  |
| --- |
| Online-AUTH>kg    Enter LMK id [0-1]: 0  Enter key length [1,2,3]: 2  Enter key type: 009  Enter key scheme (LMK):  Enter key scheme (ZMK):  Enter ZMK:    Key under LMK: U2F00 8E27 08D7 3336 402C 9D1F E25B 82FD  **Key check value: 94EBB3** |

# Importação da LMK

A LMK do tipo Variant será inserido no slot de transição e junto com a LMK Key Block que está localizado no slot 01. Esse slot de transição será utilizado pelo comando de host BW para realizar o processo de transição das chaves que estão protegidas pela LMK Variant para a nova LMK, LMK Key Block.

## Console

Para poder executar o comando LO, é necessário que a LMK localizada no slot 01 esteja em modo autorizado.

|  |
| --- |
| Secure-AUTH>lo  Enter LMK id [0-1]: 1  Enter comments: variant  Load old LMK from components or shares  Insert card and press ENTER:  Enter PIN: \*\*\*\*\*  Check: 268604  Load more components? [Y/N]: n  LMK Check: 268604  LMK id: 01  LMK key scheme: Variant  LMK algorithm: 3DES(2key)  LMK status: Test  Comments: variant  Confirm Details? [Y/N]: y |

## payShield Manager

Acessar o payShield Manager e ir em Operacional:

|  |
| --- |
|  |

Verificar se a LMK está autorizada. Nesse procedimento iremos criar uma Variant no Slot de transição. Então a LMK 01 KeyBlock deverá estar em modo autorizado. Para prosseguir temos que colocar em modo Seguro.

Clicar em Install:

|  |
| --- |
|  |

Adicione o comentário, e tenha certeza do ID escolhido. No nosso caso 1:

|  |
| --- |
|  |

Será solicitado os cartões da LMK:

|  |
| --- |
|  |

Após finalizar clique em OK.

|  |
| --- |
|  |

## LMK

|  |
| --- |
| Secure-AUTH>vt  LMK table:  ID Authorized Scheme Algorithm Status Check Comments  00 No Variant 3DES(2key) Test 268604 variant  01 Yes(H,C) KeyBlock AES-256 Test 9D04A0 key block  Key change storage table:  ID Old/New Scheme Algorithm Status Check Comments  01 Old Variant 3DES(2key) Test 268604 variant |

# Migração da chave de criptografia

|  |
| --- |
| Message Header 0000  Command Code BW  Key Type Code 09  Key Length Flag 1  Key U13CFE7A0407961658C333162E709E04D  Delimiter %  LMK Identifier 01  Delimiter #  Key Usage B0  Mode of Use X  Key Version Number 00  Exportability S  Optional Blocks 00  Delimiter ! !  Key Check Return Flag 1  Key Check Value Type 1  Command 0000BW091U2F008E2708D73336402C9D1FE25B82FD%01#B0X00S00!11  Received response 0000BX00S10096B0TN00S000154B915D30D1AD7931C54C30A9FA9C8C244BBFE7E19A259023E85ABBC70F7FE93E7D2682A36DD2FAE94EBB3  Message Header 0000  Response Code BX  Error Code 00  Key S10096B0TN00S000154B915D30D1AD7931C54C30A9FA9C8C244BBFE7E19A259023E85ABBC70F7FE93E7D2682A36DD2FAE  **Key Check Value 94EBB3** |

# Resumo das Chaves

BKD protegida pela LMK do tipo Variant de teste da Thales.

|  |
| --- |
| Key under LMK: U2F00 8E27 08D7 3336 402C 9D1F E25B 82FD  **Key check value: 94EBB3** |

BKD protegida pela LMK do tipo key Block de teste da Thales.

|  |
| --- |
| Key under LMK: S10096B0TN00S000154B915D30D1AD7931C54C30A9FA9C8C244BBFE7E19A259023E85ABBC70F7FE93E7D2682A36DD2FAE  **Key Check Value: 94EBB3** |

Como o valor do KCV é o mesmo em ambas as chaves, isso indica que a chave é a mesma só que agora ela está protegida pela LMK do tipo Key Block.

# Simulação

## M0 – criptografar dados

|  |
| --- |
| Menssage Header 0000  Command Code M0  Mode Flag 00  Input Format Flag 0  Output Format Flag 0  Key Type 009  Key (BDK) U2F008E2708D73336402C9D1FE25B82FD  KSN Descriptor A05  Key Serial Number BC75601201000DE00003  Message Length 0008  Message 1111111100000000  Delimiter %  LMK Identifier 00  Command 0000M00000009U2F008E2708D73336402C9D1FE25B82FDA05BC75601201000DE000030008<1111111100000000>%00  Received response 0000M100[30303038B8E9AB4BF0CF80A0]  Message Header 0000  Response Code M1  Error Code 00  Message Length 30303038 = 0008  Encrypted Message B8E9AB4BF0CF80A0 |

## M2 – descriptografar dados

|  |
| --- |
| Menssage Header 0000  Command Code M2  Mode Flag (CBC) 00  Input Format Flag 0  Output Format Flag 0  Key Type FFF  Key (BDK) S10096B0TN00S000154B915D30D1AD7931C54C30A9FA9C8C244BBFE7E19A259023E85ABBC70F7FE93E7D2682A36DD2FAE  KSN Descriptor A05  KSN BC75601201000DE00003  Message Length 0008  Encrypted Message <B8E9AB4BF0CF80A0>  Delimiter %  LMK Identifier 01  Command 0000M20000FFFS10096B0TN00S000154B915D30D1AD7931C54C30A9FA9C8C244BBFE7E19A259023E85ABBC70F7FE93E7D2682A36DD2FAEA05BC75601201000DE000030008<B8E9AB4BF0CF80A0>%01  Received response 0000M300[303030381111111100000000]  Message Header 0000  Response Code M3  Error Code 00  Message Length 30303038  Decrypted Message 1111111100000000 |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 11/02/2021 |
| Caio Ferreira | Comando M0 e M2 | 04/03/2021 |
| Evelin Possas | payShield Manager | 22/03/2021 |