

Error Code 41

Índice

[1. Problema 3](#_Toc65573154)

[2. Solução 4](#_Toc65573155)

[2.1. QS = YES 4](#_Toc65573156)

[2.1.1. QS 4](#_Toc65573157)

[2.1.2. LMK 4](#_Toc65573158)

[2.1.3. ZMK - Variant 4](#_Toc65573159)

[2.1.4. BDK – Variant 5](#_Toc65573160)

[2.1.5. KE – Variant 5](#_Toc65573161)

[2.1.6. ZMK – Key Block 6](#_Toc65573162)

[2.1.7. IK 6](#_Toc65573163)

[2.1.8. M0 7](#_Toc65573164)

[2.2. QS = NO 8](#_Toc65573165)

[2.2.1. QS 8](#_Toc65573166)

[2.2.2. M0 8](#_Toc65573167)

[3. Conclusão 9](#_Toc65573168)

[3.1. Cabeçalho 9](#_Toc65573169)

[4. Release Notes 10](#_Toc65573170)

# Problem

|  |
| --- |
| Received response 0000KF41  Message Header 0000  Response Code KF  Error Code 41  Message Length  Encrypted Message |

# Description

## LMK

|  |
| --- |
| Online-AUTH>vt    LMK table:  ID Authorized Scheme Algorithm Status Check Comments  01 Yes(H,C) Variant 3DES(2key) Test 268604 variant  Key change storage table:No keys loaded in key change storage |

### ZMK - Variant

|  |
| --- |
| 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: 8980 CEBC 4F43 299B D916 4AB9 8543 CD86  Encrypted component: U8A9C C00C 8D15 C612 497F E1A5 083B 2301  Key check value: 0CA36C  Clear component: 3145 024A E516 F7A1 32BF 3E34 7C08 C270  Encrypted component: U77BA 3B3C D4E4 C31A B132 259F 104D E671  Key check value: 5072EB  Clear component: 3DA8 37E3 5D38 25C8 BC94 2523 ECDF 62F8  Encrypted component: UB78D B9F1 9FE8 AB65 11E3 7490 D5F6 BF47  Key check value: DD0005  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 [1-9]: 3  Encrypted key: U9CC9 65DE B4B6 774F 5531 9BC7 5840 142F  Key check value: 33166A |

### BDK – Variant

|  |
| --- |
| Online-AUTH>gc    Enter LMK id [0-1]: 0  Enter key length [1,2,3]: 2  Enter key type: 009  Enter key scheme: u    Clear component: 764C 6B15 BF23 9497 408F 0E64 3740 02E6  Encrypted component: UF342 12CB 47D6 B264 69B5 E096 22EF A73E  Key check value: EF690C  Clear component: 01A8 3DFE 5B8A 68E9 AE08 01EF 7FC4 6D94  Encrypted component: UDB18 1662 169D 76D1 D523 BD08 D906 BD5F  Key check value: DFC2EF  Clear component: AE68 863B 942A 769B 6E98 D980 010B 6816  Encrypted component: UDADE 44E7 0B7C BC62 C906 497E 8A47 0D89  Key check value: 3AEF12  Online-AUTH>fk    Enter LMK id [0-1]: 0  Enter key length [1,2,3]: 2  Enter key type: 009  Enter key scheme: u  Enter component type [X,H,T,E,S]: x  Enter number of components [1-9]: 3    Encrypted key: U17BE D661 29A2 CFDB 0C9C E3AD 790A EC92  Key check value: 08AF5C |

### KE – Variant

|  |
| --- |
| Online-AUTH>ke    Enter LMK id [0-1]: 0  Enter key type: 009  Enter key scheme: x  Enter ZMK: U9CC9 65DE B4B6 774F 5531 9BC7 5840 142F  Enter key under LMK: U17BE D661 29A2 CFDB 0C9C E3AD 790A EC92    Key under ZMK: X5A33 096D F9B5 5812 15F4 33CE 98B3 6BCB  Key check value: 08AF5C |

### ZMK – Key Block

|  |
| --- |
| 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 [1-9]: 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: S10096K0TN00S0001B6C2B85F1E849E72C5FAEC4EC0BE6C3D18425F8226EA2B5F6B59ADF67E091843AB11052E5FBD9683  Key check value: 33166A |

### IK

|  |
| --- |
| Online-AUTH>ik    Enter LMK id [0-1]: 1  Enter key scheme: s  Enter ZMK: S10096K0TN00S0001B6C2B85F1E849E72C5FAEC4EC0BE6C3D18425F8226EA2B5F6B59ADF67E091843AB11052E5FBD9683  Enter key: X5A33 096D F9B5 5812 15F4 33CE 98B3 6BCB  Enter Key Usage: b0  Enter Mode of Use: n  Enter Key Version Number: 000  Invalid Key Version Number; please re-enter: 00  Enter Exportability: s  Enter Optional Blocks? [Y/N]: n    Encrypted key: S10096B0TN00S0001C3F33EDC9F134B0886719387159BC49B22706329C8686028BB00770FD18DB8450EF59FFC68CA99EB  Key check value: 08AF5C |

### M0

|  |
| --- |
| Menssage Header 0000  Command Code M0  Mode Flag (ECB) 00  Input Format Flag 2  Output Format Flag 1  Key Type FFF  Key S10096B0TN00S0001C3F33EDC9F134B0886719387159BC49B22706329C8686028BB00770FD18DB8450EF59FFC68CA99EB  KSN Descriptor A05  Key Serial Number BC75601201000DE00003  Message Length 0020  Message 3194A9F6805322923194A9F680532292  Delimiter %  LMK Identifier 01  Command 0000M00021FFFS10096B0TN00S0001C3F33EDC9F134B0886719387159BC49B22706329C8686028BB00770FD18DB8450EF59FFC68CA99EBA05BC75601201000DE0000300203194A9F6805322923194A9F680532292%01  Received response 0000M10000408E1DDF0A3C02A73C3CFD9C133B49358E8E1DDF0A3C02A73C3CFD9C133B49358E  Message Header 0000  Response Code M1  Error Code 00  Message Length 0040  Encrypted Message 8E1DDF0A3C02A73C3CFD9C133B49358E8E1DDF0A3C02A73C3CFD9C133B49358E |

## QS = NO

### QS

|  |
| --- |
| Ignore LMK ID in Key Block Header: NO |

### M0

|  |
| --- |
| Menssage Header 0000  Command Code M0  Mode Flag (ECB) 00  Input Format Flag 2  Output Format Flag 1  Key Type FFF  Key S10096B0TN00S0001C3F33EDC9F134B0886719387159BC49B22706329C8686028BB00770FD18DB8450EF59FFC68CA99EB  KSN Descriptor A05  Key Serial Number BC75601201000DE00003  Message Length 0020  Message 3194A9F6805322923194A9F680532292  Delimiter %  LMK Identifier 00  Command 0000M00021FFFS10096B0TN00S0001C3F33EDC9F134B0886719387159BC49B22706329C8686028BB00770FD18DB8450EF59FFC68CA99EBA05BC75601201000DE0000300203194A9F6805322923194A9F680532292%00  Received response 0000M1A2  Message Header 0000  Response Code M1  Error Code A2  Message Length  Encrypted Message |

# Conclusão

## Cabeçalho

Cabeçalho de uma chave de criptografia do tipo Key Block

|  |  |  |
| --- | --- | --- |
| **Byte(s)** | **Field** | **Comments** |
| 0 | Version ID | value = "0" (X'30) when protected by a 3-DES key value = "1" (X'31) when protected by an AES key |
| 1-4 | Key Block Length | total length of key block |
| 5-6 | Key Usage | e.g. key encryption, data encryption |
| 7 | Algorithm | e.g. DES, 3-DES, AES |
| 8 | Mode of Use | e.g. encrypt only |
| 9-10 | Key Version Number | e.g. version of key in the key block or used to indicate that the key is a key component |
| 11 | Exportability | e.g. exportable under a trusted key |
| 12-13 | Number of optional  blocks | number of Optional Header Blocks |
| 14-15 | LMK ID | LMK identifier (to support multiple LMKs); numeric values "00" - "19" (X'3030 - X'3139) |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 02/03/2021 |
|  |  |  |