

**Comando L6**

Índice

[1. HSM 3](#_Toc68600583)

[1.1. LMK 3](#_Toc68600584)

[1.2. ZMK 3](#_Toc68600585)

[2. OpenSSL 4](#_Toc68600586)

[3. Tools 6](#_Toc68600587)

[3.1. Crypto - Ajuste 6](#_Toc68600588)

[3.2. BPTools - criptografia 8](#_Toc68600589)

[3.3. Crypto - criptografia 9](#_Toc68600590)

[4. Comando 11](#_Toc68600591)

[4.1. L6 11](#_Toc68600592)

[4.2. L7 12](#_Toc68600593)

[5. Release Notes 13](#_Toc68600594)

# HSM

## LMK

|  |
| --- |
| Online-AUTH>vt  LMK table:  ID Authorized Scheme Algorithm Status Check Comments  00 Yes(H,C) Variant 3DES(2key) Test 268604 variant  Key change storage table:No keys loaded in key change storage |

## ZMK

# Componente

|  |
| --- |
| Online-AUTH>gc    Enter LMK id [0-1]: 0  Enter key length [1,2,3]: 3  Enter key type: 000  Enter key scheme: t    Clear component: **E008 4FE3 5E83 6E2A 0154 0102 BF01 540B 1FBC 70B3 D01F 1FC7**  Encrypted component: TC159 C0B6 BEAE 4851 3634 0788 6D31 8963 F578 F585 CCF2 37D8  Key check value: 550B57 |

# Chave

|  |
| --- |
| Online-AUTH>fk    Enter LMK id [0-1]: 0  Enter key length [1,2,3]: 3  Enter key type: 000  Enter key scheme: t  Enter component type [X,H,T,E,S]: x  Enter number of components [1-9]: 1    Enter component 1: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Component 1 check value: 550B57  Continue? [Y/N]: y      Encrypted key: **T4A49 3C7E 7F5D 6ABB 05D7 D93E DD90 0E6D 8CB4 8D3D A427 CFDA**  Key check value: 550B57 |

# OpenSSL

# Gerar par de chave RSA

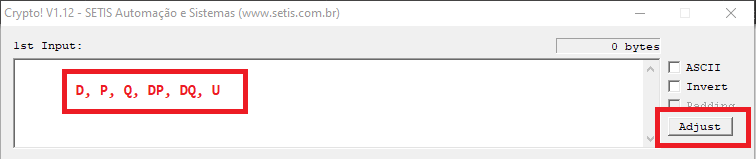
|  |
| --- |
| openssl genrsa -aes128 -passout pass:12345 -out rsakey.pem 2048 |

# Exibir dados da chave RSA

|  |
| --- |
| openssl pkey -in rsakey.pem -passout pass: -text  modulus(chave pública):  00:bc:b5:14:72:96:57:7b:c5:54:0c:39:46:95:7d:  20:7a:20:8e:90:cf:84:45:f4:5b:fe:45:b2:9b:f0:  96:4f:e4:08:aa:68:b5:8c:16:38:30:12:67:10:74:  1e:65:f1:d4:12:b2:83:99:36:f9:ef:32:25:79:4d:  7e:52:35:fb:f1:99:b5:00:8d:97:92:bb:4d:3e:80:  a3:62:d1:fc:64:a0:7b:b0:9e:b8:76:c8:0e:35:53:  eb:b3:90:3e:ee:ef:06:74:73:57:8c:d1:c0:7f:c3:  b4:60:7d:63:8c:9f:99:af:87:f9:7b:87:32:c3:fb:  1d:2c:39:aa:f8:38:e8:5f:65:40:27:42:e9:5e:e3:  ee:9e:c8:5e:a8:47:0e:9f:1a:23:58:87:d7:67:b4:  17:7c:92:0b:6f:26:58:10:d2:74:f6:d1:a8:bd:a5:  68:72:b9:e5:17:1e:d6:67:dd:22:7b:c6:24:10:72:  f6:97:78:b7:02:9b:a9:5f:28:0f:fd:c6:57:5a:2e:  4a:1f:9f:be:d4:c9:57:ee:af:c0:fd:4c:40:65:41:  df:51:0b:03:ce:26:d2:b1:97:19:45:57:1b:5c:b9:  79:32:f1:9e:8e:8d:d8:62:45:9d:d5:e6:68:47:18:  da:2d:37:a6:ce:db:af:63:02:22:0d:f3:b7:6b:bc:  78:01  (…)  prime1(P):  00:f4:15:87:a6:fe:2f:47:c3:c4:c7:d0:19:cf:64:  a4:2b:3f:ad:ea:08:4e:a6:8f:53:1b:01:3c:b0:9f:  d3:7c:60:10:d0:f3:fd:e6:b1:a6:a2:c2:a9:bc:60:  ba:d1:4a:e2:be:a0:31:36:63:4b:f4:eb:30:f9:8e:  f5:dd:03:81:d2:a4:6c:3f:ef:8c:cb:1d:ac:4b:73:  8b:89:f4:6a:c8:b5:dc:a4:3e:f0:75:93:23:4a:fb:  76:95:bb:11:91:95:f0:bf:bd:77:26:da:4f:06:74:  2b:8d:b7:68:d1:c5:b5:80:ff:f5:43:47:c2:cf:64:  25:74:a5:cd:a2:b2:02:3d:f9  prime2(Q):  00:c5:eb:78:ec:78:9f:c7:5e:70:b5:42:9e:08:52:  f5:19:4b:b7:24:f2:3a:23:0d:c0:19:b9:a7:6b:bf:  62:c7:ae:94:e4:ad:9f:48:da:e4:c8:5a:4f:aa:7e:  11:cd:2e:66:5a:89:14:92:32:91:41:59:9d:fd:7a:  78:b7:6b:b6:46:97:44:ee:a2:0c:f6:19:ec:80:4c:  07:ff:3c:8b:46:75:ca:13:e8:f8:94:a3:ef:a6:ce:  8d:bc:e8:ad:fa:39:01:31:da:6e:ac:d9:09:19:a2:  dd:eb:d3:6c:80:48:43:03:1c:b9:38:37:58:b2:58:  9c:44:b8:25:58:be:82:2c:49  exponent1(DP):  00:e3:37:67:a0:3c:df:26:9f:47:7f:fa:69:0c:77:  53:9c:2f:1b:66:d1:74:e5:f8:66:14:ad:82:21:a9:  a6:e6:11:47:96:3c:8c:0f:45:31:2a:32:ac:6f:80:  5c:68:98:9d:9b:76:e4:59:0c:f6:98:78:98:8e:b8:  56:87:f7:cb:d2:9a:dd:6a:67:45:59:8f:b5:e4:47:  1b:8e:c0:c8:e7:2e:e4:c6:c1:10:77:63:11:67:ab:  cf:28:73:8c:57:4a:8d:62:f0:ad:0a:ae:0f:02:a3:  02:28:5a:a4:69:22:f3:63:b2:e2:4e:4f:6f:3a:40:  af:dd:76:bb:86:c8:ce:ed:81  exponent2(DQ):  00:9b:fd:94:28:24:86:21:f7:70:33:9c:96:bb:8e:  ce:b8:aa:31:65:c0:38:4c:0a:79:5e:8d:31:c4:3d:  6a:98:61:23:de:fc:6c:af:5a:3e:b9:1e:5c:ed:ce:  41:2f:8b:23:86:b5:c5:ed:d8:47:1d:cf:89:33:10:  04:f6:e3:c1:1c:ef:fa:97:6e:47:72:ec:49:b7:70:  b5:58:d8:9a:18:e5:9b:68:87:d4:ec:2a:2d:27:36:  63:06:02:09:a5:4e:aa:7f:65:5e:97:82:d3:a6:4d:  f4:44:fb:34:e8:02:8c:36:76:bc:10:ef:a6:4b:a2:  85:3f:b0:37:57:33:87:9b:69  Coeficiente(U):  22:1e:95:23:ee:0a:65:ee:47:6f:7a:7b:22:a1:cf:  00:98:9a:ab:ec:63:9e:3e:86:72:95:0d:f0:82:10:  95:cb:3f:9a:b7:bb:40:24:d0:bf:52:97:89:87:1f:  87:5b:f9:eb:bf:b4:d3:cf:ce:92:d3:69:84:a7:f1:  8b:db:b7:9e:d6:41:53:bc:0a:7a:24:5d:ea:6a:ff:  d1:34:b6:90:88:88:78:23:d3:69:25:3b:64:cf:84:  a9:43:85:96:c5:6d:07:af:1b:96:14:17:95:b8:49:  ea:2b:3d:00:30:b3:08:ad:42:ef:b7:58:36:ec:b4:  93:01:56:03:c4:a8:a4:20 |

# Tools

## Crypto - Ajuste



# Modulus (chave pública):

|  |
| --- |
||

# P (em claro)

|  |
| --- |
| F41587A6FE2F47C3C4C7D019CF64A42B3FADEA084EA68F531B013CB09FD37C6010D0F3FDE6B1A6A2C2A9BC60BAD14AE2BEA03136634BF4EB30F98EF5DD0381D2A46C3FEF8CCB1DAC4B738B89F46AC8B5DCA43EF07593234AFB7695BB119195F0BFBD7726DA4F06742B8DB768D1C5B580FFF54347C2CF642574A5CDA2B2023DF9 |

# Q (em claro)

|  |
| --- |
| C5EB78EC789FC75E70B5429E0852F5194BB724F23A230DC019B9A76BBF62C7AE94E4AD9F48DAE4C85A4FAA7E11CD2E665A891492329141599DFD7A78B76BB6469744EEA20CF619EC804C07FF3C8B4675CA13E8F894A3EFA6CE8DBCE8ADFA390131DA6EACD90919A2DDEBD36C804843031CB9383758B2589C44B82558BE822C49 |

# DP (em claro)

|  |
| --- |
| E33767A03CDF269F477FFA690C77539C2F1B66D174E5F86614AD8221A9A6E61147963C8C0F45312A32AC6F805C68989D9B76E4590CF69878988EB85687F7CBD29ADD6A6745598FB5E4471B8EC0C8E72EE4C6C11077631167ABCF28738C574A8D62F0AD0AAE0F02A302285AA46922F363B2E24E4F6F3A40AFDD76BB86C8CEED81 |

# DQ (em claro)

|  |
| --- |
| 9BFD9428248621F770339C96BB8ECEB8AA3165C0384C0A795E8D31C43D6A986123DEFC6CAF5A3EB91E5CEDCE412F8B2386B5C5EDD8471DCF89331004F6E3C11CEFFA976E4772EC49B770B558D89A18E59B6887D4EC2A2D273663060209A54EAA7F655E9782D3A64DF444FB34E8028C3676BC10EFA64BA2853FB0375733879B69 |

# U (em claro)

|  |
| --- |
| 221E9523EE0A65EE476F7A7B22A1CF00989AABEC639E3E8672950DF0821095CB3F9AB7BB4024D0BF529789871F875BF9EBBFB4D3CFCE92D36984A7F18BDBB79ED64153BC0A7A245DEA6AFFD134B69088887823D369253B64CF84A9438596C56D07AF1B96141795B849EA2B3D0030B308AD42EFB75836ECB493015603C4A8A420 |

## BPTools - criptografia



## Crypto - criptografia



# P (criptografado pela ZMK em claro)

|  |
| --- |
| 4D72E4F85C11A1F0FA673468E3C3E414FA3BC315A8C2201D9B1357AF156D2AD28238B7F60E6BC6335B3FFB4F93E149364E268AA61B244219E30EE4C477B35E744A108CC615BE37E810CBD5DE0F8E1EB7FBD1B2B647EABEC08D9954EB5BE35DFDBEF5117675937610D65577B07F9244E9390CFCC4E87C38D8453AA6825601A69B |

# Q (criptografado pela ZMK em claro)

|  |
| --- |
| 1EB29E53FE6D8A06CA2FE679558083CE4B825DDEC5BA0F8FD7CA0F86F1E260C6ED77E4D4C1C3EDBF09F4917B0EB2C2668A84163943AD089BB071E0C6026FA695DBDFAC77A74BB789163927FE4628D188813026059390B25F37BCE4678648683B71E74B2BB32CC93F2F9C0B52D0328C4DF5E52A8E0A9160D27F286694C86DF325 |

# DP (criptografado pela ZMK em claro)

|  |
| --- |
| 1854AFC4932533281D2337E9CA36C439B8E71FC7F55EE7391C3A3F1AFA422F740ABE135F5912C083CA8A42CA8C28F346B2A626EACEFF4F3A9574D22F0A9E89D6CFAB0FACF099FE20DDDE790BB6D650897FF0E83A7A225ADCE10D1293C72F10ABB78E6594C5CB48C7158DFA6CC4C788F41F507F69E4B2D17686FC26B8F818B443 |

# DQ (criptografado pela ZMK em claro)

|  |
| --- |
| 4FB8EEDA5E5CE3A29EAB1B913987CE6D3C3E07C344913DF87D9C99A68FAA3BEF8A8F154AAC9C335E860E6B004C49BC0399F1E1F1160A1B9BDCE32245521F482B50B1DA06AABD8E954494E9E717B333046EE78386E4836CDE7065A130C29A8343EC0207A892C4183974E3AD880722211B74BDA0A1965108B5952653A5B3040E22 |

# U (criptografado pela ZMK em claro)

|  |
| --- |
| 7E2A8DFA7E4010ADBD88BAB23983CA9F6B70FAA5F5775F8F37569C207375810CD028DB0CDDB0EB4290D1A38D704E779FE677433EF282B87FCA141BD57BC30692B1B253C49941BDF93F3BB8A057981218E30433DEA6F21C90F26C6297689632E42B5729211089753E8DB948E78C0B8D20471B74EE27162AAD218016EC2BBED808 |

# Comando

## L6

|  |
| --- |
| Message Header 0000  Command Code L6  ZMK T4A493C7E7F5D6ABB05D7D93EDD900E6D8CB48D3DA427CFDA  Key Format 0  Block Cipher Mode 0  Pad mode 1  Private key length 0280  Private keyalidate 1  Public Key length 0100  Public Keyublic Exponent Length 0003  Public Exponent <010001>  Delimiter %  LMK Identifier 00  Command|

## L7

|  |
| --- |
| Received responseessage Header 0000  Response Command L7  Error Code 00  Private Key Length 30323930 (0290)  Private Key|

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Caio Ferreira | Primeira versão | 05/04/2021 |
| Eduardo Campo | Revisão | 05/04/2021 |