FIRST TECH®

Construindo relações duradouras

Mobile Wallet

Import RSA Private Key

Processo:	ORIGINAL - Mobile-Wallet - Import Private Key	Versão:	1.0
Autor:	Eduardo Mendes Campos	Data:	05/04/2021
Revisor:	Caio Abreu Ferreira	Data:	05/04/2021
Aprovador:		Data:	

Índice

1. Etapas

- Criar o par de chaves RSA no OpenSSL (com senha)
- Gerar um componente de chave 3DES tamanho triplo
- Formar uma ZMK 3DES tamanho triplo com o componente criado
- Criptografar cada componente do par de chaves RSA (p, q, dp, dq, u) com a ZMK 3DES tamanho triplo
- Formar o comando de host L6

2. Criar o par de chaves RSA no OpenSSL (com senha)

2.1. Comando de criação

```
OpenSSL> genrsa -aes128 -passout pass:12345 -out rsakey.pem 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.............................................+++++
.............................................+++++
e is 65537 (0x010001)
```

2.2. Comando de exibição da chave RSA e seus componentes

```
OpenSSL> pkey -in rsakey.pem -passout pass: -text
Enter pass phrase for rsakey.pem:

-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQDZ4KtxrX+odKqG
3Viju4fIdq2ywldU81sPfqNck7bRrOzlB0aj1blVEsCiUG9oqhhqGx3XWUBB2dtb
ltoJZT40Crx14xKVSMAU2k+1luk6I9coX1WHPLu93cjo7lyorLu6ljAV3KOMm+Cz
LWu+3cuD93vGQszF04wb8JzPKA4dQ7hojYZhPlsjdcwiIZpdC75+WUB8bnfd+LyF
A0E2C+8sqAO8acrgtjD8SE35iKCdcrJY3QIIrjKfdoTvhWX38oyp7YXOUoVUYPOG
Eu+Bn5G1ev5YIHZ/ARXOQKGk1EI3a0urtMmL4r6lMWJlDGTLbSfHAP5OHQHQ17FG
692dyb4zAgMBAAECggEAa/FwXyibB4WNerWtFalyMzIBCoBYLiFHKx0NqG8Scz0e
PLXnHIJliK16vK/nEk67O85lcWypdjaOBAlvypnbQINVLX6rlURuzaX/ObMjp4dc
MIdS42aGiSGZSTXWuEaj12RTPHGMobwUjhDhwbU3ABGbw/USaKxPTQRfXA63N22M
nqgjHO2aLKWDEBEousVb+/aTgNFG8C6L7iT/aNR0HgUABcKgmiCCftK1fjS4XvZT
eMx4cUT9Btc4k6NipECAH3EddYbc2K3C1FfnhnWh42LdKScdjvsDmvaPlSz4StTv
qP3ujjQSvorPckBvu18g7CJAkSfyMclkz+12H49IEQKBgQDw3ty1Ivb1YqWzvtKq
UXkKE34FARcoLFQbh8jD/VMUcTVJogy3NeIfQUbcTJX+L68J3M70LiYEylWIsbzL
4H8onJv2ftUl6QHQUnx5WJfW6i492Td+tuPVQp+pxSLkqIm9QioXtg1kl6O4tZEn
QzfG2fQPY0eYGBODmzq/LYrD2wKBgQDnkBY+oawk4soW8MTwF9MlcDikwHU0Ag19
t3OjnL7Gq6OQGLfvLhZ1kY413WdmB07u9GtVQ91ePIoM1NF8SIvKTEYk14Bx2VbM
tVYUBxIWSv+LDAYMSdMaKgSfkfKnISK9siMWuTtIQsLX72TFEzZcooBxVqxK93Vy
j/nULr8qiQKBgFAfUftO7ich8UyhJSJSh5i6cyjm+/T5CeE+gaHwGjqqjbc4mFI5
MkaDSDbvotUyt17ofE7tKuhdBaa6uLp4qtOvhJGyDuTVZS0Owyj6N0feDhO0takI
3TCLQOEQGlNFXMv/vlC01i+n4WYHv4j36w3SYkTcGWyWVadpc1k0pPwRAoGAAoMe
qqlIW9IWDS+pg01O3h4cjzUDUIAhM1b1KzY9H5ynFp4eCLtARSBCIbV4NLQpmBAQ
xgkJcsdHXCJG74k98wDm1el8nD+WYHwrJeZ5vMItiY2k1ydJ4gPIrw5/Sm7imJpB
JTL3QK5wvLT9K+Isec7Ng+1Dy0BqBscnF7U2H7kCgYAteuExFE/ayO613MvRemtb
```

```
s+gN7AM/dnQO+7smWE0FX8BgFITMCqHOGRuky8dfo/+DnX5v07F+9QqeWHzz0ubT
22MxRnBlWibERdcLruyV8g+p7m5Z6kaP9nPlP7eJ/O7jWgIZ3WfJcGDFPRLJBG9m
lksMaWNdOK/V5VMtbfs/MQ==
-----END PRIVATE KEY-----
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:d9:e0:ab:71:ad:7f:a8:74:aa:86:dd:58:a3:bb:
    87:c8:76:ad:b2:c2:57:54:f3:5b:0f:7e:a3:5c:93:
    b6:d1:ac:ec:e5:07:46:a3:d5:b9:55:12:c0:a2:50:
    6f:68:aa:18:6a:1b:1d:d7:59:40:41:d9:db:5b:96:
    da:09:65:3e:34:0a:bc:75:e3:12:95:48:c0:14:da:
    4f:b5:96:e9:3a:23:d7:28:5f:55:87:3c:bb:bd:dd:
    c8:e8:ee:5c:a8:ac:bb:ba:96:30:15:dc:a3:8c:9b:
    e0:b3:2d:6b:be:dd:cb:83:f7:7b:c6:42:cc:c5:d3:
    8c:1b:f0:9c:cf:28:0e:1d:43:b8:68:8d:86:61:3e:
    5b:23:75:cc:22:21:9a:5d:0b:be:7e:59:40:7c:6e:
    77:dd:f8:bc:85:03:41:36:0b:ef:2c:a8:03:bc:69:
    ca:e0:b6:30:fc:48:4d:f9:88:a0:9d:72:b2:58:dd:
    02:08:ae:32:9f:76:84:ef:85:65:f7:f2:8c:a9:ed:
    85:ce:52:85:54:60:f3:86:12:ef:81:9f:91:b5:7a:
    fe:58:20:76:7f:01:15:ce:40:a1:a4:d4:42:37:6b:
    4b:ab:b4:c9:8b:e2:be:a5:31:62:65:0c:64:cb:6d:
    27:c7:00:fe:4e:1d:01:d0:d7:b1:46:eb:dd:9d:c9:
    be:33
publicExponent: 65537 (0x10001)
privateExponent:
    6b:f1:70:5f:28:9b:07:85:8d:7a:b5:ad:15:a9:72:
    33:32:01:0a:80:58:2e:21:47:2b:1d:0d:a8:6f:12:
    73:3d:1e:3c:b5:e7:1c:82:65:88:ad:7a:bc:af:e7:
    12:4e:bb:3b:ce:65:71:6c:a9:76:36:8e:04:09:6f:
    ca:99:db:40:83:55:2d:7e:ab:95:44:6e:cd:a5:ff:
    39:b3:23:a7:87:5c:30:87:52:e3:66:86:89:21:99:
    49:35:d6:b8:46:a3:d7:64:53:3c:71:8c:a1:bc:14:
    8e:10:e1:c1:b5:37:00:11:9b:c3:f5:12:68:ac:4f:
    4d:04:5f:5c:0e:b7:37:6d:8c:9e:a8:23:1c:ed:9a:
    2c:a5:83:10:11:28:ba:c5:5b:fb:f6:93:80:d1:46:
    f0:2e:8b:ee:24:ff:68:d4:74:1e:05:00:05:c2:a0:
    9a:20:82:7e:d2:b5:7e:34:b8:5e:f6:53:78:cc:78:
    71:44:fd:06:d7:38:93:a3:62:a4:40:80:1f:71:1d:
    75:86:dc:d8:ad:c2:d4:57:e7:86:75:a1:e3:62:dd:
    29:27:1d:8e:fb:03:9a:f6:8f:95:2c:f8:4a:d4:ef:
    a8:fd:ee:8e:34:12:be:8a:cf:72:40:6f:bb:5f:20:
    ec:22:40:91:27:f2:31:c9:64:cf:ed:76:1f:8f:48:
    11
prime1:
    00:f0:de:dc:b5:22:f6:f5:62:a5:b3:be:d2:aa:51:
    79:0a:13:7e:05:01:17:28:2c:54:1b:87:c8:c3:fd:
    53:14:71:35:49:a2:0c:b7:35:e2:1f:41:46:dc:4c:
    95:fe:2f:af:09:dc:ce:f4:2e:26:04:ca:55:88:b1:
    bc:cb:e0:7f:28:9c:9b:f6:7e:d5:25:e9:01:d0:52:
    7c:79:58:97:d6:ea:2e:3d:d9:37:7e:b6:e3:d5:42:
    9f:a9:c5:22:e4:a8:89:bd:42:2a:17:b6:0d:64:97:
```

```
    a3:b8:b5:91:27:43:37:c6:d9:f4:0f:63:47:98:18:
    13:83:9b:3a:bf:2d:8a:c3:db
prime2:
    00:e7:90:16:3e:a1:ac:24:e2:ca:16:f0:c4:f0:17:
    d3:25:70:38:a4:c0:75:34:02:0d:7d:b7:73:a3:9c:
    be:c6:ab:a3:90:18:b7:ef:2e:16:75:91:8e:35:dd:
    67:66:07:4e:ee:f4:6b:55:43:dd:5e:3c:8a:0c:d4:
    d1:7c:48:8b:ca:4c:46:24:d7:80:71:d9:56:cc:b5:
    56:14:07:12:16:4a:ff:8b:0c:06:0c:49:d3:1a:2a:
    04:9f:91:f2:a7:21:22:bd:b2:23:16:b9:3b:48:42:
    c2:d7:ef:64:c5:13:36:5c:a2:80:71:56:ac:4a:f7:
    75:72:8f:f9:d4:2e:bf:2a:89
exponent1:
    50:1f:51:fb:4e:ee:27:21:f1:4c:a1:25:22:52:87:
    98:ba:73:28:e6:fb:f4:f9:09:e1:3e:81:a1:f0:1a:
    3a:aa:8d:b7:38:98:52:39:32:46:83:48:36:ef:a2:
    d5:32:b7:5e:e8:7c:4e:ed:2a:e8:5d:05:a6:ba:b8:
    ba:78:aa:d3:af:84:91:b2:0e:e4:d5:65:2d:0e:c3:
    28:fa:37:47:de:0e:13:b4:b5:a9:08:dd:30:8b:40:
    e1:10:1a:53:45:5c:cb:ff:be:50:b4:d6:2f:a7:e1:
    66:07:bf:88:f7:eb:0d:d2:62:44:dc:19:6c:96:55:
    a7:69:73:59:34:a4:fc:11
exponent2:
    02:83:1e:aa:a9:48:5b:d2:16:0d:2f:a9:83:4d:4e:
    de:1e:1c:8f:35:03:50:80:21:33:56:f5:2b:36:3d:
    1f:9c:a7:16:9e:1e:08:bb:40:45:20:42:21:b5:78:
    34:b4:29:98:10:10:c6:09:09:72:c7:47:5c:22:46:
    ef:89:3d:f3:00:e6:d5:e9:7c:9c:3f:96:60:7c:2b:
    25:e6:79:bc:c2:2d:89:8d:a4:d7:27:49:e2:03:c8:
    af:0e:7f:4a:6e:e2:98:9a:41:25:32:f7:40:ae:70:
    bc:b4:fd:2b:e2:2c:79:ce:cd:83:ed:43:cb:40:6a:
    06:c7:27:17:b5:36:1f:b9
coefficient:
    2d:7a:e1:31:14:4f:da:c8:ee:b5:dc:cb:d1:7a:6b:
    5b:b3:e8:0d:ec:03:3f:76:74:0e:fb:bb:26:58:4d:
    05:5f:c0:60:14:84:cc:0a:a1:ce:19:1b:a4:cb:c7:
    5f:a3:ff:83:9d:7e:6f:d3:b1:7e:f5:0a:9e:58:7c:
    f3:d2:e6:d3:db:63:31:46:70:65:5a:26:c4:45:d7:
    0b:ae:ec:95:f2:0f:a9:ee:6e:59:ea:46:8f:f6:73:
    e5:3f:b7:89:fc:ee:e3:5a:02:19:dd:67:c9:70:60:
    c5:3d:12:c9:04:6f:66:96:4b:0c:69:63:5d:38:af:
    d5:e5:53:2d:6d:fb:3f:31
```

3. Gerar um componente de chave 3DES tamanho triplo (HSM)

```
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: 37B0 EC94 B594 839D 2370 585E AD75 A262 3D5B 13C1 F297
85C7
Encrypted component: T8EBF 9E8B A568 04E0 362D CE35 5E97 6D94 F8D0 1711
24DD F5D3
Key check value: AD8A47
```

4. Formar uma ZMK 3DES tamanho triplo com o componente criado (HSM)

```
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: 37B0 EC94 B594 839D 2370 585E AD75 A262 3D5B 13C1 F297
85C7
Component 1 check value: AD8A47
Continue? [Y/N]: y

Encrypted key: T3B0C E92B 3BB7 94FF CBD3 7DD5 0B43 291C 683D 4B24 80CE
8BA0
Key check value: AD8A47
```

5. Criptografar cada componente do par de chaves RSA (p, q, dp, dq, u) com a ZMK 3DES tamanho triplo

5.1. Organizando os componentes

5.1.1. *Prime1* em claro (p):

```
F0DEDCB522F6F562A5B3BED2AA51790A137E050117282C541B87C8C3FD5314713549A20CB
735E21F4146DC4C95FE2FAF09DCCEF42E2604CA5588B1BCCBE07F289C9BF67ED525E901D0
527C795897D6EA2E3DD9377EB6E3D5429FA9C522E4A889BD422A17B60D6497A3B8B591274
337C6D9F40F6347981813839B3ABF2D8AC3DB
```

5.1.2. *Prime2* em claro (q):

```
E790163EA1AC24E2CA16F0C4F017D3257038A4C07534020D7DB773A39CBEC6ABA39018B7E
F2E1675918E35DD6766074EEEF46B5543DD5E3C8A0CD4D17C488BCA4C4624D78071D956CC
B556140712164AFF8B0C060C49D31A2A049F91F2A72122BDB22316B93B4842C2D7EF64C51
3365CA2807156AC4AF775728FF9D42EBF2A89
```

5.1.3. *Exponent1* em claro (dp):

```
501F51FB4EEE2721F14CA12522528798BA7328E6FBF4F909E13E81A1F01A3AAA8DB738985
2393246834836EFA2D532B75EE87C4EED2AE85D05A6BAB8BA78AAD3AF8491B20EE4D5652D
0EC328FA3747DE0E13B4B5A908DD308B40E1101A53455CCBFFBE50B4D62FA7E16607BF88F
7EB0DD26244DC196C9655A769735934A4FC11
```

5.1.4. *Exponent2* em claro (dq):

```
02831EAAA9485BD2160D2FA9834D4EDE1E1C8F35035080213356F52B363D1F9CA7169E1E0
8BB4045204221B57834B429981010C6090972C7475C2246EF893DF300E6D5E97C9C3F9660
7C2B25E679BCC22D898DA4D72749E203C8AF0E7F4A6EE2989A412532F740AE70BCB4FD2BE
22C79CECD83ED43CB406A06C72717B5361FB9
```

5.1.5. *Coefficient* em claro (u):

```
2D7AE131144FDAC8EEB5DCCBD17A6B5BB3E80DEC033F76740EFBBB26584D055FC0601484C
C0AA1CE191BA4CBC75FA3FF839D7E6FD3B17EF50A9E587CF3D2E6D3DB63314670655A26C4
45D70BAEEC95F20FA9EE6E59EA468FF673E53FB789FCEEE35A0219DD67C97060C53D12C90
46F66964B0C69635D38AFD5E5532D6DFB3F31
```

5.2. Componentes criptografados pela ZMK 3DES tamanho triplo

5.2.1. *Prime1* criptografado (d):

```
58CFD9AA9E586F61D57BA8998816B8509C7FFAD398B6B4068C08F44971B2D4A6AB9E3F10A
8A9DADF743844938195F8906DAB55F109ED68D16A6CCCC1D8E2F71E040862A862CE131A22
ED1AFB27AE4ADE39B37EF9C092BD39E211A4628CDA98AA9D89F6203D1571EB84B16A6790D
B834544E9F8D1B7BA0962007C11F374A58048
```

5.2.2. *Prime2* criptografado (q):

```
3A1FECA0B67611E9482D4D2A03CE605F7104275D8BC96FA9A5B3E7B0C43DA3AF40B2489F4
985D0255C03C37F022AF1388F384B48DC1DAFC963465E8D1481B69572171CB1132D82857A
04FCC78B182C87E7632D8F816E64836AC14749C45977A671131C4E972F995F73DE527B5FA
0C01C91B20540BC0710FB2EDD4475C78A65FE
```

5.2.3. *Exponent1* criptografado (dp):

```
89A042B9990CE8112D16F2C5C8B2B4D19C57CD8056D61C9C742BE23A130122E4C48D4B64F
95882C3A8E03839571C79E3C107792F85A877448A6091026965CEEA6A612B9E999E286F20
1DF4CF11EAB0D658CE2ED5AB9E15733522BD2A067AE855DE8D98C8CEEC3D085AF9AC03251
CFB3493CC947079EC9B831158AAF4670451C2
```

5.2.4. *Exponent2* criptografado (dq):

```
AB0EF267F11BD6E898FB2017FF616E8045EDF19A7A64F4299DDBD4B669A55A530A5EDCD47
6823567799CCCD897308FCE5F812CF20A689E95A7A2F27AB1023E9087C78DD8A70026F66E
C7F1274EC134D4076C9CF2C41E2CB4DF2FE4D8BDAFDD0258ABFDA9B186460ACAFBDE7D143
EE10D8CE2DDD654D901C080E5834948FF61B7
```

5.2.5. *Coefficient* criptografado (u):

```
93FAF1E934C37A2097B9DC330ADB2D636DF1FB7D3DDED4DC5CC8E08D09CFA46A04B23A155
39CF6FCBA91784A2BDDACBAB09B72C678D364075196DFF4F8411A09F06227761AF3355B74
1A8ED6E07CCF6F8AC9A0EA64267036466748B60DAD067C32388CBB751DE7646E5EDB6D10D
0728303271B9D759DD11514276C4D576BE489
```

6. Formar o comando de host L6

6.1. Detalhamento do Comando

```
Message Header                                  0000

Command Code                                    L6

ZMK
      T3B0CE92B3BB794FFCBD37DD50B43291C683D4B2480CE8BA0

Key Format                                      0

Block Cipher Mode                               0

Pad mode                                        1

Private key length                              0280

Private key
      <58CFD9AA9E586F61D57BA8998816B8509C7FFAD398B6B4068C08F44971B2D4A6AB
9E3F10A8A9DADF743844938195F8906DAB55F109ED68D16A6CCCC1D8E2F71E040862A862C
E131A22ED1AFB27AE4ADE39B37EF9C092BD39E211A4628CDA98AA9D89F6203D1571EB84B1
6A6790DB834544E9F8D1B7BA0962007C11F374A580483A1FECA0B67611E9482D4D2A03CE6
05F7104275D8BC96FA9A5B3E7B0C43DA3AF40B2489F4985D0255C03C37F022AF1388F384B
48DC1DAFC963465E8D1481B69572171CB1132D82857A04FCC78B182C87E7632D8F816E648
36AC14749C45977A671131C4E972F995F73DE527B5FA0C01C91B20540BC0710FB2EDD4475
C78A65FE89A042B9990CE8112D16F2C5C8B2B4D19C57CD8056D61C9C742BE23A130122E4C
48D4B64F95882C3A8E03839571C79E3C107792F85A877448A6091026965CEEA6A612B9E99
9E286F201DF4CF11EAB0D658CE2ED5AB9E15733522BD2A067AE855DE8D98C8CEEC3D085AF
9AC03251CFB3493CC947079EC9B831158AAF4670451C2AB0EF267F11BD6E898FB2017FF61
6E8045EDF19A7A64F4299DDBD4B669A55A530A5EDCD476823567799CCCD897308FCE5F812
CF20A689E95A7A2F27AB1023E9087C78DD8A70026F66EC7F1274EC134D4076C9CF2C41E2C
B4DF2FE4D8BDAFDD0258ABFDA9B186460ACAFBDE7D143EE10D8CE2DDD654D901C080E5834
948FF61B793FAF1E934C37A2097B9DC330ADB2D636DF1FB7D3DDED4DC5CC8E08D09CFA46A
04B23A15539CF6FCBA91784A2BDDACBAB09B72C678D364075196DFF4F8411A09F06227761
AF3355B741A8ED6E07CCF6F8AC9A0EA64267036466748B60DAD067C32388CBB751DE7646E
5EDB6D10D0728303271B9D759DD11514276C4D576BE489>

Validate                                        1

Public Key length                               0100

Public Key
      <D9E0AB71AD7FA874AA86DD58A3BB87C876ADB2C25754F35B0F7EA35C93B6D1ACEC
E50746A3D5B95512C0A2506F68AA186A1B1DD7594041D9DB5B96DA09653E340ABC75E3129
548C014DA4FB596E93A23D7285F55873CBBBDDDC8E8EE5CA8ACBBBA963015DCA38C9BE0B3
2D6BBEDDCB83F77BC642CCC5D38C1BF09CCF280E1D43B8688D86613E5B2375CC22219A5D0
BBE7E59407C6E77DDF8BC850341360BEF2CA803BC69CAE0B630FC484DF988A09D72B258DD
0208AE329F7684EF8565F7F28CA9ED85CE52855460F38612EF819F91B57AFE5820767F011
5CE40A1A4D442376B4BABB4C98BE2BEA53162650C64CB6D27C700FE4E1D01D0D7B146EBDD
9DC9BE33>
```

Public Exponent Length	0003
Public Exponent	<010001>
Delimiter	%
LMK Identifier	00

6.2. Comando concatenado

```
0000L6T3B0CE92B3BB794FFCBD37DD50B43291C683D4B2480CE8BA00010280<58CFD9AA9E
586F61D57BA8998816B8509C7FFAD398B6B4068C08F44971B2D4A6AB9E3F10A8A9DADF743
844938195F8906DAB55F109ED68D16A6CCCC1D8E2F71E040862A862CE131A22ED1AFB27AE
4ADE39B37EF9C092BD39E211A4628CDA98AA9D89F6203D1571EB84B16A6790DB834544E9F
8D1B7BA0962007C11F374A580483A1FECA0B67611E9482D4D2A03CE605F7104275D8BC96F
A9A5B3E7B0C43DA3AF40B2489F4985D0255C03C37F022AF1388F384B48DC1DAFC963465E8
D1481B69572171CB1132D82857A04FCC78B182C87E7632D8F816E64836AC14749C45977A6
71131C4E972F995F73DE527B5FA0C01C91B20540BC0710FB2EDD4475C78A65FE89A042B99
90CE8112D16F2C5C8B2B4D19C57CD8056D61C9C742BE23A130122E4C48D4B64F95882C3A8
E03839571C79E3C107792F85A877448A6091026965CEEA6A612B9E999E286F201DF4CF11E
AB0D658CE2ED5AB9E15733522BD2A067AE855DE8D98C8CEEC3D085AF9AC03251CFB3493CC
947079EC9B831158AAF4670451C2AB0EF267F11BD6E898FB2017FF616E8045EDF19A7A64F
4299DDBD4B669A55A530A5EDCD476823567799CCCD897308FCE5F812CF20A689E95A7A2F2
7AB1023E9087C78DD8A70026F66EC7F1274EC134D4076C9CF2C41E2CB4DF2FE4D8BDAFDD0
258ABFDA9B186460ACAFBDE7D143EE10D8CE2DDD654D901C080E5834948FF61B793FAF1E9
34C37A2097B9DC330ADB2D636DF1FB7D3DDED4DC5CC8E08D09CFA46A04B23A15539CF6FCB
A91784A2BDDACBAB09B72C678D364075196DFF4F8411A09F06227761AF3355B741A8ED6E0
7CCF6F8AC9A0EA64267036466748B60DAD067C32388CBB751DE7646E5EDB6D10D07283032
71B9D759DD11514276C4D576BE489>10100<D9E0AB71AD7FA874AA86DD58A3BB87C876ADB
2C25754F35B0F7EA35C93B6D1ACECE50746A3D5B95512C0A2506F68AA186A1B1DD7594041
D9DB5B96DA09653E340ABC75E3129548C014DA4FB596E93A23D7285F55873CBBBDDDC8E8E
E5CA8ACBBBA963015DCA38C9BE0B32D6BBEDDCB83F77BC642CCC5D38C1BF09CCF280E1D43
B8688D86613E5B2375CC22219A5D0BBE7E59407C6E77DDF8BC850341360BEF2CA803BC69C
AE0B630FC484DF988A09D72B258DD0208AE329F7684EF8565F7F28CA9ED85CE52855460F3
8612EF819F91B57AFE5820767F0115CE40A1A4D442376B4BABB4C98BE2BEA53162650C64C
B6D27C700FE4E1D01D0D7B146EBDD9DC9BE33>0003<010001>%00
```

7. Resposta L7

7.1. Mensagem recebida

```
0000L700[30323930EF4E020F4E42C927CEC33FF3C7D85D61D7B8FB2DAF2BC6EC53C95A69
B1A59E4BE163A7AA6BB4B65BB8AC1D59157F029E54CB6B099142A94C52D36C8758358E9F4
A5F1C48F058787FE2BC4A889C47DA8F0EF0D133125094DDE5036D8B2955E29C278358277B
7E376F9367E64CA3D5CD093EC45C58B886480844A4F88E0E3D343A37464EEA7CE0F85DC23
7D4C3CC974B0E64F1826A7CE9DDB03E2BDFA5AD02CC1B6BC9B6E505B338A2B96139A3DB06
F110B0FA04EFE5E2397513DE8D40D08C34595E8D5D4575CCDD8E0BE62383765B5DAE7EB28
B20B9EB04C890F933E7BD6550F8E4CAB809FF1C249DDE9C9EBD40C6E96DBA62A5A4906909
6969A7EDC12CD58D53E4EC4A813AB379E61B8B75208EDF38EE06482FED972936EED91F22F
C3BD625F8EE7B005E4D4BBFACEC192A343326A7DC2B72C37062C9C7D552748B9466C91FA7
DF0DD9B7D4D76CB64286214D26BDA3010A467C9FEA3B99193BEEFC90E866DABF48014BF0A
A856CE42B7986E4081B5F20079FC55AF071FD2D1096667ADFD32C4E7BE4E47ACB9B0B75EC
B0ABBEF5BC4DD9A4727C3E7FD3EC02B82545009EBDEE58ABA71826A681729DC146990985E
CB4BBE6AEFCB8E1B759519F402D7802E64394680FF32601EB711A03A9448B6D080A1D1224
90A061D4E3BB8B64C6FA580DA15E4D433345129702E35B318867F2A38CF8D5D26168F8EEC
06043FC4DE5B694F5C35E5D39B3F6629B6AC0713AF0C9F7E4BD39F7C895225A3EDD1B2BD5
B90625CA113B8B41558311FA0295DA999631DD8E1E1B0AC2F661BC7421228579906132EA0
407640761D499ABF30DBC515D23E6696E5E9777A0B3C6FEBE17070018B8D0745A17632620
D0241AA51587C17B6677A7EE7306EE7770B45E4E9081B02B96911C66B789EA58A7302D262
58F5AA0F368E675]
```

7.2. Resposta detalhada

```
Message Header                                  0000

Response Command                                L7

Error Code                                      00

Private Key Length                              30323930 (0290)

Private Key
      EF4E020F4E42C927CEC33FF3C7D85D61D7B8FB2DAF2BC6EC53C95A69B1A59E4BE16
3A7AA6BB4B65BB8AC1D59157F029E54CB6B099142A94C52D36C8758358E9F4A5F1C48F058
787FE2BC4A889C47DA8F0EF0D133125094DDE5036D8B2955E29C278358277B7E376F9367E
64CA3D5CD093EC45C58B886480844A4F88E0E3D343A37464EEA7CE0F85DC237D4C3CC974B
0E64F1826A7CE9DDB03E2BDFA5AD02CC1B6BC9B6E505B338A2B96139A3DB06F110B0FA04E
FE5E2397513DE8D40D08C34595E8D5D4575CCDD8E0BE62383765B5DAE7EB28B20B9EB04C8
90F933E7BD6550F8E4CAB809FF1C249DDE9C9EBD40C6E96DBA62A5A49069096969A7EDC12
CD58D53E4EC4A813AB379E61B8B75208EDF38EE06482FED972936EED91F22FC3BD625F8EE
7B005E4D4BBFACEC192A343326A7DC2B72C37062C9C7D552748B9466C91FA7DF0DD9B7D4D
76CB64286214D26BDA3010A467C9FEA3B99193BEEFC90E866DABF48014BF0AA856CE42B79
86E4081B5F20079FC55AF071FD2D1096667ADFD32C4E7BE4E47ACB9B0B75ECB0ABBEF5BC4
DD9A4727C3E7FD3EC02B82545009EBDEE58ABA71826A681729DC146990985ECB4BBE6AEFC
B8E1B759519F402D7802E64394680FF32601EB711A03A9448B6D080A1D122490A061D4E3B
B8B64C6FA580DA15E4D433345129702E35B318867F2A38CF8D5D26168F8EEC06043FC4DE5
B694F5C35E5D39B3F6629B6AC0713AF0C9F7E4BD39F7C895225A3EDD1B2BD5B90625CA113
B8B41558311FA0295DA999631DD8E1E1B0AC2F661BC7421228579906132EA0407640761D4
```

```
99ABF30DBC515D23E6696E5E9777A0B3C6FEBE17070018B8D0745A17632620D0241AA5158
7C17B6677A7EE7306EE7770B45E4E9081B02B96911C66B789EA58A7302D26258F5AA0F368
E675
```

8. Considerações

1. Notar que na exibição dos componentes da chave privada (item 2.2) o ***prime1*** e ***prime2*** possuem 1 (um) Byte inicial composto por `00`. Este Byte não faz parte do componente e deve ser desconsiderado. Todos os 5 itens que compõe os componentes da chave RSA tem o mesmo tamanho, 128 Bytes (256 caracteres).
2. O comando de host L6, em seus processos internos, verifica a chave privada. Porém, seria pertinente realizar um teste paralelo de geração de assinatura (comando de host **EW**) e validação (externo ao HSM) para comprovarmos a usabilidade da chave.

9. TCPUDPSIM

Os comandos de host foram enviados com a ferramenta tcpudpsim.

9.1. Arquivo de envio (L6.txt)

A construção do arquivo de envio deve seguir o modelo abaixo:

```
[L6]


%Importa RSA Keys
$0000L6T3B0CE92B3BB794FFCBD37DD50B43291C683D4B2480CE8BA00010280<58CFD9AA9
E586F61D57BA8998816B8509C7FFAD398B6B4068C08F44971B2D4A6AB9E3F10A8A9DADF74
3844938195F8906DAB55F109ED68D16A6CCCC1D8E2F71E040862A862CE131A22ED1AFB27A
E4ADE39B37EF9C092BD39E211A4628CDA98AA9D89F6203D1571EB84B16A6790DB834544E9
F8D1B7BA0962007C11F374A580483A1FECA0B67611E9482D4D2A03CE605F7104275D8BC96
FA9A5B3E7B0C43DA3AF40B2489F4985D0255C03C37F022AF1388F384B48DC1DAFC963465E
8D1481B69572171CB1132D82857A04FCC78B182C87E7632D8F816E64836AC14749C45977A
671131C4E972F995F73DE527B5FA0C01C91B20540BC0710FB2EDD4475C78A65FE89A042B9
990CE8112D16F2C5C8B2B4D19C57CD8056D61C9C742BE23A130122E4C48D4B64F95882C3A
8E03839571C79E3C107792F85A877448A6091026965CEEA6A612B9E999E286F201DF4CF11
EAB0D658CE2ED5AB9E15733522BD2A067AE855DE8D98C8CEEC3D085AF9AC03251CFB3493C
C947079EC9B831158AAF4670451C2AB0EF267F11BD6E898FB2017FF616E8045EDF19A7A64
F4299DDBD4B669A55A530A5EDCD476823567799CCCD897308FCE5F812CF20A689E95A7A2F
27AB1023E9087C78DD8A70026F66EC7F1274EC134D4076C9CF2C41E2CB4DF2FE4D8BDAFDD
0258ABFDA9B186460ACAFBDE7D143EE10D8CE2DDD654D901C080E5834948FF61B793FAF1E
934C37A2097B9DC330ADB2D636DF1FB7D3DDED4DC5CC8E08D09CFA46A04B23A15539CF6FC
BA91784A2BDDACBAB09B72C678D364075196DFF4F8411A09F06227761AF3355B741A8ED6E
07CCF6F8AC9A0EA64267036466748B60DAD067C32388CBB751DE7646E5EDB6D10D0728303
271B9D759DD11514276C4D576BE489>10100<D9E0AB71AD7FA874AA86DD58A3BB87C876AD
B2C25754F35B0F7EA35C93B6D1ACECE50746A3D5B95512C0A2506F68AA186A1B1DD759404
1D9DB5B96DA09653E340ABC75E3129548C014DA4FB596E93A23D7285F55873CBBBDDDC8E8
EE5CA8ACBBBA963015DCA38C9BE0B32D6BBEDDCB83F77BC642CCC5D38C1BF09CCF280E1D4
```

```
3B8688D86613E5B2375CC22219A5D0BBE7E59407C6E77DDF8BC850341360BEF2CA803BC69
CAE0B630FC484DF988A09D72B258DD0208AE329F7684EF8565F7F28CA9ED85CE52855460F
38612EF819F91B57AFE5820767F0115CE40A1A4D442376B4BABB4C98BE2BEA53162650C64
CB6D27C700FE4E1D01D0D7B146EBDD9DC9BE33>0003<010001>%00
!0000L6T3B0CE92B3BB794FFCBD37DD50B43291C683D4B2480CE8BA00010280<58CFD9AA9
E586F61D57BA8998816B8509C7FFAD398B6B4068C08F44971B2D4A6AB9E3F10A8A9DADF74
3844938195F8906DAB55F109ED68D16A6CCCC1D8E2F71E040862A862CE131A22ED1AFB27A
E4ADE39B37EF9C092BD39E211A4628CDA98AA9D89F6203D1571EB84B16A6790DB834544E9
F8D1B7BA0962007C11F374A580483A1FECA0B67611E9482D4D2A03CE605F7104275D8BC96
FA9A5B3E7B0C43DA3AF40B2489F4985D0255C03C37F022AF1388F384B48DC1DAFC963465E
8D1481B69572171CB1132D82857A04FCC78B182C87E7632D8F816E64836AC14749C45977A
671131C4E972F995F73DE527B5FA0C01C91B20540BC0710FB2EDD4475C78A65FE89A042B9
990CE8112D16F2C5C8B2B4D19C57CD8056D61C9C742BE23A130122E4C48D4B64F95882C3A
8E03839571C79E3C107792F85A877448A6091026965CEEA6A612B9E999E286F201DF4CF11
EAB0D658CE2ED5AB9E15733522BD2A067AE855DE8D98C8CEEC3D085AF9AC03251CFB3493C
C947079EC9B831158AAF4670451C2AB0EF267F11BD6E898FB2017FF616E8045EDF19A7A64
F4299DDBD4B669A55A530A5EDCD476823567799CCCD897308FCE5F812CF20A689E95A7A2F
27AB1023E9087C78DD8A70026F66EC7F1274EC134D4076C9CF2C41E2CB4DF2FE4D8BDAFDD
0258ABFDA9B186460ACAFBDE7D143EE10D8CE2DDD654D901C080E5834948FF61B793FAF1E
934C37A2097B9DC330ADB2D636DF1FB7D3DDED4DC5CC8E08D09CFA46A04B23A15539CF6FC
BA91784A2BDDACBAB09B72C678D364075196DFF4F8411A09F06227761AF3355B741A8ED6E
07CCF6F8AC9A0EA64267036466748B60DAD067C32388CBB751DE7646E5EDB6D10D0728303
271B9D759DD11514276C4D576BE489>10100<D9E0AB71AD7FA874AA86DD58A3BB87C876AD
B2C25754F35B0F7EA35C93B6D1ACECE50746A3D5B95512C0A2506F68AA186A1B1DD759404
1D9DB5B96DA09653E340ABC75E3129548C014DA4FB596E93A23D7285F55873CBBBDDDC8E8
EE5CA8ACBBBA963015DCA38C9BE0B32D6BBEDDCB83F77BC642CCC5D38C1BF09CCF280E1D4
3B8688D86613E5B2375CC22219A5D0BBE7E59407C6E77DDF8BC850341360BEF2CA803BC69
CAE0B630FC484DF988A09D72B258DD0208AE329F7684EF8565F7F28CA9ED85CE52855460F
38612EF819F91B57AFE5820767F0115CE40A1A4D442376B4BABB4C98BE2BEA53162650C64
CB6D27C700FE4E1D01D0D7B146EBDD9DC9BE33>0003<010001>%00
@0000L700
```

9.2. Arquivo de parâmetros (tcpudpsim.bat)

```
tcpudpsim -f L6.txt -d 10.20.60.167 -s 1500 -r -c 1 -i 1 -o L6_out.txt
```

9.3. Arquivo de saída (L6_out.txt)

```
Mon Apr 05 23:52:20 2021
Test Configuration:
-----------------------------------------------------------
Iterations (per thread): 1
Command File: L6.txt
Protocol Used: tcp
Destination IP: 10.20.60.167
Destination Port: 1500
Destination timeout: 60
Output: L6_out.txt
Error Output: stderr
-----------------------------------------------------------
```

```
Sending Command 0
Section            : [L6]
Description        : Importa RSA Keys
Command            :
0000L6T3B0CE92B3BB794FFCBD37DD50B43291C683D4B2480CE8BA00010280<58CFD9AA9E
586F61D57BA8998816B8509C7FFAD398B6B4068C08F44971B2D4A6AB9E3F10A8A9DADF743
844938195F8906DAB55F109ED68D16A6CCCC1D8E2F71E040862A862CE131A22ED1AFB27AE
4ADE39B37EF9C092BD39E211A4628CDA98AA9D89F6203D1571EB84B16A6790DB834544E9F
8D1B7BA0962007C11F374A580483A1FECA0B67611E9482D4D2A03CE605F7104275D8BC96F
A9A5B3E7B0C43DA3AF40B2489F4985D0255C03C37F022AF1388F384B48DC1DAFC963465E8
D1481B69572171CB1132D82857A04FCC78B182C87E7632D8F816E64836AC14749C45977A6
71131C4E972F995F73DE527B5FA0C01C91B20540BC0710FB2EDD4475C78A65FE89A042B99
90CE8112D16F2C5C8B2B4D19C57CD8056D61C9C742BE23A130122E4C48D4B64F95882C3A8
E03839571C79E3C107792F85A877448A6091026965CEEA6A612B9E999E286F201DF4CF11E
AB0D658CE2ED5AB9E15733522BD2A067AE855DE8D98C8CEEC3D085AF9AC03251CFB3493CC
947079EC9B831158AAF4670451C2AB0EF267F11BD6E898FB2017FF616E8045EDF19A7A64F
4299DDBD4B669A55A530A5EDCD476823567799CCCD897308FCE5F812CF20A689E95A7A2F2
7AB1023E9087C78DD8A70026F66EC7F1274EC134D4076C9CF2C41E2CB4DF2FE4D8BDAFDD0
258ABFDA9B186460ACAFBDE7D143EE10D8CE2DDD654D901C080E5834948FF61B793FAF1E9
34C37A2097B9DC330ADB2D636DF1FB7D3DDED4DC5CC8E08D09CFA46A04B23A15539CF6FCB
A91784A2BDDACBAB09B72C678D364075196DFF4F8411A09F06227761AF3355B741A8ED6E0
7CCF6F8AC9A0EA64267036466748B60DAD067C32388CBB751DE7646E5EDB6D10D07283032
71B9D759DD11514276C4D576BE489>10100<D9E0AB71AD7FA874AA86DD58A3BB87C876ADB
2C25754F35B0F7EA35C93B6D1ACECE50746A3D5B95512C0A2506F68AA186A1B1DD7594041
D9DB5B96DA09653E340ABC75E3129548C014DA4FB596E93A23D7285F55873CBBBDDDC8E8E
E5CA8ACBBBA963015DCA38C9BE0B32D6BBEDDCB83F77BC642CCC5D38C1BF09CCF280E1D43
B8688D86613E5B2375CC22219A5D0BBE7E59407C6E77DDF8BC850341360BEF2CA803BC69C
AE0B630FC484DF988A09D72B258DD0208AE329F7684EF8565F7F28CA9ED85CE52855460F3
8612EF819F91B57AFE5820767F0115CE40A1A4D442376B4BABB4C98BE2BEA53162650C64C
B6D27C700FE4E1D01D0D7B146EBDD9DC9BE33>0003<010001>%00
Length of Command Sent: 973
Command Test OK
Command
:0000L6T3B0CE92B3BB794FFCBD37DD50B43291C683D4B2480CE8BA00010280<58CFD9AA9
E586F61D57BA8998816B8509C7FFAD398B6B4068C08F44971B2D4A6AB9E3F10A8A9DADF74
3844938195F8906DAB55F109ED68D16A6CCCC1D8E2F71E040862A862CE131A22ED1AFB27A
E4ADE39B37EF9C092BD39E211A4628CDA98AA9D89F6203D1571EB84B16A6790DB834544E9
F8D1B7BA0962007C11F374A580483A1FECA0B67611E9482D4D2A03CE605F7104275D8BC96
FA9A5B3E7B0C43DA3AF40B2489F4985D0255C03C37F022AF1388F384B48DC1DAFC963465E
8D1481B69572171CB1132D82857A04FCC78B182C87E7632D8F816E64836AC14749C45977A
671131C4E972F995F73DE527B5FA0C01C91B20540BC0710FB2EDD4475C78A65FE89A042B9
990CE8112D16F2C5C8B2B4D19C57CD8056D61C9C742BE23A130122E4C48D4B64F95882C3A
8E03839571C79E3C107792F85A877448A6091026965CEEA6A612B9E999E286F201DF4CF11
EAB0D658CE2ED5AB9E15733522BD2A067AE855DE8D98C8CEEC3D085AF9AC03251CFB3493C
C947079EC9B831158AAF4670451C2AB0EF267F11BD6E898FB2017FF616E8045EDF19A7A64
F4299DDBD4B669A55A530A5EDCD476823567799CCCD897308FCE5F812CF20A689E95A7A2F
27AB1023E9087C78DD8A70026F66EC7F1274EC134D4076C9CF2C41E2CB4DF2FE4D8BDAFDD
0258ABFDA9B186460ACAFBDE7D143EE10D8CE2DDD654D901C080E5834948FF61B793FAF1E
934C37A2097B9DC330ADB2D636DF1FB7D3DDED4DC5CC8E08D09CFA46A04B23A15539CF6FC
BA91784A2BDDACBAB09B72C678D364075196DFF4F8411A09F06227761AF3355B741A8ED6E
```

```
07CCF6F8AC9A0EA64267036466748B60DAD067C32388CBB751DE7646E5EDB6D10D0728303
271B9D759DD11514276C4D576BE489>10100<D9E0AB71AD7FA874AA86DD58A3BB87C876AD
B2C25754F35B0F7EA35C93B6D1ACECE50746A3D5B95512C0A2506F68AA186A1B1DD759404
1D9DB5B96DA09653E340ABC75E3129548C014DA4FB596E93A23D7285F55873CBBBDDDC8E8
EE5CA8ACBBBA963015DCA38C9BE0B32D6BBEDDCB83F77BC642CCC5D38C1BF09CCF280E1D4
3B8688D86613E5B2375CC22219A5D0BBE7E59407C6E77DDF8BC850341360BEF2CA803BC69
CAE0B630FC484DF988A09D72B258DD0208AE329F7684EF8565F7F28CA9ED85CE52855460F
38612EF819F91B57AFE5820767F0115CE40A1A4D442376B4BABB4C98BE2BEA53162650C64
CB6D27C700FE4E1D01D0D7B146EBDD9DC9BE33>0003<010001>%00
Expected response: 0000L700
Received response:
0000L700[30323930EF4E020F4E42C927CEC33FF3C7D85D61D7B8FB2DAF2BC6EC53C95A69
B1A59E4BE163A7AA6BB4B65BB8AC1D59157F029E54CB6B099142A94C52D36C8758358E9F4
A5F1C48F058787FE2BC4A889C47DA8F0EF0D133125094DDE5036D8B2955E29C278358277B
7E376F9367E64CA3D5CD093EC45C58B886480844A4F88E0E3D343A37464EEA7CE0F85DC23
7D4C3CC974B0E64F1826A7CE9DDB03E2BDFA5AD02CC1B6BC9B6E505B338A2B96139A3DB06
F110B0FA04EFE5E2397513DE8D40D08C34595E8D5D4575CCDD8E0BE62383765B5DAE7EB28
B20B9EB04C890F933E7BD6550F8E4CAB809FF1C249DDE9C9EBD40C6E96DBA62A5A4906909
6969A7EDC12CD58D53E4EC4A813AB379E61B8B75208EDF38EE06482FED972936EED91F22F
C3BD625F8EE7B005E4D4BBFACEC192A343326A7DC2B72C37062C9C7D552748B9466C91FA7
DF0DD9B7D4D76CB64286214D26BDA3010A467C9FEA3B99193BEEFC90E866DABF48014BF0A
A856CE42B7986E4081B5F20079FC55AF071FD2D1096667ADFD32C4E7BE4E47ACB9B0B75EC
B0ABBEF5BC4DD9A4727C3E7FD3EC02B82545009EBDEE58ABA71826A681729DC146990985E
CB4BBE6AEFCB8E1B759519F402D7802E64394680FF32601EB711A03A9448B6D080A1D1224
90A061D4E3BB8B64C6FA580DA15E4D433345129702E35B318867F2A38CF8D5D26168F8EEC
06043FC4DE5B694F5C35E5D39B3F6629B6AC0713AF0C9F7E4BD39F7C895225A3EDD1B2BD5
B90625CA113B8B41558311FA0295DA999631DD8E1E1B0AC2F661BC7421228579906132EA0
407640761D499ABF30DBC515D23E6696E5E9777A0B3C6FEBE17070018B8D0745A17632620
D0241AA51587C17B6677A7EE7306EE7770B45E4E9081B02B96911C66B789EA58A7302D262
58F5AA0F368E675]
Total Time      : 0.026
Transactions/Sec: 38.427
Avg Time        : 0.026



Test End: Mon Apr 05 23:52:20 2021


------------------------------------------------
Thread Test Statistics for: ID 14376
------------------------------------------------
Target IP address : 10.20.60.167
Target Port       : 1500
Protocol Used:    : tcp
Total Socket Sends: 1
Total Socket Fails: 0
Total Socket Pass : 1
------------------------------------------------
Test Statistics
------------------------------------------------
Total Tests       : 1
```

```
Passed Tests      : 1
Failed Tests      : 0
-------------------------------------------------
Started:          : Mon Apr 05 23:52:20 2021
Ended:            : Mon Apr 05 23:52:20 2021
Total Time Spent  : 0.0260 seconds
Transactions/Sec  : 38.4267 trans/sec
Avg Time          : 0.0260 sec/cmd
-------------------------------------------------




-------------------------------------------------
Test Statistics for all threads
  (NOTE: low resolution timer -- seconds only)
-------------------------------------------------
Total Tests       : 1
Passed Tests      : 1
Failed Tests      : 0
-------------------------------------------------
Earliest start:   : Mon Apr 05 23:52:20 2021
Latest end:       : Mon Apr 05 23:52:20 2021
Total Time Spent  : 0 seconds
Transactions/Sec  : 1.#INF trans/sec
Avg Time          : 0.0000 sec/cmd
-------------------------------------------------
```