

**Secure Host Communications - TLS**

Índice

[1. Licença 3](#_Toc66362162)

[2. Interface de Rede 3](#_Toc66362163)

[3. Generate HRK 4](#_Toc66362164)

[4. Generate Certificate Signing Request 5](#_Toc66362165)

[5. Signed certificate 6](#_Toc66362166)

[5.1. Site 6](#_Toc66362167)

[5.2. Renomear arquivo 6](#_Toc66362168)

[6. Import 6](#_Toc66362169)

[6.1. Import CA 6](#_Toc66362170)

[6.2. Import Cert assinado pela CA 7](#_Toc66362171)

[6.3. Validar 7](#_Toc66362172)

[7. Validação pelo BPTools 10](#_Toc66362173)

[8. Release Notes 16](#_Toc66362174)

# Licença

O comando VR permite visualizar se o HSM suporta TLS.

|  |
| --- |
| Online>vr  Base release: 3.5a  Revision: 1407-0921  Build Number: 0002    PCI HSM Compliance:  Some security settings are not PCI HSM compliant    HSM Core API Version: 8.20.3    Serial Number: XXXXXXXXXXXXX  Unit info: Licensed    Host Configuration: Async,Ethernet,**(optional) TLS/SSL**  (…) |

# Interface de Rede

Habilitar a função de TLS na interface de rede do HSM. Para poder executar essa tarefa, é necessário que o HSM seja colocado em modo SECURE.

|  |
| --- |
| Secure-AUTH>ch  Please make a selection. The current setting is in parentheses.  Message header length [1-255] (4):  Disable host connections when no LMKs are installed? [Y/N] (N):  Host interface [[A]sync, [E]thernet] (E):  Enter Well-Known-Port (1500):  **Enter Well-Known-TLS-Port (2500):**  UDP [Y/N] (N):  TCP [Y/N] (Y):  **Enable TLS [Y/N] (N): y**  ACL Enabled [Y/N] (N):  Number of connections [1-64] (64):  Enter TCP keep alive timeout [1-120 minutes] (120):  Number of interfaces [1/2] (1):  Interface Number [1/2] (1):  (…) |

# Generate HRK

Para gerar uma nova chave de recuperação HSM (HRK). Uma vez instalado, o HRK será usado para fazer backup de material de chave secreta dentro do HSM na memória persistente (um processo conhecido como sincronização de chave).

O seguinte material de chave secreta é copiado nesse processo:

Material chave do TLS de comunicações de host seguro:

* Chave privada do HSM

Material chave do payShield Manager TLS:

* Chave privada do HSM
* Certificado de chave pública do HSM
* Certificado de chave pública da CA

|  |
| --- |
| Secure> SK |
| \*\*\*\* NOTE \*\*\*\* |
| Passphrase rules as follows: |
| 1 - Must be between 8 and 30 characters long. |
| 2 - Can contain spaces |
| 3 - Must be comprised of (at a minimum): |
| 2 - digits |
| 2 - uppercase characters |
| 2 - lowercase characters |
| 2 - symbols (e.g. !/?.#:') |
| Enter administrator 1 passphrase: \*\*\*\*\*\*\*\* |
| Re-enter administrator 1 passphrase: \*\*\*\*\*\*\*\* |
| Enter administrator 2 passphrase: \*\*\*\*\*\*\*\* |
| Re-enter administrator 2 passphrase: \*\*\*\*\*\*\*\* |
| Creating HRK. Please, wait ... DONE |
| HRK generated successfully |
| Key synchronization complete |
|  |

# Generate Certificate Signing Request

Para gerar o par de chaves pública/privada do HSM para uso com o TLS de host ou gerenciamento e gerar a chave pública na forma de uma Solicitação de assinatura de certificado (CSR).  
 A chave privada é armazenada na memória protegida do HSM contra violação. O backup é feito internamente usando a HSM Master Key (HRK).

|  |
| --- |
| Secure-AUTH>sg    What type of certificate do you want to generate (using specific key type)?  1 - Host TLS  2 - Management TLS    Type: 1    Select key type:  1 - RSA  2 - ECDSA P-256  3 - ECDSA P-384  4 - ECDSA P-521    Type [4]: 4    Please enter the certificate Subject information:    Country Name (2 letter code) []: **br**  State or Province Name (full name) []: **sao paulo**  Locality Name (eg, city) []: **sao paulo**  Organization Name (eg, company) []: **ft**  Organizational Unit Name (eg, section) []: **ft.local**  Common Name (e.g. server FQDN or YOUR name) [**B4665303046N**]:  Email Address []: **ft@ft.local**    Do you wish to save the CSR to a file [Y/N]:N  -----BEGIN CERTIFICATE REQUEST-----  MIICFTCCAXYCAQAwgYgxCzAJBgNVBAYTAmJyMRIwEAYDVQQIDAlzYW8gcGF1bG8x  EjAQBgNVBAcMCXNhbyBwYXVsbzELMAkGA1UECgwCZnQxETAPBgNVBAsMCGZ0Lmxv  Y2FsMRUwEwYDVQQDDAxCNDY2NTMwMzA0Nk4xGjAYBgkqhkiG9w0BCQEWC2Z0QGZ0  LmxvY2FsMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBIImUvNRtp6MMIxEoa/kQ  0xfs7jUTVnfEVyG3o7H0TLuv+YdjGXocq/OI8OEg1eUbPSaLyFl7UQ9A1qzkjlbl  5wkA3Yl7OlQI/l7A6kGHAXOo1B+Ij9Hy3+42aMfQXeoXE5hqDcDD2MPZR+3DoUn1  iBLaK4RyBtD0jUakpUyd7OaL19igSDBGBgkqhkiG9w0BCQ4xOTA3MAwGA1UdEwEB  /wQCMAAwDgYDVR0PAQH/BAQDAgeAMBcGA1UdEQQQMA6CDEI0NjY1MzAzMDQ2TjAK  BggqhkjOPQQDAgOBjAAwgYgCQgCYRiNek/gZZUznEmHuJkc6C0+6s4gEP5HcptHX  Malq6OviFJkeNTf16ABbYDEpb3wqbiL/fFsODMQq6NtFys6EIgJCAUePZ6jCmhQx  ytlA4wN3EKrW7SethZ6liZ6jkjG8K9UsUnZgwmhg2X+H2AynShrerCoYrZa1tfZF  /i3uEaY3evvv  -----END CERTIFICATE REQUEST-----    Successfully generated TLS management certificate |

# Signed certificate

## Site

O CSR deve ser assinado.

|  |
| --- |
| -----BEGIN CERTIFICATE REQUEST-----  MIICFTCCAXYCAQAwgYgxCzAJBgNVBAYTAmJyMRIwEAYDVQQIDAlzYW8gcGF1bG8x  EjAQBgNVBAcMCXNhbyBwYXVsbzELMAkGA1UECgwCZnQxETAPBgNVBAsMCGZ0Lmxv  Y2FsMRUwEwYDVQQDDAxCNDY2NTMwMzA0Nk4xGjAYBgkqhkiG9w0BCQEWC2Z0QGZ0  LmxvY2FsMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBIImUvNRtp6MMIxEoa/kQ  0xfs7jUTVnfEVyG3o7H0TLuv+YdjGXocq/OI8OEg1eUbPSaLyFl7UQ9A1qzkjlbl  5wkA3Yl7OlQI/l7A6kGHAXOo1B+Ij9Hy3+42aMfQXeoXE5hqDcDD2MPZR+3DoUn1  iBLaK4RyBtD0jUakpUyd7OaL19igSDBGBgkqhkiG9w0BCQ4xOTA3MAwGA1UdEwEB  /wQCMAAwDgYDVR0PAQH/BAQDAgeAMBcGA1UdEQQQMA6CDEI0NjY1MzAzMDQ2TjAK  BggqhkjOPQQDAgOBjAAwgYgCQgCYRiNek/gZZUznEmHuJkc6C0+6s4gEP5HcptHX  Malq6OviFJkeNTf16ABbYDEpb3wqbiL/fFsODMQq6NtFys6EIgJCAUePZ6jCmhQx  ytlA4wN3EKrW7SethZ6liZ6jkjG8K9UsUnZgwmhg2X+H2AynShrerCoYrZa1tfZF  /i3uEaY3evvv  -----END CERTIFICATE REQUEST----- |
|  |

<https://getacert.com/signacert.html>

## Renomear arquivo

- B4665303046N-2020-10-02-133002.cer > B4665303046N-2020-10-02-133002.crt

- getacert.cer => getacert.crt

# Import

O arquivo do certificado deve ter a extensão .crt. Deve-se importá-lo, comando de console SI “Import Certificate”

## Import CA

Deve-se primeiro importar o certificado root (CA) para depois importar o certificado assinado.

|  |
| --- |
| Secure> si |
| Please select the function that the key was created for: |
| 1 - Host TLS |
| 2 - Management TLS |
| Type: 1 |
| Select File |
| 1 - B4665310361O\_cert.crt |
| 2 - B4665303046N\_cert.crt |
| 3 - getacertca.crt |
| File: 3 |
| Imported Trusted CA Certificate |
| Issued to: getaCert - www.getacert.com, Issued by: getaCert - www.getacert.com |
| Validity : Nov 6 16:46:48 2016 GMT to Jan 15 16:46:48 2038 GMT |
| Unique ID: B8D1B40F2AF4AD49 - 3A537BAF (Root) |

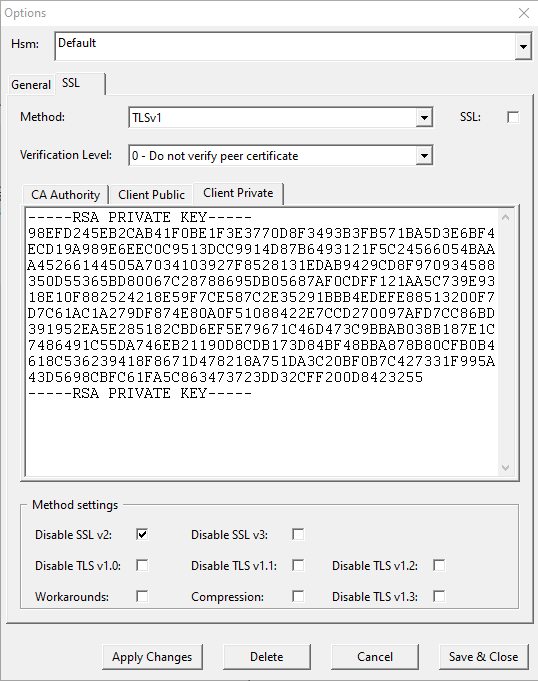
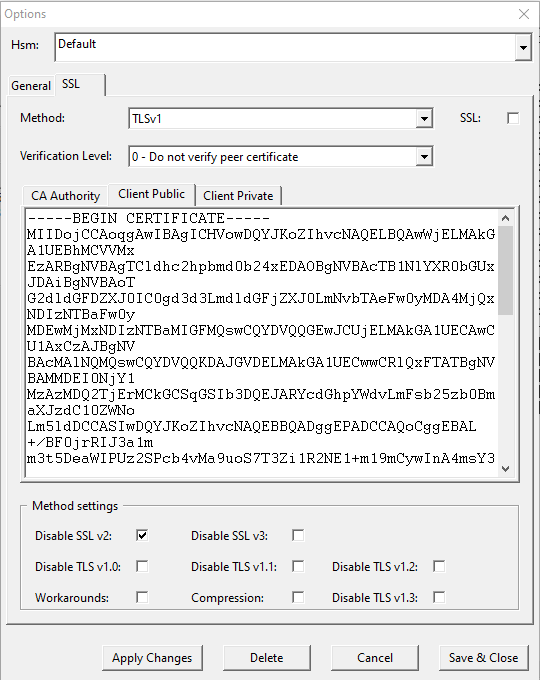
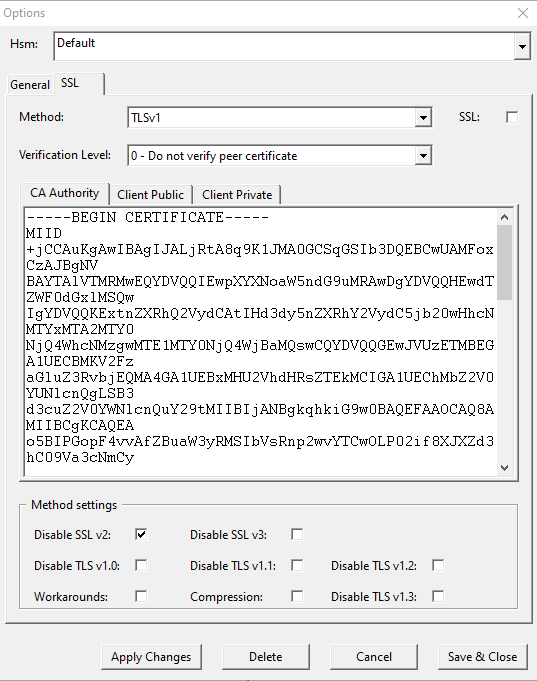
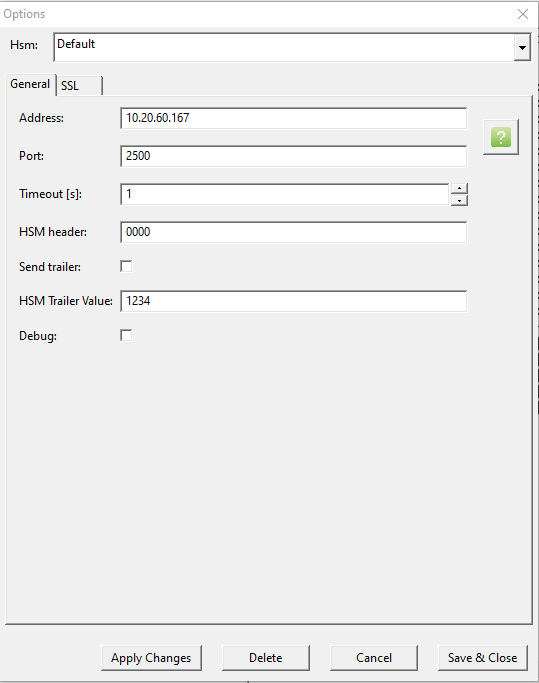
## Import Cert assinado pela CA

|  |
| --- |
|  |
| Secure>si |
| Please select the function that the key was created for: |
| 1 - Host TLS |
| 2 - Management TLS |
|  |
| Type: 1 |
| Select File |
| 1 - B4665310361O\_cert.crt |
| 2 - B4665303046N\_cert.crt |
| 3 - getacertca.crt |
|  |
| File: 2 |
|  |
| Imported CA-signed HSM Certificate |
| Issued to: B4665303046N, Issued by: getaCert - www.getacert.com |
| Validity : Aug 24 14:23:50 2020 GMT to Oct 23 14:23:50 2020 GMT |
| Unique ID: 1D5A - 3A537BAF |
| Chain of Trust validated |
| getaCert - www.getacert.com (Root) |

## Validar

|  |
| --- |
| Secure-AUTH>sv    Please select the function that the key was created for:  1 - Host TLS  2 - Management TLS    Type: 1  Secure Host Comms Private Key installed: Yes  Secure Host Comms Certificate installed:  1 - Issued to: B4665303046N, Issued by: getaCert - www.getacert.com  Validity : Oct 2 15:13:05 2020 GMT to Dec 1 15:13:05 2020 GMT  Unique ID: 2266 - 3A537BAF    Secure Host Comms Client certificate(s) installed: No  Secure Host Comms CA Certificate(s) installed:    2 - Issued to: getaCert - www.getacert.com, Issued by: getaCert - www.getacert.com  Validity : Nov 6 16:46:48 2016 GMT to Jan 15 16:46:48 2038 GMT  Unique ID: B8D1B40F2AF4AD49 - 3A537BAF (Root)    Chain of Trust validated:    getaCert - www.getacert.com (Root)    Select an item to view: 1    Certificate:  Data:  Version: 3 (0x2)  Serial Number: 8806 (0x2266)  Signature Algorithm: sha256WithRSAEncryption  Issuer: C=US, ST=Washington, L=Seattle, O=getaCert - www.getacert.com  Validity  Not Before: Oct 2 15:13:05 2020 GMT  Not After : Dec 1 15:13:05 2020 GMT  Subject: C=br, ST=sao paulo, L=sao paulo, O=ft, OU=ft.local, CN=B4665303046N/emailAddress=ft@ft.local  Subject Public Key Info:  Public Key Algorithm: id-ecPublicKey  Public-Key: (521 bit)  pub:  04:01:20:89:94:bc:d4:6d:a7:a3:0c:23:11:28:6b:  f9:10:d3:17:ec:ee:35:13:56:77:c4:57:21:b7:a3:  b1:f4:4c:bb:af:f9:87:63:19:7a:1c:ab:f3:88:f0:  e1:20:d5:e5:1b:3d:26:8b:c8:59:7b:51:0f:40:d6:  ac:e4:8e:56:e5:e7:09:00:dd:89:7b:3a:54:08:fe:  5e:c0:ea:41:87:01:73:a8:d4:1f:88:8f:d1:f2:df:  ee:36:68:c7:d0:5d:ea:17:13:98:6a:0d:c0:c3:d8:  c3:d9:47:ed:c3:a1:49:f5:88:12:da:2b:84:72:06:  d0:f4:8d:46:a4:a5:4c:9d:ec:e6:8b:d7:d8  ASN1 OID: secp521r1  NIST CURVE: P-521  X509v3 extensions:  X509v3 Basic Constraints:  CA:FALSE  Netscape Cert Type:  SSL Client, SSL Server, S/MIME, Object Signing  X509v3 Key Usage:  Key Encipherment  X509v3 Subject Alternative Name:  DNS:B4665303046N  Signature Algorithm: sha256WithRSAEncryption  16:fb:aa:b7:b0:27:51:c9:62:2b:f3:63:00:cc:06:e0:8f:dd:  90:e9:71:ad:c5:4e:bd:f5:e7:0a:fe:d9:0c:94:75:d9:8d:ea:  5c:17:5a:63:fb:9d:39:74:b4:28:0a:99:a6:f7:da:ca:98:7f:  71:45:89:ba:4e:5b:5e:83:2f:d9:ee:ec:59:e1:f3:a5:a0:a1:  e5:f9:99:ca:3a:c8:38:48:56:df:34:7c:81:bb:ce:d3:25:f5:  01:6e:66:9a:ff:75:61:d2:27:c3:f0:c2:db:2f:28:39:dd:d4:  f4:db:32:de:dd:c6:4d:cc:48:e4:d2:8b:f3:b3:b6:5a:91:30:  7b:2c:bc:52:c5:56:b2:83:8c:62:d0:b0:48:76:a2:83:f5:df:  e8:2a:37:8c:fe:fe:8c:9d:2a:2a:60:51:ba:ee:19:46:ff:6b:  24:90:be:4f:42:13:ff:d5:93:a9:bb:70:a0:ce:d5:7c:1b:0d:  ae:18:0e:af:5e:df:f0:02:46:e4:0d:51:9c:dd:5f:ae:97:bb:  11:e0:24:32:95:48:54:3f:d8:96:03:bc:cf:a0:61:92:ec:95:  2c:1e:2e:b5:77:b7:e7:72:79:12:00:1b:56:b9:25:a9:69:1d:  36:3a:8c:bb:32:13:20:5d:f5:c7:3d:e8:38:0b:f4:d3:fd:96:  a1:c8:ca:70    Do you wish to view another item? N |

# Validação pelo BPTools





 [2020-08-24 14:34:14] BP-Tools - HSM Commander is ready  
 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 [2020-08-24 14:34:34] Error: HSM response timed out. Check the configuration and try again.  
 ----------------------------------------  
TCP/IP Header............ =\*[010A] 266 Bytes  
Message Header........... = [0000]  
Command Code............. = [B2] Echo Command Request  
Length................... = [0100]  
Data..................... = [7A30FD618D7C23612A77EA6762916571A7646332DB10D42F92260460ED741B567657B9C0D41DAA07A1C2F1FDB1F50FD5CBC0348FF4E752DA2F6BE9C00CAF217D4E56F62B227ED3C55E9B6803E4A2C39AC9195513A5CCF77C7DF317BE26D9C0764526D690B22C10D7A3D50782057ED4B2102B135B97314C09A9E9D7D9EC3996B4]

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Eduardo Campos | Primeira versão | ??/??/???? |
| Caio Ferreira | Novo formato do documento | 30/07/2020 |