

**Secure Host Communications - TLS**

Índice

[1. Interface de Rede 3](#_Toc65146501)

[2. Generate HRK 3](#_Toc65146502)

[3. Generate Certificate Signing Request 4](#_Toc65146503)

[4. Signed certificate 5](#_Toc65146504)

[5. Import 6](#_Toc65146505)

[5.1. Import CA 6](#_Toc65146506)

[5.2. Import Cert assinado pela CA 6](#_Toc65146507)

[5.3. Validar 7](#_Toc65146508)

[6. Validação pelo BPTools 8](#_Toc65146509)

[7. Release Notes 14](#_Toc65146510)

# 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

|  |
| --- |
| 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

|  |
| --- |
| 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) [**S0246377501Q**]:  Email Address []: **ft@ft.local**    Do you wish to save the CSR to a file [Y/N]:N  -----BEGIN CERTIFICATE REQUEST----------END CERTIFICATE REQUEST-----    Successfully generated TLS management certificate |

# Signed certificate

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----- |
|  |

Para assinar o certificado gerado pelo HSM será utilizado o site[1] getaCert.

Os arquivos gerados pelo site getaCert devem ser renomeados.

|  |  |
| --- | --- |
| **DE** | **PARA** |
| getacert.cer | getacert.crt |
| S0246377501Q-2020-10-02-133002.cer | S0246377501Q-2020-10-02-133002.crt |

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

# Import

## 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 - S0246377501Q-2020-10-02-133002.crt |
| 2 - getacertca.crt |
| File: 2 |
| 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

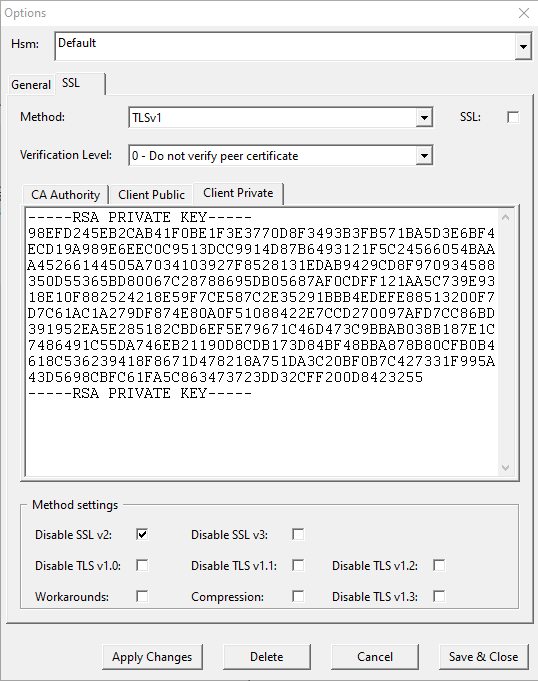
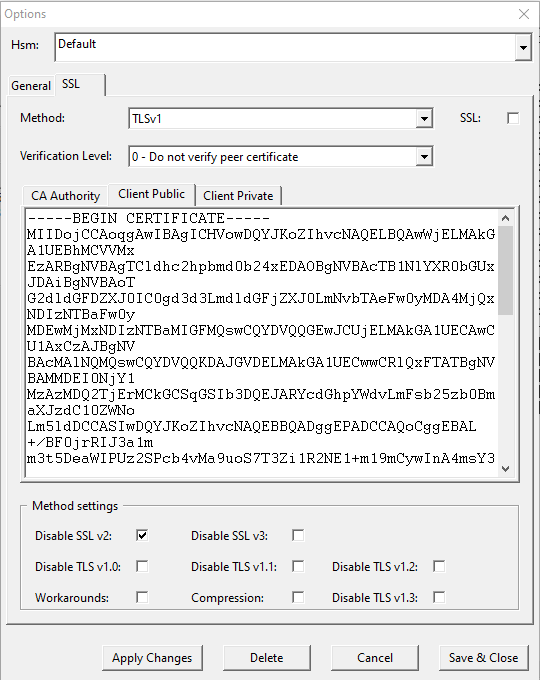
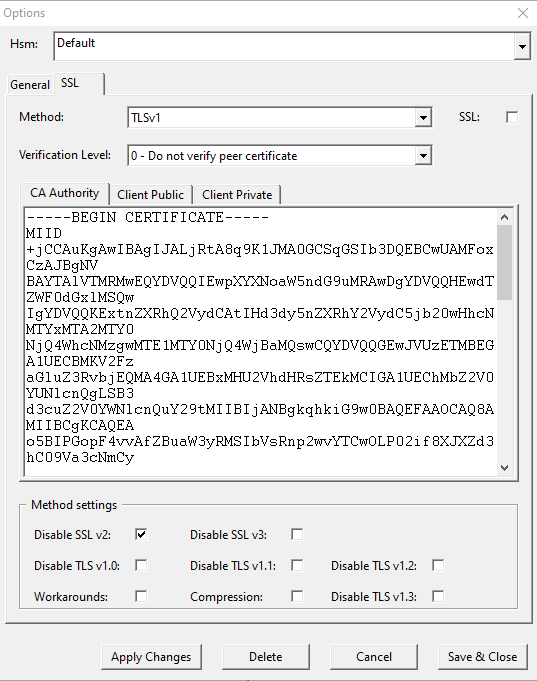
|  |
| --- |
|  |
| Secure>si |
| Please select the function that the key was created for: |
| 1 - Host TLS |
| 2 - Management TLS |
|  |
| Type: 1 |
| Select File |
| 1 - S0246377501Q-2020-10-02-133002.crt |
| 2 - getacertca.crt |
|  |
| File: 1 |
|  |
| Imported CA-signed HSM Certificate |
| Issued to: S0246377501Q, 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

|  |
| --- |
| Online-AUTH>sv  Please select the function that the key was created for:  1 - Host TLS  2 - Management TLS  Type: 1  Host TLS Private Key installed: Yes  Host TLS Certificate installed:  1 - Issued to: **S0246377501Q**, Issued by: getaCert - www.getacert.com  Validity : Feb 25 12:25:10 2021 GMT to Apr 26 12:25:10 2021 GMT  Unique ID: 0B33 - 3A537BAF  Host TLS Client certificate(s) installed: No  Host TLS 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: |

# 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 |