SIEMENS

FAQ • 10/2014

How to Manage HTTPS Certificates

RUGGEDCOM WIN v4.3

http://support.automation.siemens.com/WW/view/en/103949128

This entry is from the Siemens Industry Online Support. The general terms of use (http://www.siemens.com/terms_of_use) apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Table of Contents

1 Introduction

This document provides a procedure for managing X.509 certificates for HTTPS support in the BS and CPE.

2 HTTPS Certificate Generation

X.509 certificates generation has to be done on a Linux host or Cygwin running on Windows. All the certificates are in X.509v3 format.

The procedure consists of two parts:

1. Modifying the “ca.cnf” file in the “Main/CA” directory.

   The certificate is self-signed, thus it’s server and CA certificates are in a single file.

2. Running the “run.sh” script from the “CA” folder where the “ca.cnf” file is located. The following files are relevant to the certificate generation procedure: ca.cnf

2.1 Self-Signed Server Certificate

The “ca.cnf” file contains all the needed parameters for HTTPS self-signed server certificate generation. As a part of the server certificate generation, a server private key is created as well.

Make sure that OpenSSL version 0.9.8 (or earlier) is used on the Linux PC (or Cygwin) that the tool is run on.

Any later versions such as 1.0.0, 1.0.1 will result in having a client private key in incompatible format for our CPE and the AAA as well.

Here are the sample differences between the keys.

Openssl 0.9.8 private key (the good format)

Figure 2-1

```
BEGIN·RSA·PRIVATE·KEY¶
Proc-Type:·4,ENCRYPTED¶
DEK-Info:·DES-EDE3-CBC,327E4B06D51C7728¶
grestO9v2wfiqFwBy8bBbpNjMWpFrrc/9y8q68n6c48enCFyDsdVlyqToOQ+Razt·
d98I+rkTow33X83e9+Zt8rGlKJlPXn3zHTKbjNhfc7j6kk+ssWJft5OAvu5NShMx·
FOATl4pW97qCf1x4pFwQGm8/8MhCqOpqv2cLfjz2T4Egu1qP2sHZ35QU/gHBLHYh¶
```

Openssl 1.0.0 private key (the bad format)

Figure 2-2

```
BEGIN·ENCRYPTED·PRIVATE·KEY¶
MIIJnzBJBgkqhkiG9w0BBQ0wPDAbBgkqhkiG9w0BBQwwDgQI0Z45oYYRJ1cCAggA·
MB0GCWCGSAFlAwQBAgQQF4QLI0IILDItqQFXHJeAxgSCCVBAo1Ed9BHwyhHeBzx2·
rQELkAghar26CFsP7qvMwZ+vnATbArA2MvFWJWy0l2pl7/Rn7RcoztbSzg82c8IG¶
```

The following subset of parameters is presented with their default values and can be modified in order to reflect the customer's specifics for the certificate. Also, an explanation of the parameter meaning is provided.

Table 2-1: Self-Signed Server Certificate Properties

Parameter	Explanation
default_days = 10000	Certificate validity period.
[req] input_password = password output_password = password	Both input and output fields have to have the same server private key password. **Make sure the password is at least 8 characters.** This password shall be entered in the relevant section in "Certificate loading" GUI screen (see chapter 3).
[certificate_authority] countryName = CA stateOrProvinceName = N/A localityName = N/A organizationName = N/A emailAddress = N/A commonName = "Server Certificate"	The country name must be 2 letters. This name will be shown in the "Issued to" field (when the certificate is presented in ".der" format). If the certificate is signed correctly, the "Issued by" field will be the same (as it's a self-signed certificate).

2.2 Certificate Generation Script

Once all the above-mentioned certificate properties are modified and all the relevant ".cnf" files are saved, the "run.sh" scripts have to be executed from the "CA" directory.

For example: Perform cd /home/user/ca and then ./run.sh for generating the certificate.

The generated certificates in ".pem" and in ".der" formats will be stored in the "Main/ca/output" directory.

NOTE

Important!

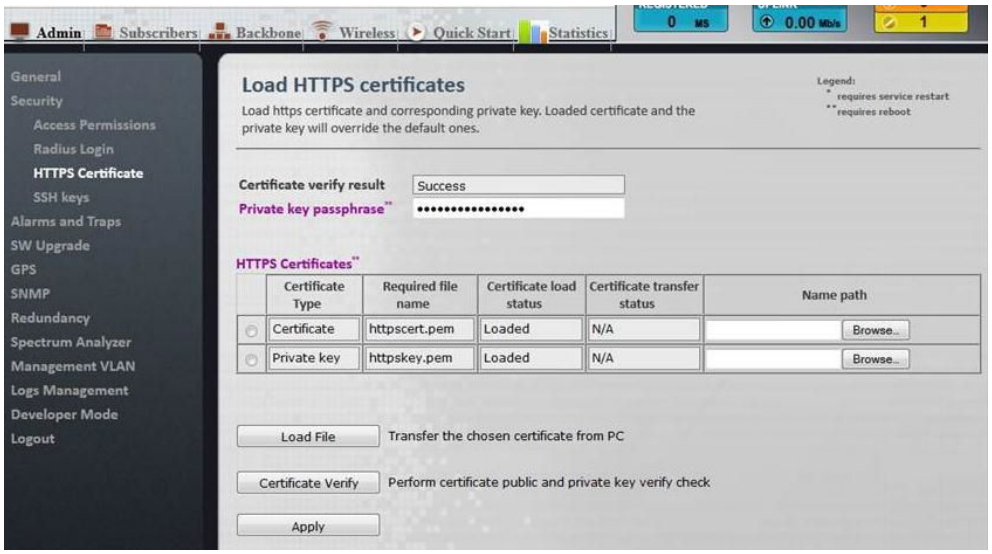
As a part of the script, for Linux machines, there is a command that shifts the date on the generation machine to the year 2008. After the generation is over, the date is set back to the current date. The reason for shifting the date back is due to a CPE internal clock that is set to this date (there is no GPS in the CPE) and the certificate validity start time has to match it in order to work properly. In v4.3, there will be no need for this time shift, as the NTP protocol will be supported. Also, if Cygwin is used, the date on the Windows PC has to be set manually.

3 Certificate Loading

3.1 BS

1. The certificate upload to the BS shall be performed from the GUI.
2. The required GUI screen is located under Admin/Security/HTTPS Certificate:

Figure 3-1: BS Certificate Loading GUI Screen



3. The generated certificate and key shall be loaded from the management PC by browsing the local directories and clicking the “Load” button. The certificate file name shall be “httpscert.pem” and the key file name shall be “httpskey.pem”. Other names will be rejected by the GUI upon clicking the “Load” button. Load status indicates if the required files are loaded or not.
4. The key passphrase shall be exactly as the generated key passphrase configured in the “ca.cnf” file. This passphrase will be stored encrypted in the BS UV file.
5. Upon loading the certificate, the key and configuring the passphrase it is possible to perform the “Certificate Verify” function. If any of the three components (certificate, key, passphrase) is missing or corrupt, the Verify function will show a failure result.
6. In order for the BS to start using the loaded certificate and key, the BS has to be rebooted. Until then, the BS will still use the default (or previously loaded) certificates.

3.2 CPE

1. The certificate upload to the BS shall be performed from the GUI.
2. The required GUI screen is located under Management/Security/HTTPS Certificate:

Figure 3-2: CPE Certificate Loading GUI Screen

3. The rest of the steps are as in the BS case in v4.1.