24 Certificates

Devices that send unencrypted data are susceptible to attacks which might cause deliberate damage to the user system. Therefore it is highly advised to use cryptography to secure sensitive data. WCC Lite offers means to easily store certificates for their later usage.

Some protocols, namely IEC60870-5-104 Slave, DNP v3.0 Slave and Master might be configured to send data over TCP/IP. For these protocols, a secured connection over TCP/IP using TLS certificates can be made. For this purpose, certificate storage has been created and is available since firmware version 1.3.0.

To make storage secure, multiple steps have been taken:

- By default certificate storage is only accessible for root users and users with group level 15 permissions;
- By default, certificates are not added to the backup to avoid private key leakages; Private keys should never be revealed to the public
- By default, certificates are deleted after system upgrade;
- Only basic information is shown on a web interface; Certificates can be uploaded, deleted but not downloaded

Certificates can be split into three parts local (private) certificates, certificates from peers (usually called Certificate Authority (CA)) and private keys. It has to be noted that all of these certificates sometimes can be found in one file, therefore ideally a user should have at least a minimal understanding of the formats in which certificates are stored.

Certificates should conform to the X509 standard. The difference between local certificates and certificate authority certificates is that only certificate authority generates certificates for others. Therefore Issuer and Subject fields are always the same for certificate authority certificates whereas they differ for local certificates. Both of these certificates are usually stored in a device to validate if incoming connections have valid certificates and are to be trusted. Both of the certificates have the public key which together with the public key enables encrypted connections.

The private key is a text file used initially to generate a Certificate Signing Request (CSR), and later to secure and verify connections using the certificate created per that request. It usually contains a unique hash made in a way that chances of guessing it by using brute force are technically infeasible. The private key should be closely guarded since anyone with access to it uses it in nefarious ways. If you lose your private key or believe it was compromised in any way, it is recommended to rekey your certificate – reissue it with a new private key.

To make certificate upload more intuitive, certain restrictions are imposed. Only files with certain extensions (*.crt, *.pem, *.der, *.key) can be uploaded. Trying to upload other files will result in an error message. Certificate storage should be considered a folder with certain access restrictions, therefore file names should be unique for every file.

It should be noted that this chapter only reviews main certificates and suggests means to use them for Protocol Hub services. Certificates can also be used for other causes, e.g. to secure VPN connections. For the sake of simplicity, uploading certificates and their usage are explained in their respective chapters where applicable.

Interface for certificate storage

To get more details about how one could use TLS for Protocol Hub protocols please check the section Excel configuration format.

To find out more about why certificates help keep devices secure please check the sectionCyber security or check X.509 and RFC 5755 standard.

Revision #1

★Created 22 November 2024 07:15:14 by Gabriele
✎Updated 22 November 2024 07:24:23 by Gabriele