Table of contents

Certificate management

Certificate management

A secure connection between the OPC UA Server and the OPC UA Client is based on trustworthy certificates. Currently, only the self-signed certificate management is supported. There is based on a manual exchange of certificates between the OPC UA server and the client. Certificates are exchanged when establishing a connection between the client and the server. Server and client have to trust the certificates manually.

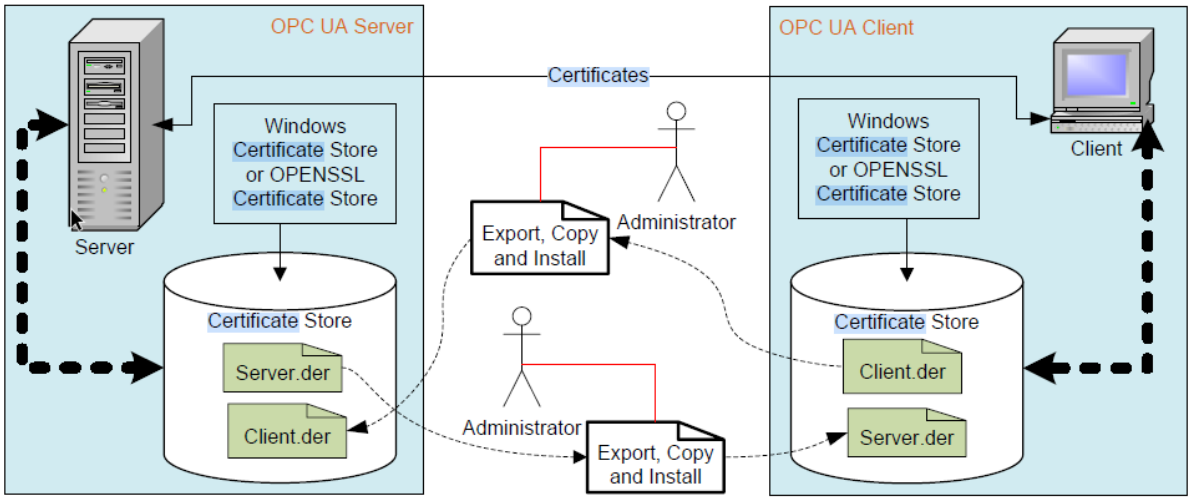

Fig. 12: Manual certificate management from “OPC UA Specification Part 2: Security“

For the ctrlX OPC UA Server, the certificates are trusted via the ctrlX CORE Certificate Manager (under *Settings ➔ Certificates & Keys* in the web interface).

The following steps are required:

1. First, set up a secure connection (SecureChannel) using the OpenSecureChannel. The certificate is transferred from the client to the server.
   ⇒ The server reports the error "BadSecurityChecksFailed" and enters the client certificate into its “Reject" list for certificates.
2. The certificate of the client is shown as “rejected" in the Certificate Manager under *Certificates & Keys ➔ OPC UA Server*. This certificate can be trusted manually. The client has to trust the server certificate as well.
3. The client can now set up a secure OPC UA connection to the server.

The certificate of the client can also be uploaded directly in the Certificate Manager. Thus, step 1 is omitted. However, the certificate has to be renamed before. The file name has to correspond to the SHA1 value of the file. This can for example be determined using the fingerprint of the certificate. When renaming, all characters of the SHA1 have to be

shown in capitals. The file schema is "*[SHA1 value capitalized]*.der".

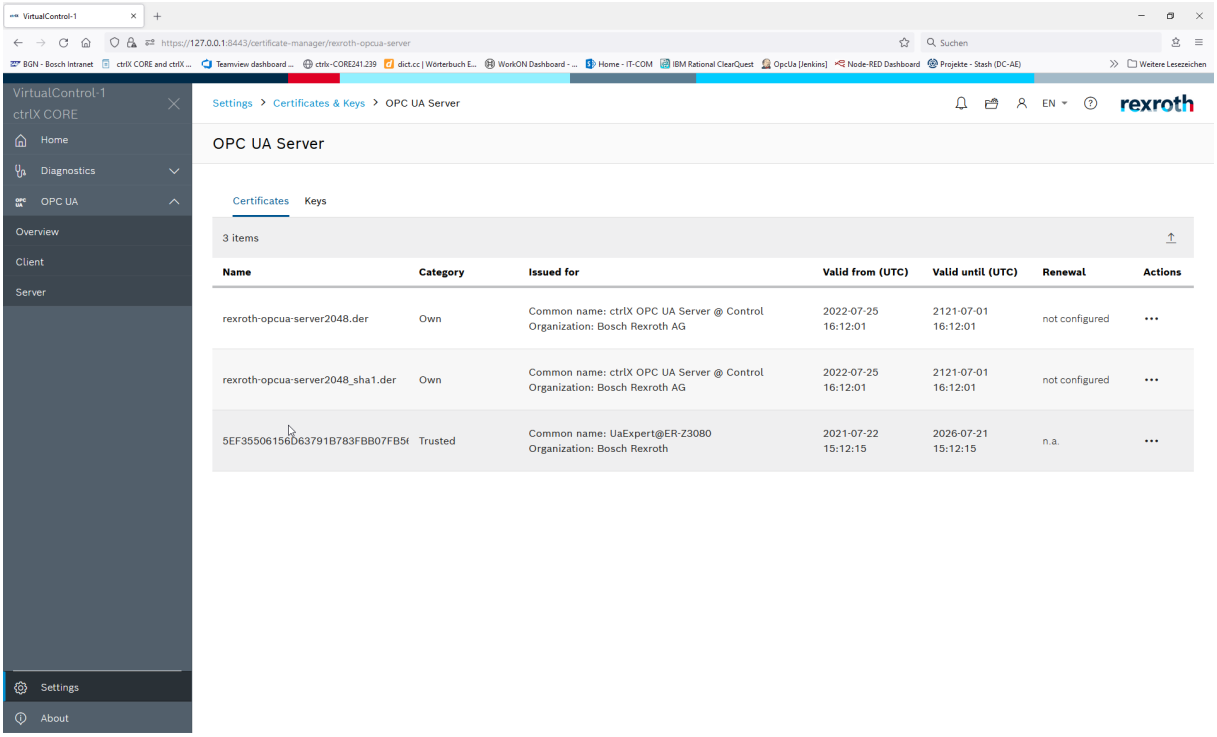

Fig. 13: Certificate Manager for the ctrlX OPC UA Server

Technical information on certificates and private keys

The certificates of the ctrlX OPC UA Server are currently self-generated and signed and valid for 36135 (ca. 99 year) by default.

The encryption methods used are "sha256" and "sha1".

The ctrlX OPC UA Server supports DER-encoded certificates and CRLs (Certificate Revocation List) according to the OPC UA specification. The private key has to be a PEM-encoded RSA private key.

Technical information on the storage of certificates

Certificates are stored in the Certificate Store.

For the Certificate Store, go to *$SNAP_COMMON/package-certificates/rexroth-opcua-server/rexroth-opcua-server/*.

The path for VirtualControl is for example:

/var/snap/rexroth-opcua-server/common/package-certificates/rexroth-opcua-server/rexroth-opcua-server/

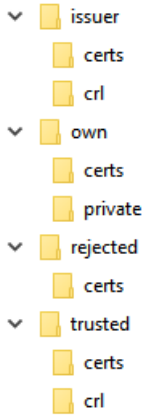

Fig. 14: Certificate Store - Folders and subfolders

The Certificate Store consists of the following folders:

- issuer:
  Currently not supported
- own:
  Includes the Application Instance Certificate from the OPC UA server or client and the respective private keys
- rejected:
  Includes certificates from the UA client or server that intend to set up a connection to the OPC UA server or client, but they have not yet been trusted
- trusted:
  Includes certificates of the UA client or servers. The OPC UA server or client trusts these certificates
  The respective subfolder “certs“ includes the certificates belonging to the individual categories, e.g. which certificates can be trusted (below the folder “trusted“) and which cannot be trusted (below the folder “rejected“). There is a Certificate Revocation List (CRL) in the subfolder “crl“.