D2000 OPC UA Server

OPC Unified Architecture (OPC UA) is a protocol for industrial automation. This protocol, which is managed by OPC Foundation, is a successor of the successful and often used OPC (OPC DA or OPC Classic) protocol. Unlike its predecessor, it is not based on Windows technologies (OLE, COM), thus available also on other platforms (e.g. PLC Simatic, or Bernecker & Rainer).

D2000 OPC UA Server allows OPC UA third-party clients to access the objects of D2000 system - to read them and to write their values.

D2000 OPC UA Server is located in the installation directory of D2000 installation under the name "opcuaserver.exe" (i.e. "opcuaserver" on Linux and Raspbian).

Characteristics of D2000 OPC UA Server

Support of **opc.tcp://** protocol

Support of identities:

- ANONYMOUS
- name:password

Support of security policies:

- None
- Basic128Rsa15
- Basic256
- Basic256Sha256

Message Security Modes:

- None
- Sign
- Sign&Encrypt

Configuration of an user for D2000 OPC UA Server

For D2000 OPC UA Server to access the individual objects of D2000 system, it is necessary to create a user in D2000 system under which OPC UA Server logs in to D2000 Server. OPC UA Server receives access rights of this user. User name must be in "OPCUA_User_*<process_name_opcua>*" format For instance, if OPC UA Server is named "SELF.OUS" (default, the process name can be changed with /W switch), then the name of the relevant user will be "OPCUA_User_SELF". It is necessary to set this user's access rights to objects of D2000 system. These access rights will be monitored while reading /writing values by OPC client.

Configuration of D2000 OPC UA Server

OPC UA Server configuration is read from a file. It is vital to specify the path to a configuration file by the starting parameter --cfg=*<path_to_configuration_file>*, for example "`opcuaserver.exe --cfg=c:\D2000\D2000_APP\application1\opcuaserver\opcuaserver.conf`". Sample configuration file is located in the program directory in subdirectory `Templates\opcuaserver\opcuaserver.conf.in` (resp. `./sys\templates\opcuaserver\opcuaserver.conf.in` on Linux). In this file, some parameters are already preset. It is necessary to set at least `pki_dir` parameter and create a directory structure for PKI.

It is possible to specify following parameters in the configuration file:

Parameter	Value
application_name	name of the application
application_uri	URI applications
pki_dir	full path to PKI directory structure (e.g. `'c:\D2000\D2000_APP\application1\opcuaserver\pki'`)
tcp_config.host	the address of network adapter on which OPC UA Server accept connections (*0.0.0.0* for all network adapters)
tcp_config.port	the port on which OPC UA Server accept connections
user_tokens	the list of configured users under which OPC UA clients can log in
endpoints	the list of access points of OPC UA Server

Configuration file is read during the OPC UA Server startup, so the adjustments of parameters in the file will show only after a restart. If PKI directory structure does not exist, OPC UA Server creates it (empty, without keys and certificates), based on the settings of `pki_dir` parameter.

Configuration of PKI (public key infrastructure)

For running a secure communication between OPC UA Server and OPC UA client, it is necessary for OPC UA Server to create PKI directory structure, private key and a certificate.

Directory structure consists of directories:

directory name	description
`pki/`	PKI directory
`pki/private/`	directory with a private key of OPC UA Server
`pki/own/`	directory with a public certificate of OPC UA Server
`pki/rejected/`	directory with a certificate of denied clients
`pki/trusted/`	directory with a certificate of allowed clients

It is essential to secure the private key against an unauthorized access.

Private key generation and certificate signing request using utility `openssl`:

```
openssl req -out csr.csr -new -newkey rsa:2048 -nodes -keyout pki/private/private.pem
```

Creation of self-signed certificate:

```
openssl x509 -req -days 365 -in csr.csr -signkey pki/private/private.pem -outform der -out pki/own/cert.der
```

Management of OPC UA Clients certificates

OPC UA Server sends its certificate to OPC UA client during establishment of a secured connection. When unknown OPC UA client connects, OPC UA Server rejects the client and saves their certificate into "`pki/rejected/`" directory. After that, administrator of D2000 application has to manually move that certificate into "`pki/trusted/`" directory. This ensures that server will consider the given client trustworthy and will accept the connection.

Management of OPC UA Clients names and passwords

Configuration of OPC UA clients' names and passwords is in the `opcuaserver.conf` configuration file. Only a single user token *sample_user* with user name *sample* and password *sample1* is predefined:

```
user_tokens:
  sample_user:
    user: sample
    pass: sample1
```

User tokens as well as anonymous access (ANONYMOUS) permitted for individual endpoints are defined in definition of respective endpoints:

```
basic256sha256_sign_encrypt:
    path: /
    security_policy: Basic256Sha256
    security_mode: SignAndEncrypt
    security_level: 4
    user_token_ids:
      - ANONYMOUS
      - sample_user
```