

D2000 OPC UA Server

OPC Unified Architecture (OPC UA) je protokol pre priemyselnú automatizáciu. Tento protokol, ktorý spravuje organizácia OPC Foundation, je nástupcom úspešného aasto používaného protokolu OPC (OPC DA alebo OPC Classic). Na rozdiel od svojho predchodcu nie je postavený na Windows technológiách (OLE, COM) a je tak dostupný aj na iných platformách (napr. PLC Simatic, alebo Bernecker & Rainer).

D2000 OPC UA Server umožňuje OPC UA klientom tretích strán pristupovať k objektom systému D2000 - číta a zapisovať ich hodnoty.

D2000 OPC UA Server sa nachádza v programovom adresári D2000 inštalácie pod menom "opcuaserver.exe" (resp. "opcuaserver" na Linuxe a na Raspbiane).

Vlastnosti D2000 OPC UA Servera

podpora protokolu **opc.tcp://**

podpora identít:

- ANONYMOUS
- meno:heslo

podpora bezpečnostných politík:

- None
- Basic128Rsa15
- Basic256
- Basic256Sha256

módy zabezpečenia správ (Message Security Modes):

- None
- Sign
- Sign&Encrypt

Konfigurácia užívateľa pre D2000 OPC UA Server

Aby D2000 OPC UA Server mohol pristupovať k jednotlivým objektom systému D2000, je potrebné vytvoriť v systéme D2000 užívateľa, pod ktorým sa OPC UA Server prihlási k serveru D2000. OPC UA Server dostane prístupové práva tohto užívateľa. Meno užívateľa musí byť vo formáte „OPCUA_User_<meno_procesu_opcua>“. Napríklad, ak je OPC UA Server nazvaný „SELF.OUS“ (default, meno procesu je možné zmeniť prepínaním /W), tak meno príslušného užívateľa bude „OPCUA_User_SELF“. Tomuto užívateľovi je potrebné nastaviť k objektom systému D2000 prístupové práva, ktoré budú kontrolované pri operáciách čítania/zapisu hodnôt OPC klientom.

Konfigurácia D2000 OPC UA Servera

Konfiguráciu OPC UA Server číta zo súboru. Cestu ku konfiguračnému súboru je nutné špecifikovať štartovacím parametrom `--cfg=<cesta_ku_konfiguracnemu_u_souboru>`, napríklad `"opcuaserver.exe --cfg=c:\D2000\D2000_APP\application1\opcuaserver\opcuaserver.conf"`. Vzorový konfiguračný súbor sa nachádza v [programovom adresári](#) v podadresári `Templates\opcuaserver\opcuaserver.conf.in` (resp. `sys\templates\opcuaserver\opcuaserver.conf.in` na Linuxe). V tomto súbore sú niektoré parametre už predvyplnené, je nutné nastaviť aspoň parameter `pki_dir` a vytvoriť adresárovú štruktúru pre [PKI](#).

V súbore je možné špecifikovať nasledujúce parametre:

Parameter	Hodnota
application_name	meno aplikácie
application_uri	URI aplikácie
pki_dir	plná cesta k adresáru PKI štruktúry (napríklad 'c:\D2000\D2000_APP\application1\opcuaserver\pki')
tcp_config.host	adresa sievového adaptéra na ktorom OPC UA server prijíma spojenia (0.0.0.0 pre všetky sievové adaptéry)
tcp_config.port	port na ktorom OPC UA server prijíma spojenia
user_tokens	zoznam nakonfigurovaných používateľov, pod ktorými sa môžu prihlasovať OPC UA klienti
endpoints	zoznam prístupových bodov OPC UA servera

Konfiguračný súbor je čítaný len pri štarte OPC UA servera, takže úpravy parametrov v súbore sa prejaví až po jeho reštarte. Ak adresárová štruktúra PKI neexistuje, OPC UA server ju vytvorí (prázdnu, bez kúov a certifikátov) podľa nastavenia parametra `pki_dir`.

Konfigurácia PKI (public key infrastructure)

Pre prevádzkovanie zabezpečenej komunikácie medzi OPC UA serverom a OPC UA klientami je potrebné pre OPC UA server vytvoriť PKI adresárovú štruktúru, privátny kľúč a certifikát.

Adresárová štruktúra pozostáva z adresárov:

názov adresára	popis
pki/	adresár PKI
pki/private/	adresár s privátnym kúom OPC UA servera
pki/own/	adresár s verejným certifikátom OPC UA servera
pki/rejected/	adresár s certifikátmi zamietnutých klientov
pki/trusted/	adresár s certifikátmi povolených klientov



Privátny kú je nutné zabezpečiť proti neoprávnenému prístupu.

Generovanie privátneho kúa a certificate signing request pomocou utility openssl:

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

Vytvorenie self-signed certifikátu:

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

Manažment certifikátov OPC UA klientov

Pri vytváraní zabezpečeného pripojenia OPC UA klient pošle OPC UA serveru svoj certifikát. Po pripojení neznámeho OPC UA klienta OPC UA server klienta odmietne a jeho certifikát uloží do adresára "pki/rejected/". Správca D2000 aplikácie následne musí manuálne presunúť daný certifikát do adresára "pki/trusted/". To zabezpečí, že daného klienta bude server považovať za dôveryhodného a spojenie prijme.

Manažment mien a hesiel OPC UA klientov

Konfigurácie mien a hesiel OPC UA klientov sú v konfiguracom súbore `opcua_server.conf`. Preddefinovaný je jediný užívateľský token `sample_user` s menom `sample` a heslom `sample1`:

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

V definíciách jednotlivých endpointov sú vymenované povolené užívateľské tokeny, prípadne je povolený aj anonymný prístup (ANONYMOUS):

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