Nastavenie zabezpeenej komunikácie (SSL/TLS)

Systém D2000 je možné nakonfigurova tak, aby komunikácia medzi serverom a klientami prebiehala zabezpeeným šifrovaným komunikaným kanálom. Zabezpeenie je implementované protokolom **Transport Layer Security** (TLS v1.2).

Pre aktiváciu zabezpeenej komunikácie je potrebné vykona nasledujúce kroky:

1. Pre server je nutné získa/vygenerova šifrovací kú a certifikát. Certifikát je potrebné distribuova klientským procesom.

Kú a certifikát je možné vygenerova napr. pomocou utility **openssl** (https://slproweb.com/products/Win32OpenSSL.html).

Generovanie šifrovacieho kúa

```
openssl genrsa -out server.pem 4096
```

Generovanie certificate signing request

```
openssl req -new -key server.pem -out server.csr
```

Generovanie self-signed certifikátu

```
openssl x509 -req -days 730 -in server.csr -signkey server.pem -out server.crt
```

2. Nastavi TLS podporu v registroch pre kernel

```
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Server\TLS_CertFile = c:\<cesta>\server.
crt
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Server\TLS_KeyFile = c:\<cesta>\server.pem
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Server\TLS_RequiredLevel = <level>
```

Nastavenie vyžadovanej úrovne zabezpeenia pripájajúceho sa klienta <level>:

- **None** - kernel dovolí pripoji sa klientovi aj bez zabezpeenia aj so zabezpeením
- **TLSNoPeerAuth** - kernel dovolí pripojenie len od klienta, ktorý komunikuje zabezpeene ale nemusí by overený certifikátom
- **TLSPeerAuth** - kernel dovolí pripojenie len od klienta, ktorý komunikuje zabezpeene a zárove je overený certifikátom

3. Nastavi TLS podporu v registroch pre klientov

```
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Client\TLS_TrustedCerts = c:
\<cesta>\server.crt
 HKEY_LOCAL_MACHINE\SOFTWARE\Ipesoft\<instalacia>\cfg_<aplikacia>\TLS_Client\TLS_RequiredLevel = <level>
```

Nastavenie vyžadovanej úrovne zabezpeenia pripájajúceho sa klienta <level>:

- **None** - klient sa pripojí na kernel aj v prípade, že kernel podporuje zabezpeenú komunikáciu, aj v prípade, že nepodporuje
- **TLSPeerAuth** - klient sa pripojí len na kernel podporujúci zabezpeenú komunikáciu a je overený certifikátom

4. Pre použitie TLS musí by klient štartovaný okrem obvyklých parametrov (/S, /RD prípadne /RF) **aj s parametrom @*<názov_aplikácie>***

Dôvodom je, aby už pred pripojením sa k aplikanému serveru vedel názov aplikácie a naítal parametre TLS z registrov (vi bod 3).

Výmena kúov a certifikátov

D2000 Server naítava konfiguráciu TLS pri každom pripájaní klienta, takže je možné zmeni poas behu D2000 Servera konfiguráciu (vítane výmeny súborov s certifikátom a so súkromným kúom).

Súvisiace stránky:

Procesy systému D2000
Štartovacie parametre procesov