

Nastavenie zabezpečenej komunikácie (SSL/TLS)

System D2000 je možné nakonfigurovať tak, aby komunikácia medzi serverom a klientami prebiehala zabezpečeným šifrovaným komunikačným kanálom. Zabezpečenie je implementované protokolom **Transport Layer Security** (TLS v1.3).

Pre aktiváciu zabezpečenej komunikácie je potrebné vykonať nasledujúce kroky:

1. Pre server je nutné získať/vygenerovať šifrovací kľúč a certifikát. Certifikát je potrebné distribuovať klientským procesom.

Kľúč a certifikát je možné vygenerovať napríklad pomocou utility **openssl** (<https://slproweb.com/products/Win32OpenSSL.html>).

Generovanie šifrovacieho kľúča

```
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. Nastaviť 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 zabezpečenia pripájajúceho sa klienta <level>:

- **None** - kernel dovolí pripojiť sa klientovi aj bez zabezpečenia aj so zabezpečením
- **TLSNoPeerAuth** - kernel dovolí pripojenie len od klienta, ktorý komunikuje zabezpečené (ale nemusí byť overený certifikátom)

3. Nastaviť 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>
```

TLS_TrustedCerts: nastavenie serverového certifikátu - cesta k serverovému certifikátu. Je možné zadať aj viacero certifikátov oddelených bodkočiarkou (;). To je použité pre redundantné systémy alebo v procese výmeny certifikátov, keď môže byť nakonfigurovaný starý aj nový serverový certifikát.

TLS_RequiredLevel: Nastavenie vyžadovanej úrovne zabezpečenia pripájajúceho sa klienta:

- **None** - klient sa pripojí na kernel aj v prípade, že kernel podporuje zabezpečenú komunikáciu, aj v prípade, že nepodporuje
- **TLSNoPeerAuth** - klient sa pripojí len na kernel podporujúci zabezpečenú komunikáciu (ale nemusí byť overený certifikátom, t.j. neporovnáva sa certifikát so zoznamom *TLS_TrustedCerts*)
- **TLSPeerAuth** - klient sa pripojí len na kernel podporujúci zabezpečenú komunikáciu, ktorého certifikát je v zozname *TLS_TrustedCerts*

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

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

Alternatívou je nastavenie parametra [DefaultApplication](#) v registry.

Pozn: odporúame nastavenie [DefaultApplication](#) v registry kvôli tomu, aby nebolo nutné zadáva parameter /C<názov_aplikácie> nielen vo všetkých skratkách na ploche, ale aj pri runom spúšaní aplikácií.

Klient pripájajúci sa na server s použitím TLS to vypíše do logu. Ak je vyžadované aj overenie certifikátu a certifikát je korektne overený, v logu je slovo **VERIFIED**:

```
[2022-09-23 07:48:11.289] CLIENT - Connecting to D2000 Server [localhost] TCP/IP[TLS...
```

```
[2022-09-23 07:48:11.348] CLIENT - Connection established to D2000 Kernel V22.00.074 s380 [TCP/IP localhost:3119][TLSv1.3 VERIFIED].  
ConnectionSqlId = 1
```

Kernel pripájajúci klienta cez TLS takisto túto informáciu zapíše do logu:

```
[2022-09-23 07:48:10.598] BACKEND - RegistrateProces request from DispPC.HIP V22.00.074 s380 [TCP/IP 127.0.0.1:50481][TLSv1.3]. ClientName:  
DispPC.HIP
```

```
[2022-09-23 07:48:10.600] SERVER - RegistrateProces OK. ClientName: DispPC.HIP Id: 7652 ComputerName: PC1PHUM1v SAS: 0
```



Výmena kúov a certifikátov

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



Blog

O nastavovaní TLS si môžete preíťa blog:

- [Bezpenos - Konfigurácia TLS \(za 15 minút\)](#)



Súvisiace stránky:

[Procesy systému D2000](#)

[Štartovacie parametre procesov](#)