

# Nastavenie zabezpečenej komunikácie (SSL/TLS)

Systém D2000 je možné nakonfigurovať tak, aby komunikácia medzi serverom a klientami prebiehala zabezpečeným šifrovaným komunikačným kanálom. Zabezpečenie je implementované protokolom **Transport Layer Security** (TLS v1.2).

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.key 4096
```

### Generovanie certificate signing request

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

### Generovanie self-signed certifikátu

```
openssl x509 -req -days 730 -in server.csr -signkey server.key -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.key  
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
- **TLSPeerAuth** - kernel dovolí pripojenie len od klienta, ktorý komunikuje zabezpečené a zároveň je 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>
```

Nastavenie vyžadovanej úrovne zabezpečenia pripájajúceho sa klienta <level>:

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

## 4. Pre použitie TLS musí byť klient štartovaný okrem obvyklých parametrov (/S, /RD prípadne /RF) aj s parametrom **/C<názov\_aplikácie>**

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



**Súvisiace stránky:**

[Procesy systému D2000](#)

[Štartovacie parametre procesov](#)