
A) REKAPITULACE POŽADAVKŮ NA TLS/CA CERTIFIKÁTY (NSOL R18)

V souvislosti s vydáním verze **R18 systému NSOL** dochází ke změně poskytovatele SSL certifikátů. Nový poskytovatel je **Sectigo** a všechna zařízení, která se připojují přímo k NSOL (ověřovací systém léků – FMD aplikace), musí mít nainstalovány dva konkrétní certifikáty certifikační autority (CA):

Certifikát	Název	Ke stažení
Root CA	Sectigo Public Server Authentication Root R46	https://crt.sh/?d=4256644734
Subordinate CA	Sectigo Public Server Authentication CA DV R36	https://crt.sh/?d=4267304690

Termíny:

- **Od 18. března 2026** – certifikáty jsou požadovány v IQE (testovacím) prostředí
- **Od 20. května 2026** – certifikáty jsou povinné v produkčním prostředí

Co se stane bez certifikátů: Systém NSOL se bude jevit jako nedostupný, ačkoli bude fungovat. FMD aplikace nebude moci ověřovat léčivé přípravky.

Kdo je ohrožen:

- ✅ **MS Windows plně aktualizovaný** – certifikáty by již měly být přítomny automaticky
- ⚠️ **Linux a Java prostředí** – certifikáty pravděpodobně chybí, nutná ruční instalace
- ⚠️ **MS Windows bez pravidelných aktualizací** – může chybět Root CA; Subordinate CA se instaluje automaticky při prvním připojení (pokud není tato funkce vypnuta)

Které zařízení kontrolovat:

- Pokud lékárna/distributor používá aplikaci přímo na PC či jiném zařízení → kontroluje se **PC/zařízení**
- Pokud se připojuje přes centrální server → kontroluje se **centrální server**

B) JAK OVĚŘIT PŘÍTOMNOST CERTIFIKÁTŮ – NÁVOD PRO UŽIVATELE (WINDOWS)

Na zařízení s MS Windows

1. Stiskněte klávesy **Windows + R**, napište „*certmgr.msc*“ a stiskněte **Enter**
2. Otevře se „**Správce certifikátů**"
3. V levém panelu rozbalte **Důvěryhodné kořenové certifikační autority → Certifikáty**
4. Vyhledejte certifikát: **„Sectigo Public Server Authentication Root R46"**
    - Pokud ho vidíte → ✅ Root CA je v pořádku
    - Pokud ho nevidíte → ⚠️ je nutná instalace (viz část c)

5. Dále v levém panelu otevřete **Zprostředkující certifikační autority → Certifikáty**
6. Vyhledejte: **„Sectigo Public Server Authentication CA DV R36"**
    - Pokud ho vidíte → ✅ Subordinate CA je v pořádku
    - Pokud ho nevidíte → Windows ho pravděpodobně doinstaluje automaticky při prvním připojení; pokud ne, postupujte dle části c)

💡 **Tip:** V okně správce certifikátů můžete použít scroll nebo kliknout na záhlaví sloupce „Vydáno pro" a seřadit abecedně – certifikáty Sectigo najdete v sekci „S".

C) JAK CERTIFIKÁTY NAINSTALOVAT – NÁVOD PRO UŽIVATELE (MS WINDOWS)

Krok 1 – Stáhněte certifikáty

1. Otevřete webový prohlížeč a přejděte na:
    - **Root CA:** https://crt.sh/?d=4256644734 → soubor se automaticky stáhne (přípona .crt)
    - **Subordinate CA:** https://crt.sh/?d=4267304690 → stejný postup
2. Oba soubory uložte na plochu nebo do složky Stažené soubory

Krok 2 – Nainstalujte Root CA certifikát

1. Klikněte **pravým tlačítkem** na stažený soubor Root CA (.crt)
2. Vyberte **„Instalovat certifikát"**
3. Zobrazí se Průvodce importem certifikátu → klikněte **Další**
4. Vyberte **„Místní počítač"** → klikněte **Další** (může být vyžadováno potvrzení správce)
5. Zvolte **„Umístit všechny certifikáty do následujícího úložiště"** → klikněte **Procházet**
6. Vyberte **„Důvěryhodné kořenové certifikační autority"** → **OK** → **Další** → **Dokončit**
7. Zobrazí se hláška „Import byl úspěšný" → **OK**

Krok 3 – Nainstalujte Subordinate CA certifikát

1. Stejný postup jako v Kroku 2, ale v bodě 6 vyberte **„Zprostředkující certifikační autority"**

Krok 4 – Ověřte instalaci

- Opakujte postup z části **b)** – certifikáty by nyní měly být viditelné

⚠️ **Důležité upozornění:** Pokud vaše lékárna/sklad používá **centrální server** (a ne lokální PC pro připojení k NSOL), musí certifikáty nainstalovat váš IT správce na server, nikoli na každý jednotlivý počítač.

🔒 Instalace certifikátu do úložiště „Místní počítač" vyžaduje **administrátorská práva!** Pokud nemáte tato práva, kontaktujte svého IT správce nebo dodavatele FMD aplikace.