

Zprovoznění HTTPS pro přístup k serveru Praetora

Možné účely

- I. Mobilní aplikace
 - a. Praetor server je provozován na vlastním serveru (on-premise) a je potřeba zřídit přístup pro mobilní aplikaci. Komunikaci je potřeba zabezpečit mj. proto, že nezabezpečenou komunikaci některé telefony blokuji.
- II. Klientský portál (WebClient)
 - a. Praetor server je provozován na vlastním serveru (on-premise) a je potřeba zřídit přístup pro zákazníky advokátní kanceláře. Komunikaci je potřeba zabezpečit, aby data zákazníků neputovala přes internet nešifrovaná.
- III. GraphQL API
 - a. Praetor server je provozován na vlastním serveru (on-premise) a je potřeba zřídit přístup k API Praetora. Pokud není přístup využíván ze stejného stroje, doporučujeme komunikaci zabezpečit pomocí HTTPS jako obranu proti odposlechu (byť ve vnitřní síti). Je-li API využíváno přes internet, je zabezpečení prakticky nezbytné.
- IV. Praetor exportér – pro komunikaci s účetnictvím
 - a. Praetor server se připojuje na jiný stroj k Praetor exportéru, který zprostředkovává přístup k účetnictví. Doporučujeme zabezpečení pomocí HTTPS provést i když komunikace probíhá jen ve vnitřní síti jako obranu proti odposlechu. Probíhá-li komunikace přes internet, je zabezpečení pomocí HTTPS prakticky nezbytné, aby data zákazníků advokátní kanceláře neputovala přes internet nezašifrovaná.
 - b. * Pokud Praetor exportér běží na serveru účetní firmy, je za účelem zjednodušení tohoto dokumentu pod zkratkou AK myšlena i účetní firma. Tedy pokud návod zmiňuje „nutnost spolupráce IT správce AK“, může to znamenat i spolupráci IT správce účetní firmy.

Možná řešení

- A. Nastavení certifikátu provede Wolters Kluwer (= vývojáři Praetora) v součinnosti s IT správou AK*
 - + obnovování certifikátu je zcela automatické, nastavení provede Wolters Kluwer
 - je potřeba mít otevřený port 80 na serveru s Praetorem (musí být dostupný z internetu) – pro ověřování domény při obnově certifikátu
- B. Nastavení certifikátu v Praetoru provede IT správce AK*
 - nutná práce IT správce AK*: ruční obnovování certifikátu (obvykle 1× ročně) nebo nastavení automatizace získávání certifikátu
 - + nemusí být potřeba otevřený port 80 nebo může být otevřen jen ve chvíli ověřování
- C. Migrace Praetora na Praetor cloud (není řešením pro IV. Praetor exportér)
 - + po provedení migrace není ke zprovoznění služeb od AK* vyžadována žádná akce

A. Nastavení certifikátu provede Wolters Kluwer v součinnosti s IT správou AK*

Toto je doporučený postup, pokud je možné splnit podmínky v následujících bodech 1–2.

1. AK* zajistí doménovou adresu (např. praetor.vase-ak.cz) – předpokládáme, že doména bude používána jen Praetorem.
2. AK* zajistí směrování této domény na server s Praetorem (DNS „A“ záznam, přesměrování portů routeru). Porty:
 - a. Ověřování domény při obnově certifikátu (nutné vždy): 80

- b. Mobilní aplikace: 14025
 - c. Klientský portál: 443
 - d. GraphQL API: 443
 - e. Praetor exportér: 6025
3. AK* umožní přístup společnosti Wolters Kluwer na server s Praetorem pro instalaci a konfiguraci nástroje pro získávání a automatickou obnovu certifikátu (jedná se o nástroj win-acme: <https://www.win-acme.com/>).

(Tato varianta je možná pouze při splnění podmínek dle bodů 1–2.)

B. Nastavení certifikátu provede IT správce AK*

Toto je doporučený postup nastavení pro ručně obnovované certifikáty nebo pokročilejší nastavení automatické obnovy certifikátů. V případě zájmu poskytneme konzultace v standardní hodinové sazbě.

1. AK* zajistí doménovou adresu (např. praetor.vase-ak.cz) – předpokládáme, že doména bude používána jen Praetorem.
2. AK* zajistí směrování této domény na server s Praetorem (DNS „A“ záznam, přesměrování portů routeru). Porty:
 - a. Mobilní aplikace: 14025
 - b. Klientský portál: 443
 - c. GraphQL API: 443
 - d. Praetor exportér: 6025
3. AK* si zajistí vydání SSL certifikátu pro danou doménu. Tento certifikát musí být vydaný autoritou (CA), která je v seznamu důvěryhodných CA na zařízeních, ze kterých se uživatelé budou připojovat.
4. Tento certifikát AK* nainstaluje na server s Praetorem (konzole certlm.msc – **místní počítač** / osobní / certifikáty), **včetně privátního klíče**.
5. AK* zaregistruje certifikát pomocí nástroje netsh
 - a. Parametry
 - %1 = doménové jméno (např. praetor.vase-ak.cz)
 - %2 = otisk certifikátu
 - b. Mobilní aplikace

```
netsh http delete sslcert hostnameport=%1:14025
netsh http add sslcert hostnameport=%1:14025 certhash=%2
certstorename=MY appid={005528a7-198a-4c14-802c-023649ac2574}
```
 - c. Klientský portál / GraphQL API

```
netsh http delete sslcert hostnameport=%1:443
netsh http add sslcert hostnameport=%1:443 certhash=%2
certstorename=MY appid={005528a7-198a-4c14-802c-023649ac2574}
```
 - d. Praetor exportér

```
netsh http delete sslcert hostnameport=%1:6025
netsh http add sslcert hostnameport=%1:6025 certhash=%2
certstorename=MY appid={005528a7-198a-4c14-802c-023649ac2574}
```
6. AK* umožní přístup společnosti Wolters Kluwer na server s Praetorem pro zapnutí objednaných služeb.

(Body 3–5 je potřeba provádět opakovaně dle platnosti certifikátu.)

C. Migrace Praetora na Praetor cloud (není řešením pro IV. Praetor exportér)

Po provedení migrace veškerá nastavení zmíněných služeb provede Wolters Kluwer. (Pokud mají služby běžet na doméně AK, bude stále vyžadována součinnost IT správce AK.)