

REST API PNT – test zabezpečené komunikace

Obsah

| | |
|--|----------|
| Princip zabezpečené komunikace | 2 |
| Získání SSL certifikátu ze služeb Let's Encrypt a certbot | 2 |
| Vygenerování vlastního SSL certifikátu..... | 2 |
| Registrace SSL certifikátu v IIS..... | 3 |
| Konfigurace testovací aplikace Postman | 4 |
| Otestování HTTPS komunikace z aplikace Postman..... | 5 |
| Zhodnocení testu zabezpečené komunikace | 5 |

Princip zabezpečené komunikace

Základní komunikace s REST Api PNT může probíhat HTTP protokolem. S ohledem na větší zabezpečení této komunikace je doporučena komunikace zabezpečeným protokolem HTTPS.

Takové zabezpečené spojení je realizováno SSL/TLS protokolem, k jeho realizaci je třeba SSL certifikát nainstalovaný do úložiště certifikátů serveru a jeho zaregistrování v IIS.

Získání SSL certifikátu ze služeb Let's Encrypt a certbot

Cílem bylo získat SSL certifikát pro IIS na serveru **fenix-sql.asol.local**.

Na radu kolegů (J. Rosol. R. Klášterka) bylo testováno použití SSL certifikátu, který poskytuje služba **Let's Encrypt** na adrese <https://letsencrypt.org>.

Při získání SSL certifikátu z této služby se objevil problém, že tímto způsobem není možné získat SSL certifikát pro server ležící v privátní (firemní vnitřní) doméně.

Další cestou bylo získání SSL certifikátu ze služby **certbot** na adrese <https://certbot.eff.org>, ale i tady byl problém stejný jako v případě služby Let's Encrypt.

Vygenerování vlastního SSL certifikátu

Nakonec byl nalezen postup, kterým lze vygenerovat vlastní certifikáty pro HTTPS komunikaci s REST API PNT prostřednictvím skriptů Power Shellu.

Uvedený postup byl proveden na serveru **fenix-sql.asol.local**.

Postup generování certifikátu:

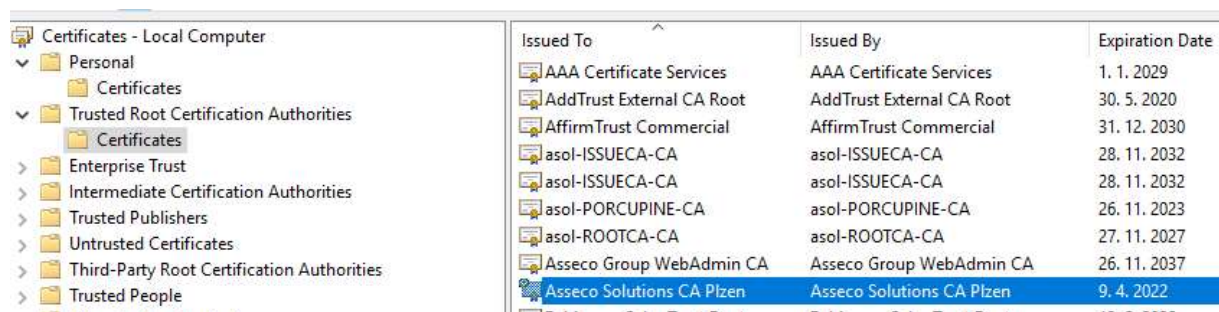
- spustit Windows **Power Shell ISE** jako admin
- otevřít v něm skript **SSL Certifikát pro REST API 02.ps1**
- změnit **DnsName** na **fenix-sql.asol.local**

- skript spustit F5

- spustit MMC: Certifikáty - Místní počítač



- certifikát **Asseco Solutions Plzen CA** přesunout do **Důvěryhodných certifikačních autorit**



Registrace SSL certifikátu v IIS

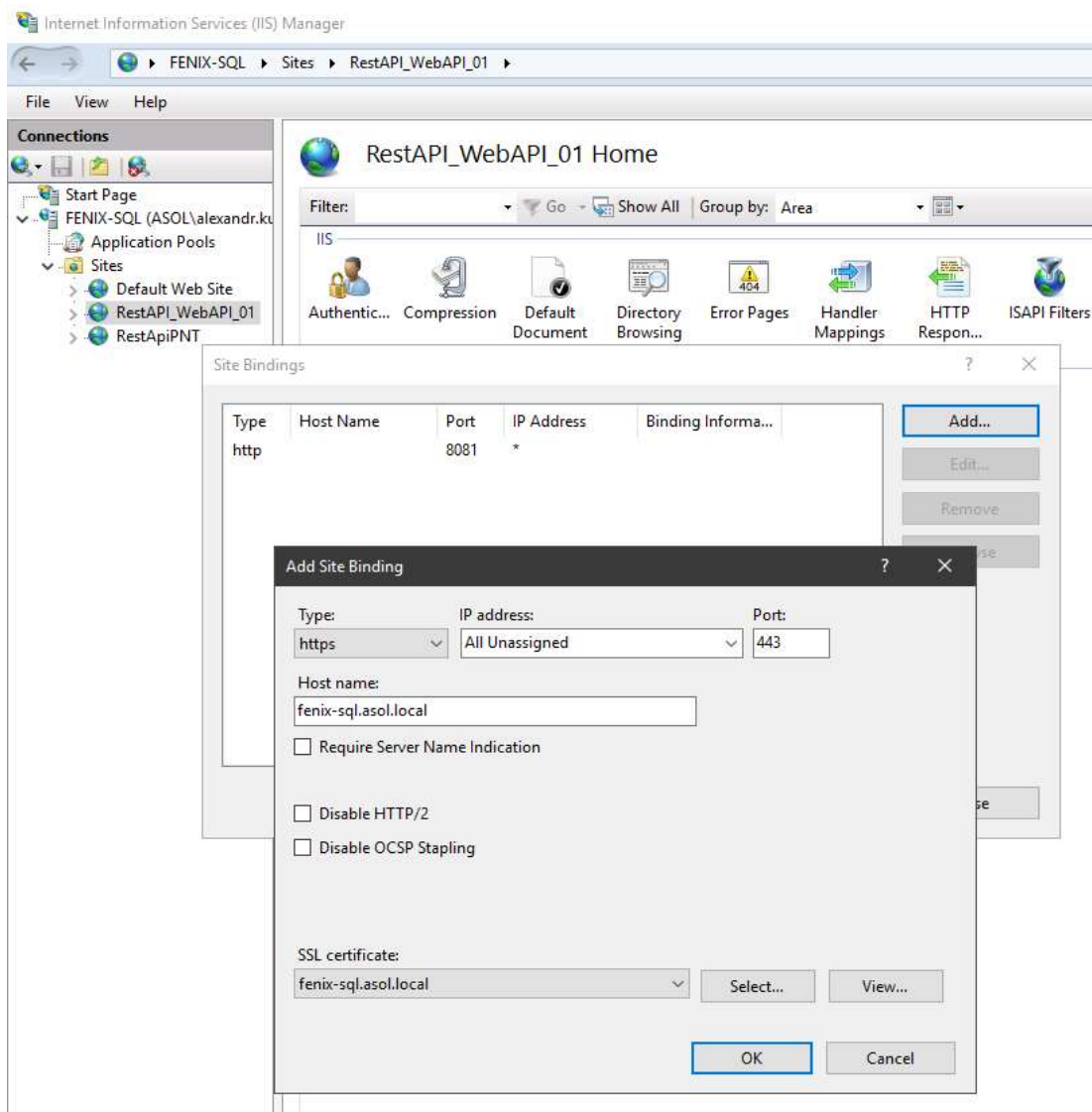
Registrace certifikátu a vytvoření vazby HTTPS:

- pro web **RestAPI_WebAPI_01** přidat vazbu (Binding) pro zabezpečený protokol HTTPS (add Bindings/Vazby)

- editovat řádek vazby pro HTTPS a vyplnit:

Host name (Název hostitele): fenix-sql.asol.local

SSL certifikát: vybrat certifikát Asseco Solutions CA Plzen



Konfigurace testovací aplikace Postman

V aplikaci Postman přidán Environment **FENIX-SQL HTTPS** s hodnotami pro **host**:fenix-sql.asol.local:443

| FENIX-SQL HTTPS | | | |
|-------------------------------------|--------------------|---------------------------------|----------------------------------|
| | VARIABLE | INITIAL VALUE ⓘ | CURRENT VALUE ⓘ |
| <input checked="" type="checkbox"/> | host | https://fenix-sql.asol.local:44 | https://fenix-sql.asol.local:443 |
| <input checked="" type="checkbox"/> | UserPswd | ██████████ | ██████████ |
| <input checked="" type="checkbox"/> | UserName | alexandr.kupec | alexandr.kupec |
| <input checked="" type="checkbox"/> | token | | |
| | Add a new variable | | |

Otestování HTTPS komunikace z aplikace Postman

Zabezpečená HTTPS komunikace byla vyzkoušena odesláním požadavku na autentizační endpoint našeho REST API PNT.

Komunikace s REST Api PNT proběhla a byl vrácen autentizační token. Nebylo ale možné certifikát ověřit zřejmě vzhledem k tomu, že nebyl vydán důvěryhodnou certifikační autoritou.

Body Cookies Headers (9) Test Results

Status: 200 OK Time: 12.85 s

Pretty Raw Preview Visualize JSON

```

1 {
2   "success": true,
3   "statusCode": "ok",
4   "errorMessage": "",
5   "userName": "alexandr.kupec",
6   "userId": "UserId 1ef39844883c2f9721cb8609d32806b2f6249538276434e01b8:"
7 }

```

Network

Local Address 172.29.16.31

Remote Address 172.29.13.246

TLS Protocol TLSv1.2

Cipher Name ECDHE-RSA-AES256-GCM-SHA...

Certificate CN fenix-sql.asol.local

Issuer CN Asseco Solutions CA Pízen

Valid Until Apr 9 08:37:58 2031 GMT

Unable to verify the first certificate

Zhodnocení testu zabezpečené komunikace

Zabezpečená komunikace s REST API PNT byla vyzkoušena a měla by takto fungovat i u zákazníků.

Předpokladem je, že u zákazníků bude použit SSL/TLS certifikát vydaný důvěryhodnou certifikační autoritou.