

Naudojantis žiniatinklio paslaugomis (angl. Webservice) duomenys iš mokesčių mokėtojų kompiuterinių programų į i.SAF ar i.VAZ posistemį bus perduodami tiesiogiai – t. y. be žmogaus įsikišimo. Langa "Žiniatinklio paslaugos" suteikiama galimybė atlikti žiniatinklio paslaugų naudojimo nustatymus, užsisakant žiniatinklio paslaugų naudojimui būtiną sertifikato sugeneravimą. Norėdami sugeneruoti autentifikavimo sertifikatą, turite savo priemonėmis paruošti CSR (angl. Certificate Signing Request) failą. Žemiau pateikiama detali instrukcija kaip paruošti CSR, generuoti autentifikavimo sertifikatą ir jį konvertuoti į PKCS12 formato failą tinkamą importavimui į Windows sertifikatų tarnybą.

CSR generavimas su OpenSSL (galima įdiegti OpenSSL for Windows arba jeigu naudojama Windows 10 operacinė sistema – įsidiekite „Windows subsystem for Linux“ ir paleiskite „Bash“).

https://msdn.microsoft.com/en-us/commandline/wsl/install_guide

1. Sukurkite privatų raktą: `openssl genrsa -out vardenis.pavardenis.key 2048` ;

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Tomas>bash
Tomas@TOMAS-DESKTOP:/mnt/c/Users/Tomas$ openssl genrsa -out vardenis.pavardenis.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
```

2. Sugeneruokite CSR failą (angl. Certificate Signing Request): `openssl req -new -sha256 -key vardenis.pavardenis.key -out vardenis.pavardenis.csr` ;

```
Tomas@TOMAS-DESKTOP:/mnt/c/Users/Tomas$ openssl req -new -sha256 -key vardenis.pavardenis.key -out vardenis.pavardenis.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

3. Prisijunkite prie i.MAS;
4. Kairiajame meniu spauskite **[Žiniatinklio paslaugos]**;
5. Atsidariusiame puslapyje, spauskite **[Užsakyti sertifikatą]**;

6. Paspaudę **[ikelti dokumentą]**, pasirinkite CSR failą;

7. Norėdami generuoti / atsisiųsti sertifikatą, spauskite **[Generuoti sertifikatą]** (po paspaudimo sertifikatas bus parsiončiamas automatiškai);

8. Paverskite sertifikatą iš DEP į PEM formatą: openssl x509 -inform der -in vardenis.pavardenis.crt -out vardenis.pavardenis.pem ;

9. Supakuokite sertifikatą ir privatą raktą į PKCS12 formato sertifikatą (praplėtimas - PFX): openssl pkcs12 -export -out vardenis.pavardenis.pfx -inkey vardenis.pavardenis.key -in vardenis.pavardenis.pem

Tokį PFX failą jau galima importuoti į Windows sertifikatų tarnybą. Patikrinimui ar gerai suimportavote pažiūrėkite ar su naršykle pasiekiate pageidaujamos paslaugos WSDL specifikaciją. Pavyzdžiui: <https://imas-ws.vmi.lt/ivaz-processor/services/sync?wsdl> arba <https://imas-ws.vmi.lt/isaf-uploader/services/uploader?wsdl>

Žemiau pateikiamas .NET pavyzdys kaip naudojant sertifikatą kreiptis į žiniatinklio servisą iš kliento aplikacijos:

```

using System.Security.Cryptography.X509Certificates;
BasicHttpsBinding binding = new BasicHttpsBinding
{
    Security = new BasicHttpsSecurity
    {
        Transport = new HttpTransportSecurity
        {
            ClientCredentialType = HttpClientCredentialType.Certificate
        }
    }
};
Client client = new Client(binding, new EndpointAddress("https://imasws.vmi.lt/ivaz-processor/services/sync"));
client.ClientCredentials.ClientCertificate.SetCertificate(
    StoreLocation.CurrentUser,
    StoreName.My,
    X509FindType.FindBySerialNumber,
    "00f0b1191d24d04e93a403135a9d5d1c95"); // Pakeiskite į savo sertifikato serijinį numerį

```

Pakartotinai atsisiųsti sugeneruotą sertifikatą galite paspaudę **[Nustatymai -> Žiniatinklio paslaugos]**, sąrašė išsirinkite norimą atsisiųsti sertifikatą, spauskite **[Atsisiųsti]**.

Pastabos:

1. Tinkamas CSR elemento formatas - .csr arba .txt failas.
2. Sertifikatas užsakomas mokesčių mokėtojo apskaitos sistemai, kurią ruošiama integruoti su i.SAF ar i.VAZ. Sertifikato nereikia generuoti kiekvienam naudotojo kompiuteriui.
3. Sertifikato užsakymas turi būti atliekamas atstovaujant įmonę, o ne fizinį asmenį.