DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Návod na instalaci Referenčního agenta

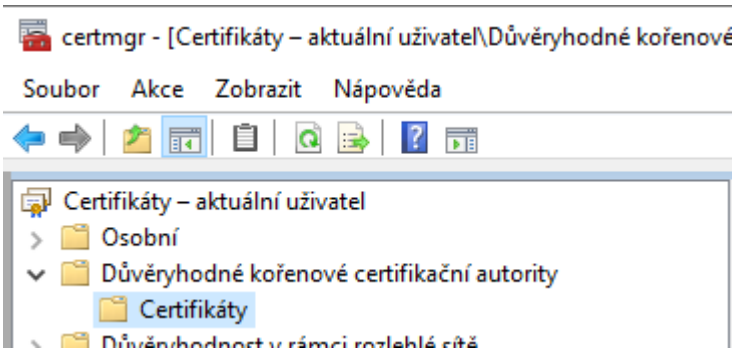
Nainstalovat kořenové a mezilehlé certifikáty certifikačních autorit (CA SZR a CA DIA) do úložiště Windows.

Ke stažení zde:

https://szrcr.cz/images/dokumenty/v%C3%BDvoj%C3%A1%C5%99i/Korenove_certifikaty_Referencniho_agenta_CA_DIA_CA_SZR.zip

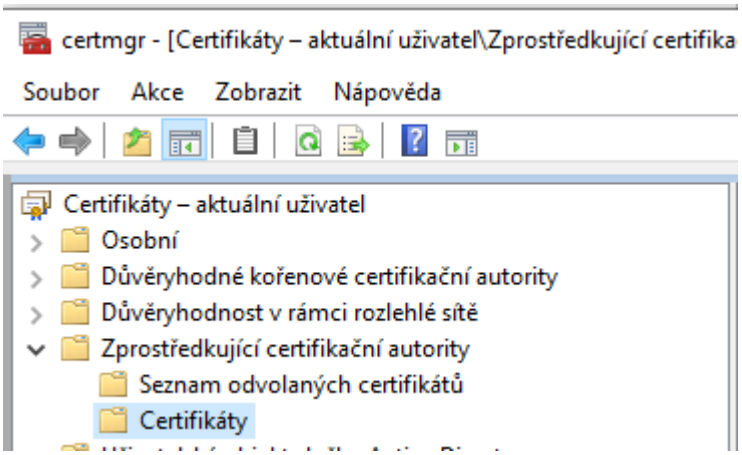
Mezi důvěryhodné kořenové certifikační autority přidat:

- ISZRRootCA
- RootCA_Test

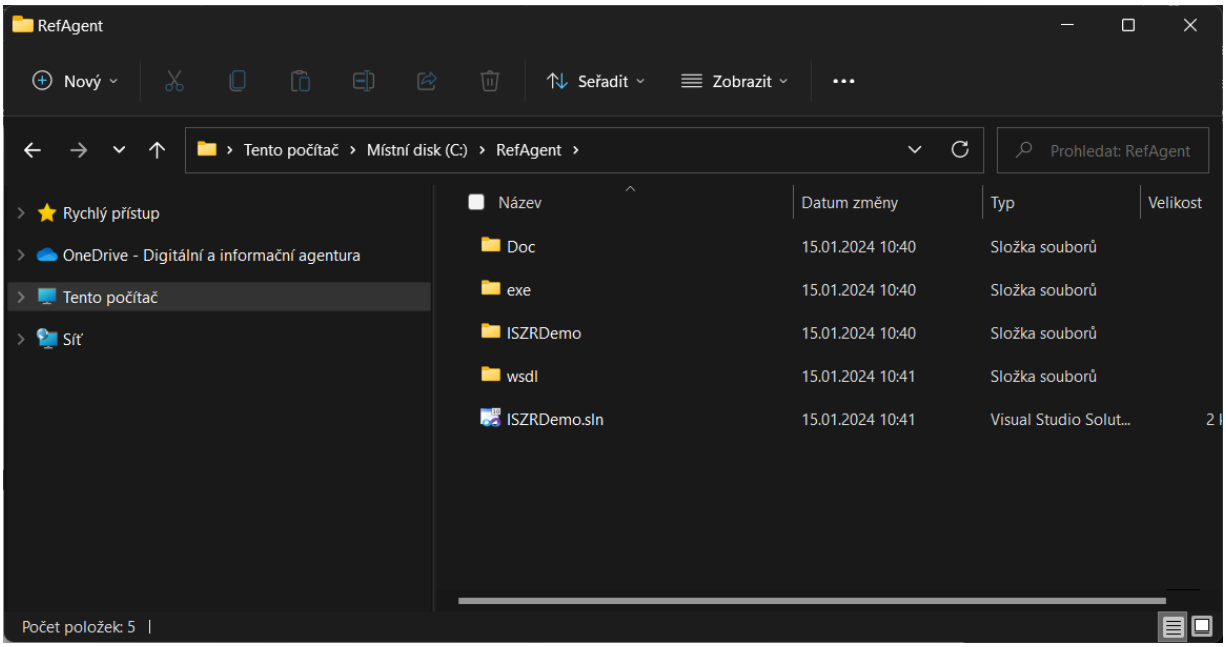


Mezi zprostředkující certifikační autority přidat

- ISZR_CA_TEST
- ISZRSubCA

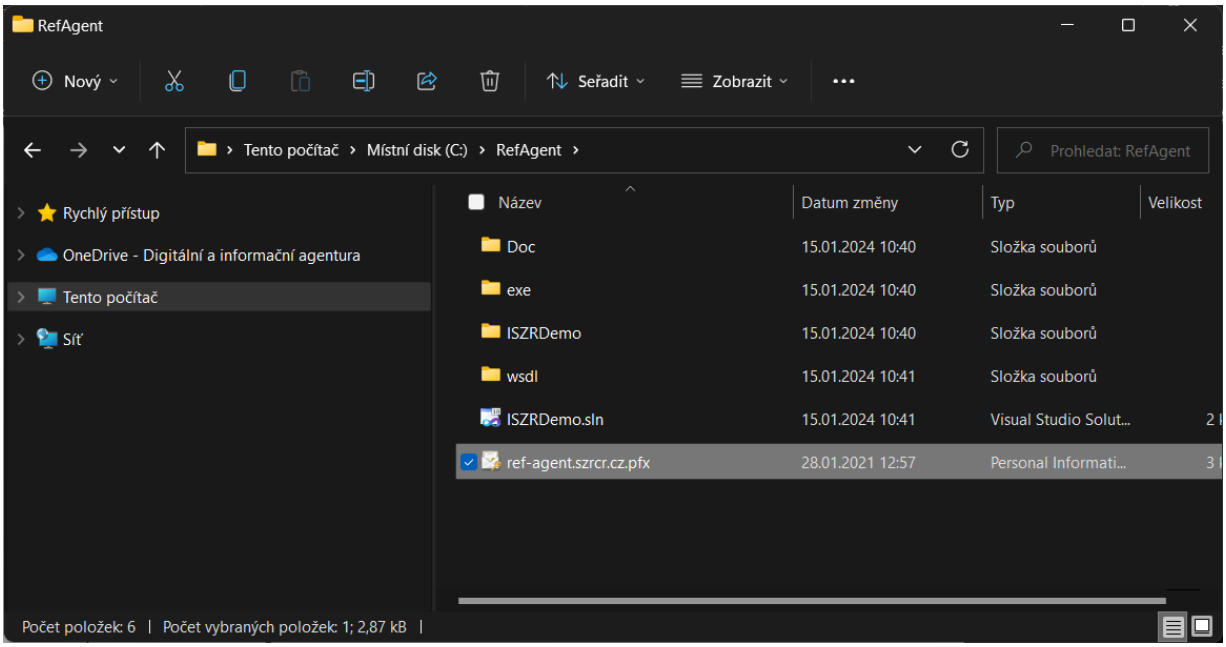


Nakopírovat Referenčního agenta do adresáře C:\

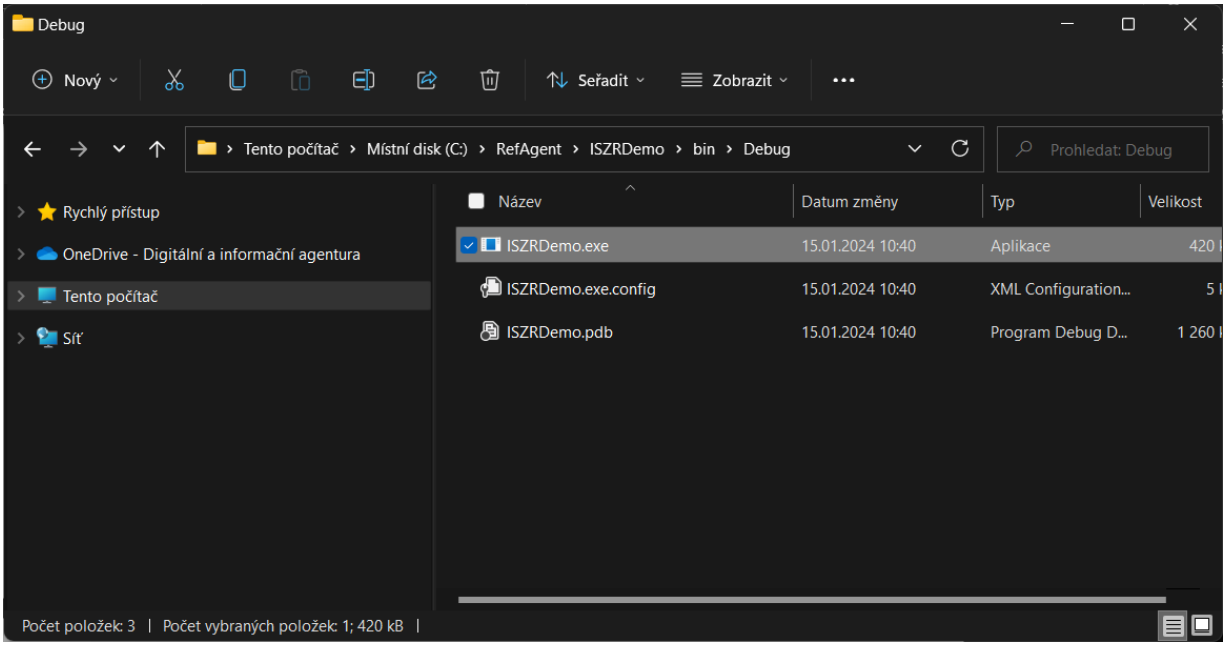


Stáhnout Referencni_agent.pfx zde
https://www.szrcr.cz/images/dokumenty/v%C3%BDvoj%C3%A1%C5%99i/Certifikaty_pro_referencniho_agenta_pfx_15012024.zip

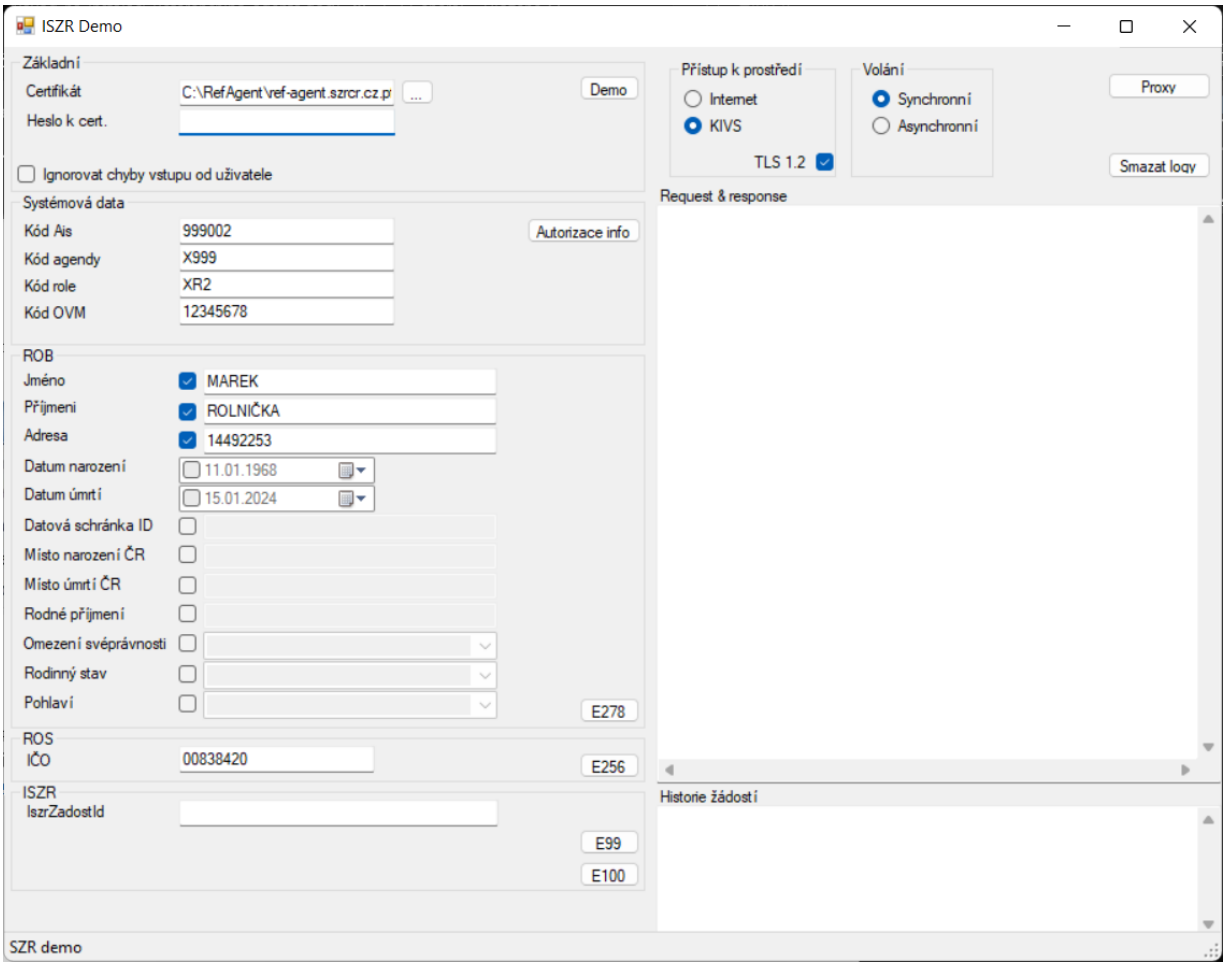
Jedná se o soubor s certifikátem a soukromým klíčem Referenčního agenta. Soubor zkopírujeme do adresáře C:\RefAgent



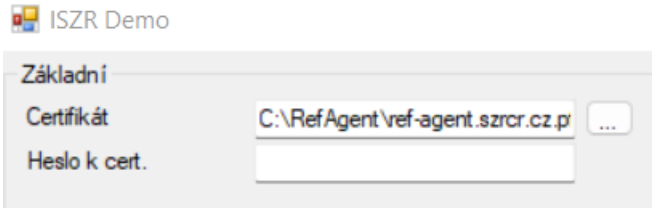
Spuštění aplikace můžeme provést z následujícího adresáře C:\RefAgent\ISZRDemo\bin\Debug\ aplikace se jmenuje ISZRDemo.exe



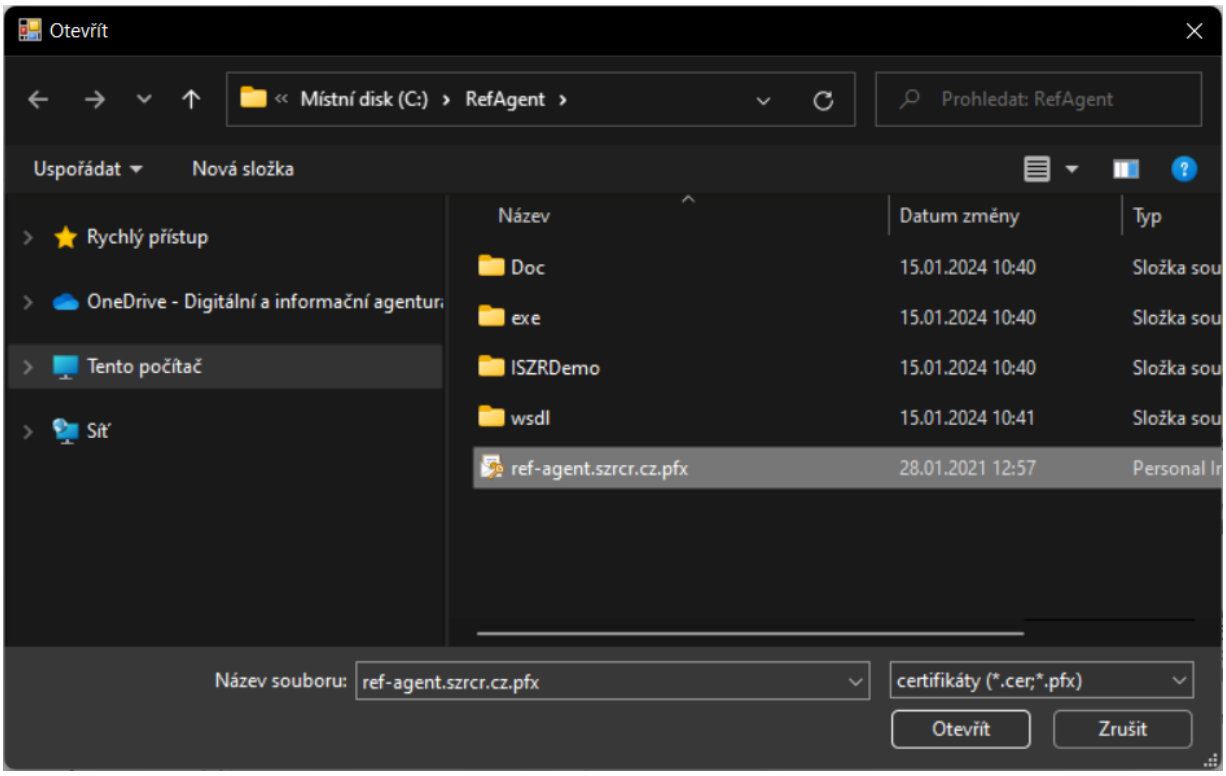
Pokračujeme spuštěním Referenčního agenta – program ISZRDemo.exe.



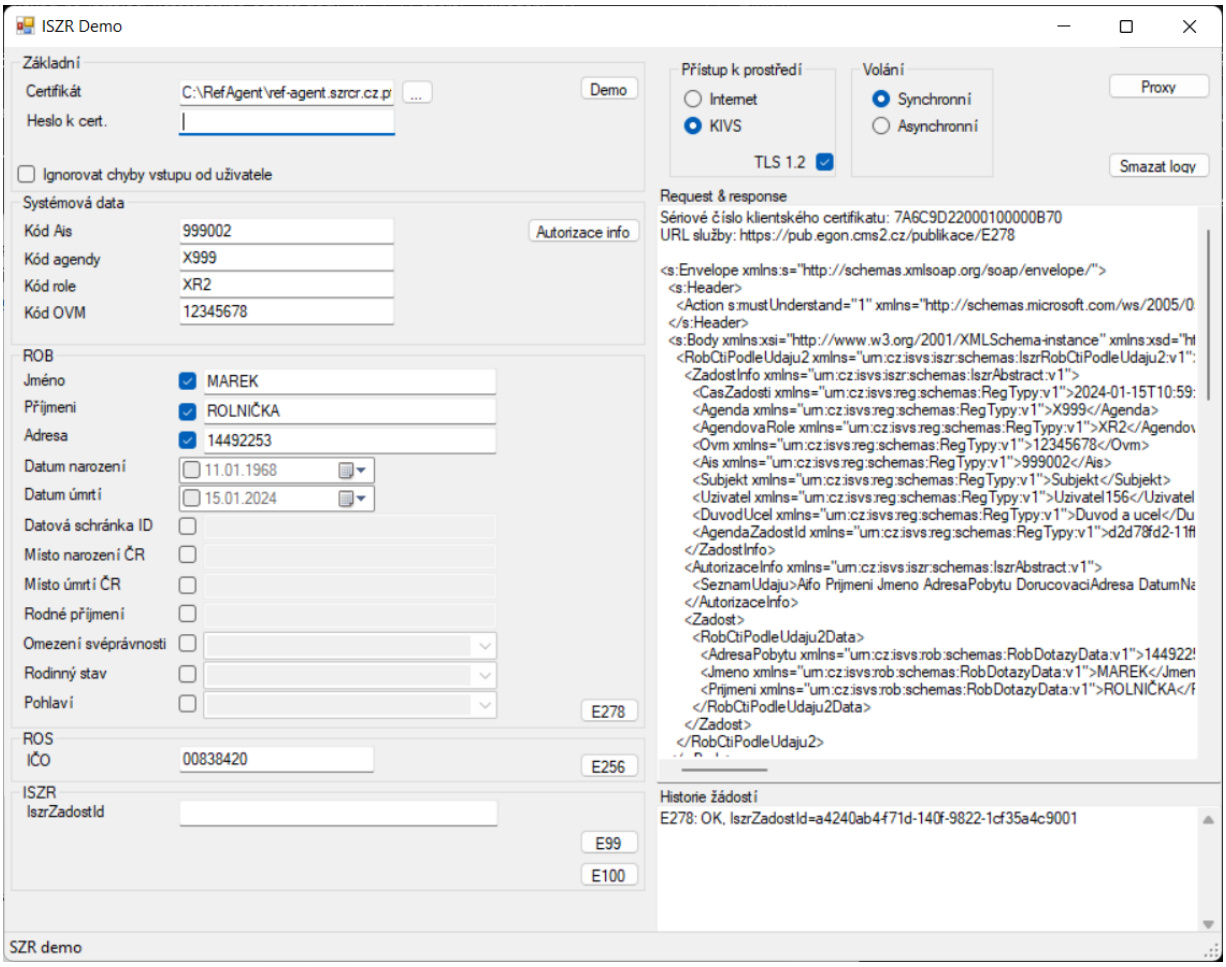
V prvním kroku nastavíme cestu k certifikátu s privátním klíčem, pokud jste postupovali dle předchozích bodů tak je cesta k souboru „C:\RefAgent“, heslo k certifikátu není záměrně na obrázku uvedeno, obdržíte ho v SMS po podání žádosti: Žádost o používání soukromého klíče referencniho agenta.docx. Klikneme na tři tečky vedle textového pole s cestou a otevře se nám dialogové okno s možností výběru souboru.



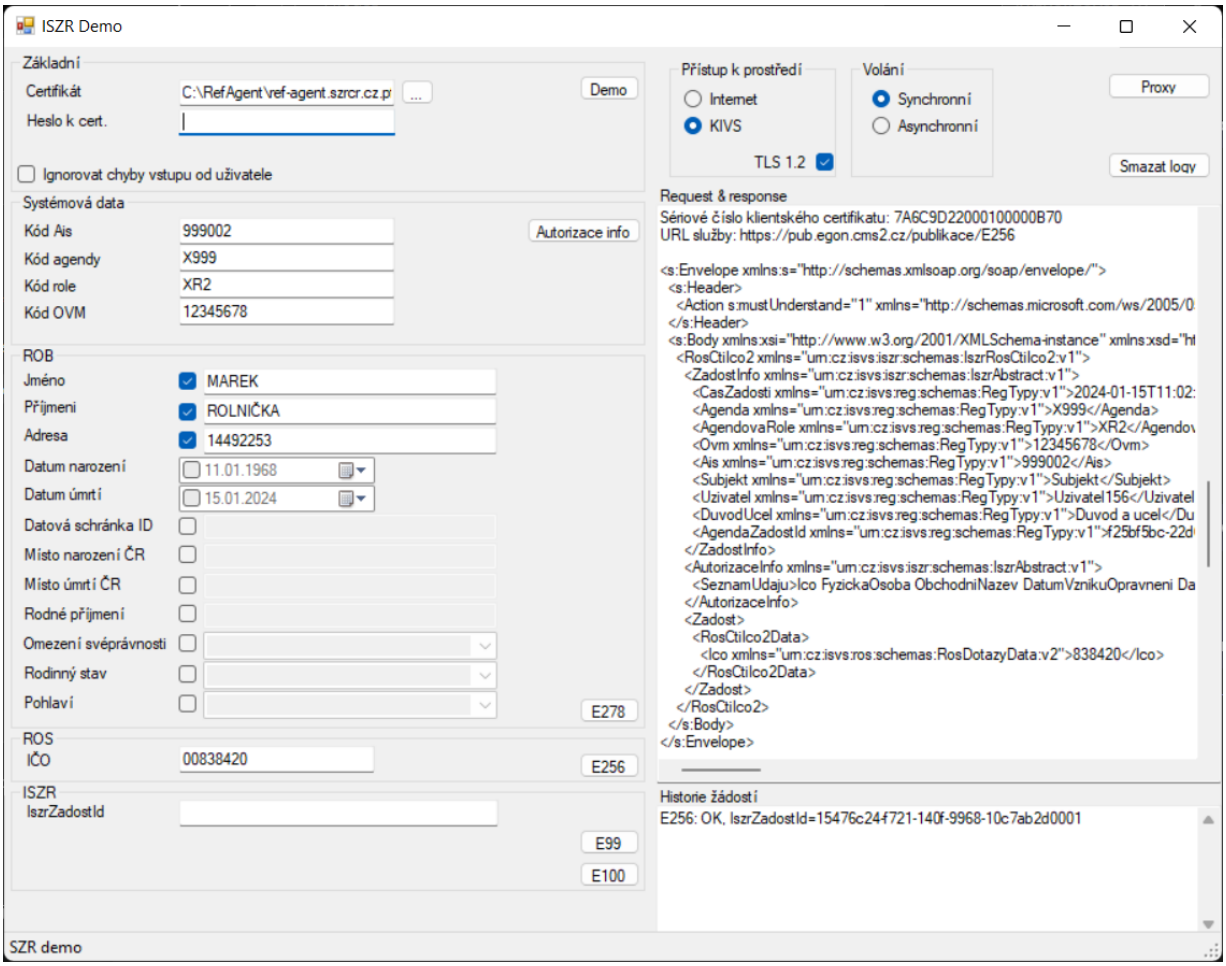
V okně vybereme soubor s certifikátem „ref-agent.szrcr.cz.pfx“ a klikneme na možnost otevřít.



Požádat o službu, např. o službu E278, stisknutím příslušného tlačítka v rozhraní Referenčního agenta. V příkladu jde o volání z internetu. Veřejná IP adresa počítače odkud se Referenční agent komunikuje musí být registrována na DIA viz Žádost o používání soukromého klíče referencniho agenta.docx.


ISZR Demo
Základní
Certifikát
C:\RefAgent\ref-agent.szrcr.cz.p
Heslo k cert.
Demo
Ignorovat chyby vstupu od uživatele
Systémová data
Kód Ais
999002
Kód agendy
X999
Kód role
XR2
Kód OVM
12345678
Autorizace info
ROB
Jméno
MAREK
Příjmení
ROLNIČKA
Adresa
14492253
Datum narození
11.01.1968
Datum úmrtí
15.01.2024
Datová schránka ID
Místo narození ČR
Místo úmrtí ČR
Rodné příjmení
Omezení svéprávnosti
Rodinný stav
Pohlaví
E278
ROS
IČO
00838420
E256
ISZR
IszrZadostId
E99
E100
Přístup k prostředí
Internet
KIVS
TLS 1.2
Volání
Synchronní
Asynchronní
Proxy
Smazat logy
Request & response
Sériové číslo klientského certifikatu: 7A6C9D22000100000B70
URL služby: https://pub.egon.cms2.cz/publikace/E278
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
<s:Header>
<Action s:mustUnderstand="1" xmlns="http://schemas.microsoft.com/ws/2005/0
</s:Header>
<s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="ht
<RobCtiPodleUdaju2 xmlns="um:cz:isvs:iszr:schemas:IszrRobCtiPodleUdaju2:v1">
<ZadostInfo xmlns="um:cz:isvs:iszr:schemas:IszrAbstract:v1">
<CasZadosti xmlns="um:cz:isvs:reg:schemas:RegTypy:v1">2024-01-15T10:59:
<Agenda xmlns="um:cz:isvs:reg:schemas:RegTypy:v1">X999</Agenda>
<AgendovaRole xmlns="um:cz:isvs:reg:schemas:RegTypy:v1">XR2</Agendov
<Ovm xmlns="um:cz:isvs:reg:schemas:RegTypy:v1">12345678</Ovm>
<Ais xmlns="um:cz:isvs:reg:schemas:RegTypy:v1">999002</Ais>
<Subjekt xmlns="um:cz:isvs:reg:schemas:RegTypy:v1">Subjekt</Subjekt>
<Uzivatel xmlns="um:cz:isvs:reg:schemas:RegTypy:v1">Uzivatel156</Uzivatel
<DuvodUcel xmlns="um:cz:isvs:reg:schemas:RegTypy:v1">Duvod a ucel</Du
<AgendaZadostId xmlns="um:cz:isvs:reg:schemas:RegTypy:v1">d2d78fd2-11ff
</ZadostInfo>
<AutorizaceInfo xmlns="um:cz:isvs:iszr:schemas:IszrAbstract:v1">
<SeznamUdaju>Aifo Prijmeni Jmeno AdresaPobytu DorucovaciAdresa DatumNa
</AutorizaceInfo>
<Zadost>
<RobCtiPodleUdaju2Data>
<AdresaPobytu xmlns="um:cz:isvs:rob:schemas:RobDotazyData:v1">144922
<Jmeno xmlns="um:cz:isvs:rob:schemas:RobDotazyData:v1">MAREK</Jmen
<Prijmeni xmlns="um:cz:isvs:rob:schemas:RobDotazyData:v1">ROLNIČKA</
</RobCtiPodleUdaju2Data>
</Zadost>
</RobCtiPodleUdaju2>
Historie žádostí
E278: OK, IszrZadostId=a4240ab4-f71d-140f-9822-1cf35a4c9001
SZR demo

Příklad výsledku volání služby E256 z prostředí KIVS.



Pro úspěšné navázání SSL spojení musí být na PC s Referenčním agentem nastavena správně také konfigurace SSL/TLS. Tj. operační systém na počítači uživatele musí umožňovat komunikaci s využitím TLS 1.2 a využívat alespoň jednu z uvedených ciphers.

TLSv1.2:

server selection: uses client preferences

3-- (key: RSA) RSA_WITH_AES_128_CBC_SHA

3-- (key: RSA) RSA_WITH_AES_256_CBC_SHA

3-- (key: RSA) RSA_WITH_AES_128_CBC_SHA256

3-- (key: RSA) RSA_WITH_AES_256_CBC_SHA256

3f- (key: RSA) ECDHE_RSA_WITH_AES_256_GCM_SHA384