IPNew web szolgáltatások elérése claims és tanúsítvány alapú azonosítással

Bevezetés

Az FGSZ IPNew rendszerének bevezetésével némileg változik a web szolgáltatások elérésének módja. A web szolgáltatások a SOAP 1.1 és a WS-Trust 1.3 protokollok használatával, felhasználónév/jelszó vagy tanúsítvány alapú azonosítással, claims-based módon érhetőek el.

A dokumentum célja

Ez a leírás segítséget nyújt az FGSZ azon partnerei részére, akik a szolgáltatásokat web service (gép-gép) interfészen érik el, hogy a szükséges módosításokat, fejlesztéseket elvégezhessék a saját rendszereikben.

Felhasználók azonosítása

A szolgáltatásokat csak azonosított felhasználók érhetik el. A felhasználók azonosítása egy külső azonosítási szolgáltatással történik (ami jelen esetben Active Directory Federation Services – AD FS), az azonosítást még a web szolgáltatás meghívása előtt el kell végezni. Az azonosított felhasználó adatait tartalmazó adatcsomagot (SAML token) a web szolgáltatás hívás kérés üzenetekhez csatolni kell, hogy a szerver kiszolgálja a kéréseket.

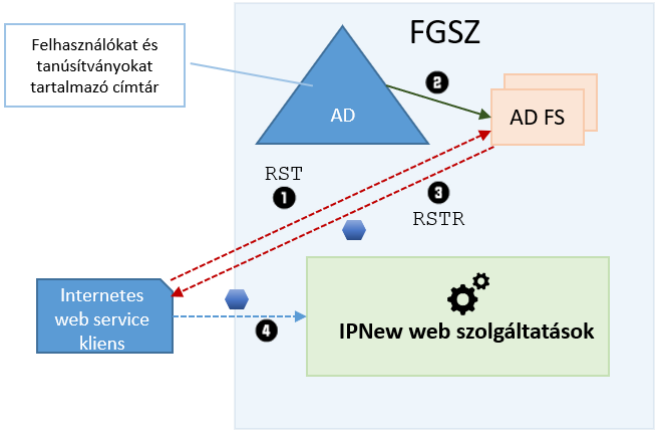
Azonosítás folyamata SOAP web szolgáltatás hívás esetén

AZ IPNew SOAP web szolgáltatásainak hívása esetén a hívó alkalmazásnak (kliensnek) a WS-Trust 1.3 protokollt kell használnia. A WS-Trust egyébként elég bonyolult és sok képességgel rendelkezik, de jelen esetben csak a számunkra releváns részét kell megismernünk.

Szerver oldalon a címtáron kívül két komponensnek van kiemelt szerepe az azonosításban:

- Relying Party (RP): Az az alkalmazás vagy szolgáltatás, amely az üzleti logikát valósítja meg, esetünkben ez az IPNew rendszer.
- Security Token Service (STS, más néven még Identity Provider, vagy Issuer): az azonosítást és a token kibocsájtást végző szolgáltatás, esetünkben az AD FS. WS-Trust esetében maga az STS is egy SOAP web szolgáltatás.

Az azonosítás és a web szolgáltatás hívása az alábbi módon, több lépésben történik:



1.) Első lépésként a kliens meghívja az STS egy speciális végpontját, az RST (Request Security Token) metódust, amely hívásban közli, hogy milyen típusú tokent igényel (pl. SAML 1.1) és

mely RP-vel való kommunikációban szeretné azt használni. A kérésnek tartalmaznia kell az azonosításhoz szükséges adatokat. Jelenleg mind a felhasználónév/jelszó, mind a tanúsítvány alapú azonosítás engedélyezett.

2.) Az STS ellenőrzi az azonosítási adatokat.
3.) Ha a megadott azonosítási információk helyesek, akkor az STS egy RSTR (Request Security Token Response) válaszban visszaadja a kért tokent.
4.) A kliens eltárolja a tokent, és a továbbiakban (a token érvényességi idején belül) az IPNew web szolgáltatás hívásokban csatolja azt a SOAP üzenethez (annak security header részében).

UAT teszt környezet web szolgáltatás címek

ADFS WSDL: https://sts.test.rbp.eu/adfs/services/trust/mex

ADFS végpont felhasználónév/jelszó alapú azonosításhoz:
https://sts.test.rbp.eu/adfs/services/trust/13/usernamemixed

ADFS végpont X.509 tanúsítvány alapú azonosításhoz:

https://sts.test.rbp.eu/adfs/services/trust/13/certificatemixed

PROD környezet web szolgáltatás címek

ADFS WSDL: https://sts.rbp.eu/adfs/services/trust/mex

ADFS végpont felhasználónév/jelszó alapú azonosításhoz:
https://sts.rbp.eu/adfs/services/trust/13/usernamemixed

ADFS végpont X.509 tanúsítvány alapú azonosításhoz:
https://sts.rbp.eu/adfs/services/trust/13/certificatemixed

Az üzleti web szolgáltatások tekintetében a kapcsolódó interfész leírásban megadott szolgáltatás cím használandó, a <servername> adott környezethez tartozó konkrét értékének behelyettesítésével. Az UAT teszt környezetben ez az érték **ipnew.test.fgsz.hu**. Az éles környezetben pedig **ipnew.fgsz.hu**

Minta web service kliens készítése Visual Studio-val

A web szolgáltatás meghívását érdemes modern fejlesztőeszközzel (pl. Visual Studio) végezni, ami a bonyolult technikai részleteket elfedve jelentősen leegyszerűsíti a feladatot. Tesztelés céljából kliensként használhatunk például egy egyszerű console application-t. Ha tanúsítvány alapú azonosítást használunk, szükségünk van egy X.509 kliens tanúsítványra, amit előzetesen az FGSZ hozzárendelt egy címtárbeli felhasználóhoz. Érdemes továbbá importálni a tanúsítványt a kliens gépen egy tanúsítvány tárba (pl. Current User /Personal), hogy a kódból egyszerűen tudjunk rá hivatkozni.

A mintaalkalmazás készítését az FGSZNNOService szolgáltatás meghívásának példáján keresztül mutatjuk be.

app.config beállítása

Adjunk hozzá a Visual Studio projekthez egy Service Reference-t, és adjuk meg a web service WSDL-jét. Service reference hozzáadásakor a Visual Studio olyan App.config-ot generál, amely az sts.test.fgsz.hu ADFS enpoint-okra hivatkozik. Külső felhasználóknak le kell cserélni a generált App.config-ban az `issuer address`, `issuerMetadata address` és a binding name- ben szereplő

sts.test.fgsz.hu-t sts.test.rbp.eu-ra. Az éles rendszer elérése estén pedig sts.rbp.eu-t kell használni. App.config minta:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6.1" />
  </startup>
  <system.serviceModel>
    <bindings>
      <ws2007FederationHttpBinding>
        <binding name="WS2007FederationHttpBinding_IFGSZNNOServiceSoapWrapper">
          <security mode="TransportWithMessageCredential">
            <message establishSecurityContext="false" issuedKeyType="BearerKey">
              <!--<issuer
address="https://sts.test.rbp.eu/adfs/services/trust/13/usernamemixed"
                  binding="ws2007HttpBinding" bindingConfiguration="adfs" />-->
              <issuer
address="https://sts.test.rbp.eu/adfs/services/trust/13/certificatemixed"
                  binding="ws2007HttpBinding" bindingConfiguration="adfs" />
              <issuerMetadata
address="https://sts.test.rbp.eu/adfs/services/trust/mex" />
              <tokenRequestParameters>
                <trust:SecondaryParameters xmlns:trust="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
                  <trust:KeyType xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-
trust/200512">http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</trust:KeyType>
                  <trust:CanonicalizationAlgorithm xmlns:trust="http://docs.oasis-
open.org/ws-sx/ws-trust/200512">http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>
                  <trust:EncryptionAlgorithm xmlns:trust="http://docs.oasis-
open.org/ws-sx/ws-trust/200512">http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>
                </trust:SecondaryParameters>
              </tokenRequestParameters>
            </message>
          </security>
        </binding>
      </ws2007FederationHttpBinding>
      <ws2007HttpBinding>
        <binding name="adfs">
          <security mode="TransportWithMessageCredential">
            <transport clientCredentialType="None" />
            <!--<message clientCredentialType="UserName"
negotiateServiceCredential="false" establishSecurityContext="false" />-->
            <message clientCredentialType="Certificate"
negotiateServiceCredential="false" establishSecurityContext="false" />
          </security>
        </binding>
      </ws2007HttpBinding>
    </bindings>
    <behaviors>
      <endpointBehaviors>
        <behavior name="certificateEndpointBehavior">
          <clientCredentials>
            <serviceCertificate>
              <authentication certificateValidationMode="None"
revocationMode="NoCheck"/>
            </serviceCertificate>
          </clientCredentials>
        </behavior>
      </endpointBehaviors>
```

```
    </behaviors>
    <client>
      <endpoint
address="https://ipnew.test.fgsz.hu/Fgsz.Ip.Web.UAT/Services/SoapFGSZNNOService.svc"
          binding="ws2007FederationHttpBinding"
bindingConfiguration="WS2007FederationHttpBinding_IFGSZNNOServiceSoapWrapper"
          contract="FgszService.IFGSZNNOServiceSoapWrapper"
name="WS2007FederationHttpBinding_IFGSZNNOServiceSoapWrapper"
          behaviorConfiguration="certificateEndpointBehavior" />
    </client>
  </system.serviceModel>
  <system.net>
    <defaultProxy enabled="true" useDefaultCredentials="true">
      <!--<bypasslist> … </bypasslist>
      <proxy> … </proxy>
      <module> … </module>-->
    </defaultProxy>
  </system.net>
</configuration>
```

Minta .Net/C# Kód

Az alábbi, vagy ehhez hasonló C# kód használható a szolgáltatás meghívásához. A példakód (és a korábbi app.config) a tanúsítvány alapú azonosításhoz használható. Ha felhasználónév/jelszó alapú azonosítást szeretnénk használni, akkor kommentezzük vagy töröljük ki a // Certificate authentication alatti kódsort, és a // Windows authentication alatti két kódsorról vegyük le a kommentezést és írjuk be a helyes felhasználónevet és a jelszót a csillagozott rész helyett, valamint az app.config-ban az issuer address és message clientCredentialType elemeket cseréljük le a username-es változatra (jelenleg kikommentezett sorok).

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Net.Security;
using System.Security.Cryptography.X509Certificates;
using System.Text;
using System.Threading.Tasks;

namespace WsClientTest
{
    class Program
    {
        static void Main(string[] args)
        {
            System.Net.ServicePointManager.ServerCertificateValidationCallback =
                delegate (object sender, X509Certificate certificate, X509Chain chain,
SslPolicyErrors sslPolicyErrors)
                { return true; };

            var proxy = new FgszService.FGSZNNOServiceSoapWrapperClient();

            // Certificate authentication
            // tempClientcert helyett a tanúsítvány Subject mezőjének értékét kell
használni

proxy.ClientCredentials.ClientCertificate.SetCertificate(StoreLocation.CurrentUser,
StoreName.My, X509FindType.FindBySubjectName, "tempClientcert");

//proxy.ClientCredentials.ServiceCertificate.Authentication.CertificateValidationMode
= System.ServiceModel.Security.X509CertificateValidationMode.None;
            //proxy.ClientCredentials.ServiceCertificate.Authentication.RevocationMode
= X509RevocationMode.NoCheck;
```

```
            // Windows Authentication
            //proxy.ClientCredentials.UserName.UserName = "testuser@ipnewtest.local";
            //proxy.ClientCredentials.UserName.Password = "********";
            string result = proxy.CheckAlive();
            Console.WriteLine(result);

            Console.ReadLine();

        }
    }
}
```

Példa üzenetváltás

A mintaprogramot futtatva az alábbi http üzenetváltáshoz hasonló forgalmat figyelhetjük meg.

Token igénylés

Request minta

```
POST https://sts.test.rbp.eu/adfs/services/trust/13/certificatemixed HTTP/1.1
Content-Type: application/soap+xml; charset=utf-8
Host: sts.test.rbp.eu
Content-Length: 4638
Expect: 100-continue
Accept-Encoding: gzip, deflate
Connection: Keep-Alive

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"><s:Header><a:Action
s:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</a:Action><a:MessageID>urn:uuid:f9aa5885-174e-4fa8-8e38-
4b35520078a5</a:MessageID><a:ReplyTo><a:Address>http://www.w3.org/2005/08/addressing/a
nonymous</a:Address></a:ReplyTo><a:To s:mustUnderstand="1"
u:Id="_1">https://sts.test.rbp.eu/adfs/services/trust/13/certificatemixed</a:To><o:Sec
urity s:mustUnderstand="1" xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd"><u:Timestamp u:Id="_0"><u:Created>2018-03-
09T12:35:18.852Z</u:Created><u:Expires>2018-03-
09T12:40:18.852Z</u:Expires></u:Timestamp><o:BinarySecurityToken u:Id="uuid-d4b24929-
31e2-49ad-95a3-b8f4e8275032-1" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-
1.0#Base64Binary">MIIDBjCCAfKgAwIBAgIQY2AkvW4NyY9ARCBjGn1CKjAJBgUrDgMCHQUAMBsxGTAXBgNV
BAMTEFJvb3RDYUNsaWVudFRlc3QwHhcNMTgwMzAxMDkxNDIzWhcNMzkxMjMxMjM1OTU5WjAZMRcwFQYDVQQDEw
50ZW1wQ2xpZW50Y2VydDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANVOrgbeL/kgdRrD3DnnQZ6G
O7+LaLDAPum/bdgFeA4LkCiYUP6QHGCUw57kEZ1ZaKU+jJHRfxZzbussuuILGNJaw3gEy533R7O2MNeDyglvSS
YHU9mnfKkirO/Jj/asn6Wkk+W6zwXkbH3uTRV3Z6OYv5r55QK/4cryCsvz1qYASLYBe0gW9nhoW8V79a6OU+Yd
w8pXZsTaz7xbzfX4am6q+TpoGYCEBpknI0Golt/H7MaOud8XybUv/RnqjIUetbzzOf36Ynom1sviiKXv29H3QT
91E0BaLKXj4AhBsvQ245nf1kKVT/gd0oQ4gWqP30ZMWJub9fK0nF24UiZUDpECAwEAAaNQME4wTAYDVR0BBEUw
Q4AQ3osAzHoU12fYNO9rdfjTvqEdMBsxGTAXBgNVBAMTEFJvb3RDYUNsaWVudFRlc3SCEJ563a9OH6OmRjCpyU
VHj1kwCQYFKw4DAh0FAAOCAQEAVKv8ox/Wi+dmncXccJZDQjuVhYEKRvgXCNWlJcfhf57SsIq4CV4P9NSKaKAs
ez1sDWFSJ3Luava9nZT/hx6mcC/enCulo8gW4P1gsaGz2Z4pgtI8V7cF/vkYA4k4od9wTnN82zzH1szdHQuN2C
WTo+QmvK9QhNffuwehBL5dJGPcxKWq1ldZzQ76KbKdzR2+NHN24m7qYZ+pcNEge5yENT3XFqHMVXFRaBnjqkBp
zCLDvYhvt9BQC2e7DAPK5fngdMvfut1Qgh43V4LAnW4KTs5ZldMHriWidAs73VcysxidYKFgAOD6IrrQW71wdT
UGkWUqdvF0/UjgRCMm9yUQGQ==</o:BinarySecurityToken><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><Reference
URI="#_0"><Transforms><Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>FlASDEG7MEZw8w0FX2G4V
```

```
D3yXy0=</DigestValue></Reference><Reference URI="#_1"><Transforms><Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>GFhi1zZiaiGWSD/4Ovt2X
yoaQvw=</DigestValue></Reference></SignedInfo><SignatureValue>CQoemS3joXqnHzS54lE8u34B
C74jzHDQu7vkQJF/8T46OllXxhmhVuSuxb7ubCzX2M3AnKynBtBVq08ZnWyFBhVABOqWfhICOCqAUl9hvEkPNl
oW97ZWExjxmIsaX0WHpNpdWcojG/szZOGsTF6yivCaXoIYz4hBUxYyCbX6iYYbK96vuLHZJhWTrkwagyxnu/3o
CVJHIielHmS6nl8zsJehMBOo2OKFr1s3zKOiVIdfG4Xjt5In1JobxT6cSnQKDBKJduJQG6Nn/2WYEwZxIpqexl
c+SMeQEMq3xYeK5dk3uCWMr+4a0GbHh9d1lRnpXE04h9XA3O6zl2p2kWLyrg==</SignatureValue><KeyInf
o><o:SecurityTokenReference><o:Reference ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" URI="#uuid-
d4b24929-31e2-49ad-95a3-b8f4e8275032-
1"/></o:SecurityTokenReference></KeyInfo></Signature></o:Security></s:Header><s:Body><
trust:RequestSecurityToken xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-
trust/200512"><trust:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</trust:RequestType><wsp:AppliesTo
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"><EndpointReference
xmlns="http://www.w3.org/2005/08/addressing"><Address>https://ipnew.test.fgsz.hu/Fgsz.
Ip.Web.UAT/Services/SoapFGSZNNOService.svc</Address></EndpointReference></wsp:AppliesT
o><trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Bearer</trust:KeyType><trust:SecondaryParameters>&#xD;
                  <trust:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Bearer</trust:KeyType>&#xD;
                  <trust:CanonicalizationAlgorithm>http://www.w3.org/2001/10/xml-exc-
c14n#</trust:CanonicalizationAlgorithm>&#xD;
                  <trust:EncryptionAlgorithm>http://www.w3.org/2001/04/xmlenc#aes256-
cbc</trust:EncryptionAlgorithm>&#xD;

</trust:SecondaryParameters></trust:RequestSecurityToken></s:Body></s:Envelope>
```

Response minta

```
HTTP/1.1 200 OK
Content-Length: 6803
Content-Type: application/soap+xml; charset=utf-8
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 09 Mar 2018 12:35:21 GMT

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"><s:Header><a:Action
s:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RSTRC/IssueFinal</a:Action><a:RelatesTo>urn:uuid:f9aa5885-174e-4fa8-8e38-
4b35520078a5</a:RelatesTo><o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"><u:Timestamp
u:Id="_0"><u:Created>2018-03-09T12:35:21.894Z</u:Created><u:Expires>2018-03-
09T12:40:21.894Z</u:Expires></u:Timestamp></o:Security></s:Header><s:Body><trust:Reque
stSecurityTokenResponseCollection xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-
trust/200512"><trust:RequestSecurityTokenResponse><trust:Lifetime><wsu:Created
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">2018-03-09T12:35:21.894Z</wsu:Created><wsu:Expires
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">2018-03-09T13:35:21.894Z</wsu:Expires></trust:Lifetime><wsp:AppliesTo
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"><wsa:EndpointReference
xmlns:wsa="http://www.w3.org/2005/08/addressing"><wsa:Address>https://ipnew.test.fgsz.
hu/Fgsz.Ip.Web.UAT/Services/SoapFGSZNNOService.svc</wsa:Address></wsa:EndpointReferenc
e></wsp:AppliesTo><trust:RequestedSecurityToken><saml:Assertion MajorVersion="1"
MinorVersion="1" AssertionID="_4e0cb07c-4a87-44bf-92ce-0b3bd02582bb"
Issuer="http://sts.test.rbp.eu/adfs/services/trust" IssueInstant="2018-03-
09T12:35:21.894Z" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><saml:Conditions
NotBefore="2018-03-09T12:35:21.894Z" NotOnOrAfter="2018-03-
09T13:35:21.894Z"><saml:AudienceRestrictionCondition><saml:Audience>https://ipnew.test
.fgsz.hu/Fgsz.Ip.Web.UAT/Services/SoapFGSZNNOService.svc</saml:Audience></saml:Audienc
eRestrictionCondition></saml:Conditions><saml:AttributeStatement><saml:Subject><saml:S
ubjectConfirmation><saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</sam
```

```
l:ConfirmationMethod></saml:SubjectConfirmation></saml:Subject><saml:Attribute
AttributeName="name"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:Attri
buteValue>IPNEWTEST\eburany</saml:AttributeValue><saml:AttributeValue>tempClientcert</
saml:AttributeValue></saml:Attribute><saml:Attribute AttributeName="upn"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:Attri
buteValue>eburany@ipnewtest.local</saml:AttributeValue></saml:Attribute></saml:Attribu
teStatement><saml:AuthenticationStatement
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:X509-PKI"
AuthenticationInstant="2018-03-
09T12:35:21.878Z"><saml:Subject><saml:SubjectConfirmation><saml:ConfirmationMethod>urn
:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod></saml:SubjectConfirmation
></saml:Subject></saml:AuthenticationStatement><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMetho
d Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><ds:Reference
URI="#_4e0cb07c-4a87-44bf-92ce-0b3bd02582bb"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>IbJHvrT2lrACeoovH
/76Hrez/8yXgQ1UM3y63O0fdO8=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:Signatu
reValue>KKu6oopRUSUvDuIdDuo7y/x+0HsRLs125yeHzCRMEcgtHldYXyBQIvuSjqoDkO8scg9Gyib9U8AUQJ
AVlXxsnZt2Wnx19webYrk0nH7VEZffoJpycQHjWN6+R3lHsXc8OwBqtF+m1VlPEImNhSv+cmCnHiMkNfGCxEZM
t3vIZR01oDCSFm3u05enOnILq4hkgb7kd/jhSfa7kZHgzjyY6QmfcYIRBPu27p9zyT495DVSR+L9etkZHlBrvz
CPTTh3TbX9CTWh1uZUsE++mu/nmY84VUV2nwdqd1fwKQM2nAeh02HzmGy/a2kHZdF6GIAlg2NNmtcrQX49NUv7
a3CZFg==</ds:SignatureValue><KeyInfo
xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Data><X509Certificate>MIIDEDCCAfigAwIB
AgIQHIgjaxlQUI9Fpn/u6ofQnjANBgkqhkiG9w0BAQsFADBEMUIwQAYDVQQDEzlBREZTIFNpZ25pbmcgLSBpcG
5ld3Rlc3RhZC5ub3J0aGV1cm9wZS5jbG91ZGFwcC5henVyZS5jb20wHhcNMTgwMjE3MTYxMjUzWhcNMTkwMjE3
MTYxMjUzWjBEMUIwQAYDVQQDEzlBREZTIFNpZ25pbmcgLSBpcG5ld3Rlc3RhZC5ub3J0aGV1cm9wZS5jbG91ZG
FwcC5henVyZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC138SfR2bsFXZobfoWIDZrqRy8
//lyF06iVYf20Qa/rJyBlZkKZFvwXt5L0+Nzt0FqbRHv37qAbEwuu0NyNzVzFa99hd3AncKuYHXgJr5PFEXNUu
7eI2nxtpxQNsjgedxqtlR2dRs/k3wvWy+ltEQKYyZ3maZmXEz+vU2kQhbzajTne0C+XEjNGic5+dhBbCKcRU7a
YUljZJy/Nv+U5hMGCCwAomziZ5rAPtpO9vU781zUhczpDa6tPqQiY4N/a8qong+kYV1lLyJvluYkaizHzMyJU7
b0aKTZfV8vMuEERc6WDseI4HfdhtTY0OM55TpQgBaphW80x/8/OgG85w3rAgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAAucCoXRfg4mnwfzBVah36NAQn2kCfdaU3sqet8nQXPXWStU28lP2tiF8pspz5Bb1Uw1bEO3MwGm6+o2YP
d6gnYpwYtWdmCYYFIZgQRU8nCzk4zw98I2O6JXs7kDMAocaIInIjs//4SnVHH3PSe29lw26ga2yAk6WmMSdPWz
e6zCspNskBjww8wvhhK9GknAPXWu0gCyHfG+ehEzfxXIx4ieJEodFNgmGuk97SWnMAkZdBlrZ1mVZWAMQI7Ata
Ou6JjvgDOGgmwyHMvEV83GdKOvKzR+vCb3X41L4Me/Fym7nxWZBEiRDqZEzidA6EQK2ceuiobFzhKx/xwJIoVk
nUI=</X509Certificate></X509Data></KeyInfo></ds:Signature></saml:Assertion></trust:Req
uestedSecurityToken><trust:RequestedAttachedReference><o:SecurityTokenReference
k:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1"
xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd" xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd"><o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-
token-profile-1.0#SAMLAssertionID">_4e0cb07c-4a87-44bf-92ce-
0b3bd02582bb</o:KeyIdentifier></o:SecurityTokenReference></trust:RequestedAttachedRefe
rence><trust:RequestedUnattachedReference><o:SecurityTokenReference
k:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1"
xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd" xmlns:k="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-
1.1.xsd"><o:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-
token-profile-1.0#SAMLAssertionID">_4e0cb07c-4a87-44bf-92ce-
0b3bd02582bb</o:KeyIdentifier></o:SecurityTokenReference></trust:RequestedUnattachedRe
ference><trust:TokenType>urn:oasis:names:tc:SAML:1.0:assertion</trust:TokenType><trust
:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</trust:RequestType><trust:KeyType>http://docs.oasis-open.org/ws-
sx/ws-
trust/200512/Bearer</trust:KeyType></trust:RequestSecurityTokenResponse></trust:Reques
tSecurityTokenResponseCollection></s:Body></s:Envelope>
```

Web service hívás a token beszerzése után

Request minta

```
POST https://ipnew.test.fgsz.hu/Fgsz.Ip.Web.UAT/Services/SoapFGSZNNOService.svc
HTTP/1.1
Content-Type: application/soap+xml; charset=utf-8
Host: ipnew.test.fgsz.hu
Content-Length: 5029
Expect: 100-continue
Accept-Encoding: gzip, deflate

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"><s:Header><a:Action
s:mustUnderstand="1">http://service.fgsz.hu/IFGSZNNOServiceSoapWrapper/CheckAlive</a:A
ction><a:MessageID>urn:uuid:55832272-64d9-420a-a946-
69de57a66df9</a:MessageID><a:ReplyTo><a:Address>http://www.w3.org/2005/08/addressing/a
nonymous</a:Address></a:ReplyTo><a:To
s:mustUnderstand="1">https://ipnew.test.fgsz.hu/Fgsz.Ip.Web.UAT/Services/SoapFGSZNNOSe
rvice.svc</a:To><o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"><u:Timestamp
u:Id="_0"><u:Created>2018-03-09T12:35:21.904Z</u:Created><u:Expires>2018-03-
09T12:40:21.904Z</u:Expires></u:Timestamp><saml:Assertion MajorVersion="1"
MinorVersion="1" AssertionID="_4e0cb07c-4a87-44bf-92ce-0b3bd02582bb"
Issuer="http://sts.test.rbp.eu/adfs/services/trust" IssueInstant="2018-03-
09T12:35:21.894Z" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><saml:Conditions
NotBefore="2018-03-09T12:35:21.894Z" NotOnOrAfter="2018-03-
09T13:35:21.894Z"><saml:AudienceRestrictionCondition><saml:Audience>https://ipnew.test
.fgsz.hu/Fgsz.Ip.Web.UAT/Services/SoapFGSZNNOService.svc</saml:Audience></saml:Audienc
eRestrictionCondition></saml:Conditions><saml:AttributeStatement><saml:Subject><saml:S
ubjectConfirmation><saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</sam
l:ConfirmationMethod></saml:SubjectConfirmation></saml:Subject><saml:Attribute
AttributeName="name"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:Attri
buteValue>IPNEWTEST\eburany</saml:AttributeValue><saml:AttributeValue>tempClientcert</
saml:AttributeValue></saml:Attribute><saml:Attribute AttributeName="upn"
AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:Attri
buteValue>eburany@ipnewtest.local</saml:AttributeValue></saml:Attribute></saml:Attribu
teStatement><saml:AuthenticationStatement
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:X509-PKI"
AuthenticationInstant="2018-03-
09T12:35:21.878Z"><saml:Subject><saml:SubjectConfirmation><saml:ConfirmationMethod>urn
:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod></saml:SubjectConfirmation
></saml:Subject></saml:AuthenticationStatement><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMetho
d Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></ds:CanonicalizationMethod><ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"></ds:SignatureMethod><ds:Reference URI="#_4e0cb07c-4a87-44bf-92ce-
0b3bd02582bb"><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></ds:Transform><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds:DigestMethod><ds:DigestValue>
IbJHvrT2lrACeoovH/76Hrez/8yXgQ1UM3y63O0fdO8=</ds:DigestValue></ds:Reference></ds:Signe
dInfo><ds:SignatureValue>KKu6oopRUSUvDuIdDuo7y/x+0HsRLs125yeHzCRMEcgtHldYXyBQIvuSjqoDk
O8scg9Gyib9U8AUQJAVlXxsnZt2Wnx19webYrk0nH7VEZffoJpycQHjWN6+R3lHsXc8OwBqtF+m1VlPEImNhSv
+cmCnHiMkNfGCxEZMt3vIZR01oDCSFm3u05enOnILq4hkgb7kd/jhSfa7kZHgzjyY6QmfcYIRBPu27p9zyT495
DVSR+L9etkZHlBrvzCPTTh3TbX9CTWh1uZUsE++mu/nmY84VUV2nwdqd1fwKQM2nAeh02HzmGy/a2kHZdF6GIA
lg2NNmtcrQX49NUv7a3CZFg==</ds:SignatureValue><KeyInfo
xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Data><X509Certificate>MIIDEDCCAfigAwIB
AgIQHIgjaxlQUI9Fpn/u6ofQnjANBgkqhkiG9w0BAQsFADBEMUIwQAYDVQQDEzlBREZTIFNpZ25pbmcgLSBpcG
```

```
5ld3Rlc3RhZC5ub3J0aGV1cm9wZS5jbG91ZGFwcC5henVyZS5jb20wHhcNMTgwMjE3MTYxMjUzWhcNMTkwMjE3
MTYxMjUzWjBEMUIwQAYDVQQDEzlBREZTIFNpZ25pbmcgLSBpcG5ld3Rlc3RhZC5ub3J0aGV1cm9wZS5jbG91ZG
FwcC5henVyZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC138SfR2bsFXZobfoWIDZrqRy8
//lyF06iVYf20Qa/rJyBlZkKZFvwXt5L0+Nzt0FqbRHv37qAbEwuu0NyNzVzFa99hd3AncKuYHXgJr5PFEXNUu
7eI2nxtpxQNsjgedxqtlR2dRs/k3wvWy+ltEQKYyZ3maZmXEz+vU2kQhbzajTne0C+XEjNGic5+dhBbCKcRU7a
YUljZJy/Nv+U5hMGCCwAomziZ5rAPtpO9vU781zUhczpDa6tPqQiY4N/a8qong+kYV1lLyJvluYkaizHzMyJU7
b0aKTZfV8vMuEERc6WDseI4HfdhtTY0OM55TpQgBaphW80x/8/OgG85w3rAgMBAAEwDQYJKoZIhvcNAQELBQAD
ggEBAAucCoXRfg4mnwfzBVah36NAQn2kCfdaU3sqet8nQXPXWStU28lP2tiF8pspz5Bb1Uw1bEO3MwGm6+o2YP
d6gnYpwYtWdmCYYFIZgQRU8nCzk4zw98I2O6JXs7kDMAocaIInIjs//4SnVHH3PSe29lw26ga2yAk6WmMSdPWz
e6zCspNskBjww8wvhhK9GknAPXWu0gCyHfG+ehEzfxXIx4ieJEodFNgmGuk97SWnMAkZdBlrZ1mVZWAMQI7Ata
Ou6JjvgDOGgmwyHMvEV83GdKOvKzR+vCb3X41L4Me/Fym7nxWZBEiRDqZEzidA6EQK2ceuiobFzhKx/xwJIoVk
nUI=</X509Certificate></X509Data></KeyInfo></ds:Signature></saml:Assertion></o:Securit
y></s:Header><s:Body><CheckAlive xmlns="http://service.fgsz.hu"
xmlns:b="http://schemas.datacontract.org/2004/07/WsClientTest.FgszService"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance"/></s:Body></s:Envelope>
```

Response minta

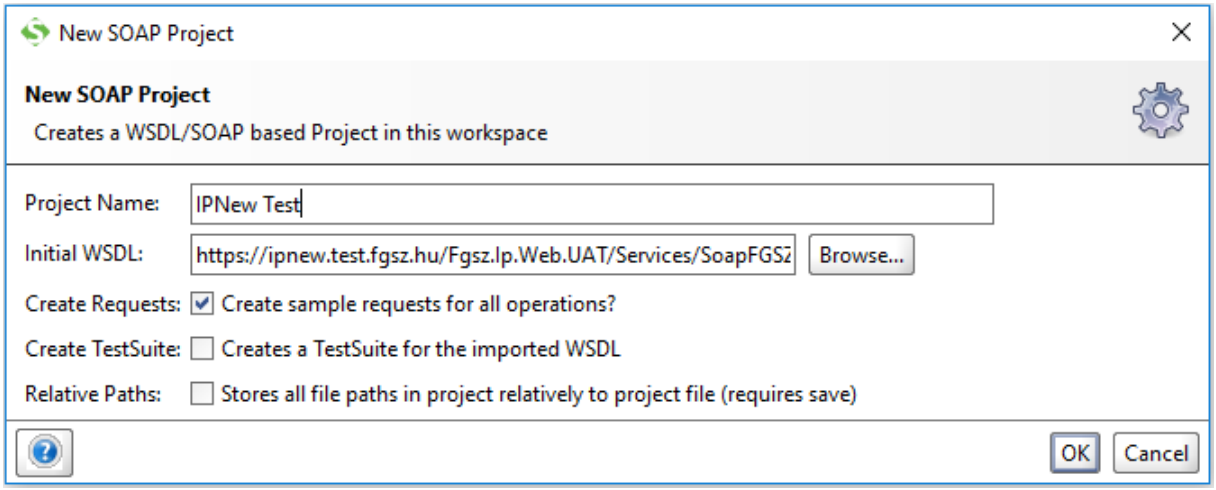
```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Fri, 09 Mar 2018 12:35:22 GMT
Content-Length: 1567

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
   <s:Header>
      <a:Action
s:mustUnderstand="1">http://domain.service.fgsz.hu/IFGSZNNOServiceSoapWrapper/CheckAli
veResponse</a:Action>
      <o:Security s:mustUnderstand="1" xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
         <u:Timestamp u:Id="_0">
            <u:Created>2018-09-02T09:11:03.596Z</u:Created>
            <u:Expires>2018-09-02T09:16:03.596Z</u:Expires>
         </u:Timestamp>
      </o:Security>
   </s:Header>
   <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <CheckAliveResponse xmlns="http://domain.service.fgsz.hu">
         <CheckAliveResult>The service is alive.</CheckAliveResult>
      </CheckAliveResponse>
   </s:Body>
</s:Envelope>
```

Tesztelés SoapUI eszközzel

A web szolgáltatásokat tesztelhetjük program készítése nélkül is, például az ingyenesen elérhető SoapUI eszközzel (https://www.soapui.org/), az alábbi módon.

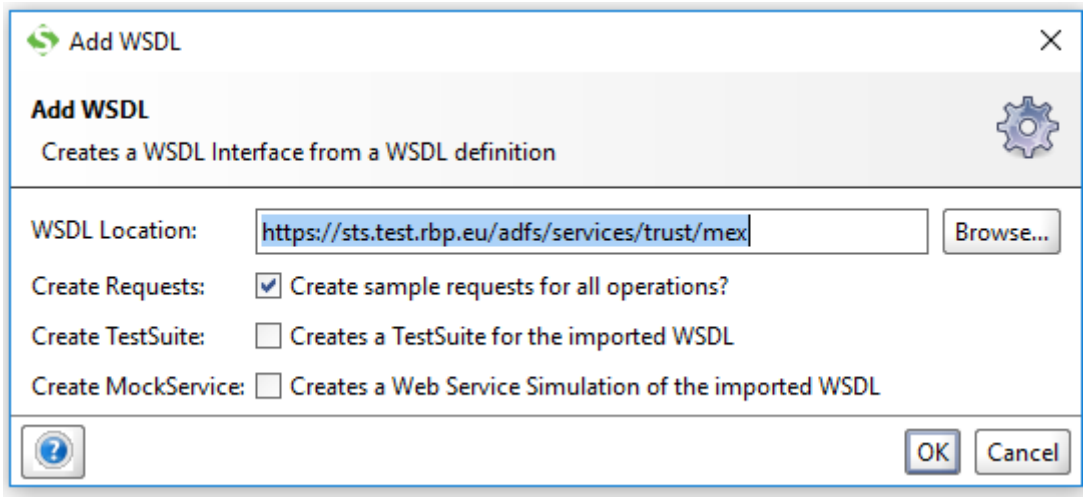
SoapUI Projekt létrehozása

Hozzunk létre egy új SOAP Projektet pl. IPNew Test néven (File menü -> New SOAP Project menüpont). Az Initial WSDL mezőbe írjuk be a használni kívánt IPNew web szolgáltatás WSDL címét (pl. https://ipnew.test.fgsz.hu/Fgsz.Ip.Web.UAT/Services/SoapFGSZNNOService.svc?singleWsdl)



Létrejön az új projekt, benne a WSDL-nek megfelelő interfésszel és azon belül minden web metódushoz egy minta kérés üzenettel. Ezeket fel fogjuk használni a tesztelés során.

Adjuk hozzá a projekthez az ADFS web szolgáltatások műveleteit is. Jobb klikk a projekt nevére, majd Add WSDL. A WSDL Location mezőben adjuk meg az ADFS WSDL címét, pl.: https://sts.test.rbp.eu/adfs/services/trust/mex. Létrejönnek az ADFS műveletekhez tartozó minta üzenetek is.

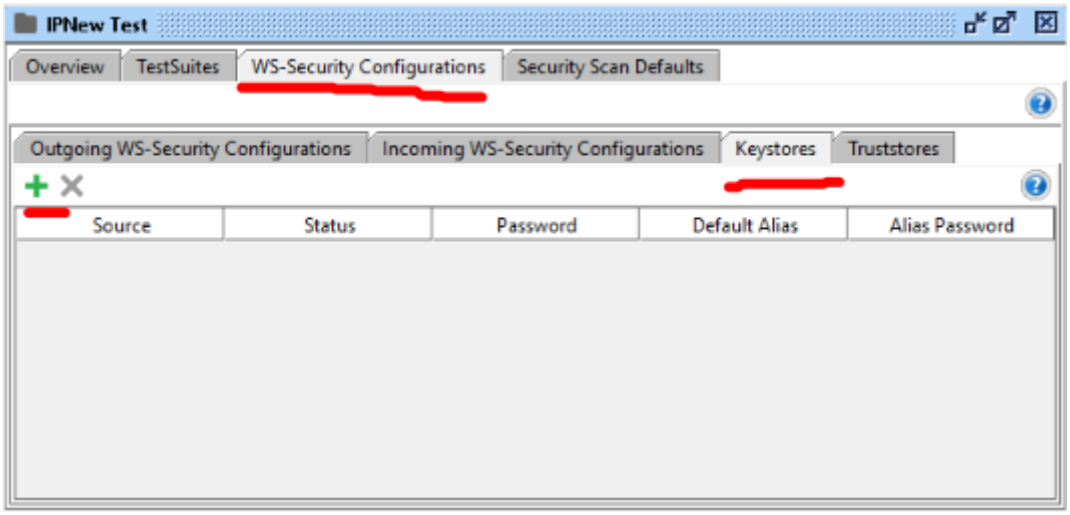


Projekt paraméterek beállítása

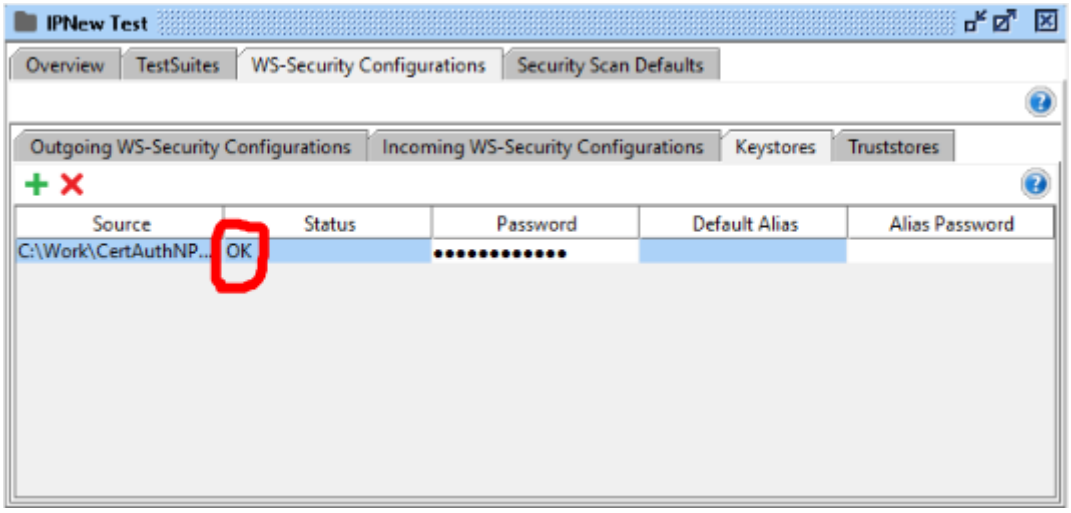
Tanúsítvány alapú azonosításhoz szükséges paraméterek beállítása

Tanúsítvány alapú azonosításhoz szükségünk van egy kliens tanúsítványra, amit előzetesen az FGSZ hozzárendelt egy AD felhasználóhoz. A web szolgáltatás meghívásához szükségünk lesz a tanúsítvány privát és publikus kulcsát tartalmazó fájlra (pl. testClient.pfx).

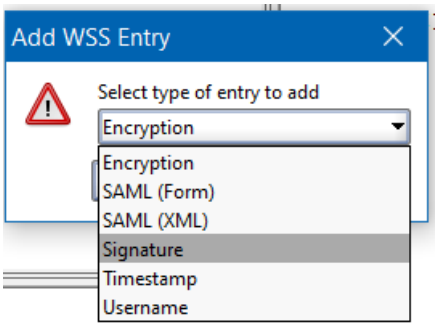
Kattintsunk duplán a SoapUI projekt nevére, a megjelenő ablakban kattintsunk a WS-Security Configuration fülre, azon belül a Keystores fülre.



Kattintsunk a zöld + ikonra, és a megjelenő fájlválasztó ablakban válasszuk ki a tanúsítvány fájlt. Ha a fájl jelszóval védett, adjuk meg a jelszót a következő ablakban, majd nyomjuk meg az OK gombot. Ellenőrizzük, hogy a Status mezőben OK felirat jelenik meg.



Váltsunk át az Outgoing WS-Security Configurations fülre és kattintsunk a zöld + ikonra. A megjelenő ablakban adjunk tetszőleges nevet a konfigurációnak, pl. clientCert. Az ablak alsó szekciójában kattintsunk a zöld + ikonra (Add a new WSS Entry). A lenyíló listából válasszuk a Signature opciót.



A Signature ablak paramétereit töltsük ki az alábbi módon:

Keystore: az a keystore, amit korábban hozzáadtunk (tanúsítvány fájl).

Alias: a keystore-ban levő kulcs neve.

Password: a tanúsítvány fájlt védő jelszó.

Key Identifier Type: Binary Security Token

Signature Algorithm: http://www.w3.org/2000/09/xmldsig#rsa-sha1

Signature Canonicalization: http://www.w3.org/2001/10/xml-exc-c14n#

Digest Algorithm: http://www.w3.org/2000/09/xmldsig#sha1

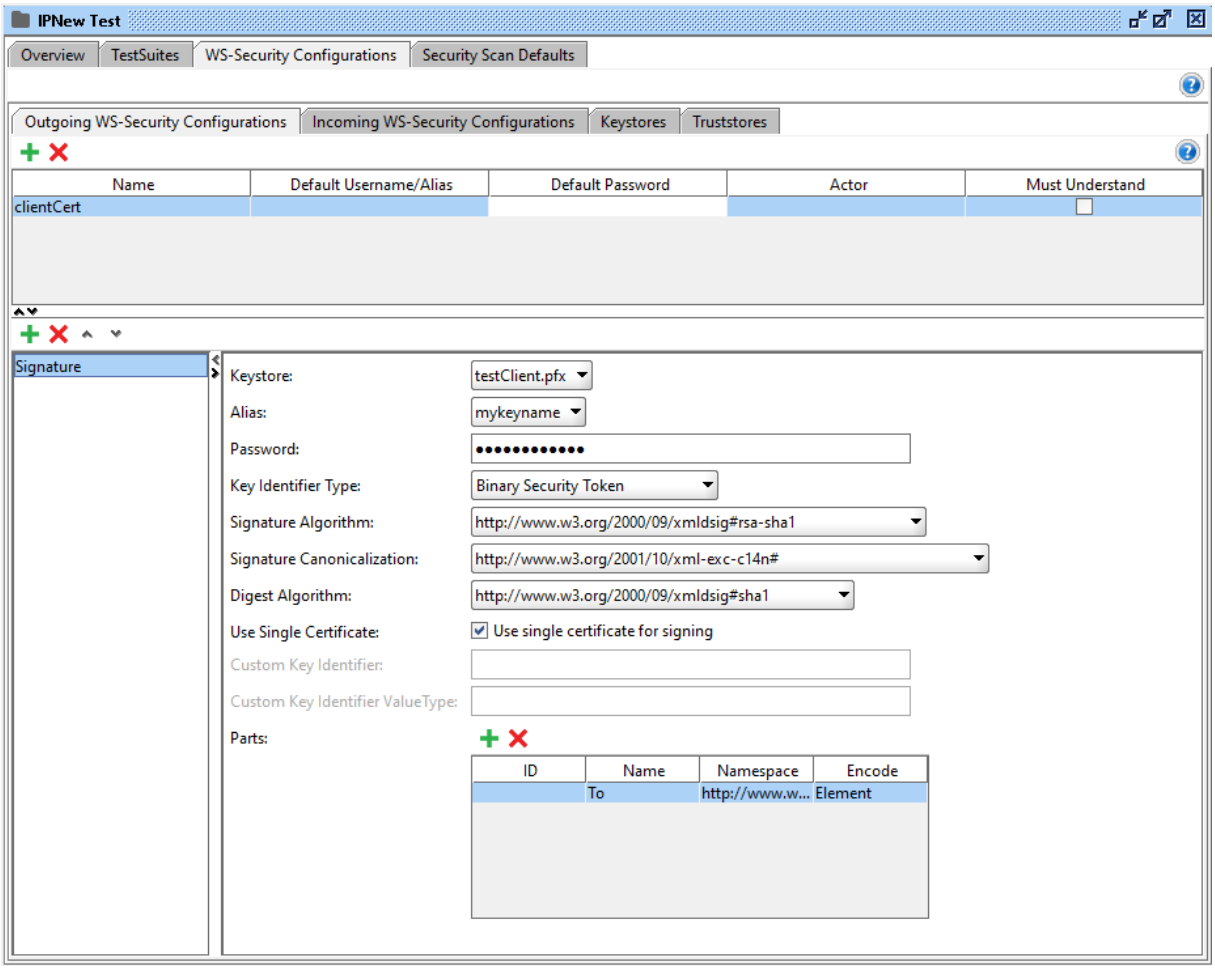
Jelöljuk be a Use Single Certificate négyzetet.

Az alsó Part szekcióban töltsünk ki egy sort a következő adatokkal:

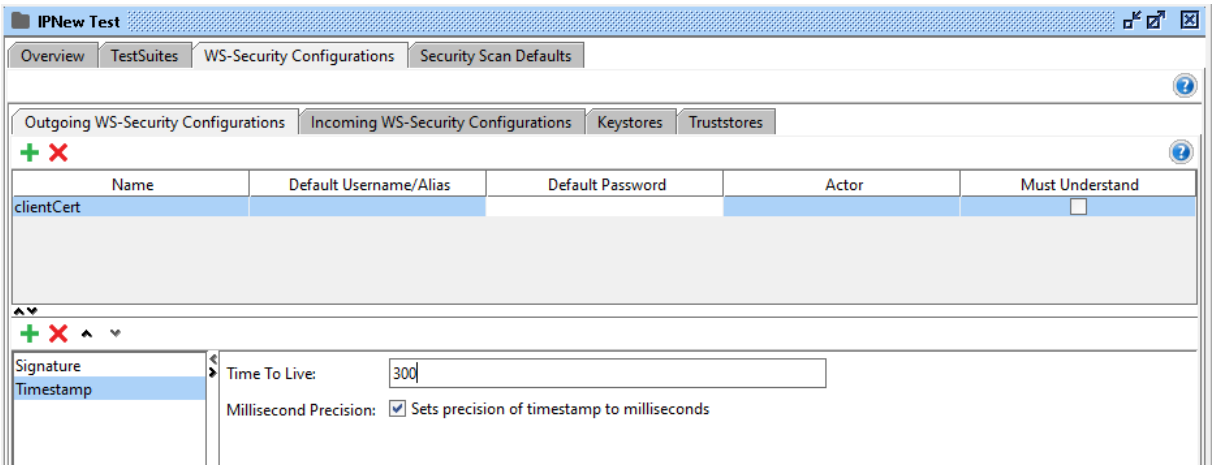
Name oszlop: To

Namespace oszlop: http://www.w3.org/2005/08/addressing

Encode oszlop: Element

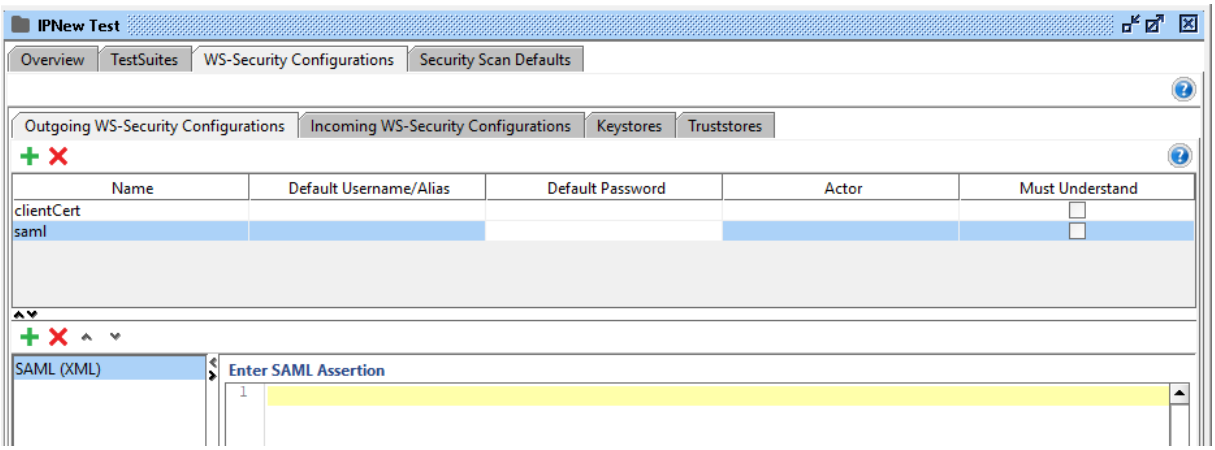


Hozzunk létre még egy sort a Signature entry alatt a zöld + ikonnal, válasszuk a Timestamp opciót. A Time to live mezőbe írjunk 300-at.



Hozzunk létre egy újabb konfiguráció sort a clientCert alatt a felső zöld + ikonra kattintva. A neve legyen saml.

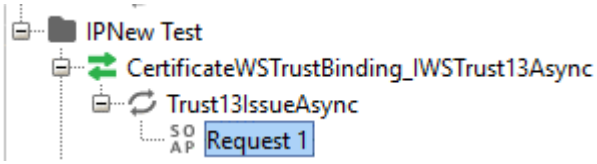
Az alsó szekcióban adjunk hozzá egy új Entry-t, a típusa legyen SAML (XML). Egyelőre ne adjunk neki értéket.



Request-ek beállítása

Token kérés request összeállítása tanúsítvány alapú azonosításhoz

A bal oldali Navigator fában az ADFS műveletek között nyissuk ki a CertificateWSTRustBinding_IWSTrust13Async ágat egészen a Request 1 szintig. Kattintsunk duplán a Request 1 elemre.



A bal oldali XML nézetben a zöld XML kommentek helyére illesszük be az alábbi XML részletet:

```
<ns:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</ns:RequestType>
<wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
 <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
```

<Address>https://ipnew.test.fgsz.hu/Fgsz.Ip.Web.UAT/Services/SoapFGSZNNOService.svc</Address>

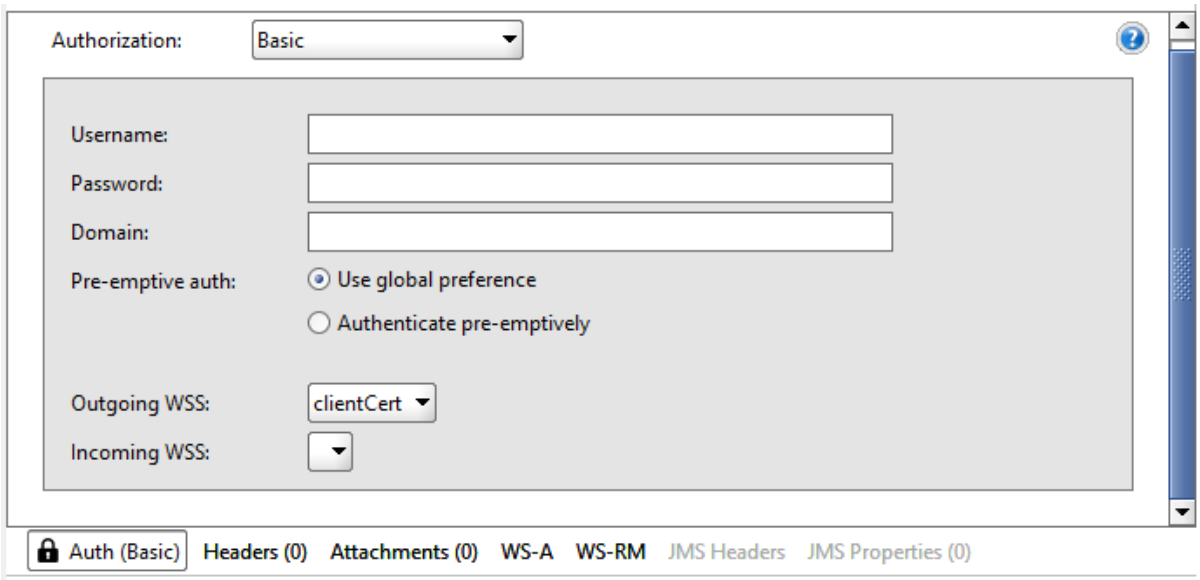
</EndpointReference>

</wsp:AppliesTo>

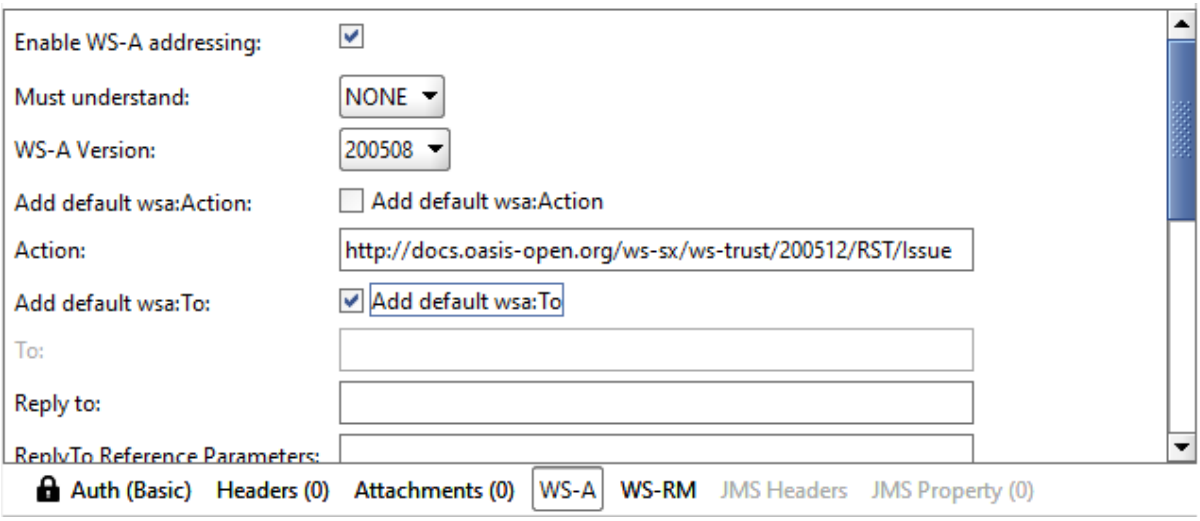
<ns:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</ns:KeyType>

Ügyeljünk arra, hogy az Address XML elemben a megfelelő IPNew web szolgáltatás címe szerepeljen (szükség szerint módosítsuk).

Kattintsunk az ablak alján az Auth feliratra, a megjelenő ablakban válasszuk ki az Add New Authorization elemet az Authorization mezőben, majd a felugró ablakban a Basic opciót. Az Outgoing WSS listából válasszuk a clientCert konfigurációt.



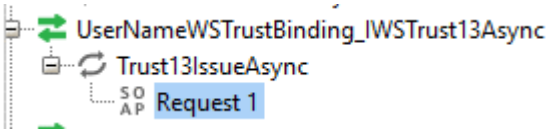
Kattintsunk a WS-A feliratra. Jelöljük be az Add default wsa:To opciót.



Kattintsunk a zöld Play gombra a web szolgáltatás hívás elvégzéséhez. A jobb oldali XML nézetben megjelenik a web szolgáltatás válasz a visszaadott SAML tokennel.

Token kérés request összeállítása felhasználónév/jelszó azonosításhoz

A bal oldali Navigator fában az ADFS műveletek között nyissuk ki a UserNameWSTrustBinding_IWSTrust13Async ágat egészen a Request 1 szintig. Kattintsunk duplán a Request 1 elemre.



A baloldali XML nézetben a <soap:Header/> elemet cserélük le az alábbi XML részletre:

```
<soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <wsse:Security soap:mustUnderstand="1" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
    <wsse:UsernameToken wsu:Id="UsernameToken-348E3F3C81E7E21F39152094195633514">
      <wsse:Username>testusername@ipnewtest.local</wsse:Username>
      <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">password</wsse:Password>
    </wsse:UsernameToken>
  </wsse:Security>
<wsa:To>https://sts.test.rbp.eu/adfs/services/trust/13/usernamemixed</wsa:To>
</soap:Header>
```

A bal oldali XML nézetben a zöld XML kommentek helyére illesszük be az alábbi XML részletet:

```
<ns:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</ns:RequestType>
<wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
 <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
<Address>https://ipnew.test.fgsz.hu/Fgsz.Ip.Web.UAT/Services/SoapFGSZNNOService.svc</Address>
 </EndpointReference>
</wsp:AppliesTo>
<ns:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer</ns:KeyType>
```

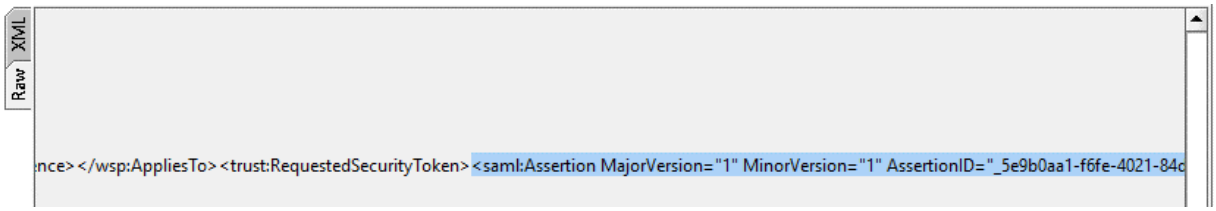
Ügyeljünk arra, hogy az Address XML elemben a megfelelő IPNew web szolgáltatás címe szerepeljen (szükség szerint módosítsuk).

Kattintsunk a zöld Play gombra a web szolgáltatás hívás elvégzéséhez. A jobb oldali XML nézetben megjelenik a web szolgáltatás válasz a visszaadott SAML tokennel.

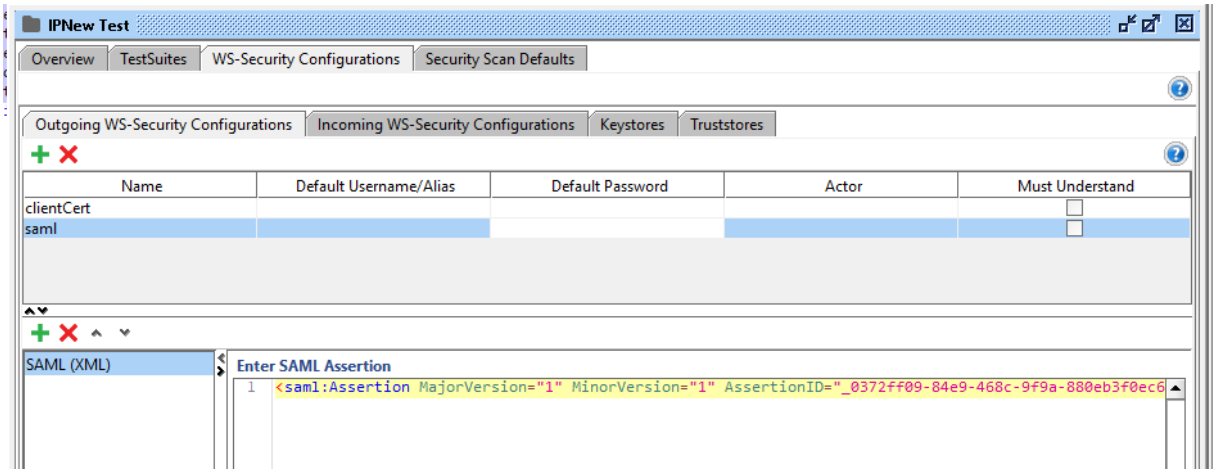
IPNew web szolgáltatás hívás request összeállítása

1. Az XML nézetről váltsunk át a Raw nézetre:

2. Másoljuk ki a formázatlan XML-ből a <saml:Assertion> kezdetű részletet egészen a záró </saml:Assertion> részig. Fokozottan ügyeljünk arra, hogy ne kerüljön bele szóköz vagy új sor, ne módosuljon egyetlen karakter sem, ne rontsuk el a formázást, mert az érvényteleníti a digitális aláírást.



3. A kimásolt részt illesszük be a korábban létrehozott saml konfigurációs elem mezőjébe (Enter SAML Assertion):



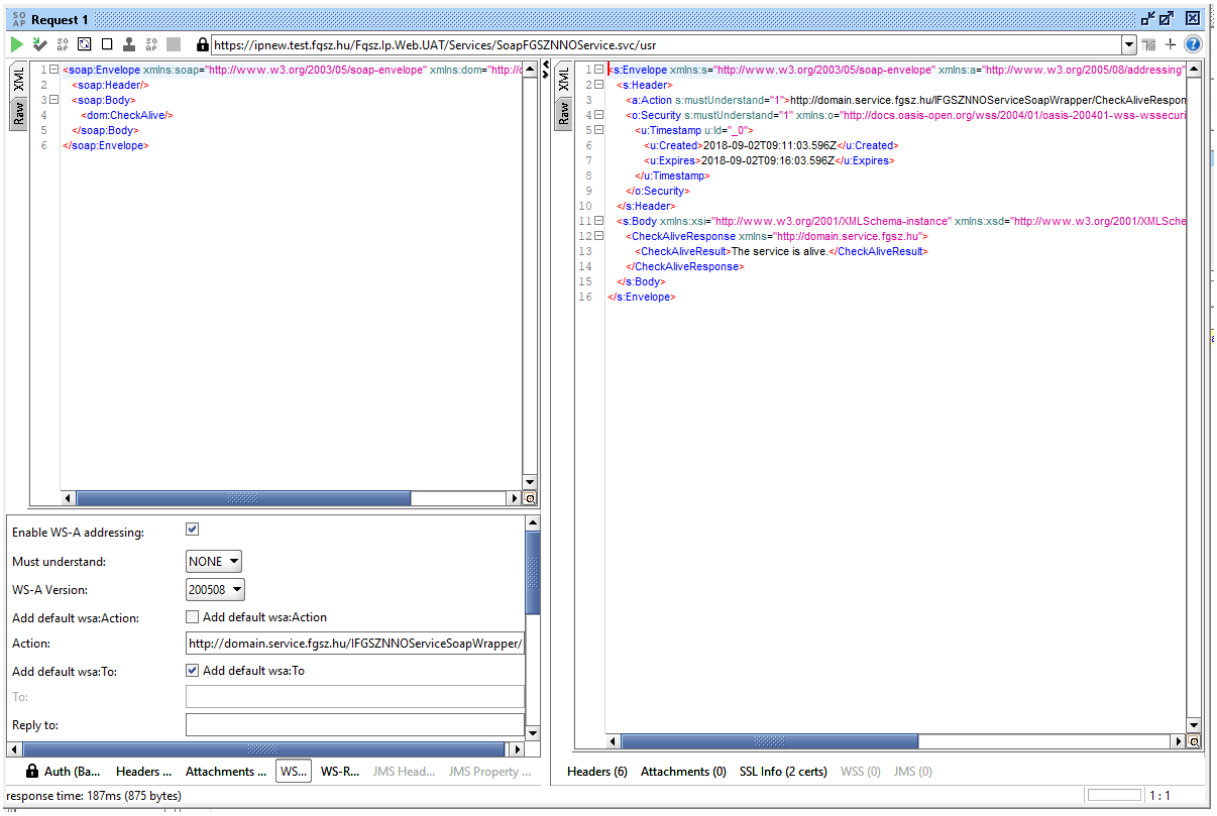
4. A bal oldali Navigator fában az IPNew web szolgáltatás műveletek között nyissuk ki a kívánt művelet ágat egészen a Request 1 szintig. Kattintsunk duplán a Request 1 elemre.

5. Kattintsunk az ablak alján az Auth feliratra, a megjelenő ablakban válasszuk ki az Add New Authorization elemet az Authorization mezőben, majd a felugró ablakban a Basic opciót. Az Outgoing WSS listából válasszuk a saml konfigurációt.

6. Kattintsunk a WS-A feliratra. Jelöljük be az Add default wsa:To opciót.

7. Ha szükséges, módosítsuk a SoapUI által létrehozott minta XML-t.

8. Kattintsunk a zöld Play gombra a web szolgáltatás hívás elvégzéséhez. A jobb oldali XML nézetben megjelenik a web szolgáltatás válasz.



Ismert hibajelenségek, hibaüzenetek

- **„At least one security token in the message could not be validated.”** hibaüzenet: valószínűleg annyi idő telt el az ADFS web szolgáltatás hívása óta, hogy időközben lejárt a token érvényessége. Ilyenkor újra meg kell hívni az ADFS web szolgáltatást, és az új <saml:Assertion> elemmel frissíteni kell a saml konfigurációt.
- **„An error occurred when verifying security for the message.”** hibaüzenet lehetséges okai:
    - Ha a <saml:Assertion> részt nem a Raw nézetből másoljuk ki, vagy bármilyen karakter megváltozik ebben az XML részletben, akkor sérül az üzenet integritása, az üzenet és az aláírás már nem feleltethető meg egymásnak. Ilyenkor a teendő az *IPNew web szolgáltatás hívás request összeállítása* részben leírtak megismétlése, különös figyelmet fordítva az első három lépésre.
    - Ha az azonosításhoz használt tanúsítványban előfordulnak ékezetes karakterek (pl. a tanúsítvány tulajdonosának nevében), akkor előfordulhat, hogy a SOAP UI által megjelenített token válaszban a saml:Assertion részben az ékezetes karakterek helyett nem megfelelő kódolással jelennek meg „olvashatatlan” karakterek, és ha az XML részletet változtatás nélkül felhasználjuk a következő web service hívásokban, akkor is „An error occurred when verifying security for the message.” hibaüzenetet kapunk. Ilyen esetben javítani kell az XML-ben az elrontott ékezetes karaktereket és a módosított XML részletet kell használni a továbbiakban.

Hivatkozások

- WS-Trust 1.3 – OASIS: http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html
- SOAP 1.1: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
- SoapUI: https://www.soapui.org/