1 Technikai segédlet – authentikáció

1.1 Web Service proxy

Az OTH próbaüzem rendszerén (teszt rendszeren) az alábbi webservice-ek érhetőek el proxy url-en keresztül HTTPS-en:

Fertőzőbeteg bejelentés, kijelentés Web Service:
https://testauth.antsz.hu:8443/AntszAuth/proxy?url=http://192.168.1.27:8086/oszir-jarvany/webservice/FertozoJelentesService?wsdl

Laboratóriumi leleteket kezelő webservice (ez tartalmazza mindhárom leleteket kezelő webservice-t, amelyet a dokumentum feljebb taglal):
https://testauth.antsz.hu:8443/AntszAuth/proxy?url=http://192.168.1.27:8086/oszir-jarvany/webservice/LeletService?wsdl

Újszülöttek kórházi jelentése, orvosi rendszerek oltási jelentése, oltási értesítő, védőoltás tartós kontraindikáció Web Service:
https://testauth.antsz.hu:8443/AntszAuth/proxy?url=http://192.168.1.27:8086/oszir-jarvany/webservice/OltasJelentesService?wsdl

Oltóanyag készlet kezelő Web Service:
https://testauth.antsz.hu:8443/AntszAuth/proxy?url=http://192.168.1.27:8086/oszir-jarvany/webservice/DistributorService?wsdl

Anonimizálás webservice (ez az interfész csupán azért van megadva, mert a fejezet végén található mellékelt fájl mintaként ezt a webservice-t tartalmazza):
https://testauth.antsz.hu:8443/AntszAuth/proxy?url=http://192.168.1.27:8086/oszir-kt/AnonimizalasWebService?wsdl

1.2 Kliens paraméterezése általánosan

A webservice-ek hívásához a kliensnek szüksége van a szerver tanúsítványára (továbbiakban SERVER_CERT) és egy kliens tanúsítványra (továbbiakban CLIENT_CERT).
A szerver tanúsítványát el kell helyezni a kliens alkalmazás megbízható tanúsítványai közé. A kliens tanúsítványt a webservice hívásakor kell megadni paraméterként. A tanúsítványokat az OTH Informatika fogja adni, a kliens tanúsítványhoz tartozó jelszóval együtt (CLIENT_PASSWORD). A **testauth.antsz.hu** domain nem létezik se külső se belső hálózaton, de a szerver tanúsítvány erre van kiállítva, ezért a hosts fájlban be kell állítani a hívó oldalon:

84.206.43.29 testauth.antsz.hu

A hosts fájl helye operációs rendszerenként eltér, részletes leírás a http://en.wikipedia.org/wiki/Hosts_%28file%29-n található.

1.3 Java kliens paraméterezése

Ha a kliens egy Java alkalmazás, akkor a szerver tanúsítványát el kell helyezni az alkalmazás TrustStore-jában (továbbiakban TRUST_STORE). Ha már létezik a TrustStore, akkor ezt meg lehet tenni a JDK-ban található keytool program segítségével, például az alábbi utasítással:

keytool -import -file <PATH_TO>/<SERVER_CERT> -alias antsz_ca -keystore <PATH_TO>/<TRUST_STORE>

A következő utasítással ellenőrizhetjük a TrustStore tartalmát:

keytool -list -v -keystore <PATH_TO>/<TRUST_STORE>

Ha a TrustStore még nem létezik, akkor az alábbi paranccsal létre lehet hozni:

keytool -genkey -alias foo -keystore <PATH_TO>/<TRUST_STORE>

Java kliens alkalmazás számára VM argumentumként lehet megadni, hogy a HTTPS kapcsolatokhoz az adott TrustStore-t és a kliens tanúsítványt használja. Az átadandó argumentumokra minta az alábbi:

-Djavax.net.ssl.keyStore=<PATH_TO>/<CLIENT_CERT>
-Djavax.net.ssl.keyStorePassword=<CLIENT_PASSWORD>
-Djavax.net.ssl.keyStoreType=pkcs12
-Djavax.net.ssl.trustStore=<PATH_TO>/<TRUST_STORE>
-Djavax.net.ssl.trustStorePassword=<KEYSTORE_PASSWORD>

A mellékelt anonim-client.zip-ben van egy Java kliens program az anonimizálás webservice-hez, forráskóddal együtt. Kicsomagolás után a kliens az alábbi paranccsal futtatható:

java -Djavax.net.ssl.keyStore=<PATH_TO>/<CLIENT_CERT>
-Djavax.net.ssl.keyStorePassword=<CLIENT_PASSWORD>
-Djavax.net.ssl.keyStoreType=pkcs12
-Djavax.net.ssl.trustStore=<PATH_TO>/<TRUST_STORE>
-Djavax.net.ssl.trustStorePassword=<KEYSTORE_PASSWORD>
-jar <PATH_TO>/anonim-client.jar

Sikeres futás esetén a program kimenete:

anonimKod=mnFJpad4a7No4G0Ixdd3dOtDpJ4=