EduID_Cloud365

Auto-generated book for EduID_Cloud365

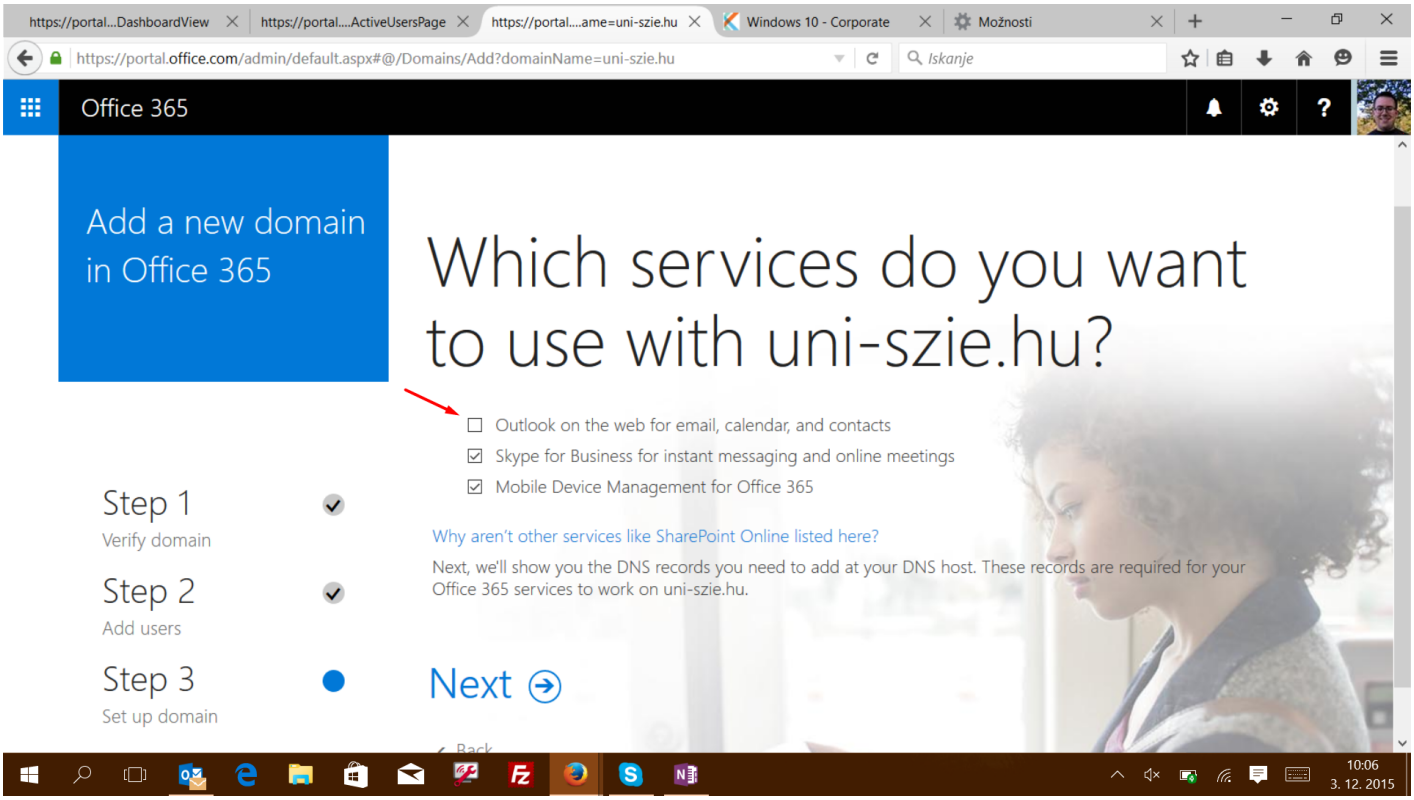
EduID_Cloud365

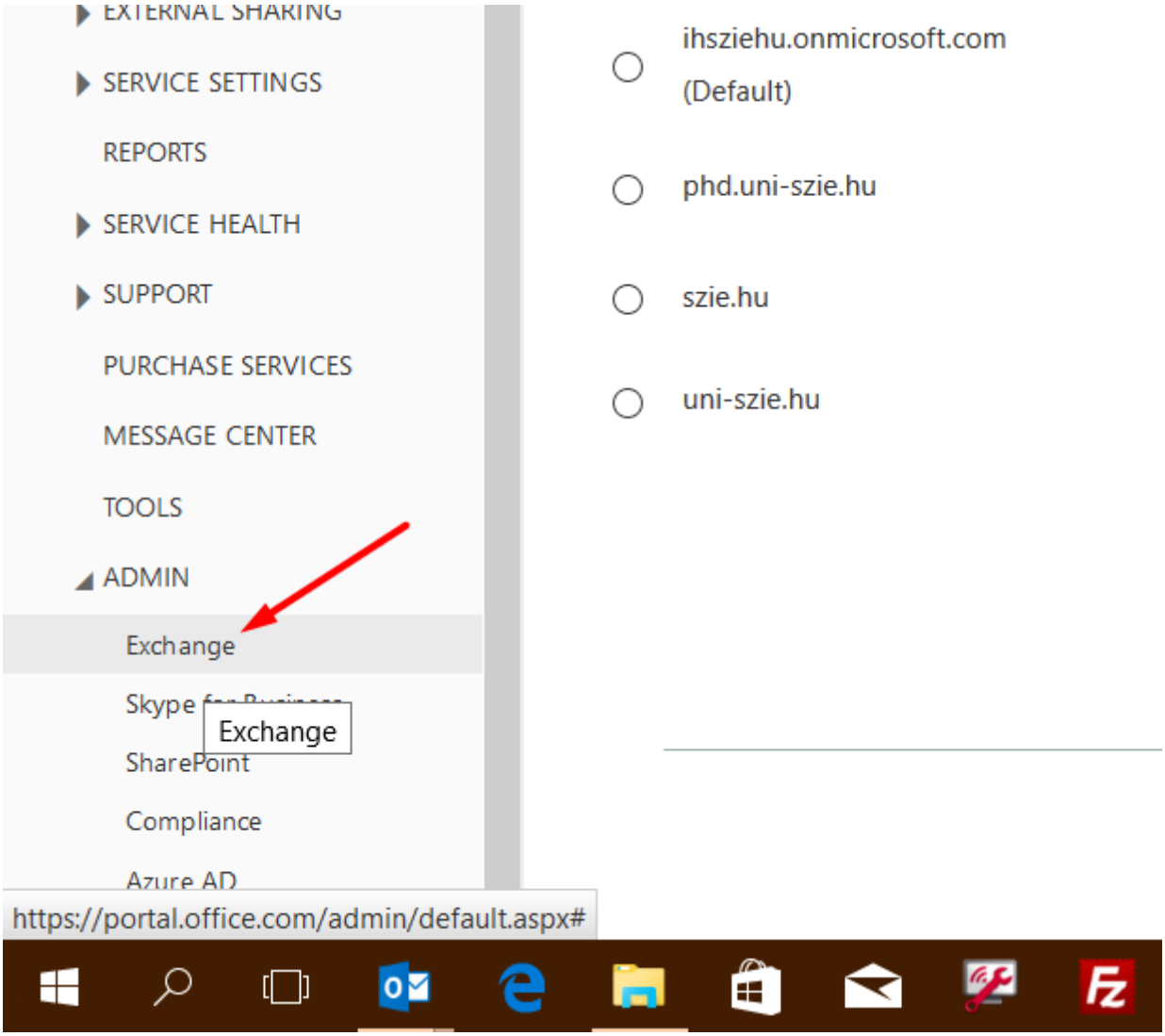
EduID Cloud365

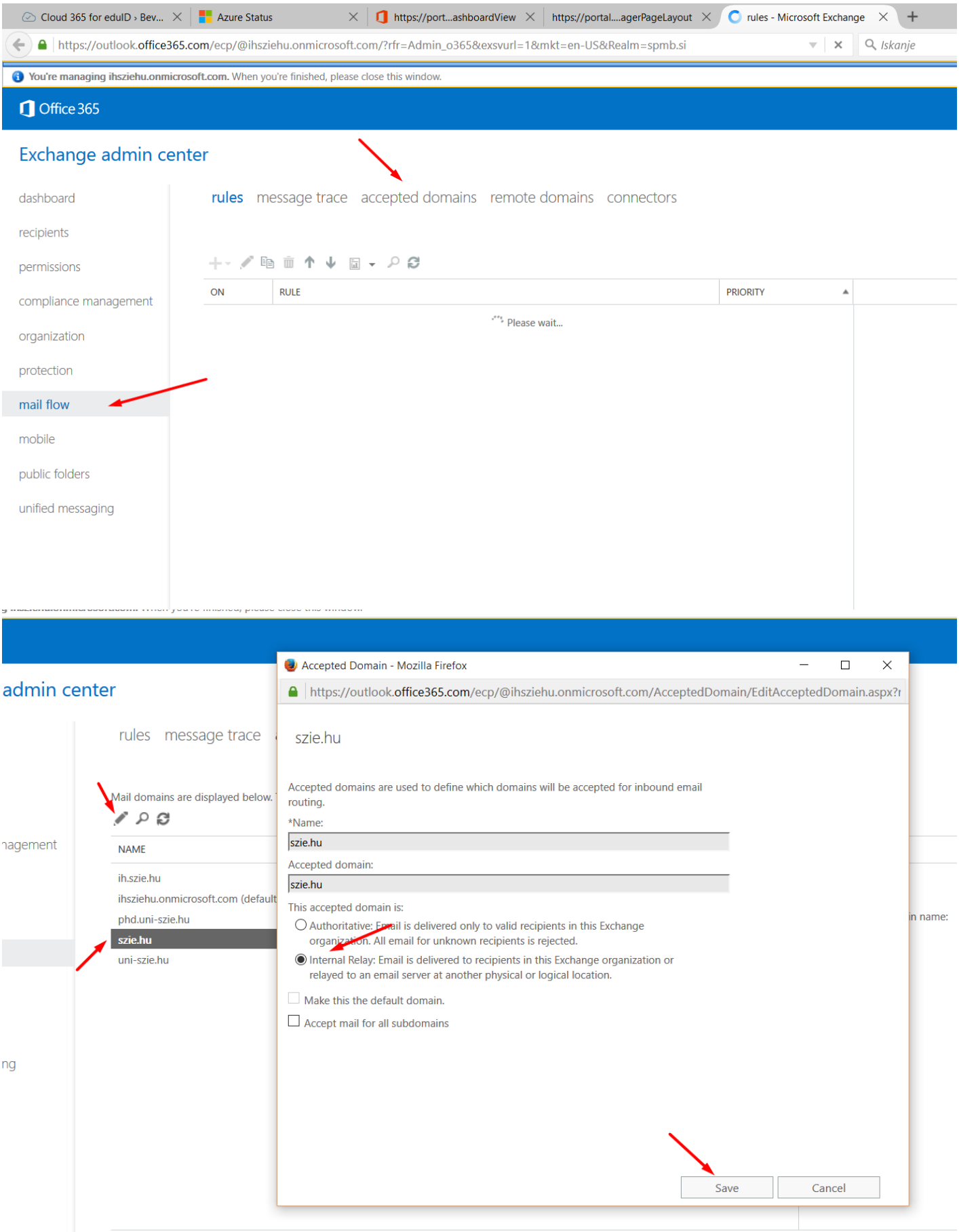
Szükséges lépések a O365.eduid.hu szolgáltatás igénybevételéhez:

1. Intézményi Office365 (intezmenynev.onmicrosoft.com) account igénylése, licenc jogosultságok ellenőrzése
2. "Modern authentication public preview" (valójában: Azure AD Authentication Library) bekapcsolása az Office365 management felületén
3. Domainek beállítása
4. SAML IdP konfiguráció
5. Jelzés küldése az aai (AT) niif . hu címre, hogy bekapcsolható a SAML átjáró
6. Adminisztrátori belépés a O365.eduid.hu portálra
   - A portálon az Office365 kapcsolat beállítása
   - Licenc jogosultságok beállítása (milyen termékek érhetők el tanárok, ill. diákok számára)

Office365MailFlow




EXTERNAL SHARING
SERVICE SETTINGS
REPORTS
SERVICE HEALTH
SUPPORT
PURCHASE SERVICES
MESSAGE CENTER
TOOLS
ADMIN
Exchange
Skype for Business
SharePoint
Compliance
Azure AD
Exchange
https://portal.office.com/admin/default.aspx#
ihsziehu.onmicrosoft.com
(Default)
phd.uni-szie.hu
szie.hu
uni-szie.hu


Cloud 365 for eduID › Bev...
Azure Status
https://port...ashboardView
https://portal....agerPageLayout
rules - Microsoft Exchange
https://outlook.office365.com/ecp/@ihszieh u.onmicrosoft.com/?rfr=Admin_o365&exsvurl=1&mkt=en-US&Realm=spmb.si
Iskanje
You're managing ihszieh u.onmicrosoft.com. When you're finished, please close this window.
Office 365
Exchange admin center
dashboard
recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
unified messaging
rules
message trace
accepted domains
remote domains
connectors
ON
RULE
PRIORITY
Please wait...
admin center
rules
message trace
Mail domains are displayed below.
NAME
ih.szie.hu
ihszieh u.onmicrosoft.com (default
phd.uni-szie.hu
szie.hu
uni-szie.hu
Accepted Domain - Mozilla Firefox
https://outlook.office365.com/ecp/@ihszieh u.onmicrosoft.com/AcceptedDomain/EditAcceptedDomain.aspx?r
szie.hu
Accepted domains are used to define which domains will be accepted for inbound email routing.
*Name:
szie.hu
Accepted domain:
szie.hu
This accepted domain is:
Authoritative: Email is delivered only to valid recipients in this Exchange organization. All email for unknown recipients is rejected.
Internal Relay: Email is delivered to recipients in this Exchange organization or relayed to an email server at another physical or logical location.
Make this the default domain.
Accept mail for all subdomains
Save
Cancel

O365_SAML

Az Office365 szolgáltatások SAML azonosítással történő használatához egy új SP-t kell konfigurálni az IdP konfigurációjában, mivel ez az SP nem szerepel a föderációs metaadatok között. A Microsoft által üzemeltetett SP-nek speciális attribútum igényei vannak:

- perzisztens NameID-t kell küldeni (**ImmutableID**)
- kell küldeni egy **IDPEmail** nevű attribútumot

Kiadott attribútumok

ImmutableID

Az ImmutableID az eduPersonPrincipalName attribútum MD5 hashének UUID formátumra konvertált változata.

IDPEmail

A kiadott e-mail értéknek meg kell egyeznie az Office365 által szolgáltatott e-mail címmel. Ez azt is jelenti, hogy az IdP-től kapott e-mail attribútum domain részét előzetesen validálni kell az Office365-ben.

SimpleSAMLphp

A `metadata/saml20-sp-remote.php` file-ba kell elhelyezni a következő bejegyzést:

```
/*
 * Office 365
 * https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml
 */
$metadata['urn:federation:MicrosoftOnline'] = array(
  'entityid' => 'urn:federation:MicrosoftOnline',
```

```
// Expose both required attributes
'attributes' => array('IDPEmail', 'ImmutableID'),
'attributes.NameFormat' => "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified",

// Configure attribute mapping and ImmutableID generation
'authproc' => array(
  31 => array(
    'class' => 'core:PHP',
    'code' => '
      $eppn = $attributes["eduPersonPrincipalName"][0];
      $chunks = str_split(md5($eppn), 4);
      $attributes["ImmutableID"][0] = vsprintf("%s%s-%s-%s-%s-%s%s%s", $chunks);
    ',
  ),
      36 => array(
    'class' => 'core:AttributeMap',
    'mail' => 'IDPEmail',
  ),
),

// Send ImmutableID as a "persistent" NameID
'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent',
'simplesaml.nameidattribute' => 'ImmutableID',

'contacts' => array(),
'metadata-set' => 'saml20-sp-remote',

'AssertionConsumerService' => array(
  0 => array(
    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
    'Location' => 'https://login.microsoftonline.com/login.srf',
    'index' => 0,
    'isDefault' => true,
  ),
  1 => array(
    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign',
    'Location' => 'https://login.microsoftonline.com/login.srf',
    'index' => 1,
```

```
  ),
  2 => array(
    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:PAOS',
    'Location' => 'https://login.microsoftonline.com/login.srf',
    'index' => 2,
  ),
),
'SingleLogoutService' => array(
  0 =>
  array(
  'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
  'Location' => 'https://login.microsoftonline.com/login.srf',
  ),
),

'keys' => array(
  0 => array(
    'encryption' => false,
    'signing' => true,
    'type' => 'X509Certificate',
    'X509Certificate' => 'MIIDYDCCAkigAwIBAgIJALLJPAyvf2sjMA0GCSqGSIb3DQEBBQUAMCkxJzAlBgNV
      BAMTHkxpdmUgSUQgU1RTIFNpZ25pbmcgUHVibGljIEtleTAeFw0xNDA3MTgxOTUz
      NDBaFw0xOTA3MTcxOTUzNDBaMCkxJzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25p
      bmcgUHVibGljIEtleTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANYD
      KgByFZdqtTnnpF4lfIp4i2XLg2rLIo+mu4DmW9gRLlBJCNc7YESUxpKzuFYaANd8
      fWsDigJZTXbhOQApSpw4xXFnor2vJ1zm94LtqjcVEXTjUml5gAIS4pwuOU3ZfO/0
      eTG0gDYp4a0L/mzzTRsnwe/8WMPIE75Bq2zAyAZ9aePvl3QX7cXYLPfeK4QTgK3B
      5lwe1wWu3y5oQidjcSok8Frf80xzuCYuOa+ZUK3JibpLLCrT4uwiqf+KREDSdc4b
      PPlq0PWI4sQr1tha8yypRSvOH+/MxcfSRSnl6Uc+gm8nVEEWWIu4hhu6NIfG91mM
      UqJuzkgLCi6Gov6JS8UCAwEAAaOBijCBhzAdBgNVHQ4EFgQUnQoq7sI3R8rde4sQ
      s6nGEbJm3LcwWQYDVR0jBFIwUIAUnQoq7sI3R8rde4sQs6nGEbJm3LehLaQrMCkx
      JzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25pbmcgUHVibGljIEtleYIJALLJPAyv
      f2sjMAsGA1UdDwQEAwIBxjANBgkqhkiG9w0BAQUFAAOCAQEAf4jaNhKzRG3k+52W
      oM9nnISP7rlWIeWwH6EQGUlF6ozSP/03gYMAdqpdhww5zNwKzi7TQVbDC0pgq/tq
      zHv6JEI0R4B6h7/TJ1pYPxdvIFQrE27RHESltH/m+5UkVnayLqRD3/fi4zf4aEpx
      SDZ73MCR5LanPGqvlAMz29AL3g1ynj+eu7xMfFsM/8+qJaCXuxT5/30eeLEe+PYi
      kA/PhEwp+qkDQWPvdAwEghuUaFvtKAgDZierjpGzHZnYkXTTDTHVe1iP7tsAJH5q
      K3qdcv3UGPyZrjC/lietJcAcnwVoZQ93v2ieGfcKKN+PFN9M59/BkPo62HPoGNNx
      2ZDQaQ==',
```

```
    ),
    1 => array(
      'encryption' => false,
      'signing' => true,
      'type' => 'X509Certificate',
      'X509Certificate' => 'MIIDYDCCAkigAwIBAgIJAKLDsqkylLefMA0GCSqGSIb3DQEBBQUAMCkxJzAlBgNV
        BAMTHkxpdmUgSUQgU1RTIFNpZ25pbmcgUHVibGljIEtleTAeFw0xNDEwMTAxODE2
        MTNaFw0xOTEwMDkxODE2MTNaMCkxJzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25p
        bmcgUHVibGljIEtleTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM7A
        3m6uvOxEsX+NlB1hnflaR8DJj597wY3qyh/FX4O6rKvU2leAfINmBWcjEFApCKi9
        p5uIaZpNlDpPQ+R3BaZx+4NhHbOMpeWlpIiZHL61lwbulzurffUPhtzQNHAVzOBk
        ZsOgN9BD/hOleU//d+IXz08ateUb3Ip2vyaodilYQDDi5M9yOhanv1cO1Usjo2xT
        LfiK+TVygu+8bo+/8JHGPRy6pnghng970DRBDkVrKzozlrnmMesdSrtuCnsgyRbE
        XckxaQ8S2nDYyFqBI0PkcBW8+0akdFWW58Os5cGbPFeHi6vtZCR5pWw5pnqtuoip
        rdk9jg1axT3vwu+RVdcCAwEAAaOBijCBhzAdBgNVHQ4EFgQUBjNylGJBvkAY/4yI
        IoD00R6p5hIwWQYDVR0jBFIwUIAUBjNylGJBvkAY/4yIIoD00R6p5hKhLaQrMCkx
        JzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25pbmcgUHVibGljIEtleYIJAKLDsqky
        lLefMAsGA1UdDwQEAwIBxjANBgkqhkiG9w0BAQUFAAOCAQEAQGZUlJ3zzJvy1OLd
        tV3NTYHlbVHm3Fty17xqW9Ui8GE8sEWeUdHA6eURNNpNpd+gAGC6Tp+k+cU1LlPw
        Xm7BAATJ/2DjY8tzRc6r6EneQWRkla8xpbvknXvUml6iFgo2ofOWLaFk6XpQ64MA
        O35wv9XEARNabJ9wJSRSevUigAx2U2GvaorV5PgqHImiKTSrL0K6j8B4OqXWUqP0
        KGf7pCdGlrq2XEl95N2zj8n/scvA9JasImztsVlZ+WxeF+OAMvWQQFc54gC6lwWc
        8kno8vPn3lwxVkTU0o9wcHnOhNi2hzVDV85sz7P9dOZYF73uy1uLshdjCcwlmQ2l
        A9OV9w==',
    ),
  ),
  'saml20.sign.assertion' => true,
  // This metadata does not contain an encryption key,
  // therefore explicitly disabling assertion encryption so it does not depend on global IDP settings.
  'assertion.encryption' => false,
);
```

ECP (Enhanced Client or Proxy) {#ecp_enhanced_client_or_proxy}

Ha szeretnénk elérni az Office365 levelezést IMAP-on keresztül, akkor be kell kapcsolni még az ECP-t is. Ehhez a `metadata/saml20-idp-hosted.php` file-ba fel kell venni az IdP metaadatai közé egy `'saml20.ecp'` elemet `true` értékkel, illetve az SP metaadatokhoz is hozzá kell adni két beállítást a `metadata/saml20-sp-remote.php` file-ban:

```
/*
 * Office 365
 * https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml
 */
$metadata['urn:federation:MicrosoftOnline'] = array(
  // ...
  'signature.algorithm'  => 'http://www.w3.org/2000/09/xmldsig#rsa-sha1',
  'saml20.sign.response' => false,
);
```

Shibboleth

Egy unicon/shibboleth-idp alapú docker image készítését mutatjuk be az alábbiakban.

Kezdeti IdP konfiguráció {#kezdeti_idp_konfiguráció}

```
# docker run -it -v $(pwd):/ext-mount --rm unicon/shibboleth-idp init-idp.sh

Please complete the following for your IdP environment:
Hostname: [64ed9b77b493.localdomain]
idp.example.com
SAML EntityID: [https://idp.example.com/idp/shibboleth]
https://idp.example.com:4443/idp/shibboleth
Attribute Scope: [localdomain]
example.com
Backchannel PKCS12 Password: XXXsecretXXX
Re-enter password: XXXsecretXXX
Cookie Encryption Key Password: XXXsecretXXX
Re-enter password: XXXsecretXXX
Warning: /opt/shibboleth-idp-tmp/bin does not exist.
Warning: /opt/shibboleth-idp-tmp/edit-webapp does not exist.
Warning: /opt/shibboleth-idp-tmp/dist does not exist.
Warning: /opt/shibboleth-idp-tmp/doc does not exist.
Warning: /opt/shibboleth-idp-tmp/system does not exist.
```

```
Generating Signing Key, CN = idp.example.com URI = https://idp.example.com:4443/idp/shibboleth ...
...done
Creating Encryption Key, CN = idp.example.com URI = https://idp.example.com:4443/idp/shibboleth ...
...done
Creating Backchannel keystore, CN = idp.example.com URI = https://idp.example.com:4443/idp/shibboleth ...
...done
Creating cookie encryption key files...
...done
Rebuilding /opt/shibboleth-idp-tmp/war/idp.war ...
...done

BUILD SUCCESSFUL
Total time: 7 minutes 4 seconds
A basic Shibboleth IdP config and UI has been copied to ./customized-shibboleth-idp/ (assuming the
default volume mapping was used).
Most files, if not being customized can be removed from what was exported/the local Docker image and
baseline files will be used.
```

Keletkezik egy `customized-shibboleth-idp` mappa a következő szerkezettel:

- conf
- credentials
- metadata
- views
- views/admin
- views/client-storage
- views/intercept
- webapp
- webapp/css
- webapp/images

Az alábbi fájlokat kell majd módosítani:

- conf/attribute-filter.xml
- conf/attribute-resolver.xml
- conf/idp.properties
- conf/ldap.properties
- conf/metadata-providers.xml
- conf/relying-party.xml
- conf/saml-nameid.properties
- conf/saml-nameid.xml
- metadata/idp-metadata.xml

Néhány másik fájlt pedig létre kell hozni:

- credentials/idp-browser.p12 (webserver SSL key/cert)
- credentials/ldap-server.crt (LDAP server certificate)
- metadata/federationmetadata.xml (Office 365 federation metadata)

Mivel ebben a példában az IdP-t a 4443-as porton fogjuk elérni, ezért ellenőrizni kell minden `Location` paramétert a `metadata/idp-metadata.xml` fájlban, hogy jó helyre mutat-e. Továbbá engedélyezni kell a `SingleLogoutService` bejegyzéseket (amelyek alapból ki vannak iktatva).

A webszerver tanúsítvány előkészítése {#a_webszerver_tanúsítvány_előkészítése}

A felhasználók által látogatott oldalakhoz célszerű valamilyen hitelesítés szolgáltató által aláírt tanúsítványt használni. Másoljuk be a webszerver tanúsítványt, a tanúsítvány láncot és a szerver kulcsot PEM formátumban egy mappába, majd egyesítsük őket egyetlen p12-es fáljba az openssl segítségével:

```
# cat webserver.crt intermediate_ca.crt > cert-chain.txt
# openssl pkcs12 -export -inkey webserver.key -in cert-chain.txt -out idp-browser.p12
Enter Export Password: XXX_secret_XXX
Verifying - Enter Export Password: XXX_secret_XXX
```

Az előállított `idp-browser.p12` fájlt másoljuk be a `credentials` mappába.

Microsoft SAML SP metadata és föderációs beállítások {#microsoft_saml_sp_metadata_és_föderációs_beállítások}

Töltsük le a Microsoft SAML2 SP metaadatait a `metadata` könyvtárba:

```
# wget https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml
```

Készítsünk egy MetadataProvider-t a `conf/metadata-providers.xml` fájlban:

```
<MetadataProvider id="MicrosoftOnline"
                  xsi:type="FilesystemMetadataProvider"
                  metadataFile="%{idp.home}/metadata/federationmetadata.xml"/>
```

A `conf/relying-party.xml` fájlban néhány speciális beállítást kell eszközölnünk, hogy a föderáció működjön (a shibboleth.RelyingPartyOverrides szekció alatt):

```
<util:list id="shibboleth.RelyingPartyOverrides">
  <bean parent="RelyingPartyByName" c:relyingPartyIds="urn:federation:MicrosoftOnline">
    <property name="profileConfigurations">
      <list>
        <bean parent="SAML2.SSO"
              p:encryptAssertions="false" />
        <bean parent="SAML2.ECP"
              p:encryptAssertions="false"
              p:signAssertions="true"
              p:signResponses="false"
              p:nameIDFormatPrecedence="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" />
      </list>
    </property>
  </bean>
</util:list>
```

Az Office 365 megköveteli a SAML2 `NameID` használatát, amiben ugyanazt az értéket várja, mint ami az `ImmutableID` attribútumban van. Ezt a `conf/saml-nameid.xml` fájlban kell beállítani:

```
<!-- SAML 2 NameID Generation -->
<util:list id="shibboleth.SAML2NameIDGenerators">

  <ref bean="shibboleth.SAML2TransientGenerator" />
  <ref bean="shibboleth.SAML2PersistentGenerator" />

<!-- Persistent ID Generator for all entities except Microsoft -->
<bean parent="shibboleth.SAML2PersistentGenerator">
  <property name="activationCondition">
    <bean parent="shibboleth.Conditions.NOT">
      <constructor-arg>
        <bean parent="shibboleth.Conditions.RelyingPartyId"
              c:candidates="#{{'urn:federation:MicrosoftOnline'}}" />
      </constructor-arg>
```

```
    </bean>
  </property>
</bean>

<!-- Persistent ID Generator for Microsoft -->
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
      p:format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
      p:attributeSourceIds="#{ {'ImmutableID'} }">
  <property name="activationCondition">
    <bean parent="shibboleth.Conditions.RelyingPartyId"
          c:candidates="#{{'urn:federation:MicrosoftOnline'}}" />
  </property>
</bean>

</util:list>
```

LDAP adatforrás beállítása {#ldap_adatforrás_beállítása}

Mentsük el az LDAP szerver tanúsítványát PEM formátumban a `credentials/ldap-server.crt` fájlba.

Az Office 365 két attriútum kiadását kéri: `IDPEmail` és `ImmutableID`.

Az `IDPEmail` értékének meg kell egyeznie a felhasználó Office 365-ös `UserPrincipalName` attribútumával (ami egyben a hivatalos (elsődleges) felhős email címe).

Az `ImmutableID` esetünkben az `eduPerosnPrincilapName` MD5 hash értékének UUID formátumra konvertált változata lesz, amelyet egy javasccript segítségével képezünk.

Cseréljük le a `conf/attribute-resolver.xml` fájlt a `conf/attribute-resolver-full.xml` nevűvel.

```
mv conf/attribute-resolver-full.xml conf/attribute-resolver.xml
```

Az `attribute-resolver.xml` fájlban beállítunk néhány attribútumot és az LDAP adatforrást. Az `ImmutableID` egy Shibboleth `ScriptedAttribute` lesz, ami egy javasccript segítségével fogja előállítani az attribútum értékét az `eduPersonPrincipalName` LDAP attribútumot felhasználva. Az MD5 hash kiszámítása külső segítség nélkül történik, ezért a script kissé hosszú.

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<AttributeResolver
        xmlns="urn:mace:shibboleth:2.0:resolver"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:mace:shibboleth:2.0:resolver http://shibboleth.net/schema/idp/shibboleth-attribute-resolver.xsd">

    <!-- ========================================== -->
    <!--    Attribute Definitions                   -->
    <!-- ========================================== -->

    <AttributeDefinition xsi:type="Simple" id="uid">
        <InputDataConnector ref="myLDAP" attributeNames="uid"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:uid" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.1" friendlyName="uid" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="mail">
        <InputDataConnector ref="myLDAP" attributeNames="mail"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:mail" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.3" friendlyName="mail" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Prescoped" id="eduPersonPrincipalName">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonPrincipalName"/>
        <AttributeEncoder xsi:type="SAML1ScopedString" name="urn:mace:dir:attribute-def:eduPersonPrincipalName" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" friendlyName="eduPersonPrincipalName" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="IDPEmail">
        <InputDataConnector ref="myLDAP" attributeNames="mail"/>
        <AttributeEncoder xsi:type="SAML1String" name="IDPEmail" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="IDPEmail" friendlyName="IDPEmail" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="ScriptedAttribute" id="ImmutableID">
```

```
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonPrincipalName" />
        <AttributeEncoder xsi:type="SAML1String"
                          name="ImmutableID"
                          encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String"
                          name="ImmutableID"
                          friendlyName="ImmutableID"
                          encodeType="false" />
        <Script><![CDATA[
var MD5 = function(d) {
  var r = M(V(Y(X(d),8*d.length)));
  return r.toLowerCase()
};

function M(d) {
  for(var
_,m="0123456789ABCDEF",f="",r=0;r<d.length;r++)_=d.charCodeAt(r),f+=m.charAt(_>>>4&15)+m.charAt(1
5&_);
  return f
}

function X(d) {
  for(var _=Array(d.length>>2),m=0;m<_.length;m++)_[m]=0;
  for(m=0;m<8*d.length;m+=8)_[m>>5]|=(255&d.charCodeAt(m/8))<<m%32;
  return _
}

function V(d) {
  for(var _="",m=0;m<32*d.length;m+=8)_+=String.fromCharCode(d[m>>5]>>>m%32&255);
  return _
}

function Y(d,_) {
  d[_>>5]|=128<<_%32,d[14+(_+64>>>9<<4)]=_;
  for(var m=1732584193,f=-271733879,r=-1732584194,i=271733878,n=0;n<d.length;n+=16) {
    var h=m,t=f,g=r,e=i;
    f=md5_ii(
      f=md5_ii(
        f=md5_ii(
          f=md5_ii(
```

```
f=md5_hh(
  f=md5_hh(
    f=md5_hh(
      f=md5_hh(
        f=md5_gg(
          f=md5_gg(
            f=md5_gg(
              f=md5_gg(
                f=md5_ff(
                  f=md5_ff(
                    f=md5_ff(
                      f=md5_ff(
                        f=md5_ff(
                          f,r=md5_ff(
                            r,i=md5_ff(
                              i,m=md5_ff(
                                m,f,r,i,d[n+0],7,-680876936
                              ),f,r,d[n+1],12,-389564586
                            ),m,f,d[n+2],17,606105819
                          ),i,m,d[n+3],22,-1044525330
                        ),r=md5_ff(
                          r,i=md5_ff(
                            i,m=md5_ff(
                              m,f,r,i,d[n+4],7,-176418897
                            ),f,r,d[n+5],12,1200080426
                          ),m,f,d[n+6],17,-1473231341
                        ),i,m,d[n+7],22,-45705983
                      ),r=md5_ff(
                        r,i=md5_ff(
                          i,m=md5_ff(
                            m,f,r,i,d[n+8],7,1770035416
                          ),f,r,d[n+9],12,-1958414417
                        ),m,f,d[n+10],17,-42063
                      ),i,m,d[n+11],22,-1990404162
                    ),r=md5_ff(
                      r,i=md5_ff(
                        i,m=md5_ff(
                          m,f,r,i,d[n+12],7,1804603682
                        ),f,r,d[n+13],12,-40341101
                      ),m,f,d[n+14],17,-1502002290
                    ),i,m,d[n+15],22,1236535329
```

```
            ),r=md5_gg(
              r,i=md5_gg(
                i,m=md5_gg(
                  m,f,r,i,d[n+1],5,-165796510
                ),f,r,d[n+6],9,-1069501632
              ),m,f,d[n+11],14,643717713
            ),i,m,d[n+0],20,-373897302
          ),r=md5_gg(
            r,i=md5_gg(
              i,m=md5_gg(
                m,f,r,i,d[n+5],5,-701558691
              ),f,r,d[n+10],9,38016083
            ),m,f,d[n+15],14,-660478335
          ),i,m,d[n+4],20,-405537848
        ),r=md5_gg(
          r,i=md5_gg(
            i,m=md5_gg(
              m,f,r,i,d[n+9],5,568446438
            ),f,r,d[n+14],9,-1019803690
          ),m,f,d[n+3],14,-187363961
        ),i,m,d[n+8],20,1163531501
      ),r=md5_gg(
        r,i=md5_gg(
          i,m=md5_gg(
            m,f,r,i,d[n+13],5,-1444681467
          ),f,r,d[n+2],9,-51403784
        ),m,f,d[n+7],14,1735328473
      ),i,m,d[n+12],20,-1926607734
    ),r=md5_hh(
      r,i=md5_hh(
        i,m=md5_hh(
          m,f,r,i,d[n+5],4,-378558
        ),f,r,d[n+8],11,-2022574463
      ),m,f,d[n+11],16,1839030562
    ),i,m,d[n+14],23,-35309556
  ),r=md5_hh(
    r,i=md5_hh(
      i,m=md5_hh(
        m,f,r,i,d[n+1],4,-1530992060
      ),f,r,d[n+4],11,1272893353
```

```
            ),m,f,d[n+7],16,-155497632
          ),i,m,d[n+10],23,-1094730640
        ),r=md5_hh(
          r,i=md5_hh(
            i,m=md5_hh(
              m,f,r,i,d[n+13],4,681279174
            ),f,r,d[n+0],11,-358537222
          ),m,f,d[n+3],16,-722521979
        ),i,m,d[n+6],23,76029189
      ),r=md5_hh(
        r,i=md5_hh(
          i,m=md5_hh(
            m,f,r,i,d[n+9],4,-640364487
          ),f,r,d[n+12],11,-421815835
        ),m,f,d[n+15],16,530742520
      ),i,m,d[n+2],23,-995338651
    ),r=md5_ii(
      r,i=md5_ii(
        i,m=md5_ii(
          m,f,r,i,d[n+0],6,-198630844
        ),f,r,d[n+7],10,1126891415
      ),m,f,d[n+14],15,-1416354905
    ),i,m,d[n+5],21,-57434055
  ),r=md5_ii(
    r,i=md5_ii(
      i,m=md5_ii(
        m,f,r,i,d[n+12],6,1700485571
      ),f,r,d[n+3],10,-1894986606
    ),m,f,d[n+10],15,-1051523
  ),i,m,d[n+1],21,-2054922799
),r=md5_ii(
  r,i=md5_ii(
    i,m=md5_ii(
      m,f,r,i,d[n+8],6,1873313359
    ),f,r,d[n+15],10,-30611744
  ),m,f,d[n+6],15,-1560198380
),i,m,d[n+13],21,1309151649
),r=md5_ii(
  r,i=md5_ii(
    i,m=md5_ii(
```

```
            m,f,r,i,d[n+4],6,-145523070
          ),f,r,d[n+11],10,-1120210379
        ),m,f,d[n+2],15,718787259
      ),i,m,d[n+9],21,-343485551
    ),m=safe_add(m,h),f=safe_add(f,t),r=safe_add(r,g),i=safe_add(i,e)
  }
  return Array(m,f,r,i)
}

function md5_cmn(d,_,m,f,r,i) {
  return safe_add(bit_rol(safe_add(safe_add(_,d),safe_add(f,i)),r),m)
}

function md5_ff(d,_,m,f,r,i,n) {
  return md5_cmn(_&m|~_&f,d,_,r,i,n)
}

function md5_gg(d,_,m,f,r,i,n) {
  return md5_cmn(_&f|m&~f,d,_,r,i,n)
}

function md5_hh(d,_,m,f,r,i,n) {
  return md5_cmn(_^m^f,d,_,r,i,n)
}

function md5_ii(d,_,m,f,r,i,n) {
  return md5_cmn(m^(_|~f),d,_,r,i,n)
}

function safe_add(d,_) {
  var m=(65535&d)+(65535&_);
  return(d>>16)+(_>>16)+(m>>16)<<16|65535&m
}

function bit_rol(d,_) {
  return d<<_|d>>>32-_
}

var UUID = function(s) {
  return s.substring(0,8) + '-' + s.substring(8,12) + '-' + s.substring(12,16) + '-' + s.substring(16,20) + '-' +
```

```
s.substring(20)
};

ImmutableID.addValue(UUID(MD5(eduPersonPrincipalName.getValues().get(0))));
        ]]></Script>
    </AttributeDefinition>

    <!-- ========================================== -->
    <!--    Data Connectors                         -->
    <!-- ========================================== -->

    <DataConnector id="myLDAP" xsi:type="LDAPDirectory"
        ldapURL="%{idp.attribute.resolver.LDAP.ldapURL}"
        baseDN="%{idp.attribute.resolver.LDAP.baseDN}"
        principal="%{idp.attribute.resolver.LDAP.bindDN}"
        principalCredential="%{idp.attribute.resolver.LDAP.bindDNCredential}"
        useStartTLS="%{idp.attribute.resolver.LDAP.useStartTLS:true}"
        connectTimeout="%{idp.attribute.resolver.LDAP.connectTimeout}"
              trustFile="%{idp.attribute.resolver.LDAP.trustCertificates}"
        responseTimeout="%{idp.attribute.resolver.LDAP.responseTimeout}">
        <FilterTemplate>
            <![CDATA[
                %{idp.attribute.resolver.LDAP.searchFilter}
            ]]>
        </FilterTemplate>
            <ConnectionPool
            minPoolSize="%{idp.pool.LDAP.minSize:3}"
            maxPoolSize="%{idp.pool.LDAP.maxSize:10}"
            blockWaitTime="%{idp.pool.LDAP.blockWaitTime:PT3S}"
            validatePeriodically="%{idp.pool.LDAP.validatePeriodically:true}"
            validateTimerPeriod="%{idp.pool.LDAP.validatePeriod:PT5M}"
            expirationTime="%{idp.pool.LDAP.idleTime:PT10M}"
            failFastInitialize="%{idp.pool.LDAP.failFastInitialize:false}" />
    </DataConnector>

    <DataConnector id="computed" xsi:type="ComputedId"
                  generatedAttributeID="computedId"
                  salt="%{idp.persistentId.salt}"
                  algorithm="%{idp.persistentId.algorithm:SHA}"
                  encoding="%{idp.persistentId.encoding:BASE32}">
```

```
        <InputDataConnector ref="myLDAP" attributeNames="%{idp.persistentId.sourceAttribute}" />
    </DataConnector>


</AttributeResolver>
```

Ha anonymous LDAP keresést akarunk használni, akkor a `principal` és `principalCredential` paramétereket törölni kell a myLDAP DataConnector-ból.

Attribútum kiadás beállítása {#attribútum_kiadás_beállítása}

Az IdP-nek ki kell adnia az `ImmutableID` és az `IDPEmail` attribútumokat a Microsoft-nak. Ezért létre kell hozni egy új `AttributeFilterPolicy` szabályt a `conf/attribute-filter.xml` fájlban:

```
<!-- Office 365 ImmutableID and IDPEmail -->

<AttributeFilterPolicy id="PolicyForWindowsAzureAD">

  <PolicyRequirementRule xsi:type="Requester" value="urn:federation:MicrosoftOnline" />

    <AttributeRule attributeID="IDPEmail">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

    <AttributeRule attributeID="ImmutableID">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

</AttributeFilterPolicy>
```

A properties fájlok beállításai {#a_properties_fájlok_beállításai}

conf/idp.properties

```
idp.session.StorageService = shibboleth.StorageService
idp.session.trackSPSessions = true
```

```
idp.session.secondaryServiceIndex = true
```

conf/ldap.properties

```
idp.authn.LDAP.ldapURL = ldap://ldap.example.com
idp.authn.LDAP.useStartTLS = true
idp.authn.LDAP.sslConfig = certificateTrust
# idp.authn.LDAP.trustStore = %{idp.home}/credentials/ldap-server.truststore
idp.authn.LDAP.returnAttributes = uid,mail,eduPersonPrincipalName
idp.authn.LDAP.baseDN = ou=People,dc=example,dc=com
idp.authn.LDAP.userFilter = (|(uid={user})(mail={user}))
# idp.authn.LDAP.bindDN = uid=myservice,ou=system
# idp.authn.LDAP.bindDNCredential = myServicePassword
idp.authn.LDAP.dnFormat = uid=%s,ou=People,dc=example,dc=com
```

conf/saml-nameid.properties

```
idp.nameid.saml2.default = urn:oasis:names:tc:SAML:2.0:nameid-format:transient
idp.nameid.saml1.default = urn:mace:shibboleth:1.0:nameIdentifier
idp.transientId.generator = shibboleth.CryptoTransientIdGenerator
idp.persistentId.sourceAttribute = eduPersonPrincipalName
idp.persistentId.useUnfilteredAttributes = true
idp.persistentId.salt = XXX_secret_salt_XXX
idp.persistentId.generator = shibboleth.ComputedPersistentIdGenerator
```

Docker image készítése {#docker_image_készítése}

Hozzunk létre egy `Dockerfile`-t ott, ahol a `customized-shibboleth-idp` mappa található, az alábbi tartalommal:

```
FROM       unicon/shibboleth-idp
MAINTAINER John Doe <john.doe@example.com>
ADD        customized-shibboleth-idp/ /opt/shibboleth-idp/
```

Készítsük el az image fájlt:

```
docker build -t example-com/idp-shib .
```

Indítsuk el az új IdP-t. A 4443-as és 8443-as portokat adjuk ki, és ne feledjük az előzőleg az SSL kulcsok számára beállított jelszavakat sem:

```
docker run -it --rm
    -p 4443:4443
    -p 8443:8443
    --network bridge
    -e JETTY_BROWSER_SSL_KEYSTORE_PASSWORD=XXX_secret_XXX
    -e JETTY_BACKCHANNEL_SSL_KEYSTORE_PASSWORD=XXX_secret_XXX
    example-com/idp-shib
```

Hibakeresés

A `conf/idp.properties` fájlban megadható loglevel beállítások részletes hibakeresést tesznek lehetővé.

Variable	Default value	Description
idp.loglevel.idp	INFO	Log level for the IdP proper
idp.loglevel.ldap	WARN	Log level for LDAP events
idp.loglevel.messages	INFO	Set to DEBUG for protocol message tracing
idp.loglevel.encryption	INFO	Set to DEBUG to log cleartext versions of encrypted content
idp.loglevel.opensaml	INFO	Log level for OpenSAML library classes
idp.loglevel.props	INFO	Set to DEBUG to log runtime properties during startup
idp.loglevel.spring	ERROR	Log level for Spring Framework (very chatty)
idp.loglevel.container	ERROR	Log level for Tomcat/Jetty (very chatty)
idp.loglevel.xmlsec	INFO	Set to DEBUG for low-level XML Signing/Encryption logging

További leírások {#további_leírások}

- Configure Shibboleth for use with singlesign-on
- How to use Shibboleth Identity Provider v3 with Office 365

Cloud365_Domains

Domainek kezdeti konfigurálása

Két szabálynak kell megfelelni:

- az Office365 csak olyan domaineken szolgáltat, amelyet az intézmény előtte az adminisztrációs felületen validált
- az EduID365 portálon a használt domaineket fel kell venni a *portál* adminisztrációs felületén. Ennek a lépésnek az Office365 Admin felületen történő beállítása után, ám az első felhasználó belépése előtt meg kell történnie.

Az Office365 alapértelmezetten azt gondolja, hogy az intézmény az adott domain e-mail szolgáltatását is az Office365-re bízza. Amennyiben ez nincs így (márpedig gyakran nincs) az alábbiakat kell tenni:

- természetesen **nem szabad átállítani a domainhez tartozó MX rekordokat** olyan módon, ahogyan a domain beállítási segédlet javasolná;
- a validált domainek beállításait módosítani kell

Aldomainek utólagos konfigurálása

Miután az eduID Cloud 365 konfigurálta a fő domaint, újabb domainek hozzáadása már csak PowerShell használatával lehetséges.

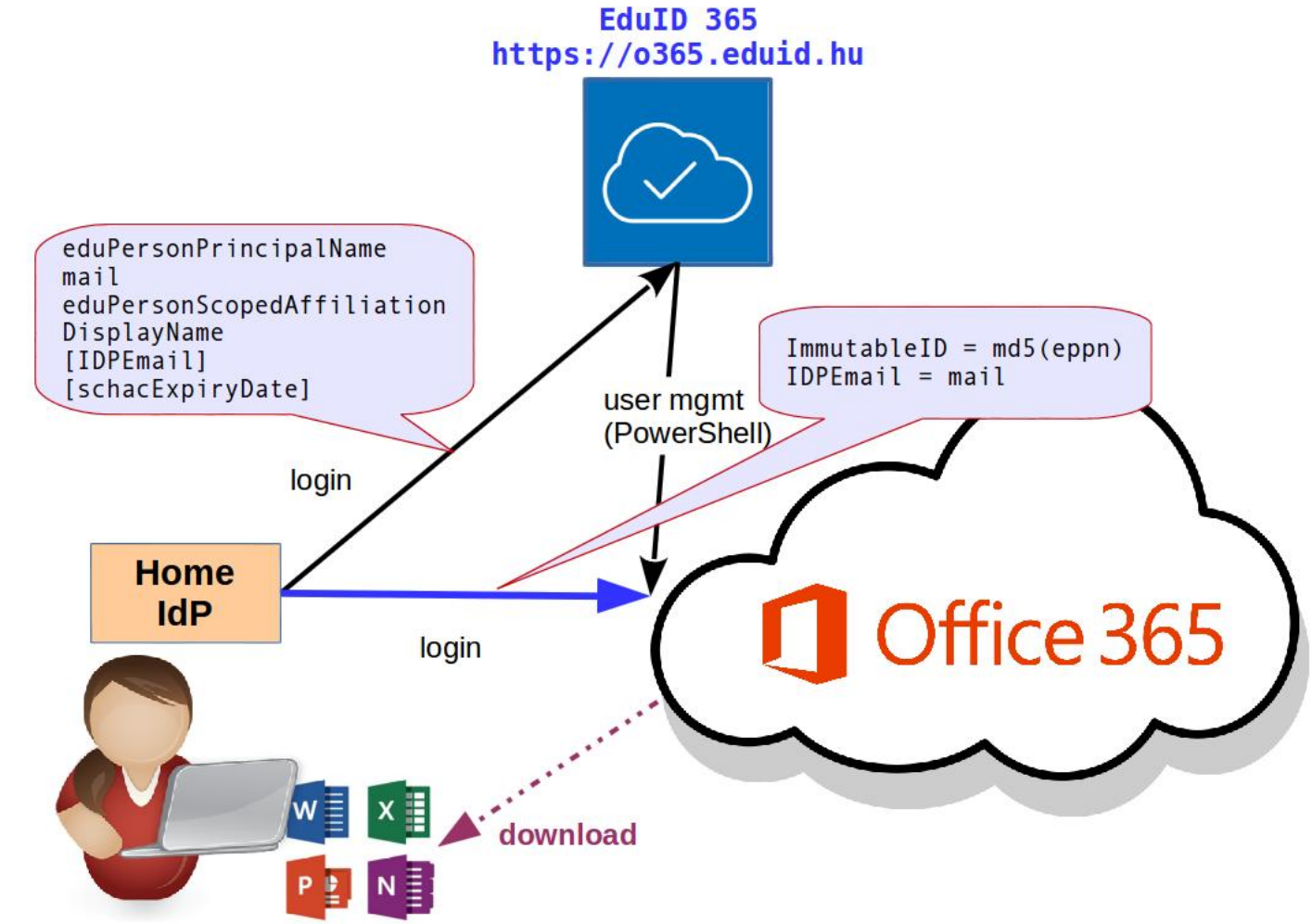
Ehhez első lépésként konfigurálni kell egy PowerShell kapcsolatot ahivatkozott leírásszerint. Ezután a következő paranccsal adhatjuk hozzá a domaint:

```
New-MsolDomain -Name {subdomain}.domain.hu -Authentication Federated
```

Ezután a lépés után a Cloud 365 portálon is hozzá kell adni az új aldomaint.

A felhasználók domainje

Az alábbi ábra azt mutatja be, hogy a rendszer egyes komponensei milyen adatok alapján dolgoznak:



Office 365 {#office_365}

Az Office 365 két attribútumot kaphat:

- *ImmutableID*: ez egy UUID formátumú azonosító, amelyet az *eduPersonPrincipalName* attribútumból kell generálni MD5 hash használatával
- *IDPEmail*: olvasható azonosító, valamint a felhős levelezésben használt e-mail cím

!!! note "Megjegyzés"

    Az **IDPEmail** domain részének olyan domainnek kell lennie, amelyet az intézmény az Office365-nél korábban validált. Amennyiben a felhasználó használja az Office365 online mail szolgáltatást, ez a cím kötelezően megegyezik a szolgáltatott e-mail címmel.

EduID Cloud 365 {#eduid_cloud_365}

A portál az alábbi attribútumokat várja:

- *EduPersonPrincipalName*: állandó azonosító, amelyből a portál az előző szakaszban leírt módszerrel állítja elő az *ImmutableID* értékét
- *eduPersonScopedAffiliation*: a felhasználó intézményhez való viszonya; ettől függ az elérhető licencek köre
- *displayName*: a felhasználó megjelenített neve
- *mail*
  - az az e-mail cím, amelyre a portál a használathoz szükséges értesítéseket küldi (pl. ha a felhasználónak a licencek megtartásához újból be kell jelentkeznie)
  - amennyiben nem érkezik az opcionális *IDPEmail* attribútum, akkor ez alapján generálja az Office365 számára ezt az értéket
- (opcionális) *schacExpiryDate*: a felhasználó licenceinek lejárati ideje
- (opcionális) *IDPEmail*: amennyiben az Office365-ben használt e-mail azonosító és az értesítési cím eltér, ebben az attribútumban lehet megadni az Office365-ben használt címet. Ennek domain részére az előző szakaszban kiemelt megjegyzés vonatkozik.