

Allgemeine Infos zu IdPs unter Univenton:

[https://wiki.univenton.de/index.php/SAML\\_Identity\\_Provider](https://wiki.univenton.de/index.php/SAML_Identity_Provider)

Zunächst erstellt man in der Adobe Admin Console einen neuen Identity Provider.

Im nächsten Schritt erhält man dann eine Adobe-Metadatendatei. Diese lädt man herunter - es handelt sich um ein XML-File.

Es enthält unter anderem folgende Informationen:

```
<md:EntityDescriptor [...] entityID="https://federatedid-na1.services.adobe.com/federated/saml/metadata/alias/a0eb6060-f6f6-4f3...">

<md:AssertionConsumerService [...] Location="https://federatedid-na1.services.adobe.com/federated/saml/SSO/alias/a0eb6060-f6f6-4...">

<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
```

Als nächstes gehen wir in die UMC am Master-DC und dort auf Domain > SAML Identity Provider > Add

In das Feld **Service provider identifier** tragen wir die entityID vom EntityDescriptor ein.

In das Feld **Respond to this service provider URL after login** tragen wir die Location vom AssertionConsumerService ein.

In das Feld **Format of NameID attribute** tragen wir das NameIDFormat ein. Das kann mehrfach in der XML vorkommen. Ich hatte z.B. noch ....persistent drin stehen, aber funktioniert hat es nur mit ....emailAddress

In das Feld **Name of the attribute that is used as NameID** tragen wir "uid" ein.

Das Ganze sieht dann in etwa so aus:

---

**General**  
Extended Settings

**Basic Settings**  
You can download the public certificate for this identity provider at </simplesamlphp/saml2/idp/certificate>.  
  
Type: SAML service provider  
Position: /univention/saml-serviceprovider

**SAML service provider basic settings** ⌵

Service provider activation status ⓘ

Service provider identifier \* ⓘ

Respond to this service provider URL after login ⓘ

Respond to this service provider URL after login ⓘ

Single logout URL for this service provider ⓘ

Format of NameID attribute ⓘ

Name of the attribute that is used as NameID ⓘ

Name of the organization for this service provider ⓘ

Description of this service provider ⓘ

Enable signed Logouts ⓘ

Adobe erwartet ein Active Directory - damit das auch mit unserem LDAP funktioniert, müssen wir noch ein paar Mappings unter "Extended Settings" setzen:

General

**Extended Settings**

**Additional configuration options**

Type: SAML service provider  
Position: /univention/saml-serviceprovider

**Extended Settings**

URL to the service provider's privacy policy ⓘ

Allow transmission of ldap attributes to the service provider ⓘ

Value for attribute format field ⓘ

<input type="text" value="mailPrimaryAddress"/> LDAP Attribute Name ⓘ	<input type="text" value="Email"/> Service Attribute Name	<input type="button" value="trash"/>
<input type="text" value="givenName"/> LDAP Attribute Name ⓘ	<input type="text" value="FirstName"/> Service Attribute Name	<input type="button" value="trash"/>
<input type="text" value="sn"/> LDAP Attribute Name ⓘ	<input type="text" value="LastName"/> Service Attribute Name	<input type="button" value="trash"/>
<input type="text"/> LDAP Attribute Name ⓘ	<input type="text"/> Service Attribute Name	<input type="button" value="trash"/>

Dieses LDAP-Objekt speichern wir dann.

Bevor wir nun in der Adobe Admin Console weitermachen können, müssen wir noch die Metadatenfile von unserem UCS Master hochladen. Diese erhalten wir hier:

<https://ucs-sso.firma.at/simplestamphp/saml2/idp/metadata.php>

(möglicherweise nur intern erreichbar)

Danach ist in der Adobe Admin Console der neue IdP als Inaktiv vorhanden:

**Inaktiv**

**SAML Anbieter**

---

PROTOKOLL  
SAML

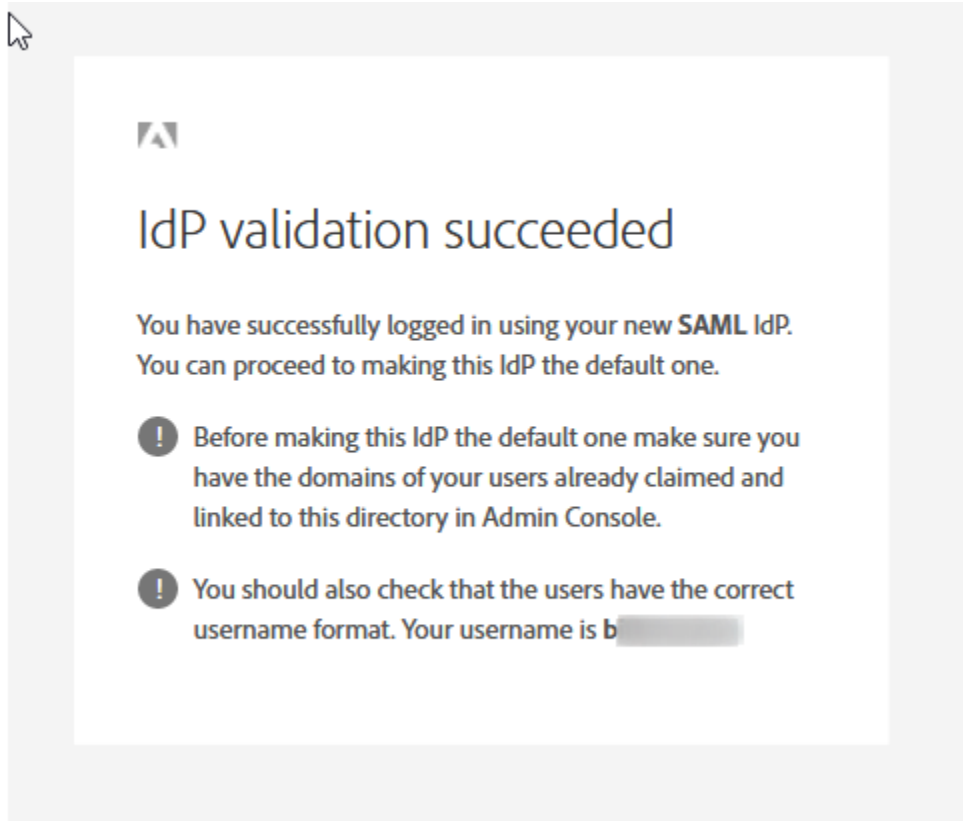
ZERTIFIKATSTYP  
SHA-256

ERSTELLUNGSDATUM  
5. August 2020

...

Wenn man nun auf Test klickt, sollte man auf die UCS-Login-Seite weitergeleitet werden.

Dort authentifiziert man sich dann und sollte schließlich das hier sehen: (das funktioniert aber nur, wenn der neue IdP für diesen Benutzer in der UMC auch aktiviert wurde - zu finden unter Account / SAML settings)



Nun kann man bei allen Benutzern, die das benötigen, diesen neuen IdP in der UMC hinzufügen. Der alte soll dort verbleiben, um eine unterbrechungsfreie Migration zu gewährleisten.

Er verschwindet später ohnehin für alle Benutzer, wenn er gelöscht wird.

Sobald man den neuen IdP in der Admin Console aktiviert, werden IdPs, welche alte Zertifikate verwenden, die nicht mehr unterstützt werden (derzeit 07 Aug 2020 etwa SHA-1) nur mehr eine Woche lang gültig sein.