KOMBIT – AULA

OPSÆTNING AF KOMMUNAL IDENTITY PROVIDER TIL AULA

Version:	1.0
Status:	Endelig
Godkender:	Erling Hansen
Forfatter:	Casper Kristiansen Vedel

netcompany

Dokumenthistorik

Version	Dato	Forfatter	Status	Bemærkninger
0.9	21-11-2018	Casper Kristiansen Vedel	Udkast	
1.0	03-12.2018	Casper Kristiansen Vedel	Endelig	

Referencer

Reference	Titel	Forfatter	Version
[OIOSAML]	**OIOSAML Profil**	**Digitaliser.dk**	**2.0.9**
[LOGIN-FAQ]	**FAQ – Login og step-up**	**Netcompany A/S**	**1.0**

Indholdsfortegnelse

1 Introduktion

1.1 Formål

Nærværende dokument er tiltænkt som et lille lynkursus og assistance i opsætningen af kommuners/institutioners lokale Identity Providers.

Der er specifikt tale om en vejledning i hvordan Aula tilføjes som "Relying Party", samt hvilke claims der forudsættes for at IdP'en kan benyttes til at logge ind i Aula. Til sidst beskrives konceptet "Account Linking" og hvordan IdP'en i så fald skal opsættes.

Såfremt IdP'en allerede er konfigureret til at overholde [OIOSAML], vil opsætningen bygge videre på dette, med tilføjelsen af Aula som Relying Party samt tilføjelse af to attributter: én påkrævet og én valgfri.

1.2 Målgruppe

Dokumentet forudsætter viden omkring opsætning af claims, da det er nødvendigt at tilpasse eksemplerne til den enkelte IdP. Der er derfor tale om et dokument skrevet med drift- og IT-medarbejdere for øje.

Der er i vejledningens eksempler taget udgangspunkt i Microsofts Active Directory Federation Services, herefter blot ADFS, men det er ikke et krav at IdP'en er baseret på AD FS. En hvilken som helst IdP kan benyttes, så længe den baserer sig på SAML 2.0. Skærmbilleder og eksempler er baseret AD FS, men de enkelte trin bør kunne overføres til andre IdP-løsninger.

1.3 Definitioner og forkortelser

I dokumentet vil der blive gjort brug af forkortelser som er beskrevet nedenfor.

Forkortelse/ definition	Fulde navn	Beskrivelse
AD	Microsoft Active Directory	
ADFS	Microsoft Active Directory Federation Services	
Claim	Claim	En påstand om hvem brugeren er. Kan både være en indkommende påstand (en forespørgsel fra Aula) og en udgående påstand (svaret på en forespørgsel). I SAML termer kaldes dette også en Assertion.
IdP	Identity Provider	Kommunens/Institutionens login løsning

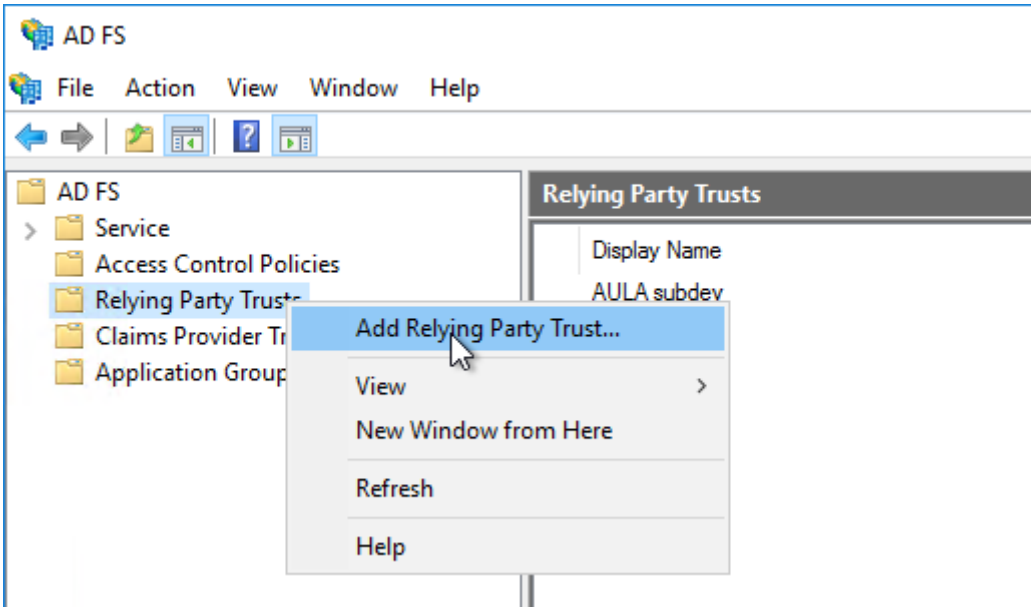
1.4 Begrænsninger

Dokumentet forudsætter en fungerende IdP, hvor brugerne allerede har mulighed for at logge ind. Der vil ikke indgå nogen beskrivelse til opsætningen af dette.

2 Tilføj Aula som Relying Party

Bemærk at vejledningen tager udgangspunkt i opsætningen i AD FS, men enhver anden SAML 2.0 IdP kan bruges.

Første skridt i opsætningen af den lokale IdP er at tilføje Aula som en såkaldt "Relying Party". Opsætningsværktøjet til AD FS åbnes og der højreklikkes på "Relying Party Trusts" og vælges "Add Relying Party Trust".



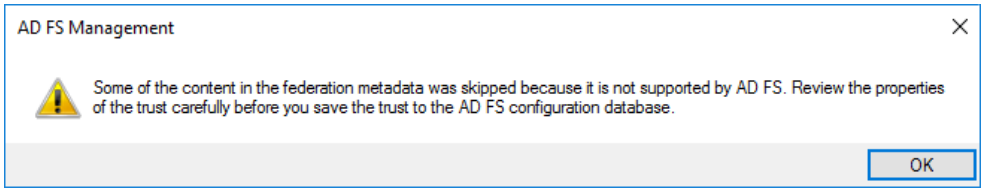
Figur 1 - Aula tilføjes som "Relying Party" i kommunens/institutionens lokale IdP

Dette åbner en wizard, hvor der vælges **Claims aware**. For at opsætte Relying Party skal bruges SAML metadata for Aula:

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
entityID="https://prod.aula.dk/simplesaml/saml2/idp/metadata.php">
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIGHTCCBQWgAwIBAgIEWg+IgDANBgkqhkiG9w0BAQsFADBBMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1QyNDA4MR4wHAY
DVQQDDBVUUlVTVDI0MDggT0NFUyBDQSBJSUkwHhcNMTgxMDE1MDY1NjM4WhcNMjExMDE1MDY1NTE2WjCBjjELMAkGA1UEBhMCREsxIzAhBgNVBAoMGktPTU
JJVCBBL1MgLy8gQ1ZSOjE5NDM1MDc1MVowIAYDVQQFExlDVlI6MTk0MzUwNzUtRklEOjE5OTMxOTQ0MDYGA1UEAwwvQVVMQV9Db250ZXh0X0hhbmRsZXJfc
HJvZCAoZnVua3Rpb25zY2VydGlmaWthdCkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdmN2XIuf7887Nc5ZX3aiodzrzHVKwVVLCyTD2DRdi
DZrcLocFQjPpPBZ60EyNiHaOaYQvOuyzWgKyLTY+hBpxizc530a2yrYBWcLSdT5SBahBihGTDbBLTtU95yZ7EJCp/Fj0iJSq3BqSX/uP70ksZJY4x/WlG2a
YlSCRsUU+shwHMc8hXDR3Pc16JVmFMMwfTiukeBgZ2mf7HyWA9XXJjXVZ1Htrhyky45P5vI7p1w3kp1zMSXEDWLDH4rEmbzdn3/30MjC3lsaxg43AHd20jI
Czx1uQMpqI0K8OXGLSdUO1pZVYJ8iFV8X6RQe2TVcWhfoF99IJLHmaux20WaRPAgMBAAGjggLNMIICyTAOBgNVHQ8BAf8EBAMCA7gwgYkGCCsGAQUFBwEBB
H0wezA1BggrBgEFBQcwAYYpaHR0cDovL29jc3AuaWNhMDMudHJ1c3QyNDA4LmNvbS9yZXNwb25kZXIwQgYIKwYBBQUHMAKGNmh0dHA6Ly9mLmFpYS5pY2Ew
My50cnVzdDI0MDguY29tL29jZXMtaXNzdWluZzAzLWNhLmNlcjCCAUMGA1UdIASCATowggE2MIIBMgYKKoFQgSkBAQEEAjCCASIwLwYIKwYBBQUHAgEWI2h
0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBvc2l0b3J5MIHuBggrBgEFBQcCAjCB4TAQFglUUlVTVDI0MDgwAwIBARqBzEZvciBhbnZlbmRlbHNlIGFmIG
NlcnRpZmlrYXRldCBn5mxkZXIgT0NFUyB2aWxr5XIsIENQUyBvZyBPQ0VTIENQLCBkZXIga2FuIGhlbnRlcyBmcmEgd3d3LnRydXN0MjQwOC5jb20vcmVwb
3NpdG9yeS4gQmVt5nJrLCBhdCBUUlVTVDI0MDggZW50ZXIgdmlsa+VyZW5lIGhhciBldCBiZWdy5m5zZXQgYW5zdmFyIGlmdC4gcHJvZmVzc2lvbmVsbGUg
cGFydGVyLjCBmAYDVR0fBIGQMIGNMC6gLKAqhihodHRwOi8vY3JsLmljYTAzLnRydXN0MjQwOC5jb20vaWNhMDMuY3JsMFugWaBXpFUwUzELMAkGA1UEBhM
CRExxEjAQBgNVBAoMCVRSVVNUMjQwODEeMBwGA1UEAwwVVFJVU1QyNDA4IE9DRVMgQ0EgSUlJMRAwDgYDVQQDDAdDUkwxMjkzMB8GA1UdIwQYMBaAFMZYMU
+WLVL79gt498rcHtjavKOEMB0GA1UdDgQWBBQNUP5TQBgt8Jt3g2u+qaFVnP+dYzAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQAR/yQN+JlJ2jWMU
+Pyu+l/lrJCjUdLQCFlFGM9aU496nPkef8eGSGdsIwVgtjhTPACJWPcwODM+8NIZgjOGM5RctKYWJJHL7eRhdzr4XRX/M6p5sd2rwZc/UIXqKqb2GVOYYsC
mIru8BnSNMWBn3nq+Pg6jF9aqzL80k0sAJkgMebPZ6vMymJwrU3DwuQpjA2+hAZJetAlKgHwfTmsu1/rlJIOuyoMy61ybaWB4Q+AaQW/D9Rbn/KhGl76ZIF
DqEsjZPwapq1k+cCGBYsKHr5r6EBz2ZQisEj6hK8B991XdXQlT6c/Sov5AVR8ANeK3QUDO0VtTri04O7UV2/KZGhx</ds:X509Certificate>
```

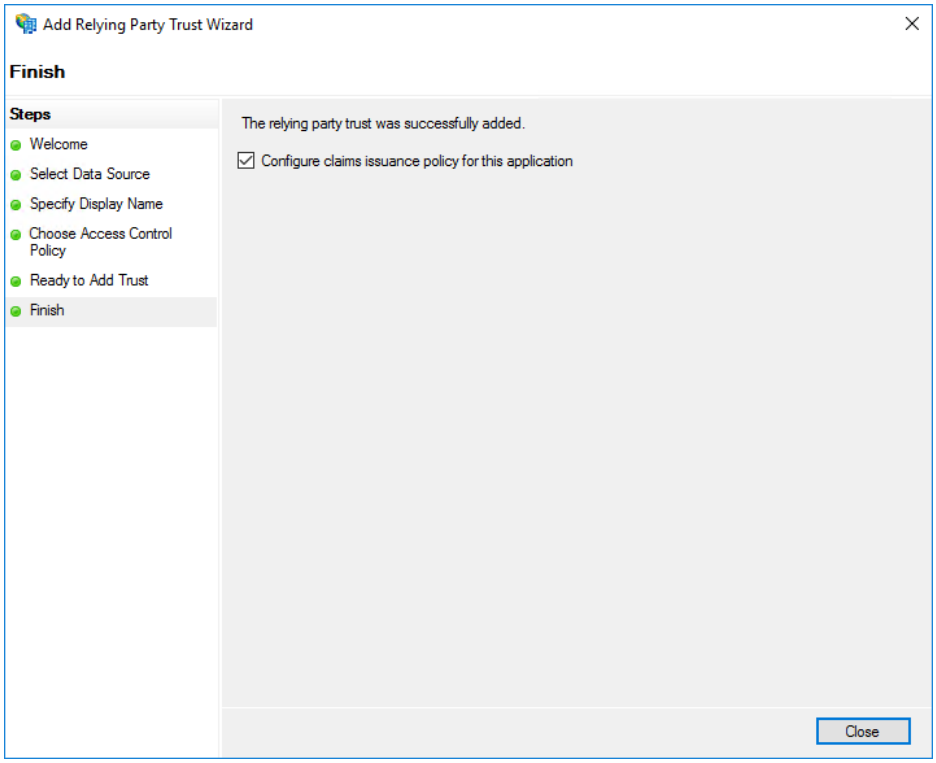
```
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIGHTCCBQWgAwIBAgIEWg+IgDANBgkqhkiG9w0BAQsFADBBMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1QyNDA4MR4wHAY
DVQQDDBVUUlVTVDI0MDggT0NFUyBDQSBJSUkwHhcNMTgxMDE1MDY1NjM4WhcNMjExMDE1MDY1NTE2WjCBjjELMAkGA1UEBhMCREsxIzAhBgNVBAoMGktPTU
JJVCBBL1MgLy8gQ1ZSOjE5NDM1MDc1MVowIAYDVQQFExlDVlI6MTk0MzUwNzUtRklEOjE5OTMxOTQ0MDYGA1UEAwwvQVVMQV9Db250ZXh0X0hhbmRsZXJfc
HJvZCAoZnVua3Rpb25zY2VydGlmaWthdCkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdmN2XIuf7887Nc5ZX3aiodzrzHVKwVVLCyTD2DRdi
DZrcLocFQjPpPBZ60EyNiHaOaYQvOuyzWgKyLTY+hBpxizc530a2yrYBWcLSdT5SBahBihGTDbBLTtU95yZ7EJCp/Fj0iJSq3BqSX/uP70ksZJY4x/WlG2a
YlSCRsUU+shwHMc8hXDR3Pc16JVmFMMwfTiukeBgZ2mf7HyWA9XXJjXVZ1Htrhyky45P5vI7p1w3kp1zMSXEDWLDH4rEmbzdn3/30MjC3lsaxg43AHd20jI
Czx1uQMpqI0K8OXGLSdUO1pZVYJ8iFV8X6RQe2TVcWhfoF99IJLHmaux20WaRPAgMBAAGjggLNMIICyTAOBgNVHQ8BAf8EBAMCA7gwgYkGCCsGAQUFBwEBB
H0wezA1BggrBgEFBQcwAYYpaHR0cDovL29jc3AuaWNhMDMudHJ1c3QyNDA4LmNvbS9yZXNwb25kZXIwQgYIKwYBBQUHMAKGNmh0dHA6Ly9mLmFpYS5pY2Ew
My50cnVzdDI0MDguY29tL29jZXMtaXNzdWluZzAzLWNhLmNlcjCCAUMGA1UdIASCATowggE2MIIBMgYKKoFQgSkBAQEEAjCCASIwLwYIKwYBBQUHAgEWI2h
0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBvc2l0b3J5MIHuBggrBgEFBQcCAjCB4TAQFglUUlVTVDI0MDgwAwIBARqBzEZvciBhbnZlbmRlbHNlIGFmIG
NlcnRpZmlrYXRldCBn5mxkZXIgT0NFUyB2aWxr5XIsIENQUyBvZyBPQ0VTIENQLCBkZXIga2FuIGhlbnRlcyBmcmEgd3d3LnRydXN0MjQwOC5jb20vcmVwb
3NpdG9yeS4gQmVt5nJrLCBhdCBUUlVTVDI0MDggZWZ0ZXIgdmlsa+VyZW5lIGhhciBldCBiZWdy5m5zZXQgYW5zdmFyIGlmdC4gcHJvZmVzc2lvbmVsbGUg
cGFydGVyLjCBmAYDVR0fBIGQMIGNMC6gLKAqhihodHRwOi8vY3JsLmljYTAzLnRydXN0MjQwOC5jb20vaWNhMDMuY3JsMFugWaBXpFUwUzELMAkGA1UEBhM
CRExxEjAQBgNVBAoMCVRSVVNUMjQwODEeMBwGA1UEAwwVVFJVU1QyNDA4IE9DRVMgQ0EgSUlJMRAwDgYDVQQDDAdDUkwxMjkzMB8GA1UdIwQYMBaAFMZYMU
+WLVL79gt498rcHtjavKOEMB0GA1UdDgQWBBQNUP5TQBgt8Jt3g2u+qaFVnP+dYzAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQAR/yQN+JlJ2jWMU
+Pyu+l/lrJCjUdLQCFlFGM9aU496nPkef8eGSGdsIwVgtjhTPACJWPcwODM+8NIZgjOGM5RctKYWJJHL7eRhdzr4XRX/M6p5sd2rwZc/UIXqKqb2GVOYYsC
mIru8BnSNMWBn3nq+Pg6jF9aqzL80k0sAJkgMebPZ6vMymJwrU3DwuQpjA2+hAZJetAlKgHwfTmsu1/rlJIOuyoMy61ybaWB4Q+AaQW/D9Rbn/KhGl76ZIF
DqEsjZPwapq1k+cCGBYsKHr5r6EBz2ZQisEj6hK8B991XdXQlT6c/Sov5AVR8ANeK3QUDO0VtTri04O7UV2/KZGhx</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://login.aula.dk/simplesaml/module.php/saml/sp/saml2-logout.php/default-sp"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://login.aula.dk/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp" index="0"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
Location="https://login.aula.dk/simplesaml/module.php/saml/sp/saml1-acs.php/default-sp" index="1"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="https://login.aula.dk/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp" index="2"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
Location="https://login.aula.dk/simplesaml/module.php/saml/sp/saml1-acs.php/default-sp/artifact" index="3"/>
</md:SPSSODescriptor>
<md:ContactPerson contactType="technical">
<md:GivenName>Administrator</md:GivenName>
<md:EmailAddress>info@netcompany.com</md:EmailAddress>
</md:ContactPerson>
</md:EntityDescriptor>
```

Bemærk at der ved import i AD FS er set følgende advarsel, når metadata forsøges importeret. Dette er ikke af betydning for Aula.



I de efterfølgende skærmbilleder kan man godt vælge bare at benytte standard indstillinger, hvis ikke man ser behov for at afvige fra disse.

Til sidst spørges om man vil opsætte **claims issuance policy**, som er markeret på forhånd:



Tryk blot **Close** med afkrydsningsfeltet markeret som ovenfor. Herefter opsættes de informationer Aula har brug for.

3 Påkrævede claims

Bemærk at følgende afsnit vil præsentere en række eksempler på claims (assertions). Disse er taget ud af en test installation af AD FS og kan derfor ikke blot kopieres som de er. Læseren forventes derfor at tage aktivt stilling til indholdet.

Aula forventer at følgende attributter er indeholdt i den token der udstedes af IdP'en:

1. AssuranceLevel
2. CvrNumberIdentifier
3. NameId

Derudover er der en sidste valgfri attribut

4. UniLoginIdentifier

3.1 Eksempler på opsætning i AD FS

Eksemplerne givet i dette afsnit er baseret på AD FS claim rules, men tilsvarende kan sættes op i andre SAML IdP'er.

I ADFS tilføjes reglerne ved at:

- Trykke på "**Relying Party Trusts**" i venstremenuen af **AD FS Management**
- Højreklikke på Aula der blev tilføjet i afsnit 2
- Vælge "**Edit Claim Issuance Policy…**"
- Trykke på "**Add rule…**"
- Vælge "**Send Claims Using a Custom Rule**"

3.2 AssuranceLevel

AssuranceLevel angiver hvilket sikkerhedsnveau login blev foretaget ved. Er der blot tale om brugernavn og password er dette sikkerhedsniveau 2, mens sikkerhedsniveau 3 opnås ved multifaktor autentificering.

Det er vigtigt at denne sættes korrekt af hensyn til datasikkerhed, men Aula har ikke mulighed for at kontrollere om den skulle være sat til 2 eller 3.

Nedenfor angives et eksempel på hvordan AssuranceLevel skal repræsenteres i den SAML token IdP'en udsteder:

```
<saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
    Name="dk:gov:saml:attribute:AssuranceLevel">
  <saml:AttributeValue xsi:type="xs:string”>{Assurance leve}</saml:AttributeValue>
</saml:Attribute>
```

3.2.1 Eksempel til AD FS

Følgende Claim rule tilføjer AssuranceLevel med en fast værdi. Værdien er markeret med rødt og hele strengen {Assurance level} skal ændres til enten 2 eller 3.

```
=> issue(Type = "dk:gov:saml:attribute:AssuranceLevel", Value = "{Assurance level}",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:basic");
```

3.3 CvrNumberIdentifier

CVR-nummeret bruges til at identificere en institution. Derefter bruges institutionen til at se om brugeren er tilknyttet denne institution og hvis ikke dette er tilfældet, får brugeren ikke adgang til Aula. Værdien skal derfor være CVR-nummeret på en institution hvor brugeren har en institutionsprofil i UNI-Login.

Nedenstående er et eksempel på det forventede format:

```
<saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
    Name="dk:gov:saml:attribute:CvrNumberIdentifier">
  <saml:AttributeValue xsi:type="xs:string">{CVR nummer}</saml:AttributeValue>
</saml:Attribute>
```

3.3.1 Eksempel til AD FS

Følgende Claim rule tilføjer CvrNumberIdentifier med en fast værdi. Værdien er markeret med rødt og hele strengen {CVR-nummer} skal ændres. Værdien skal være CVR-nummeret på en institution brugeren tilhører i UNI-Login.

```
=> issue(Type = "dk:gov:saml:attribute:CvrNumberIdentifier", Value = "{CVR-nummer}",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:basic");
```

3.4 NameID

NameID bruges til at identificere en bruger i de enkelte IdP'er. Det er således et krav at værdien er unik. Det er ligeledes et krav at værdien ikke kan genbruges, såsom initialer for én bruger der ikke længere arbejder i en institution, hvorefter en ny ansættes med samme initialer.

Bemærk, grundet en kendt fejl, understøttes der pt. kun at NameID sættes til "transient". Det er dog mest hensigtsmæssigt at værdien *ikke* skifter. Der arbejdes pt. på at understøtte "persistent".

Nedenstående er et eksempel på det forventede format:

```
<saml:Subject>
  <saml:NameID SPNameQualifier="https://dev.aula.dk/simplesaml/saml2/idp/metadata.php"
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
      {Unikt bruger id}
   </saml:NameID>
</saml:Subject>
```

3.4.1 Eksempel til AD FS

Nedenstående eksempel trækker det interne bruger id (ObjectGuid) og garanterer at værdien vil være unik.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer,
OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient");
```

3.5 UniLoginIdentifier

Attributten UniLoginIdentifier er valgfri og bruges til at binde et IdP login sammen med et UNI-Login. Såfremt den sendes med stoler Aula på at brugeren er hvem de udgiver sig for at være. Sendes den ikke med vil Aula forsøge at binde brugeren sammen med et UNI-Login, som beskrevet i afsnit 4.

Hvor de enkelte institutioner opbevarer denne oplysning – såfremt de opbevarer den. Her er det nødvendigt at institutionen selv får lavet reglen så den trækker værdien korrekt ud. Eksemplet er forberedt til at hente værdien ud af Active Directory, men uden at der er angivet et feltnavn.

Nedenstående er et eksempel på det forventede format:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:UniLoginIdentifier">
 <saml:AttributeValue xsi:type="xs:string">{UNI-Login ID}</saml:AttributeValue>
</saml:Attribute>
```

3.5.1 Eksempel til AD FS

Først tilføjes der en claim rule der henter en værdi fra Active Directory:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
 => add(store = "Active Directory", types = ("http://login.aula.dk/UniLoginIdentifier"), query = ";{UNI-login ID};{0}",
param = c.Value);
```

I ovenstående regel er det ikke muligt at forudse hvor de enkelte IdP'er vil gemme en sådan oplysninger i deres AD, og ej heller om den overhovedet ligger i AD'et. Det vil derfor være nødvendigt at se på specielt de to steder markeret med rødt. Såfremt typen sættes korrekt, bør det nedenstående kunne bruges som det er, og sørger for at tilføje nogle attributter i en ny claim rule:

```
c:[Type == "http://login.aula.dk/UniLoginIdentifier"]
 => issue(Type = "dk:gov:saml:attribute:UniLoginIdentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer,
Value = c.Value, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:basic");
```

4 Account Linking

Når der logges ind i Aula er alle informationer der knyttes til en bruger i virkeligheden knyttet til deres UNI-Login[1]. Når en bruger vælger at logge ind med en lokal IdP, vil tilknytningen til UNI-Login dermed mangle.

Afhængig af opsætningen vil login med en lokal IdP dermed følge ét af følgende scenarier:

1. Den lokale IdP medsender UniLoginIdentifier
2. Den lokale IdP medsender **ikke** UniLoginIdentifier

4.1 Lokal IdP medsender UniLoginIdentifier

Såfremt den SAML token Aula modtager fra den lokale IdP indeholder attributten UniLoginIdentifier, vil den validere følgende:

- At CvrNumberIdentifier fra SAML token er kendt af Aula.
- CVR-nummeret mappes til en institutionskode
- At UniLoginIdentifier identificerer et UNI-Login der er kendt af Aula
- At det pågældende UNI-Login er tilknyttet den institution som CVR-nummeret identificerede

Er følgende validering succesfuld vil brugeren få adgang til Aula og blive vist brugerens Dashboards.

4.2 Lokal IdP medsender ikke UniLoginIdentifier

Hvis den lokale IdP ikke er konfigureret således at SAML token indeholder UniLoginIdentifier vil brugeren efter første login blive viderestillet til at logge ind med NemID hos UNI-Login.

Når brugeren er logget ind hos UNI-Login, gemmes brugernavnet til den lokale IdP og brugernavnet til UNI-Login i Aula. Herefter har brugeren nu adgang til Aula og vises sine dashboards.

Denne ekstra foranstaltning er en nødvendighed for at den lokale IdP efterfølgende kan autentificere brugeren som havende sikkerhedsniveau 3, da Aula ikke har nogen teknisk mulighed for at kontrollere om IdP'en overholder sikkerhedsniveauerne.

Bemærk at dette ekstra login hos UNI-Login kun skal udføres første gang brugeren logger ind med den lokale IdP.

5 Levering af SAML metadata til Netcompany

Før IdP'en kan benyttes til login skal institutionen og Netcompany udveksle SAML metadata. I afsnit 2 er Aula tilføjet som **Relying Party**, og dermed mangler blot at Netcompany skal have tilsendt IdP'ens metadata samt nogle andre oplysninger.

Når en lokal IdP skal tilføjes, sker dette under pilottesten ved en manuel handling hos Netcompany, samt opsætning hos kommunen/institutionen.

Som en del af ovenstående service request er der behov for at specificere følgende:

1. Institutionskode
2. SAML metadata
3. Stepup

[1] Der overvejes pt. en løsning, hvor der ud over UNI-Login, også ville kunne AccountLinkes via CPR-nummer. Tidshorisonten for dette, er i skrivende stund dog uklar.

5.1 Institutionskode

Institutionskoden bruges til at afgøre hvordan IdP'en vælges fra Aulas brugergrænseflade og skal være institutionskoden for den institution som IdP'en tilhører. Det er således muligt at angive flere IdP'er inden for kommunen. Vælges eksempelvis institutionskode **00001**, som kunne tilhøre "**Østermark Skole**" i **Korsbæk Kommune** vil man fra brugergrænsefladen vælge at logge ind gennem en kommunal IdP og blive præsenteret for to lister, hvoraf kun den øverste indeholder data.

I denne vælger man kommunen, her **Korsbæk Kommune**, hvorefter den nederste liste nu indeholder alle institutioner i **Korsbæk Kommune** som har opsat en lokal IdP. Herefter vælges **Østermark Skole** og der trykkes videre til den pågældende IdP's loginside.

Såfremt der er tale om en kommunes IdP og ikke en institution, vil **Korsbæk Kommune** også figurere på den nederste liste.

5.2 SAML metadata

SAML metadata indeholder eksempelvis information om hvor Aula skal sende brugeren hen når der skal logges ind eller ud med den kommunale IdP.

Hvis der er tale om en AD FS IdP findes metadata generelt på adressen https://<server adresse>/FederationMetadata/2007-06/FederationMetadata.xml

Netcompany har behov for at få tilsendt hele denne fil.

5.3 Stepup

Bemærk, at på udgivelsestidspunktet for denne guide, understøtter Aula ikke muligheden for step-up med lokal IdP. Denne udvidelse er ved at blive planlagt til én af de første større releases af Aula. Nedenstående er det foreløbige design, og der kan komme ændringer.

Når en IdP skal tilføjes til Aula skal der i første omgang tages stilling til om IdP'en tillader stepup og dernæst hvordan den tillader det. Hvis den ikke tillader stepup, vil det som standard betyde at stepup i så fald sker med NEMID eller NEMID Erhverv gennem UNI-Login.

Der kan vælges at stepup skal ske med en anden IdP end UNI-Login, eksempelvis den kommende stepup med Context Handler eller at stepup skal ske med en sekundær lokal IdP, som kun foretager login ved sikkerhedsniveau 3+. Det sidste er måden UNI-Login fungerer på, da der er én IdP til login og en anden til stepup.

Hvis IdP'en selv understøtter stepup, har vi brug for at vide hvad den forventer indgår i SAML forespørgslen, som typisk vil være én af to varianter:

Variant	XML syntaks

Context Handler	`<saml:Attribute`
	`  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"`
	`  Name="dk:gov:saml:attribute:CvrNumberIdentifier">`
	`<saml:AttributeValue xsi:type="xs:string">{CVR-nummer}</saml:AttributeValue>`
	`</saml:Attribute>`

AD FS	`<saml2p:RequestedAuthnContext Comparison="exact">`
	`<saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">`
	`https://schemas.microsoft.com/claims/multipleauthn`
	`</saml2:AuthnContextClassRef>`
	`</saml2p:RequestedAuthnContext>`

6 Test af opsætningen

Når opsætningen af IdP'en er udført og Netcompany har modtaget SAML metadata, testes opsætningen ved at logge ind i Aula. Aula åbnes op for kommuner og institutioner i bølger og det er derfor først muligt at logge ind når den pågældende bølge har fået adgang.

7 Certifikater

7.1 Spærrecheck af OCES certifikater

Såfremt en lokal IdP benytter et OCES certifikat, vil Aula forsøge at spærrechecke det. Der er dog intet krav om at der skal benyttes OCES eller andet der understøtter spærrecheck og i disse tilfælde vil Aula blot ikke lave det check.

7.2 Fornyelse af AULAs certifikat

Fornyelse af AULAs certifikat sker ved at både det nye og gamle vil være aktive i en periode, således at IdP'erne har mulighed for en glidende overgang. Der vil blive givet et varsel når dette sker, samt hvornår det gamle certifikat ikke længere er aktivt.

7.3 Fornyelse af IdP'ers certifikat

AULA har ikke mulighed for automatisk at fornye IdP'ers certifikater og de skal derfor sendes til Netcompany. Det anbefales at IdP'erne ligesom Aula lader begge certifikater være gyldige i en periode, ligesom det bør varsles i god tid, således at det kan undgås at login er utilgængeligt gennem den pågældende IdP.