OS2faktor Login

Danmarks Miljøportal

1 Formål

Dette dokument beskriver kort hvordan man kan opsætte claims til Danmarks Miljøportal i OS2faktor.

Det antages at man anvender API'erne på Danmarks Miljøportals brugerstyring til at tildele rettigheder, fx via OS2rollekatalog, og at man derfor anvender den såkaldte AD FS Profil til claims mod Danmarks Miljøportal.

Hvis man i stedet anvender Azure Profilen, så kan man ikke anvende denne guide, og skal følge Miljøportalens vejledning.

Når man tilslutter sig Danmarks Miljøportal, så angiver man hvilken af disse profiler man ønsker at anvender, hvis man er i tvivl om hvilken profil man er opsat med hos Miljøportalen, skal man tage fat i dem og spørge.

2 Profiler på miljøportalen

Danmarks Miljøportal har 2 måder man kan tilslutte en Identity Provider. Disse kaldes profiler, og er navngivet efter specifikke Identity Provider produkter, omend de kan bruges af andre Identity Provider produkter også (fx OS2faktor Login).

Man kan se Miljøportalens dokumentation af den såkaldte AD FS profil her

https://github.com/danmarksmiljoeportal/brugerstyring/wiki/Connecting-Local-IdP-With-ADFS

og den tilsvarende dokumentation af den såkaldte Azure profil her

https://github.com/danmarksmiljoeportal/brugerstyring/wiki/Connecting-with-Azure-AD

Azure profilen er den nyeste af de to, og er på nogle områder simplere end AD FS profilen. Desværre kræver Azure profilen at man anvender et UUID som sit brugernavn, og hvis man kører OS2rollekatalog til at styre sine rettigheder i Miljøportalens brugerstyring, så vil det ikke fungere med et UUID, da OS2rollekatalog knytter rollerne til AD brugernavnet (sAMAccountName).

Hvis man gør brug af OS2rollekatalog til brugerstyring, eller evt har bygget sin egen integration til Miljøportalens API'er, hvor man ligeledes anvender AD brugernavnet som Miljøportal-brugernavn, så kan man anvende denne guide til at opsætte claim regler i OS2faktor Login, så de matcher AD FS profilen der er linket til ovenfor.

3 Forudsætninger

Man skal køre version 2025r2 af OS2faktor Login, eller nyere, for at alle claims fungerer som beskrevet nedenfor.

Ligeledes skal man sikre at man har indlæst UPN på brugerne, da UPN skal anvendes i en af disse claims.

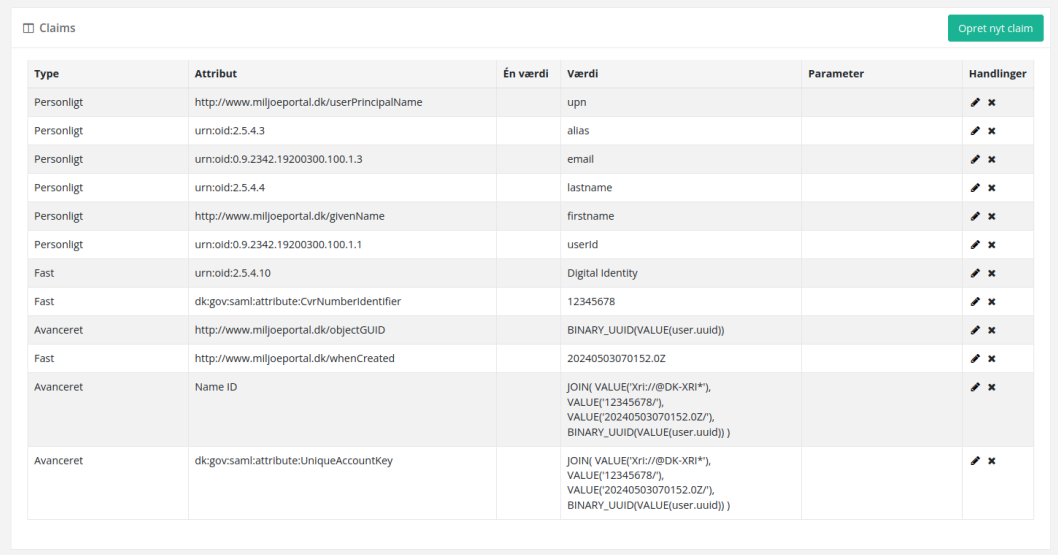
Hvis man anvender OS2sofd som indlæsningskilde, får man automatisk UPN med, og hvis man indlæser fra AD via OS2faktor Coredata Sync, så kan man tilføje UPN som ekstra stamdata ved at tilføje denne setting til konfigurationsfilen

```
<add key="ActiveDirectory.Attributes.upn" value="userPrincipalName" />
```

4 Opsætning af claims

Når man har oprettet Tjenesteudbyder-forbindelsen til Danmarks Miljøportal, skal man opsætte claims inde i OS2faktor administrationsportalen for denne tjenesteudbyder.

Slutresultatet skulle gerne se cirka sådan her ud



Type	Attribut	Én værdi	Værdi	Parameter	Handlinger
Personligt	http://www.miljoeportal.dk/userPrincipalName		upn		
Personligt	urn:oid:2.5.4.3		alias		
Personligt	urn:oid:0.9.2342.19200300.100.1.3		email		
Personligt	urn:oid:2.5.4.4		lastname		
Personligt	http://www.miljoeportal.dk/givenName		firstname		
Personligt	urn:oid:0.9.2342.19200300.100.1.1		userId		
Fast	urn:oid:2.5.4.10		Digital Identity		
Fast	dk:gov:saml:attribute:CvrNumberIdentifier		12345678		
Avanceret	http://www.miljoeportal.dk/objectGUID		BINARY_UUID(VALUE(user.uuid))		
Fast	http://www.miljoeportal.dk/whenCreated		20240503070152.0Z		
Avanceret	Name ID		JOIN(VALUE('Xri://@DK-XRI*'), VALUE('12345678/'), VALUE('20240503070152.0Z/'), BINARY_UUID(VALUE(user.uuid)))		
Avanceret	dk:gov:saml:attribute:UniqueAccountKey		JOIN(VALUE('Xri://@DK-XRI*'), VALUE('12345678/'), VALUE('20240503070152.0Z/'), BINARY_UUID(VALUE(user.uuid)))		

Bemærk at der her anvendes 12345678 som CVR nummer, og ”Digital Identity” som organisationsnavn. Disse skal selvfølgelig tilpasses så de matcher kommunens opsætning.

Faste claims

Der skal opsættes 2 faste claims, som angiver hvilken organisation brugerne kommer fra. Her skal angives kommunens CVR nummer og kommunens Navn.

For CVR nummeret sættes nedenstående værdi som Claim navn (og CVR nummeret som værdi)

dk:gov:saml:attribute:CvrNumberIdentifier

hvilket indtastes i skærmbilledet på denne måde

Og for Kommunens navn, anvendes nedenstående som Claim navn

urn:oid:2.5.4.10

Bemærk at selvom DMPs dokumentation af claim kontrakten ikke nævner det, forventer de også at modtage et whenCreated timestamp. Umiddelbart skal det ikke bruges til noget, så sæt bare en fast værdi for alle brugere, dvs opret et Fast claim med claim navn

http://www.miljoeportal.dk/whenCreated

og sæt værdien til (eller hvad man nu vælges som timestamp for alle ens brugere)

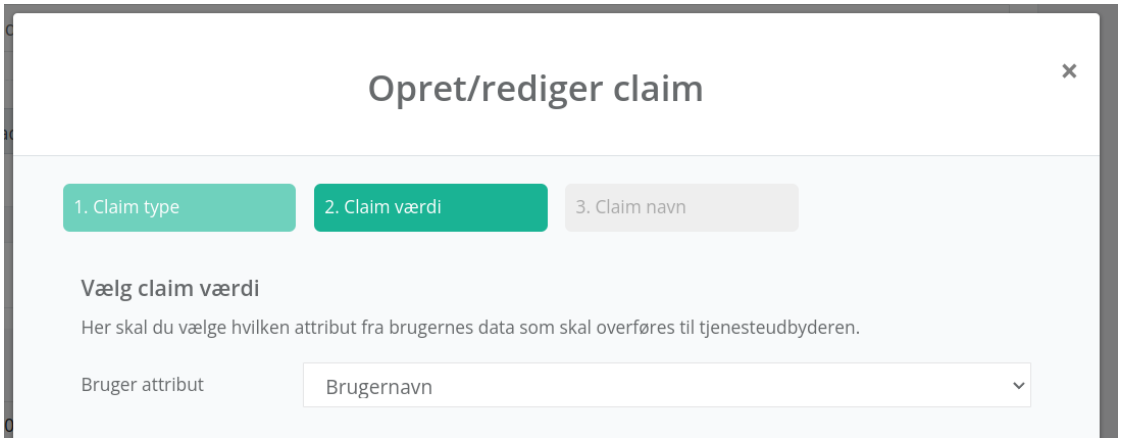
```
20240503070152.0Z
```

Personlige claims

Der skal oprettes 6 personlige claims, som angiver oplysninger om den bruger der logger ind. Disse opsættes på følgende måde

1 – Brugernavn

Til brugernavnet vælges ”Brugernavn” i dropdown’en, som vist her



Og som Claim navn, angives

urn:oid:0.9.2342.19200300.100.1.1

som vist her

2 – Fornavn

Fornavn opsættes på samme måde (dog vælges Fornavn fra dropdown listen), og der indtastes følgende værdi som Claim navn

http://www.miljoeportal.dk/givenName

3 – Efternavn

Tilsvarende her, hvor man vælger Efternavn fra dropdown listen, og angiver denne værdi i Claim navn

urn:oid:2.5.4.4

4 - Alias

Dette er brugerens fulde navn, og man kan enten vælge Navn fra dropdown listen, eller man kan vælge Kaldenavn (Navn er folkeregisternavn, Kaldenavn er displayName/kaldenavn fra ens kildesystem).

Som Claim navn angives

urn:oid:2.5.4.3

5 - Email

Her vælges email i dropdown listen, og som Claim navn angives

urn:oid:0.9.2342.19200300.100.1.3

6 - UPN

Her er det vigtigt at man har indlæst UPN fra sit kildesystem ind i OS2faktor Login. Hvis man har, kan man vælge UPN fra dropdown listen (ellers skal man have indlæst værdien først).

Som Claim navn angives

http://www.miljoeportal.dk/userPrincipalName

Avancerede claims

Endeligt skal der opsættes 2 avancerede claims. De vedrører begge brugerens identitet. Da miljøportalen både skal have et brugernavn (til opslag i rettighedsdatabasen, som vedligeholdes af fx OS2rollekatalog), samt et unikt UUID, opsættes disse på følgende måde.

1 – Name ID

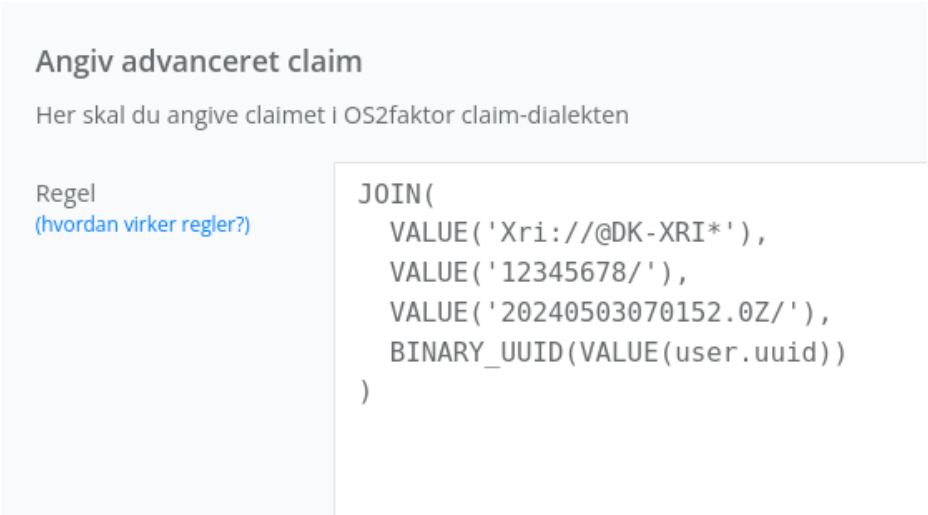
Dette claim er specielt, og overskriver en evt værdi man har valgt i Tjenesteudbyder-opsætningen i OS2faktor Login under dropdown'en Name ID øverst i opsætningsbilledet. Årsagen er at Miljøportalen skal have NameID leveret på et meget specifikt format.

Vælg her en avanceret regel, og angiv "Name ID" som Claim navn, som vist nedenfor

Som avanceret claim regel indtastes følgende, som vist nedenfor

```
JOIN(
  VALUE('Xri://@DK-XRI*'),
  VALUE('12345678/'),
  VALUE('20240503070152.0Z/'),
  BINARY_UUID(VALUE(user.uuid))
)
```

Bemærk her at 12345678 skal udskiftes med kommunens CVR nummer. Den efterfølgende talværdi er bare et timestamp – her kan stå hvad som helst, og ovenstående vil fungere, så tag evt bare den værdi (skal dog være identisk med den værdi der er valgt i whenCreated claimet længere oppe).



2 – UniqueAccountKey

Der skal sendes et ekstra claim, med præcist samme indhold som Name ID. Dette oprettes på samme måde, men som claim navn sættes i stedet

```
dk:gov:saml:attribute:UniqueAccountKey
```

3 – Brugernavn

Det sidste claim der er nødvendigt, er brugerens unikke ID, som opsættes på følgende måde

Som Claim navn anvendes

http://www.miljoeportal.dk/objectGUID

og som claim regel indtastes

```
BINARY_UUID(VALUE(user.uuid))
```

Som illustreret nedenfor