OS2faktor Login

AD FS konverteringsguide

**Version**: 1.0.0

**Date**: 10.09.2024

**Author**: BSG

Indhold

[1 Indledning 3](#_Toc176858283)

[1.1 Mini-ordbog 3](#_Toc176858284)

[2 Begrænsning af adgang til tjenesteudbyder 4](#_Toc176858285)

[3 Styring af hvornår MFA skal anvendes 5](#_Toc176858286)

[3.1 Opsætning af kendte netværk 6](#_Toc176858287)

[3.2 Special omkring NSIS 6](#_Toc176858288)

[4 Opsætning af claims 6](#_Toc176858289)

[4.1 Hvad er claims 7](#_Toc176858290)

[4.1.1 NameID claimet 7](#_Toc176858291)

[4.1.2 Alle andre claims 8](#_Toc176858292)

[4.2 Udfordringer med claims i AD FS 9](#_Toc176858293)

[4.3 Personlige claims i OS2faktor 12](#_Toc176858294)

[4.4 Faste claims i OS2faktor 13](#_Toc176858295)

[4.5 Gruppe-baserede claims i OS2faktor 13](#_Toc176858296)

[4.6 Opslag i OS2rollekatalog 15](#_Toc176858297)

[4.7 Avancerede claims i OS2faktor 16](#_Toc176858298)

[5 Eksempler på migrering af AD FS til OS2faktor 17](#_Toc176858299)

[5.1 BeKey 17](#_Toc176858300)

[5.1.1 Rettigheder 17](#_Toc176858301)

[5.1.2 Bruger-oplysninger 20](#_Toc176858302)

[5.2 Aula 22](#_Toc176858303)

[5.2.1 AssuranceLevel 23](#_Toc176858304)

[5.2.2 CvrNumberIdentifier 23](#_Toc176858305)

[5.2.3 Name ID 24](#_Toc176858306)

[5.2.4 UniLoginIdentifier 25](#_Toc176858307)

[5.2.5 CprNumberIdentifier 25](#_Toc176858308)

# Indledning

Ved anvendelsen af OS2faktor Login produktet, kan man have et ønske om migrere eksisterende tjenester væk fra sin nuværende AD FS server, og over til OS2faktor Login.

I den forbindelse kan det være en udfordring at gennemskue præcist hvordan de indstillinger der er i AD FS, kan oversættes til tilsvarende indstillinger i OS2faktor Login.

Dette dokument vil primært fokusere på claim opsætning, men vil også kort dække de andre aspekter af AD FS til OS2faktor konverteringen.

## Mini-ordbog

AD FS er et engelsk produkt, og de forskellige indstillinger og begreber fremgår alle på engelsk i brugergrænsefladen til AD FS. Tilsvarende er OS2faktor Login et dansk produkt, med danske betegnelser i brugergrænsefladen. Her følger en kort oversættelse af de centrale begreber i opsætningen i de to produkter

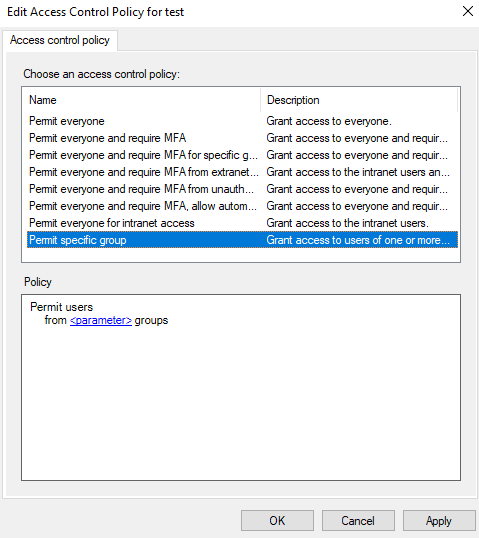
|  |  |  |
| --- | --- | --- |
| **AD FS** | **OS2faktor Login** | **Kort beskrivelse** |
| Relying Party Trust | Tjenesteudbyder | Fagsystemer koblet til ens Identity Provider |
| Access Control Policy | Begrænset adgang | En måde at afgrænse hvem der må foretage login – i AD FS anvendes typisk medlemsskab af sikkerhedsgrupper, mens OS2faktor kan kombinere forskellige aspekter, herunder også sikkerhedsgrupper |
| Claims Issuance Policy | Claims | Hvilke informationer der sendes til tjenesteudbyderen når brugeren foretager et login |
| Authentication Methods | OS2faktor MFA | Understøttede MFA klienter. AD FS har en plugin-arkitektur, mens OS2faktor gør brug af de understøttede MFA klienter i OS2faktor infrastrukturen |
| Claims Provider Trust | ”NemLog-in” | AD FS kan konfigureres til at delegere login til en anden Identity Provider – OS2faktor understøtter kun dette for delegering til NemLog-in for MitID baseret login |
| Attribute Store | Coredata API | AD FS har en plugin-arkitektur til at hente ekstra brugeroplysninger fra 3.parts databaser under login – OS2faktor tillader indlæsning af vilkårlige brugeroplysninger direkte i OS2faktor brugerdatabasen via Coredata API |
| Identifier | EntityId | Alle tjenester har et unikt ID – dette kaldes for ”EntityId” i SAML, og er det begreb OS2faktor generelt bruger om tjenesters unikke ID, uagtet teknologi – hvor AD FS anvender det mere generisk term ”Identifier”. |

# Begrænsning af adgang til tjenesteudbyder

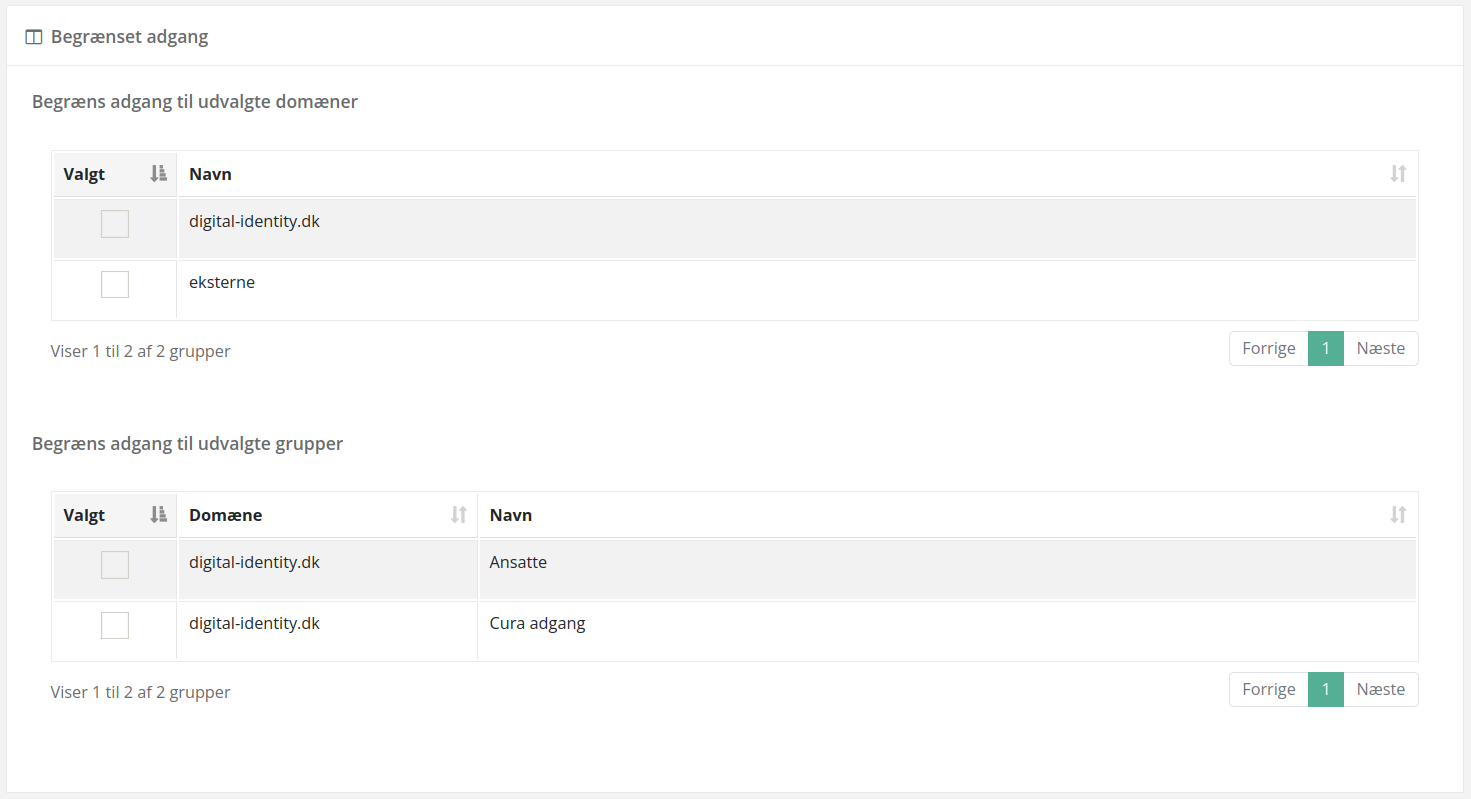
De fleste tjenesteudbydere forventer at brugeren har en eller flere roller tildelt, før de kan få adgang til tjenesten, og hermed er der en naturlig begrænsning i hvem der kan gennemføre et succesfuldt login (ingen rolle, ingen adgang).

Men der findes også tjenesteudbydere hvor man kan foretage et login uden at være tildelt en explicit rolle, og her kan det være ønsket at begrænse adgangen til udvalgte brugere.

I AD FS styres det via dette skærmbillede



OS2faktor tillader opsætningen af begrænset adgang direkte under tjenesten, hvor nedenstående sektion vises.



Man kan altid afgrænse adgangen på domæne-niveau, mens sektionen omkring grupper kun er synlig hvis man har valgt at indlæse AD sikkerhedsgrupper ind i OS2faktor.

Man kan angive både domæner og grupper, og der gives adgang til enhver bruger som er medlem af mindst én af de tilvalgte grupper (hvis grupper er anvendt som begrænsning) samt kommer fra mindst én af de valgte domæner (hvis domæner er anvendt som begrænsning).

# Styring af hvornår MFA skal anvendes

AD FS har forskellige styringsparamtre for hvornår MFA skal anvendes under login, og de opsættes i nedenstående skærmbillede

A screenshot of a computer screen

Description automatically generated

Default indstillingen i OS2faktor, når man opretter en ny tjenesteudbyder, er at der kun anvendes MFA til login hvis tjenesten explicit beder om det. SAML teknologien understøtter af tjenester kan efterspørge MFA, og fx anvender AULA denne teknologi til at tvinge et MFA login hvis brugeren forsøger at tilgå særligt følsomme områder af AULA.

Den indstilling der vælges under tjenesteudbyderen, for at lade tjenesten selv bestemme, er

A close up of a computer screen

Description automatically generated

Her vil følgende værdier, resultere i følgende opførsel under login

* **Kun ved step-up**. Her vil login næsten altid være uden MFA – kun i særlige tilfælde, hvor tjenesten explicit efterspørger MFA, vil brugeren skulle lave et 2-faktor login
* **Altid**. Her skal brugeren gennemføre et 2-faktor login ved login, uagtet hvad tjenesten evt beder om, og dermed aktivere sin MFA klient
* **Altid for ukendte netværk**. Denne funktion anvendes hvis man ønsker at brugerne skal anvende MFA hvis de kommer fra ukendte/eksterne netværk, mens de kan slippe for login uden MFA hvis de kommer fra et kendt/internt netværk

## Opsætning af kendte netværk

AD FS kører på kommunens interne netværk, og kan nemt se om en bruger sidder på samme netværk som den selv gør, eller om der er tale om en ekstern bruger. OS2faktor har ikke helt samme mulighed, så her skal man opsætte hvilke IP adresse der udgør det ”interne netværk”, så OS2faktor kan se hvor brugeren hører til (intern / ekstern netværk).

Kendte netværk kan anvendes i ovenstående regler for MFA, og opsættes under menupunktet ”Kendte netværk” under Konfiguration i højre-menuen.

A screenshot of a computer

Description automatically generated

Man angiver IP-adresser eller segmenter, via CIDR notationen, og en anbefaling er at opsætte de offentlige IP-adresser som kommunen anvender. Herefter kan man vælge om brugere der sidder på kommunens netværk, skal have andre sikkerhedsparametre under login (login uden MFA på udvalgte tjenester) baseret på disse IP-adresser til at identificere kommunens netværk.

## Special omkring NSIS

Hvis en tjeneste er underlagt NSIS, og der stilles krav om et bestemt NSIS sikringsniveau under login, så er ”Tvungen to-faktor login” dialogen ikke synlig, og man kan ikke styre hvorvidt brugeren præsenteres for MFA under login – dette styres 100% af NSIS sikringsniveauet. For tjenesteudbydere man selv opsætter i OS2faktor Login, har man muligheden for at angive at tjenesten skal anvende et NSIS loginflow, ved at ændre på denne indstilling – hvis man gør det, så forsvinder ”Tvungen to-faktor login” dialogen også

A close-up of a computer screen

Description automatically generated

Man bør kun sætte det krævede NSIS niveau, hvis det er fordi man ønsker at begrænse login til tjenesten til de brugere som har en erhvervsidentitet, og samtidig ønsker at sætte et bestemt sikkerhedsniveau (fx NSIS Betydlig) under login.

# Opsætning af claims

Opsætningen af claims i OS2faktor er forholdsvist simpelt, men er nok det område der adskiller sig mest fra hvordan AD FS fungerer. De første 2 afsnit forsøger at afdække hvad claims er, og hvordan claimopsætning kan være problematisk med udgangspunkt i en vejledning til AD FS og/eller en eksisterende AD FS opsætning.

## Hvad er claims

Claims er grundlæggende oplysninger som tjenesten modtager om brugeren, når brugerne laver et login. Typisk inderholder claims oplysninger om hvem brugeren er, hvilke adgange brugeren har og evt supplerende oplysninger om brugerens organisatoriske indplacering.

Der er dog ingen begrænsninger i hvad en tjeneste kan finde på at stille krav om, så der kan være nogle ret eksotiske claims i særlige tilfælde.

### NameID claimet

Der findes ét claim som håndteres særligt i OS2faktor, modsat AD FS hvor det håndteres på lige fod med alle andre claims, og det er brugerens identitet.

I SAML udstedes dette claim også adskilt fra de andre, og et forsimplet SAML token vil se sådan her ud

A computer code with text

Description automatically generated

Det er standard i SAML, at brugerens identitet sendes i feltet NameID, som skal identificere den bruger der logger ind. Formatet kan være op til den enkelte tjeneste, og værdien kan være alt fra AD brugernavn, email adresse, upn, cpr nummer, eller noget andet som unikt identificerer brugeren overfor tjenesten.

Alle andre claims (oplysninger om brugeren), sendes i den sektion der hedder AttributeStatement, og er en lang værdiliste med alle de claims der ellers er opsat på brugeren.

I OS2faktor håndteres NameID adskilt fra de andre claims, i denne sektion

A screenshot of a computer

Description automatically generated

Man kan her angive formatet på NameID værdien via en dropdown-liste. Det er sjældent af tjenester kræver et specielt format, så hvis det ikke er nævnt explicit, så bare anvend default, der er ”persistent” som vist ovenfor.

Selve NameID værdien vælges også fra en dropdown, og her kan man vælge mellem alle de oplysninger OS2faktor kender på brugeren – typisk vil det være Brugernavn eller E-mail der skal anvendes, men se hvad leverandøren angiver i deres vejledning. Hvis de ikke har angivet noget, så bare sæt den til Brugernavn.

Her er det vigtigt at bemærke, at hvis leverandøren har lavet en ren AD FS opsætningsvejledning, så kan informationen være angivet på forskellige måder. Fx kan det være at leverandøren har angivet det med screenshot på denne måde

A screenshot of a computer

Description automatically generated

Hvor man kan se at leverandøren her ønsker at brugerens samAccountName skal overføres som ”Name ID”, og så kan man anvende den tilsvarende værdi i OS2faktor dropdown’en (samAccountName er brugerens AD brugernavn, så vælg Brugernavn i dropdown’en i OS2faktor). Det kan også være at leverandøren har angivet hvad de ønsker at NameID skal sættes til via det tekniske ID på feltet i AD FS, hvilket er

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier>

Fx kan det være at leverandøren har angivet en tabel i deres dokumentation, og har skrevet at ovenstående skal sættes til brugerens email adresse. Så skal man tilsvarende angive i OS2faktor at Name ID skal sættes til ”E-mail”.

Her er et eksempel på hvordan en leverandør evt kan give denne information

A close-up of a phone number

Description automatically generated

Her kan vi se i første række, at der er tale om ”Name ID”, og at den værdi som leverandøren forventer er brugerens UPN (så vælg upn i dropdown-listen i OS2faktor).

### Alle andre claims

Alle claims der ikke er Name ID, sendes som nævnt i AttributeStatement sektionen i det token der udstedes. Disse claims kan indeholde flere værdier, så fx er følgende token et helt normalt og lovligt token. Oftest set claims med flere værdier i rolle/gruppe claims

A computer screen shot of text

Description automatically generated

Et claim består af et ”name”, der identificerer hvad claimet handler om, samt en ”value” der angiver værdien af det udstedte claim. Fx kan et claim name være ”e-mail” og værdien ”bsg@digital-identity.dk”.

I AD FS er claimopsætningen typisk opsat via nedenstående skærmbillede

A screenshot of a computer

Description automatically generated

Tilsvarende opsættes de i OS2faktor (minus Name ID der håndteres særskilt) i en tilsvarende tabel

A screenshot of a computer

Description automatically generated

I de følgende sektioner, gennemgås de forskellige måder at opsætte claims på i OS2faktor, og hvordan det reflekter ligende opsætninger i AD FS, men først en snak omkring udfordringer med vejledninger lavet specifikt til AD FS.

## Udfordringer med claims i AD FS

AD FS har en brugergrænseflade, der simplificerer arbejdet med claims, men som også samtidig skjuler vigtig information. Hvis vi tager udgangspunkt i denne opsætning

A screenshot of a computer

Description automatically generated

Hvor første kolonne angiver hvilket felt der læses fra AD, og den anden kolonne angiver hvilket ”claim name” der udstedes i tokenet, så kunne man ledes til at tro at et udstedt token ville se sådan her ud

A computer screen shot of a program

Description automatically generated

Hvor brugerens email-adresse vil komme i et claim der har navnet ”E-Mail Address”, og tilsvarende at brugerens navn vil stå i et claim der hedder ”Common Name”, da det er hvad AD FS brugergrænsefladen fortæller os.

Det er desværre ikke sandt, og det udstedte token fra AD FS ser i stedet sådan her ud

A computer screen shot of text

Description automatically generated

Dette skyldes at AD FS brugergrænseflade arbejder med ”pæne navne” for de faktiske værdier. Dvs at det som SKAL stå i det udstedte tokens ”name” felt, har et langt mere teknisk navn end AD FS lader en tro.

Dette kan være en udfordring hvis man forsøger at konvertere en eksisterende AD FS opsætning til OS2faktor, eller hvis den vejledning man har primært består af AD FS termer eller screenshots.

Der er heldigvis en måde at få de tekniske ID’er ud fra AD FS – her kan man åbne claim opsætningen, og trykke på ”View rule language...” knappen vist nedenfor

A screenshot of a computer

Description automatically generated

Når man gør det, så får man de faktiske værdier vist på skærmen, omend i lidt én lang køre

A screenshot of a computer program

Description automatically generated

Det er her types = (....) vi er interesseret i. Klip det over i en notepad, og tilføj linebrud ved komma, så det er nemmere at overskue

A close-up of a computer screen

Description automatically generated

Heldigvis kommer værdierne i den angive rækkefølge – så man kan her pille de værdier ud man skal bruge til opsætningen i OS2faktor.

Endelig kan der være såkaldte avancerede claims i AD FS – disse er næsten altid lavet fordi man ønsker at flette forskellige data sammen, eller fordi man har brug for at lave opslag i 3.parts systemer (fx OS2rollekatalog). Disse bør være fint understøttet i OS2faktor, men se evt afsnittet for avancerede claims i OS2faktor nedenfor, for at håndtere konverteringen af disse.

Et avanceret claim i AD FS, er claims der er opsat på denne måde, og har et AD FS specifikt sprog til at udstede claims (OS2faktor har et tilsvarende beskrevet i de næste afsnit)

A screenshot of a computer

Description automatically generated

## Personlige claims i OS2faktor

Når man opsætter et claim i OS2faktor, så præsenteres man med følgende dialog

A screenshot of a computer

Description automatically generated

Her kan man vælge mellem forskellige typer af claims, og hvis man vælger ”Personligt”, så har man mulig for at vælge mellem forskellige attributter direkte på brugeren, som skal sendes under login. Det er fx denne type claim man bruger til at sende e-mail adresse, upn, personnummer og andre personlige oplysninger om brugeren til tjenesten under login.

Først skal man vælge den information brugeren som skal indgå i tokenet

A screenshot of a computer

Description automatically generated

Bemærk at man her kan angive at der kun må sendes én værdi, hvis brugeren har flere sådanne data (fx flere e-mail adresser, flere medarbejdernumre, osv). Normalt er det ikke nødvendigt at sætte hak i denne checkboks.

Endeligt skal man angive hvad claimet skal have af navn. Det er her det er vigtigt at man finder ud af præcist hvad tjenesten forventer. Hvis deres vejledning er AD FS baseret, og der er angivet ”pæne” navne for claims, fx ”E-Mail Address”, så er det formodentligt de tekniske ID’er der gemmer sig bag facaden i AD FS, som skal anvendes

A screenshot of a computer

Description automatically generated

Endeligt trykkes bare ”Tilføj claim”, og opsætningen for dette claim er gemt, og fremgår nu i den samlede tabel over de opsatte claims.

## Faste claims i OS2faktor

Faste claims minder om personelige claims i opsætning, men indeholder statiske værdier som er ens for alle brugere. Det kan fx være at tjenesten ønsker at modtage kommunens CVR nummer under login, og så vil typisk opsætte dette som et ”Fast” claim.

A white background with black dots

Description automatically generated

Modsat personlige claims, hvor man kan vælge hvilke data der skal sendes fra en dropdown liste, skal man her angive den faste værdi der skal sendes. Fx hvis det er CVR nummer, kunne man angive

A screenshot of a phone

Description automatically generated

Endeligt skal man angive et navn til claimet, hvilket er præcist som for personlige claims – det er her vigtigt at man identificerer det præcise navn som tjenesten forventer.

## Gruppe-baserede claims i OS2faktor

Gruppe-baserede claims er kun muligt at vælge, hvis man har indlæst grupper ind i OS2faktor. Hvis man ikke har indlæst nogen grupper, er valgmuligheden skjult.

Hvis man har grupper indlæst, kan man vælge denne type claim

A white background with black dots

Description automatically generated

Når man vælger et gruppe-baseret claim, skal man angive hvilken gruppe claimet er bundet til – i praksis udstedes dette claim kun for brugere som er medlem af denne gruppe.

A screenshot of a computer

Description automatically generated

Den konkrete værdi der skal sendes kan afvige fra gruppes navn, så man skal explicit angive hvilken værdi der skal stå i tokenet hvis brugeren er medlem af denne sikkerhedsgruppe. I eksemplet er der en gruppe der hedder ”BeKey administratorer”, og alle der er medlem af denne, får udstedt et claim med værdien ”ADMINISTRATOR” indeholdt.

Endelig skal der angives hvad claimet skal hedde – dvs præcist som for de to forrige typer af claims er det vigtigt at det er den præcise værdi som tjenesten forventer, og her kan man bruge nogle af de nævnte tricks til at udlede dette fra en AD FS baseret vejledning. Man kan også være heldig at det står explicit i vejledningen.

A screenshot of a computer

Description automatically generated

Bemærk at hvis man udsteder flere claims med samme claim-navn, så samles de i ét udstedt claim, som vist i eksemplet nedenfor

A computer code with text

Description automatically generated

## Opslag i OS2rollekatalog

Hvis OS2faktor er opsat med en integration til OS2rollekatalog, kan der også udstedes claims baseret på opslag i OS2rollekatalog systemet. Hvis der ikke er opsat en integration til OS2rollekatalog, er denne valgmulighed ikke synlig

A white background with black text

Description automatically generated

Når man vælger et claim baseret på et opslag i OS2rollekatalog, er slut-resultatet stadig er at der udstedes ét claim, indeholder et claim-navn og en (eller flere) claim-værdier.

Der er dog en række valg der skal tages, for at lave præcist det opslag man ønsker i OS2rollekatalog. Brugergrænsefladen i OS2faktor forsøger at guide en til at lave dette opslag korrekt, via nedenstående skærmbillede

A screenshot of a computer

Description automatically generated

Uagtet hvilket opslag man vælger i den første dropdown, skal man angive ID’et på det it-system som man ønsker at lave rolleopslag i. Her kan man både angive det tekniske ID på it-systemet i OS2rollekatalog, og man kan angive nummer-ID’et på it-systemet i OS2rollekatalog – begge vil fungere. I OS2rollekatalog kan man se det tekniske under feltet ”System-id” når man ser detaljer på et it-system

A screenshot of a computer

Description automatically generated

Når man har valgt typen af opslag, og angivet ID’et på det it-system der skal laves opslag i, skal man igen, som på de andre claims, angive hvilket navn som claimet skal have

A screenshot of a computer

Description automatically generated

Hvis man laver et opslag på en bruger som har flere roller tildelt, så vil man få ét claim udstedt, men med flere værdier under sig, lige som i de andre eksempler ovenfor.

Det mest almindelige opslag i OS2rollekatalog er ”Alle tildelte systemroller”, hvilket giver præcist listen af tildelte rettigheder i det angivne it-system. De andre opslagstyper anvendes kun i særlige tilfælde, hvor man har brug for en alternativ formatering af data.

## Avancerede claims i OS2faktor

Den sidste type af claims man kan udstede i OS2faktor, er avancerede claims. Disse minder om den type af claims man kan opsætte i AD FS, hvor man kan angive hvad der skal udstedes ud fra et claim sprog.

A white background with black text

Description automatically generated

Når man vælger et avanceret claim, så skal man angive hvad man ønsker udstedt som claim via et kodesprog. Der er en guide til dette som tilgås ved at klikke på linket ”hvordan virker regler?”

A screenshot of a phone

Description automatically generated

I stedet for at gengive den fulde vejledning her, henvises blot til den eksisterende vejledning for avancerede claims, og der vises et simpelt eksempel nedenfor, på hvad man kan bruge avancerede claims til

A screenshot of a computer

Description automatically generated

Ovenstående eksempel fletter 3 værdier sammen til én ny værdi, som så kan udstedes som et claim. Her tages brugerens brugernavn (userId), som flettes sammen med en bindestreg, efterfulgt af brugerens navn – i praksis udstedes så et claim med værdien (hvis det var Brian Storm Graversen med brugernavnet bsg)

bsg – Brian Storm Graversen

Man kan bruge avancerede claims til at flette, konvertere eller på andre måder påvirke data, inden de udstedes som et claim.

Som altid skal et claim have et navn, hvilket vælges på den sidste side når man opsætter et avanceret claim.

# Eksempler på migrering af AD FS til OS2faktor

Nedenfor er et par eksempler, med udgangspunkt i eksisterende vejledninger til disse systemer, hvor man kan se hvordan en opsætning skal laves i OS2faktor

## BeKey

Vejledningen til BeKey er udleveret af Albertslund Kommune, og der er anvendt version 1.5 af opsætningsguiden til BeKey.

Generelt er vejledningen god, da den ikke er lavet specifikt til AD FS, men angiver med eksempler hvordan man kan opsætte forbindelsen til BeKey både fra AD FS, Azure AD og Safewhere Identify produkterne. Dette giver os en række informationer, så vi ikke alene er begrænset til AD FS opsætningsvejledningen. Da denne konverteringsguide specifikt er lavet til at flytte systemer fra AD FS til OS2faktor, tager vi dog udgangspunkt i AD FS delen af BeKey vejledningen i dette eksempel 😊

### Rettigheder

BeKey vejledningen har en tabel på side 4, der angiver at man bør oprette 3 sikkerhedsgrupper til at repræsentere rollerne i BeKey. Man kunne godt undlade sikkerhedsgrupper her, og i stedet opsætte rollerne direkte i OS2rollekatalog, eller styre det på en anden måde, men vi anvender eksemplet med grupper, og antager at de 3 grupper er indlæst i OS2faktor, under navnene

* BeKey-Administrators
* BeKey-Users
* BeKey-Locksmiths

Endeligt understøtter BeKey også at man kan styre adgangen til hver ”dør” via sikkerhedsgrupper. Mekanismen er identisk med de overordnede grupper, og vi ignorerer derfor dette aspekt i konverteringsguiden.

AD FS claimopsætningen starter på side 10 i BeKey guiden, og her angives det at man skal udstede claims via ”Send Group Membership as a claim” i AD FS opsætningen

A screenshot of a screenshot of a group

Description automatically generated

Her er der angivet et eksempel på opsætningen i BeKey guiden, hvor man peger på en bestemt sikkerhedsgruppe, og så opsætter det udgående claimtype (claim navn) til at være ”Role” og den udgående værdi til at være ”administrator”, som illustreret nedenfor

A screenshot of a computer screen

Description automatically generated

”Claim rule name” har ingen effekt, og er bare en måde at give claimet et internet navn i AD FS, så man kan referere til den – der er ikke brug for noget tilsvarende i OS2faktor. De vigtige informationer er

* Hvilken gruppe er udpeget (her bekey\_admin gruppen)
* Hvad er claim-navnet (her ”Role” – mere om det nedenfor)
* Hvad er claim-værdien (her ”administrator”)

Problemet er her at man kunne ledes til at tro at man skal udstede et claim med navnet ”Role”, men AD FS snyder lidt her, og den faktiske værdi er

<http://schemas.microsoft.com/ws/2008/06/identity/claims/role>

Hvis man har adgang til en AD FS, og gemmer ovenstående claim, og så trykker på ”View rule language...” som vist nedenfor

A screenshot of a computer

Description automatically generated

Så får man vist de tekniske detaljer, og kan se at claimnavnet ikke er ”Roles”, men i stedet det lange tekniske ID vist ovenfor

A screenshot of a computer

Description automatically generated

Heldigvis er BeKey her en af de gode vejlednings-skrivere, og de har et appendix i bunden af dokumentet (Appendix A), hvor man også kan se de fulde værdier for hvert claim, som vist med dette screenshot taget direkte fra deres vejledning

A screenshot of a computer error

Description automatically generated

I OS2faktor vil vi opsætte dette claim via et Gruppe claim, som vist med screenshots nedenfor. Bemærk at vi vil opsætte 3 næsten identiske claims, én for hver gruppe (potentielt flere hvis man gør brug af grupper for hver dør der skal gives adgang til).

A white background with black text

Description automatically generated

Udpeg gruppen og angiv værdien ”administrator” for denne gruppe

A screenshot of a computer

Description automatically generated

Angiv det tekniske ID på claimet

A screenshot of a computer

Description automatically generated

Hvilket bør resultere i et opsat claim, jf OS2faktor claim tabellen, der ser sådan her ud

A screenshot of a computer

Description automatically generated

### Bruger-oplysninger

På side 17 i BeKey vejledningen starter dokumentation af hvilke oplysninger om brugeren der skal medsendes, her anvendes en standard gennemstilling af oplysninger fra AD, hvilket opsættes med denne type claim i AD FS

A screenshot of a computer

Description automatically generated

I BeKey vejledningen er dette givet ved denne tabel

A close-up of a phone number

Description automatically generated

Og vi ser her at en af disse claims er Name ID (sat til User-Principal-Name), som skal opsættes i OS2faktor via denne dropdown

A screenshot of a computer

Description automatically generated

Af de resterende claims er det kun AD brugernavnet som er krævet, men fælles for dem alle er at de nævnte værdier i kolonne 2 er ”pæne navne”, og ikke de faktiske tekniske ID’er der skal anvendes. Her kan man enten læne sig op af Appendix A i BeKey vejledningen, som har lavet en fin oversætning af de claims de ønsker, inkl de tekniske ID’er, eller man kan opsætte det i AD FS som nævnt i flere eksempler i denne guide, og så kigge på detaljerne for claimet, så man se de faktiske værdier.

En standardopsætning af OS2faktor har SAM-AccountName (brugernavn), Given-Name (fornavn), Surname (efternavn), E-Mail-Addresses (E-mail), men desværre ikke mobilnummer, så hvis man ønsker denne værdi, skal man sikre at den også overføres til OS2faktor. Det er dog ikke et krævet felt.

Alle disse kan opsættes som personlige claims på denne måde

A screenshot of a computer

Description automatically generated

Vælg en attribut på brugerne, fx Fornavn

A screenshot of a computer

Description automatically generated

Angiv navnet på det claim der skal udstedes (AD FS tjek eller kig i Appendix A)

A screenshot of a message

Description automatically generated

Gem og fortsæt så med det næste personlige claim til de alle er oprettet.

Herefter er BeKey opsat og klar til brug via OS2faktor Login.

## Aula

AULA har publiceret en guide til opsætning her

<https://aulainfo.dk/wp-content/uploads/Vejledning-til-Ops%C3%A6tning-af-kommunal-Identity-Provider.pdf>

Guiden har eksempler til AD FS og AzureAD opsætning – vi fokuserer her på guiden til AD FS, og hvordan den kan bruges til at opsætte AULA login via OS2faktor Login.

I kapital 3 i AULA guiden, er der listet hvilke claims der er krævede, og hvilke der er optionelle. Bemærk her at AULA forventer én af de to optionelle claims for en god brugeroplevelse (uden disse skal brugeren ved første login anvende sit MitID for at finde brugerens personnummer).

A screenshot of a computer

Description automatically generated

AULA vejledningen til AD FS tager udgangspunkt i at man opsætter claims via ”custom rules”. Dette er dog sjældent nødvendigt, men det gør dog vejledningen lidt mere generisk, og faktisk nemmere at oversætte til OS2faktor Login.

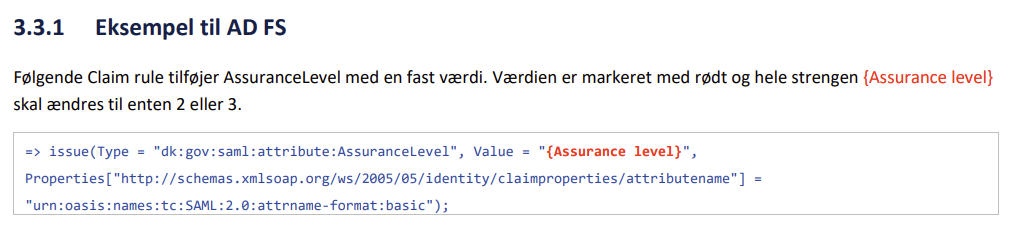
Hvis vi tager de 5 claims individuelt (bemærk man kun skal vælge én af de to sidste)

### AssuranceLevel

Dette claim anvendes af AULA til at se om brugeren er logget ind med 1-faktor login eller 2-faktor login, og hvis en bruger er logget ind med 1-faktor login, og senere forsøger at tilgå særlige følsomme data i AULA, så sendes der et nyt login-request til IdP’en (AD FS eller OS2faktor), med et ønske om et 2-faktor login.

Dette gør at dette claim skal håndteres lidt specielt, da man skal angive et 2-tal hvis der er lavet et 1-faktor login, og et 3-tal hvis der er anvendt et 2-faktor login (beklager tal-forvirringen, det er sådan det virker 😉).

I guiden kommer AULA lidt nemt hen over det, og giver bare dette eksempel



Heldigvis er AssuranceLevel et kendt dansk begreb i offentlige it-tjenester, og OS2faktor har naturlig understøttelse for dette claim. Man kan slå det til ved at sætte flueben i denne setting i OS2faktor tjenesteudbyder-skærmbilledet.

A close up of a word

Description automatically generated

AssuranceLevels som de anvendes i Danmark, er inspireret af National Institute of Standards and Technology (NIST), og disse AssuranceLevels kaldes også for NIST sikringsniveauer på dansk. Sæt blot hak i ovenstående, så udsteder OS2faktor automatisk et AssuranceLevel claim med værdien 2 eller 3, afhængig af om brugeren har lavet 1-faktor eller 2-faktor login.

### CvrNumberIdentifier

Når man logger ind i AULA, skal man fremsende det CVR nummer som hører til kommunen. Dette er angivet som eksempel i AULA vejledningen på denne måde (igen som et AD FS custom claim)

A screenshot of a computer code

Description automatically generated

CVR nummeret er det samme for alle brugere, så i OS2faktor vil vi opsætte det som et Fast claim, og vi kan i ovenstående screenshot fra AULA vejledningen, se at det claim-navn de forventer, er

dk:gov:saml:attribute:CvrNumberIdentifier

så dette opsættes i OS2faktor på denne måde

A white background with black text

Description automatically generated

Her indtastes så kommunens CVR nummer

A screenshot of a phone

Description automatically generated

Og endeligt navnet på claimet, som identificeret via guiden til AULA

A screenshot of a phone

Description automatically generated

### Name ID

Guiden til AULA nævner om Name ID alene at værdien skal være unik, ikke må ændre sig for brugeren, og ikke må genbruges. I deres eksempler angiver de at man kan anvende SID fra AD’et, men i praksis vil enhver unik værdi på brugeren kunne anvendes. Hvis man ikke genbruger AD brugernavne, vil det være en acceptabel model – alternativt kan man sende brugerens UUID eller anden unik identifikation på brugeren.

Opsætningen af Name ID i OS2faktor styres via dropdown, så fx vil disse valg opfylde kravene

A screenshot of a computer

Description automatically generated

Bemærk her at AULA ikke siger noget om hvilket format de ønsker Name ID, så vi vælger bare ”persistent”, da det er det mest almindelige format.

### UniLoginIdentifier

AULA har brug for at kende brugerens kobling til SkoleGrunddata, så de kan lave opslag her og hente supplerende oplysninger på brugeren. Dette kan angives enten med brugerens UniID, eller med brugerens personnummer. Begge modeller virker, men hvis man ønsker at sende UniID med, så er det vigtigt at denne information er indlæst i OS2faktor.

Vi kan se i guiden fra AULA, at det claim de forventer at modtage har denne form

A computer screen shot of a computer code

Description automatically generated

Dvs claimet skal udstedes med navnet

dk:gov:saml:attribute:UniLoginIdentifier

Hvis vi har oplysningen i OS2faktor, så kan der opsættes et personligt claim på denne måde

A screenshot of a computer

Description automatically generated

Her vælges UniID fra dropdown’en

A screenshot of a computer

Description automatically generated

Og navnet på claimet angives så det matcher det fra AULA vejledningen

A screenshot of a computer

Description automatically generated

### CprNumberIdentifier

Hvis UniID ikke er indlæst i OS2faktor, kan man også vælge at sende personnummeret på brugeren, hvilket har samme effekt som UniID’et. Her kan vi i AULA vejledningen se denne regel

A screenshot of a computer

Description automatically generated

Hvorfra vi kan udlede at det claim de forventer at modtage personnummeret i, hedder

dk:gov:saml:attribute:CprNumberIdentifier

Igen kan dette opsættes som et personligt claim på denne måde i OS2faktor

A screenshot of a computer

Description automatically generated

Her vælges personnummer på dropdown’en

A screenshot of a computer

Description automatically generated

Og claim-navnet fra AULA vejldningen angives

A screenshot of a computer

Description automatically generated