netcompany

Version
1.6

Status
Klar til Review

Godkender
Erling Hansen

Forfatter
Lasse Poulsen

KOMBIT

AULA

T0150 - Login og Step-up

© Copyright 2021 Netcompany. Alle rettigheder forbeholdes.

Elektronisk, mekanisk, fotografisk eller anden gengivelse, oversættelse eller kopiering af dette dokument eller dele deraf er ikke tilladt uden forudgående skriftlig tilladelse fra Netcompany.

Dokumenthistorik

Version	Dato	Forfatter	Status	Bemærkninger
0.1	14-04-2018	Lasse Poulsen	Draft	Initial version.
0.2	01-05-2018	Lasse Poulsen	Klar til Review	
0.3	03-05-2018	Lasse Poulsen	Klar til Review	Kommentarer fra KOMBIT adresseret.
0.4	07-05-2018	Lasse Poulsen	Klar til Review	Account Linking beskrevet.
1.1	25-05-2018	Lasse Poulsen	Klar til Review	Account Linking udvidet med mulighed for at sende UNI-Login med i SAML token.
1.2	30-09-2019	Per Josefsen	Klar til Review	Opdateret SAML AD FS claim
1.3	23-10-2019	Casper Kristiansen Vedel	Opdateret	Tilføjet afsnit 2.1.2 om CPR-nummer
1.4	17-11-2020	Morten Rishøj Thomsen	Opdateret	Omnavngivet Context Handler til Fælleskommunal Adgangsstyring.
1.5	04-05-2021	Caspar Oreskov	Opdateret	Tilføjet beskrivelse omkring påkrævet brugersystemrolle i afsnit 2.2
1.6	19-05-2021	Caspar Oreskov	Klar til review	Review af ændringer i afsnit 2.2

Referencer

Reference	Titel	Forfatter	Version
[1]	Beskrivelse af sikkerhedsmodellen i Rammearkitekturen https://share-komm.kombit.dk/P133/Referencedokumenter/STS%20Vilk%C3%A5r/Bilag%202A%20-%20Beskrivelse%20af%20sikkerhedsmodellen%20i%20Rammearkitekturen%20version%202.0.pdf	Kombit	2.0
[2]	OIOSAML Profil version 2.0.9 https://www.digitaliser.dk/resource/2377872	Digitaliserings-styrelsen	2.0.9

© 2021 Netcompany

Indholdsfortegnelse

© 2021 Netcompany

1 Introduktion

Dette notat beskriver hvorledes login til det kommende Aula foregår på det tekniske niveau, og beskriver hvorledes kommuner og institutioner kan koble deres brugere på løsningen.

Dokumentet beskriver primært den tekniske opkobling fra Aula løsningens side, og beskæftiger sig kun i mindre grad med præcist hvorledes en kommune eller institution kan etablere den nødvendige integration til Active Directory, to-faktor login eller migrere eksisterende brugere til en anden løsning.

1.1 Målgruppe

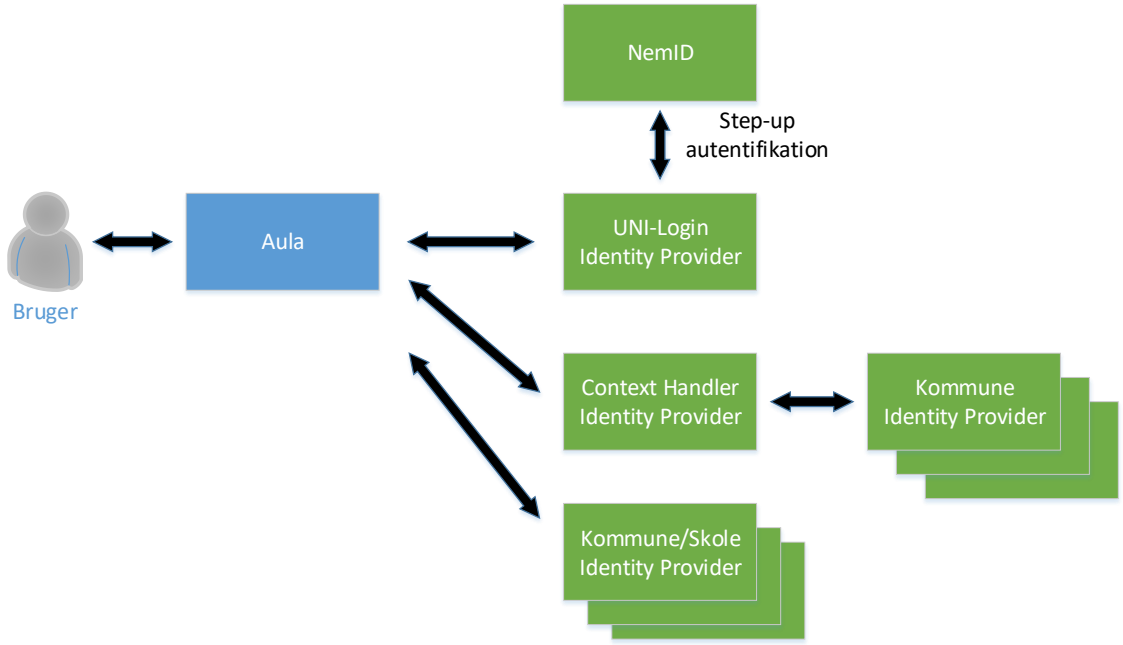
Notatet henvender sig primært til IT-afdelinger i kommuner og institutioner, således at man kan planlægge og forberede brugerstyring og loginløsninger på de behov som Aula har.

© 2021 Netcompany

2 Aula login

Login til Aula foregår via eksterne Identity Providers via SAML 2.0 protokollen som også muliggør Single-Sign-on.

De mulige kilder er illustreret på figuren nedenfor.



Figur 1: Login til Aula via SAML integration med tre mulige kilder (Identity Providers)

Værger (forældre) og børn vil som udgangspunkt altid skulle benytte UNI-Login for at logge på Aula.

For medarbejdere (lærere, pædagoger, ledere, administrativt personale mfl.) vil det være op til den enkelte kommune at fastlægge om der skal benyttes

- UNI-Login
- Login gennem opkobling til støttesystemet Fælleskommunal Adgangsstyring i KOMBIT's fælleskommunale infrastruktur
- Egne Identity Providers som enten kan være
    - En fælles Identity Provider for alle kommunens institutioner
    - Identity Providers for den enkelte institution (eller gruppe af institutioner)

Alle medarbejdere skal som en del af Aula projektet udstyres med et UNI-Login, og den enkelte kommune skal derfor sikre at alle Aula brugere oprettes i UNI-Login. Dette sker normalt i de administrative systemer. Det er derefter op til kommuner og institutioner at afgøre, hvilke medarbejdere der desuden skal oprettes/integreres i henholdsvis Fælleskommunal Adgangsstyring, fælleskommunal Identity Provider og en lokal institutions Identity Provider.

Der er ikke nogen tekniske krav til at en given institution kun benytter én login-kilde, men der kan være brugsmæssige fordele i at institutionens medarbejdere kun har en login-type at forholde sig til.

Det kan således godt lade sig gøre at én og samme bruger kan være integreret i både Fælleskommunal Adgangsstyring, en lokal kommunal Identity Provider og en lokal institutions Identity Provider. Typisk vil man dog kun oprette/integrere den enkelte medarbejders bruger i netop én af disse.

Bemærk, at Aula udelukkende bruger de eksterne Identity Providers til login (autentifikation) og ikke til at styre rettigheder og adgange (autorisation). Rettigheder og adgange styres inde i Aula af kommunale/institutionelle administratorer.

© 2021 Netcompany

Brugergrænsefladen for valg af loginkilde er endnu ikke færdigdesignet, men det vil være muligt for kommuner at lave særlige Aula medarbejderlinks (f.eks. på et intranet) hvor login-kilde er valgt på forhånd, ligesom medarbejdere vil kunne vælge at Aula skal huske sidst anvendte login-valg til næste besøg.

2.1 Mapning til UNI-Login bruger

Aula benytter altid UNI-Login som kilde til stamdata, og derfor er nødt til at mappe alle brugere til en UNI-Login bruger så vi kan placere brugeren i den rigtige kontekst (kommune, institution, rolle m.m.) og påtrykke de adgange og rettigheder som kommunale/institutionelle administratorer har opsat i forhold til UNI-Login brugeren.

For at opnå denne mapning, kan den lokale Identity provider medsende enten brugerens UNI-Login ID eller CPR-nummer i deres bruger-token til Aula. Hvis den lokale Identity Provider *ikke* medsender én af disse værdier, vil Aula i forbindelse med brugerens første login bede brugeren om at logge ind med UNI-Login for at foretage en såkaldt "Account Linking" hvor deres Id fra den lokale Identity Provider oversættes til et UNI-Login ID.

Det er kun nødvendigt at sende én af de to værdier og giver IDP'en lidt mere fleksibilitet, således at man ikke behøver at vedligeholde sine brugeres UNI-Login ID, så længe man blot har deres CPR-nummer eller omvendt.

2.1.1 UNI-Login ID

Hvis en lokal Identity Provider ønsker at medsende UNI-Login ID (for at undgå Account Linking) skal dette placeres i følgende felt:

```
<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 brugernavn}</saml:AttributeValue>
</saml:Attribute>
```

2.1.2 CPR-nummer

Hvis en lokal Identity Provider i stedet ønsker at medsende CPR-nummer (for at undgå Account Linking) skal dette placeres i følgende felt:

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

2.1.3 CVR-nummer til validering af Account Linking

En medarbejder kan i nogle tilfælde findes i flere lokale Identity Providers, f.eks. hvis vedkommende arbejder på institutioner i flere kommuner eller både har et login i kommunens forvaltning og i et evt. adskilt institutionsnet. I sådanne tilfælde vil brugeren blive mødt af dialogen til "Account Linking" for hvert nyt lokal login-Id, medarbejderen anvender.

Aula vil i forbindelse med Account Linking validere, at en given medarbejder i UNI-Login kun mappes til lokale Identity Providers som vedkommende er relateret til gennem UNI-Login stamdata. Til dette formål skal ethvert SAML login token indeholde CVR nummer, i henhold til OIOSAML standarden [2]:

```
<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">
 20688092
 </saml:AttributeValue>
</saml:Attribute>
```

Fælleskommunal Adgangsstyring medsender allerede denne værdi, men hvis man opsætter nye lokale Identity Providers er det vigtigt at disse også medsender korrekt CVR nummer for de brugere som håndteres.

© 2021 Netcompany

2.2 Fælleskommunal Adgangsstyring

Kommunernes forvaltninger er allerede tilsluttet Fælleskommunal Adgangsstyring og logger ind i en række systemer gennem Single-Sign-on via denne løsning. Det er derfor oplagt at kommunale medarbejdere fra forvaltningen benytter denne eksisterende opkobling til at tilgå Aula med SSO i stedet for at anvende et UNI-Login brugernavn/password.

2.2.1 Konfiguration af brugersystemrolle

For at kunne logge på Aula via Fælleskommunal Adgangsstyring er det påkrævet, at brugeren er tildelt en jobfunktionsrolle, der er tilknyttet brugersystemrollen "AULA adgang".

Opsætning af jobfunktionsroller skal foretages af den enkelte kommune i Serviceplatformen. Brugersystemrollen "AULA adgang" kan enten knyttes til eksisterende jobfunktionsroller, eller der kan oprettes en ny jobfunktionsrolle til formålet. Husk at sikre, at brugere, der skal kunne logge på Aula via Fælleskommunal Adgangsstyring, får den relevante jobfunktionsrolle tildelt.

Vi henviser generelt til Serviceplatformens dokumentation for konfiguration af jobfunktionsroller, herunder tilknytning af brugersystemroller.

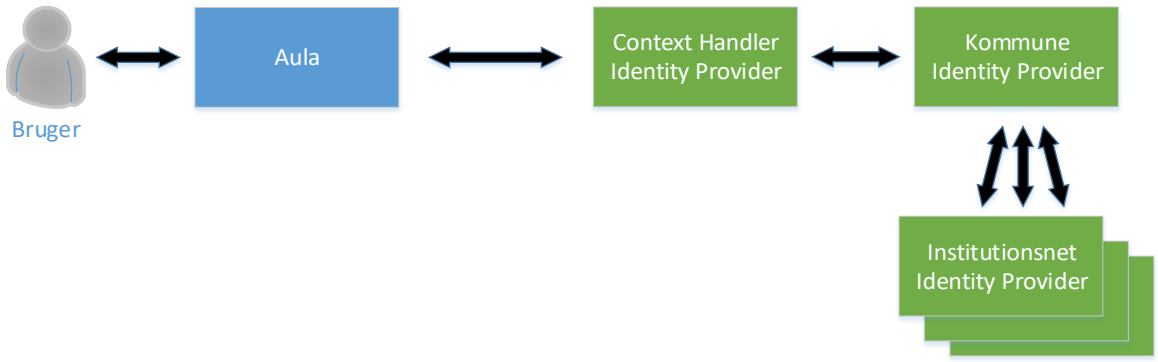
2.2.2 Opkobling af kommunale IdPer

I tillæg til de forvaltningsbrugere, der allerede er koblet på Fælleskommunal Adgangsstyring kan den enkelte kommune vælge at koble institutionernes brugere (fra Active Directory og lignende) på Fælleskommunal Adgangsstyring, enten ved at

1. Koble institutionernes brugere på samme administrative net som forvaltningen
    - Dette kan dog være en teknisk kompliceret løsning som involverer f.eks. migrering af brugere, rettigheder m.m. i Active Directory
2. Etablere en SAML 2.0 opkobling fra et fysisk adskilt institutionsnet til Fælleskommunal Adgangsstyring eller til den Identity Provider som kommunen allerede bruger til Fælleskommunal Adgangsstyring (f.eks. Microsoft AD FS)
    - Dette svarer til at etablere en kommune/skole Identity Provider, blot kobles den på Aula igennem Fælleskommunal Adgangsstyring i stedet for en direkte opkobling til Aula
    - Dette muliggør at SAML 2.0 opkoblingen på sigt kan genbruges imod andre systemer end lige netop Aula igennem en standard Fælleskommunal Adgangsstyring opkobling i stedet for punkt til punkt opkoblinger mellem kommunens/institutionens Identity Provider og det enkelte system

Figuren nedenfor illustrerer løsningsmodel 2, hvor Identity Provider fra et eller flere institutionsnet kobles på Fælleskommunal Adgangsstyring gennem SAML 2.0 føderation med den eksisterende kommunale Identity Provider for Fælleskommunal Adgangsstyring

© 2021 Netcompany



Figur 2: Identity Provider for institutionsnet koblet på Fælleskommunal Adgangsstyring gennem SAML 2.0 føderation med den eksisterende kommunale Identity Provider for Fælleskommunal Adgangsstyring.

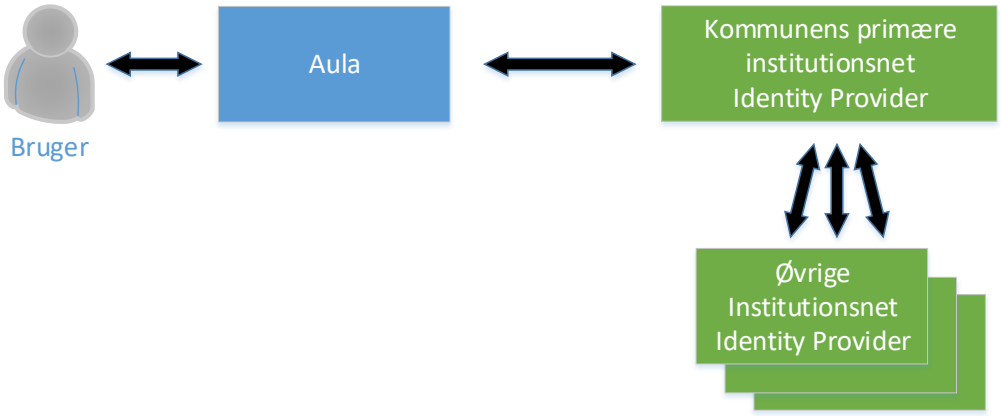
Bemærk: Ved login med Fælleskommunal Adgangsstyring vil der altid være tale om "account linking", hvor brugeren bedes om at logge ind med UNI-Login efterfølgende, for at kæde de to ting sammen.

2.3 Kommune/Skole Identity Provider

Den enkelte kommune, institution eller gruppe af institutioner kan også vælge at etablere sin egen Identity Provider som kobles på Aula via SAML 2.0 protokollen.

Dette kan f.eks. være en Microsoft AD FS løsningen som kobles op imod et institutionsnet.

Hvis en kommune opererer med flere, adskilte institutionsnet anbefales det at etablere en SAML 2.0 føderation, således at en samlet kommunal Identity Provider står for opkoblingen imod Aula, og denne så stoler på de enkelte institutionsnets Identity Providers. Dette kan f.eks. ske ved at udnævne en af institutionsnettenes Identity Providers til at være den primære og lade denne stole på de andre. Fordelen ved denne strategi er, at kommunen så selv kan håndtere interne omlægninger og justeringer, uden at dette involverer eller påvirker integrationen til Aula. Figuren herunder illustrerer dette setup.



Figur 3: Kommunens Identity Provider for institutionsnet koblet direkte på Aula og SAML 2.0 føderation med eventuelle ekstra Identity Providers i adskilte institutionsnetværk.

Kravene til SAML 2.0 opkoblingen fra egne Identity Providers til Aula er de samme, som når man foretager en opkobling til Fælleskommunal Adgangsstyring (som beskrevet i [1]).

Ligesom ved opkobling gennem Fælleskommunal Adgangsstyring skal man sørge for at CVR-nummer medsendes i SAML login-token gennem opkoblingen til Aula (som beskrevet i afsnit 2.1).

© 2021 Netcompany

3 Sikkerhed for brugerens identitet (Assurance Level)

I forbindelse med SAML login er myndighedens Identity Provider forpligtet til at vurdere og oplyse hvilket niveau af sikkerhed for brugerens identitet (Assurance Level[1]) der er opnået (på skalaen 1-4 som defineret i NSIS standarden[2]) og påstemple værdien i de tokens, der udstedes.

I vurderingen må man tage højde for både den tekniske styrke af autentifikationsmekanismen (fx kodeord, digital signatur etc.), relaterede tekniske kontroller (fx passwordpolitik, begrænsning af log-in til interne netværk etc.) men også for de organisatoriske procedurer, der er etableret til den indledende identifikation af brugeren (indrullering). Se også [1] for beskrivelse af dette emne.

Som udgangspunkt kræver Aula mindst Assurance Level 2 for at der gives adgang til systemet og informationer heri. Hvis en bruger logger ind med et SAML token med et lavere niveau vil man mødes med en fejlbesked. Normalt UNI-Login (brugernavn/password) er klassificeret som niveau 2, og kan således benyttes til almindelig adgang til Aula.

I de tilfælde hvor en bruger ønsker at tilgå følsomme personoplysninger i Aula (f.eks. en besked markeret som følsom eller dokumenter i sikker fildeling), kræves det at brugeren mindst har Assurance Level 3, hvilket blandt andet indebærer 2-faktor login (og øgede krav til den lokale sikkerhed såsom indrullering, låsning og logning). Dette kan enten ske ved at brugere fra starten logger på Aula med niveau 3 eller ved at Aula foretager et såkaldt step-up når en bruger på niveau 2 aktivt ønsker at tilgå følsomme personoplysninger.

De følgende afsnit beskriver mulighederne for enten altid at være på niveau 3 eller at koble en step-up funktionalitet på via enten UNI-Login, Fælleskommunal Adgangsstyring eller egen Identity Provider.

Bemærk, at det er den enkelte myndigheds eget ansvar at sørge for at Identity Providers, som kobles enten direkte på Aula eller kobles på gennem Fælleskommunal Adgangsstyring, altid oplyser et korrekt og retvisende niveau for Assurance Level, og at Aula ikke rådgiver om udformning af de specifikke lokale sikkerhedskrav som dette afkræver.

3.1 Konstant Assurance Level 3+

Hvis en myndighed ønsker helt at undgå behovet for at foretage step-up, skal man sørge for at alle SAML tokens fra ens Identity Provider udstedes med mindst Assurance Level 3. Dette stiller dog, som tidligere nævnt en række krav til den lokale sikkerhed i organisationen, herunder blandt andet at der benyttes en eller anden form for 2 faktor login eller tilsvarende sikker login-form.

Denne model benyttes typisk i kommunernes forvaltningers nuværende tilslutning til Fælleskommunal Adgangsstyring, hvor alle login via Identity Provider er på niveau 3.

Når en kommune vælger at etablere en eller flere Identity Providers for institutionsnet, kan man på tilsvarende vis sørge for at sikkerhedskrav i disse institutionsnet er tilstrækkelige til at alle login er på niveau 3.

En udfordring kan her være, at man som del af sikkerhedskravene er nødt til at kræve at medarbejderen benytter en godkendt computer, udleveret og beskyttet af institutionen, samt at medarbejderen tilgår Aula via institutionens beskyttede netværk. Dette kan derfor begrænse medarbejderens muligheder for at kunne tilgå Aula hjemmefra eller på farten. Her vil den enkelte myndighed kunne vælge at have et internet-vendt login på deres Identity Provider med enten

1. Assurance Level 2 – medarbejderen må så vente med at foretage handlinger der vedrører følsomme personoplysninger til de får adgang via godkendt computer og beskyttet netværk (eller der skal tilknyttes en step-up funktion som beskrevet i de efterfølgende afsnit).
2. Tvungen Assurance Level 3 (og to faktor login) straks i det indledende login, når Identity Provider kan se at login sker via internettet – dette er muligt med f.eks. Microsoft AD FS og Azure AD, hvor man kan sætte specifikke politikker på login fra extra/internet og for login fra godkendte/ukendte devices og også kan konfigurere 2 faktor login via Azure tjenester.

[1] Se http://digitaliser.dk/resource/363424 for yderligere detaljer omkring Assurance Level begrebet

[2] Se https://www.digitaliser.dk/group/3426134 for beskrivelse af NSIS (National Standard for Identiteters Sikringsniveauer)

© 2021 Netcompany

3.2 Step-up via UNI-Login

Alle brugere som logger på Aula via UNI-Login username/password starter Aula med Assurance Level 2. Når en sådan bruger aktivt ønsker at tilgå følsomme persondata sørger Aula for at fortage et step-up via UNI-Login's step-up model, hvor brugeren tvinges til at logge på med NemID:

- Børn vil som udgangspunkt ikke kunne foretage step-up (og ikke have behov for det)
- Værger (forældre) vil foretage step-up via deres private NemID
- Medarbejdere skal som udgangspunkt anvende NemID Erhverv (fordi NemID privat typisk ikke bør benyttes til arbejdsrelaterede formål), udstedt af deres myndighed/institution og registreret med CPR-nummer (for at UNI-Login kan mappe det til deres UNI-Login bruger). Teknisk set kan NemID privat også anvendes, men her skal den enkelte kommune forholde sig til Datatilsynets retningslinjer for anvendelse af NemID privat til erhvervsrelaterede formål.

Når en kommune vælger at koble deres medarbejdere på via egne Identity Providers kan man vælge stadig at anvende step-up via UNI-Login hvis man ikke har en step-up funktion tilknyttet sin Identity Provider. Dette gælder både når opkoblingen sker gennem Fælleskommunal Adgangsstyring, og når det sker via direkte opkobling imod Aula. Konfigurationen af om man ønsker at anvende UNI-Login step-up sker på den enkelte SAML 2.0 opkobling, så en kommune kan godt vælge at f.eks. deres Fælleskommunal Adgangsstyring opkobling skal benytte UNI-Login, mens en direkte opkoblet Identity Provider selv står for step-up (eller omvendt).

3.3 Step-up via Fælleskommunal Adgangsstyring

Fælleskommunal Adgangsstyring rummer i dag ikke mulighed for at foretage en egentlig step-up. Hvis man via Fælleskommunal Adgangsstyring er blevet logget på med niveau 2 har Aula således ikke nogen teknisk måde at tvinge brugeren til at foretage et nyt login med et højere niveau.

Parallelt med udviklingen af Aula er der derfor iværksat en udvidelse af Fælleskommunal Adgangsstyring og den SAML attributprofil som understøttes af denne. Der er aktuelt ikke fastlagt en dato for denne udvidelse til Fælleskommunal Adgangsstyring og step-up kan derfor alene foregå med UNI-Login.

Når udvidelsen er klar, vil det være en udvidelse af den nuværende KOMBIT SAML attributprofil til at lade Aula bede om et øget Assertion Level niveau og foretage step-up. Dette vil medføre at brugeren bedes om at foretage et nyt login (på et øget Assertion Level niveau) via kommunens opkobling på Fælleskommunal Adgangsstyring.

Fælleskommunal Adgangsstyring og Identity Providers hos myndigheder skal rent teknisk kunne modtage SAML AuthnRequests, hvor elementet `<saml2p:RequestedAuthnContext>` indeholder en angivelse af det ønskede Assurance Level for brugerautentifikationen som vist i eksemplet nedenfor:

```
<saml2p:RequestedAuthnContext Comparison="minimum">
 <saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
urn:dk:gov:saml:attribute:AssuranceLevel:3
 </saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
```

Værdien af Comparison attributten skal altid sættes til "minimum". Når ContextHandler eller en Identity Provider hos en myndighed modtager et request med et ønsket Assurance Level gøres flg.:

a) Hvis brugeren allerede har en session men på et for lavt niveau fraviges 'silent' SSO og i stedet vises en brugerflade til autentifikation. Bemærk at flaget IsPassive stadig skal respekteres på SAML AuthenticationRequest, så visninger af brugerflade gælder alene de tilfælde, hvor IsPassive ikke er sat.
b) Listen med IdP'er eller autentifikationsmekanismer, brugeren kan vælge skal filtreres, så brugeren ikke kan vælge log-in mekanismer på et lavere Assurance Level end det ønskede niveau). Efter autentifikation opdateres niveau'et med værdien for den nye autentifikation.

Tilsammen giver a) og b) mulighed for såkaldt 'step-up' autentifikation.

© 2021 Netcompany

Bemærk, at kommunen selv er ansvarlig for at deres Identity Provider understøtter `<saml2p:RequestedAuthnContext>` elementet og for at have de nødvendige autentifikationsmekanismer på det ønskede Assertion Level niveau.

Som allerede nævnt, kan kommunen vælge, at Aula i stedet skal anvende UNI-Login til step-up når kommunens brugere logges på Aula med Assertion Level 2 via Fælleskommunal Adgangsstyring.

3.4 Step-up via Skole/Kommune Identity Provider

Hvis en lokal Identity Provider er koblet direkte på Aula kan step-up understøttes via samme model som den kommende Fælleskommunal Adgangsstyring udvidelse – dvs. via `<saml2p:RequestedAuthnContext>` udvidelsen beskrevet i afsnit 3.3.

Alternativt kan man også benytte en særlig Microsoft AD FS syntaks til at foretage step-up. Dette sker ligeledes via `<saml2p:RequestedAuthnContext>`, men i stedet for at benytte den syntaks som Fælleskommunal Adgangsstyring anvender, kan Aula konfigureres til at lave et request som i eksemplet nedenfor:

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

En tredje mulighed er at anvende en særskilt Identity Provider (som kun foretager login på niveau 3+) til step-up (det er rent teknisk den måde UNI-Login step-up foregår på). Her skal man så oplyse to SAML 2.0 endepunkter i sin opkobling til Aula og dermed også vedligeholde to Identity Providers og opdatere begge når certifikater udløber og li gnende.

På den enkelte Identity Provider opkobling til Aula konfigureres om man ønsker at

1. Anvende Fælleskommunal Adgangsstyring syntaks
2. Anvende Microsoft syntaks
3. Have en dedikeret Identity Provider til step-up (herunder skal SAML 2.0 metadata for denne konfigureres)
4. Benytte UNI-Login til step-up (hvis intet andet er valgt, faldes der altid tilbage på UNI-Login)

© 2021 Netcompany