Lokal Identity Provider

En NSIS løsning

Indhold

1 Indledning

Dette dokument er en beskrivelse af en kommunal løsning til udstedelse og anvendelse af erhvervsidentiteter.

Erhvervsidentiteterne kan udstedes på niveauet NSIS Betydelig, og løsningen kan anmeldes til Digitaliseringsstyrelsen på dette niveau, og dermed anvendes som Lokal Identity Provider mod NemLog-in3 infrastrukturen.

De udstedte erhvervsidentiteter kan samtidig anvendes mod KOMBIT Adgangsstyring og STILs UniLogin broker, der begge vil begynde at kræve NSIS anmeldte lokale Identity Providers fra 2021/2022.

1.1 Hvorfor NSIS?

Som kommune skal man i flere scenarier integrere med føderations-infrastrukturer, hvor disse infrastrukturer stiller krav til de parter der tilslutter sig.

For at reducere kompleksiteten og understøtte en ensartet klassifikation af sikringsniveauer, er der udarbejdet en standard til formålet (National Standard for Identiteters Sikringsniveau – NSIS), samt en revisions- og anmeldelsespraksis, der sikrer at alle identitetsudbydere, der overholder et bestemt NSIS niveau, lever op til nogle bestemte minimumskrav.

De fælleskommunale- og fællesoffentlige infrastrukturer har taget NSIS standarden til sig, hvilket betyder at behovet for at kunne anmelde sin lokale Identity Provider på niveauet NSIS Betydelig bliver mere og mere relevant.

1.2 NSIS kravene

Den nyeste version af NSIS (version 2.0.1) kan findes her

https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/nsis-standarden/

1.3 Revision af løsningen

For at en lokal Identity Provider kan tilsluttes teknisk til de forskellige infrastrukturer, så skal den lokale Identity Provider først anmeldes til Digitaliseringsstyrelsen på et givent NSIS niveau, og en forudsætning for at kunne dette er at der udarbejdes en revisionsrapport af et revisionsfirma.

Digitaliseringsstyrelsen har udarbejdet vejledning til denne revision, som kan læses her

https://digst.dk/media/21348/nsis-revisionsvejledning-version-201a.pdf

Det er altid den ansvarlige brugerorganisation der skal anmelde løsningen, dvs Kommunen, og dermed også Kommunen der skal aflevere en revision af deres lokale Identity Provider.

Denne revision kan dog basere sig på andre revisionserklæringer, fx hvis hele eller dele af løsningen driftes og adminsitreres hos 3.part, så kan denne 3.part aflevere en revisionserklæring til Kommunen, som kan indgå i kommunens samlede revision.

Den løsning der beskrives her, er designet med det formål at blive driftet og administreret i Digital Identitys driftsmiljø, sådan at Digital Identity bliver revideret, og afleverer en revisionsrapport til Kommunen, som denne kan anvende til størstedelen af den revision som Kommunen skal have foretaget.

Afhængig af den konkrete implementation hos Kommunen, kan Kommunens egen revision reduceres til nogle af disse områder, se tabellen nedenfor for flere detaljer

2 Overordnet beskrivelse

Løsningen består af følgende del-komponenter, der håndterer forskellige aspekter af NSIS kravene, og som samlet indgår i den revisionserklæring som Digital Identity får udarbejdet, og som vil indgå som en del-erklæring i Kommunens anmeldelse til Digitaliseringsstyrelsen

2.1 Administrationsportal

Der udstilles en administrationsportal til Kommunens betroede medarbejdere, hvor de kan konfigurere de enkelte aspekter af Løsningen. Alle konfigurationsvalg falder indenfor rammen af det lovlige jf NSIS kravene, så der vil blot være tale om lokal kommunal tilpasning, herunder

- Opsætning af password politik
- Opsætning og vedligehold af vilkår for anvendelse af erhvervsidentiteten
- Mulighed for at udføre en øjeblikkelig spærring af en erhvervsidentitet
- Adgang til log og mulighed for udtræk af rapporter

Alle handlinger i administrationsportalen logges via det indbyggede lognings- og rapporteringsmodul beskrevet nedenfor.

2.2 Selvbetjeningsportal

NSIS stiller en række krav til udstedelsen og administration af erhvervsidentiter, hvilket håndteres på følgende måde

Datagrundlag for udstedelse af erhvervsidentiteter

Kommunen leverer et datagrundlag for hvilke personer der må få udstedt en erhvervsidentitet. Der udstedes ikke automatisk erhvervsidentiteter på baggrund af dette datagrundlag, men det vil kun være muligt at udstede erhvervsidentiteter til personer nævnt i dette datagrundlag.

Dette datagrundlag skal som minimum indeholde

- Unikt ID i form af et UUID, personnummer og navn på de personer som må få udstedt en erhvervsidentitet

For hver person kan der optionelt tilføjes

- En Active Directory brugerkonto som skal knyttes til erhvervsidentiteten

Hvis der er tilføjet en Active Directory brugerkonto, så tildeles personen automatisk dette brugernavn ved oprettelse af erhvervsidentiteten, og Kommunen kan samtidig vælge at passwords fra NSIS erhvervsidentiteten replikeres til kommunens AD, så slut-brugeren har en oplevelse af at have én brugerkonto.

Hvis en person senere (efter de har fået udstedt en erhvervsidentitet) får tilknyttet en AD konto, så vil de kunne bruge både deres AD brugernavn, og deres erhvervsidentitets-brugernavn når de logger ind med erhvervsidentiteten.

Obs! Hvis en person fjernes fra datagrundlaget, så lægges der en spærring ned over evt allerede udstedte erhvervsidentiter, der gør det umuligt at anvende denne erhvervsidentitet til

login. Denne spærring fjernes automatisk hvis personen tilføjes til datagrundlaget igen (og denne spærring kan ikke fjernes af personen via selvbetjeningsportalen).

Udstedelsesproces

Personen der ønsker en erhvervsidentitet, tilgår en selvbetjeningsportal på Løsningen, hvor de gennemløber følgende proces

- Personen tilgår selvbetjeningsportalen og logger ind med sit NemID/MitID
- Personens CPR nummer hentes fra NemID/MitID, og verificeres mod listen af personer der må få udstedt en erhvervsidentitet
- Personen præsenteres for vilkårene for brug af erhvervsidentiteten og skal acceptere disse
- Personen tildeles derefter et brugernavn til erhvervsidentiteten. Hvis der er indlæst en Active Directory brugerkonto på denne person i datagrundlaget, så er den forvalgt som brugernavn
- Personen skal derefter vælge et kodeord, jf den kodeordspolitik som Kommunen har opsat

Hvis kommunen har valgt at synkronisere erhvervsidentitetens kodeord med AD, så sker en sådan synkronisering (se mere under afsnittet om integrationer).

Generelt om spærring af erhvervsidentiteter

En erhvervsidentitet kan spærres på 4 måder

1. Personen, erhvervsidentiteten er udstedt til, fjernes fra datagrundlaget
2. En administrator laver en haste-spærring af den konkrete erhvervsidentitet
3. Personen som erhvervsidentiteten er udstedt til, spærrer selv erhvervsidentiteten via selvbetjeningsmodulet
4. Erhvervsidentiteten forsøges anvendt med forkert kodeord 5 gange i træk, hvorefter erhvervsidentiteten spærres midlertidigt (den åbnes automatisk igen efter 1 time)

De forskellige spærremetoder sætter forskellige spærre-flag på erhvervsidentiteten, og så længe der er blot ét spærreflag på en erhvervsidentitet, er den funktionelt spærret og kan ikke anvendes.

Løbende selvbetjening

Personer der har fået udstedt en erhvervsidentitet kan løbende logge ind i selvbetjeningsportalen (med NemID/MitID), og her foretage følgende operationer

- Se status for deres erhvervsidentitet
- Spærre sin erhvervsidentitet
- Genåbne sin erhvervsidentitet hvis den er blevet spærret (dog ikke hvis den er blevet spærret grundet fjernelse af CPR nummer fra datagrundlaget eller haste-spærret af en administrator)
- Skifte kodeord på sin erhvervsidentitet

Alle handlinger i selvbetjeningsportalen logges via det indbyggede lognings- og rapporteringsmodul beskrevet nedenfor.

2.3 Loginmodul (Identity Provider funktionalitet)

NSIS stiller en række tekniske krav til login processen. Disse krav gør sig gældende når slut-brugeren foretager et login gennem en af de nævnte føderations-infrastrukturer (KOMBIT Adgangsstyring, STIL UniLogin, NemLog-in 3), hvor det bl.a. skal sikres at

- Der udstedes den korrekte NSIS værdi (Lav eller Betydelig), der afhænger af hvordan brugeren er registreret og hvordan brugeren logger ind (1-faktor eller 2-faktor login)
- At der kun udstedes oplysninger i "login tokenet" som er beregnet til den faktiske modtager (den faktiske modtager er det fagsystem der gemmer sig bag føderations-infrastrukturen)
- At der foretages fuldstændig og korrekt logning af login-forløbet

Løsningen indeholder en SAML 2.0 Identity Provider, som forestår selve login-flowet, og håndterer autentifikation, autorisation og logning.

Autentifikation foretages via validering mod de erhvervsidentiteter der er oprettet og udstedt af Løsningen, og som den første login-faktor anvendes kodeordet til erhvervsidentiteten.

Login-flowet forløber som følger

1. En loginforespørgsel modtages fra en af de 3 infrastrukturerer (NemLog-in3, KOMBIT eller STIL)
2. Brugeren foretager login med 1-faktor (brugernavn/kodeord)
3. Det valideres om denne erhvervsidentitet må tilgå den nævnte infrastruktur (jf datagrundlaget leveret af Kommunen)
4. Hvis loginforespørgslen stiller krav om 2-faktor login (anmodning om step-up, NSIS Niveau Betydelig eller tilsvarende), så initeres et 2-faktor login forløb
5. Efter login er gennemført, hentes evt roller fra OS2rollekatalog, som medsendes SAML login billetten

Løsningen laves så den løbende kan udvides med support for flere MFA (2-faktor) løsninger, men kommer i første version med support for OS2faktor MFA.

Alle logins, succesfulde som fejlede, logges via det indbyggede lognings- og rapporteringsmodul.

2.4 Lognings- og rapporteringsmodul

For at kunne dokumentere at man overholder kravene i NSIS, og dermed kunne gennemføre en revisionskontrol, er det nødvendigt at alle relevante data logges, og udstilles så de nemt kan anvendes til revisionskontrol.

Løsningen opsamler logdata fra alle de moduler der indgår i Løsningen, og udstiller disse via en web-portal, hvor administrator kan browse i loggen (fx til fejlsøgning og support), samt trække relevante og målrettede rapporter til revisionskontrollen.

3 Integrationer

Løsningen indeholder en række integrationer til andre systemer, som er beskrevet nedenfor. Løsningen kan løbende udvides med yderligere integrationer, fx integrationer til flere MFA løsninger, andre rettighedsstyringssystemer m.m.

3.1 Integration til det kommunale datagrundlag

Løsningen udstiller et API til at indlæse og vedligeholde datagrundlaget.

Hvordan dette datagrundlag dannes lokalt i Kommunen vil påvirke omfanget af den revision som Kommunen skal have udarbejdet, og her kan man med fordel læne sig op af eksisterende systemer og processer, fx Kommunens lønsystem, hvor man så baserer datagrundlaget på udtræk fra disse systemer.

Der leveres også en standard-integration, der baserer sig på en udlæsning fra AD, hvor man styrer udtrækket på gruppe-medlemskab.

3.2 Integration til NemLog-in3

Løsningen udstiller SAML metadata, som kan indlæses direkte i NemLog-in3's kommende Administrationsmodul.

Da procesen omkring dette ikke er kendt endnu, kan dette ikke beskrives i flere detaljer, men Digital Identity vil under alle omstændigheder sikre at denne proces forløber gnidningsfrit, både den initielle oprettelse, og løbende opdateringer ved certifikat-skifte.

3.3 Integration til KOMBIT Adgangsstyring

Løsningen udstiller SAML metadata, som kan indlæses direkte i KOMBIT Adgangsstyring via KOMBITs Administrationsmodul.

Digital Identity vil stå for indlæsning og løbende opdatering (fx ved certifikat-skifte) i KOMBITs Administrationsmodul, og vil anmode om en såkaldt Føderationsaftale, som skal godkendes af Kommunens aftaleansvarlige i KOMBITs Administrationsmodul.

Integrationen sikrer at Kommunens medarbejdere kan logge ind via KOMBITs Adgangsstyring (som de gør i dag), og blot vil opleve at de skal foretage deres login via Løsningen, frem for Kommunens AD FS.

3.4 Integration til STIL UniLogin

Løsningen udstiller SAML metadata, som kan indlæses direkte i STILs uni-login broker.

Digital Identity sikrer at certifikat m.m. opdateres tidsmæssigt, og understøtter Kommunen i nemt at kunne opdatere disse metadata hos STIL. Selve opdateringen skal ske på foranledning fra Kommunen til STIL, men Digital Identity vil drive processen omkring dette.

3.5 Integration til NemID

I en overgangsfase fra Løsningen tages i brug, til NemLog-in3 er fuldt udrullet, og det kan forventes at borgere er udstyret med et MitID, vil Løsningen anvende NemID som verifikationsmekanisme i forbindelse med login til selvbetjeningsportalen.

Denne integration fases over tid ud til fordel for MitID, men dette forventes først at ske noget tid efter at NemLog-in3 er fuldt udrullet.

Kommunen skal her indgå en tjenesteudbyderaftale med Nets om brug af NemID til login, og der skal indgås en aftale med Digitaliseringsstyrelsen om PID2CPR opslag. Det er gratis for Kommunen at indgå denne aftale med Nets, men det skal ske i kontekst af Kommunen, for at opslag på CPR nummer er muligt.

3.6 Integration til NemLog-in3 (som tjensteudbyder)

Når NemLog-in3 er fuldt udrullet, erstattes NemID integrationen med en NemLog-in3 integration, hvor NemLog-in3 anvendes som verifikationsmekanisme, hvor borgerens MitID anvendes som login mekanisme til selvbetjeningsportalen.

Her er det, på lige fod med NemID integrationen, Kommunen som skal indgå en tjenesteudbyderaftale, så CPR nummeret kan modtages.

3.7 Integration til OS2rollekatalog

Både NemLog-in3 og KOMBIT Adgangsstyring understøtter et rollebegreb, hvor man kan medsende brugerens rettigheder på logintidspunktet fra den lokale Identity Provider.

Løsningen kommer med en integration til OS2rollekatalog, som kan anvendes som underliggende rettighedsstyring. Hvis Løsningen anvendes i samspil med OS2rollekatalog, vil rettigheder tildelt heri blive medsendt på login tidspunkt til hhv NemLog-in3 og KOMBIT Adgangsstyring.

Bemærk at det ikke er en forudsætning at man anvender OS2rollekatalog for at anvende løsningen, men hvis man gør, så kan rolletildelinger foretaget i OS2rollekatalog trækkes ud, og sendes med til bl.a. KOMBIT Adgangsstyring.

Løsningen designes så den kan trække rettigheder fra andre systemer, men der udvikles ikke nogen integrationer til andre systemer i første version.

3.8 Integration til Active Directory

Kommunen kan vælge at slå en integration til Active Directory til i Løsningen. En forudsætning for dette, er at datagrundlaget som leveres til Løsningen indeholder en kobling fra personen til dennes AD konto.

Når man slår synkroniseringen til, vil kodeordsskifte blive synkroniseret fra Løsningen til Kommunens Active Directory.

Man kan også vælge at slå password-validering mod AD'et til, så der foretages en validering af brugerens password op mod AD'et (som en fallback metode til fejlede password valideringer direkte mod løsningens egen database). Hvis et password valideres mod AD vil brugeren skulle foretage et step-up med NemID efterfølgende, hvis de skal logge ind på en tjeneste der kræver NSIS (fx NemLog-in3).

3.9 Integration til OS2faktor MFA

Løsningen designes så den kan understøtte forskellige MFA løsninger, men da der skal udvikles en konkret integration til hver MFA løsning, udvikles initielt kun en integration til OS2faktor MFA. Løsningen kan så løbende udvides med yderligere MFA løsninger efter behov.

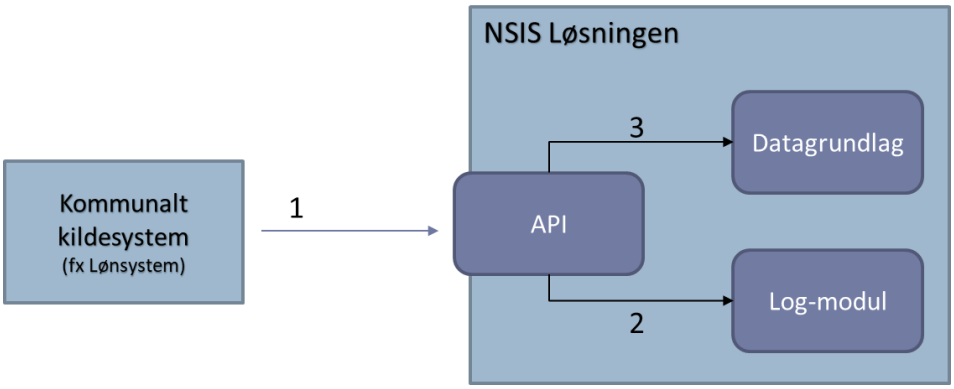
Bemærk at den valgte MFA løsning skal understøtte en registrerings- og spærreproces som lever op til kravene i NSIS, da den vil indgå i den samlede revision.

OS2faktor MFA løsningen lever op til disse krav, og vil indgå i den revision som Digital Identity får udført.

4 Komponentoverblik

Nedenfor er de forskellige del-komponter i Løsningen illustreret via forskellige anvendelses- og dataflows. Disse illustrationer er tiltænkt en bredere forståelse for sammenhængen mellem de forskellige komponenter, og de integrationer og eksterne systemer der er i spil.

4.1 Indlæsning af datagrundlag



Kommunen skal vedligeholde et datagrundlag der ligger til grund for hvem der må få udstedt en erhvervsidentitet. Der udstedes ikke automatisk en erhvervsidentitet til de personer som er nævnt i datagrundlaget, dette skal personerne selv håndtere via selvbetjeningen, men det er alene de personer som er nævnt i datagrundlaget som kan få en erhvervsidentitet udstedt, og erhvervsidentiteter spærres hvis personen fjernes fra datagrundlaget.

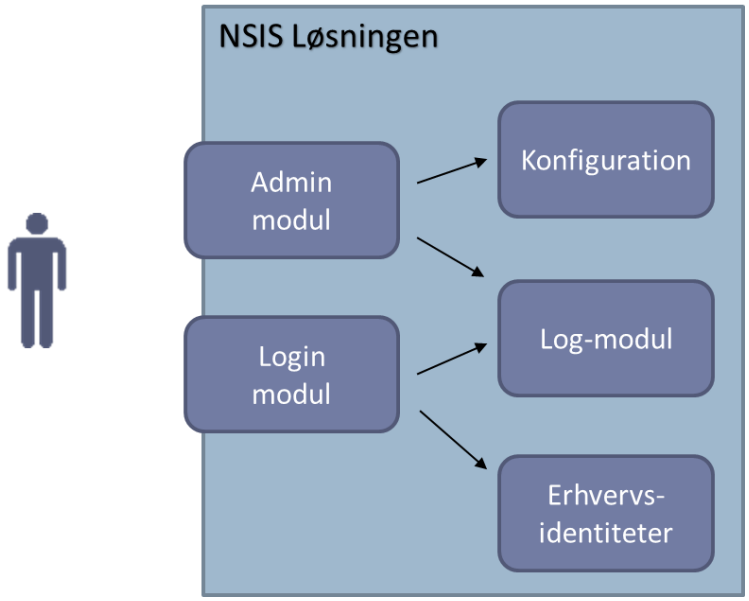
Etablering og vedligehold af dette datagrundlag vil være et område som kommunen skal have revideret, og én mulig tilgang til dette er at gøre brug af kommunens lønsystem, og basere udtrækket på data derfra.

Digital Identity kan assistere med at lave udtræk fra både OPUS Løn og Personale, SD Løn eller andre kilder til dette formål.

Når data indlæses i Løsningen, sker der følgende

1. Kildesystemet i kommunen afleverer et fuldt datagrundlag via API'et udstillet på Løsningen
2. Modtagelsen af datagrundlaget logges i Løsningens Log-modul, og datagrundlaget indlæses i konfigurations-databasen i Løsningen
3. På baggrund af det indlæste datagrundlag i Løsningen, vil evt erhvervsidentiteter, der er udstedt til personer som ikke længere findes i datagrundlaget, blive spærret.

4.2 Administration af Løsningen

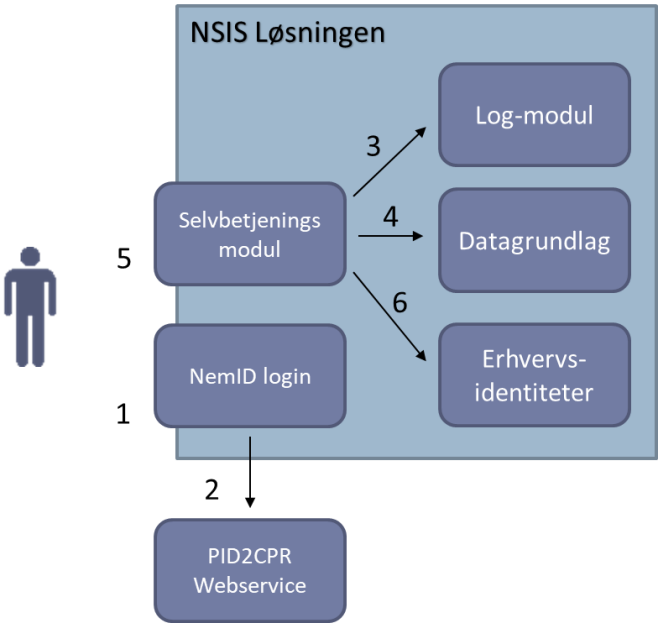


En person der har fået udstedt en erhvervsidentitet, hvor der i datagrundlaget er angivet at erhvervsidentiteten må anvendes til at tilgå Adminsitrationsportalen, kan anvende denne til at logge ind i Adminsitrationsportalen.

Adgangen til Administrationsportalen går gennem det samme Loginmodul der anvendes til login til NemLog-in3, KOMBIT og STIL, og der foretages samme adgangskontrol og logning som ved et normalt login.

Hvis login er succesfuldt (og der i datagrundlaget er angivet at erhvervsidentiteten må få adgang til administrationsportalen), får administratoren adgang, og kan ændre konfigurationen, samt tilgå log-modulet og trække data ud af denne.

4.3 Registreringsproces



Udstedelsen af erhvervsidentiteter er baseret på selvbetjening, og det er ikke muligt for en adminstrator at udstede erhvervsidentiteter for andre.

En person der ønsker en erhvervsidentitet skal logge ind i Selvbetjeningsmodulet via NemID (senere MitID), og så gennemføre udstedelsesprocessen. Dette håndteres på følgende måde

1. Personen foretager et login vha NemID
2. Løsningen henter det CPR nummer der hører til NemID'et via opslag i Digitaliseringsstyrelsens opslags-service
3. Login til selvbetjeningsløsningen logges
4. Det valideres at personens CPR nummer er indeholdt i datagrundlaget
5. Personen får nu mulighed for at læse og acceptere vilkårene for anvendelsen af erhvervsidentiteter i Kommunen, og gennemføre udstedelsen af samme
6. Erhvervsidentiteten lagres i Løsningen

Alle trin logges i log-modulet, herunder også udstedelsen.

4.4 Selvbetjeningsproces

Det samme modul som er illusteret i foregående afsnit, kan anvendes af personer med en erhvervsidentitet til at administrere disse. Login foretages altid med NemID (senere MitID), og flowet er det samme som ved registrering og udstedelse af erhvervsidentiteten.

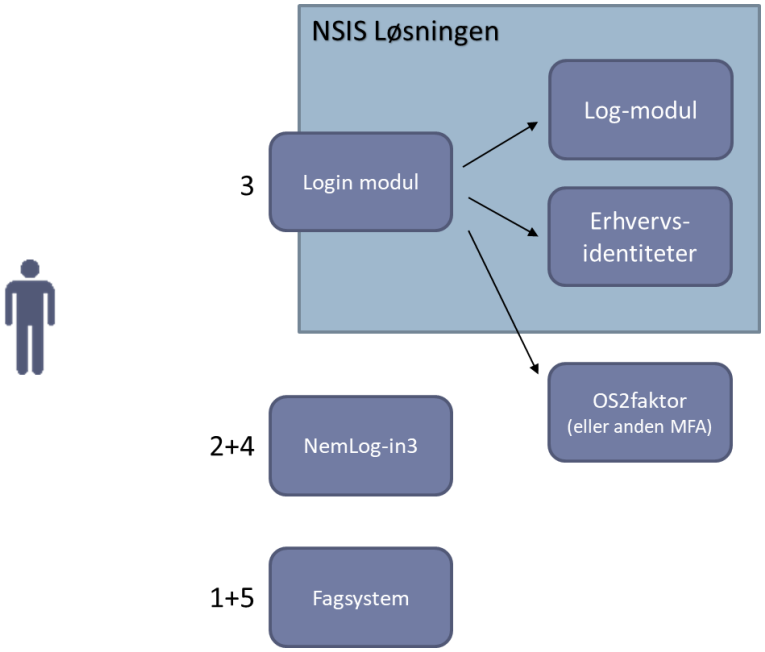
Bemærk at der ikke behøves at være udstedt en erhvervsidentitet for at tilgå selvbetjeningsportalen, og hvis der er en erhvervsidentitet udstedt, blokeres der ikke for adgang til selvbetjeningsportalen hvis erhvervsidentiteten er spærret.

I selvbetjeningsportalen får personen mulighed for at

- Se status på sin erhvervsidentitet (fx kan de her se hvis den er spærret, og hvorfor)
- Spærre sin erhvervsidentitet
- Låse sin erhvervsidentitet op (dog kun muligt at fjerne en spærring de selv har lagt på)

- Skifte kodeord på sin erhvervsidentitet (hvis den ikke er spærret)

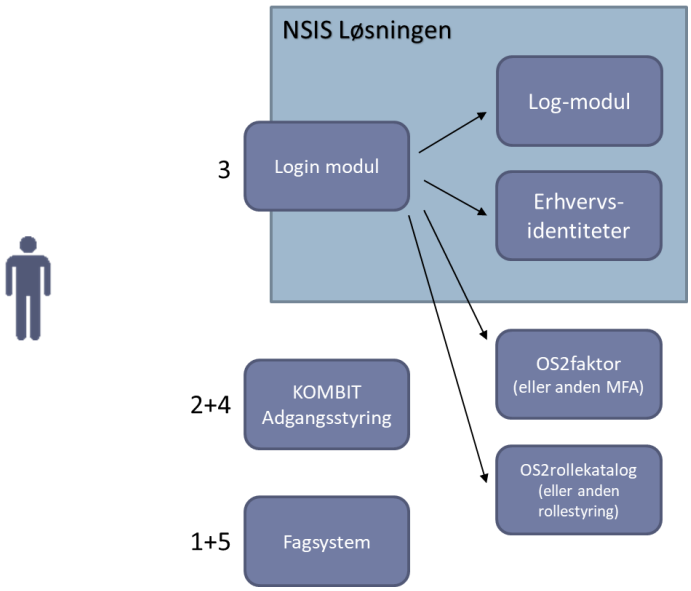
4.5 Login til NemLog-in3



Login flowet til NemLog-in3 forløber på samme måde som det vil gøre hvis der var tale om et login mod Kommunens AD FS. Den største forskel er at det ikke er Kommunens AD FS og underlæggende AD der foretages login mod, men i stedet mod Løsningens Login modul og de udstedte erhvervsidentiteter. Login forløber som følger

1. Et fagsystem (eller webportal som virk.dk, skat.dk eller lignende) der gør brug af NemLog-in3 til login, sender en Login forespørgsel til NemLog-in3
2. NemLog-in3 sender forespørgslen videre til Kommunens Lokale Identity Provider (Løsningen)
3. Løsningen gennemfører login processen på det NSIS Niveau som NemLog-in3 efterspørger (Lav eller Betydelig). Ved niveauet Betydelig gennemføres også et 2-faktor login, og ved Lav er det kun et brugernavn/kodeord login der foretages. Hele forløbet logges i Log-modulet, og der udstedes en adgangsbillet til NemLog-in3
4. NemLog-in3 veksler adgangsbilletten til en adgangsbillet til fagsystemet
5. Brugeren er nu logget ind i fagsystemet

4.6 Login til KOMBIT Context Handler

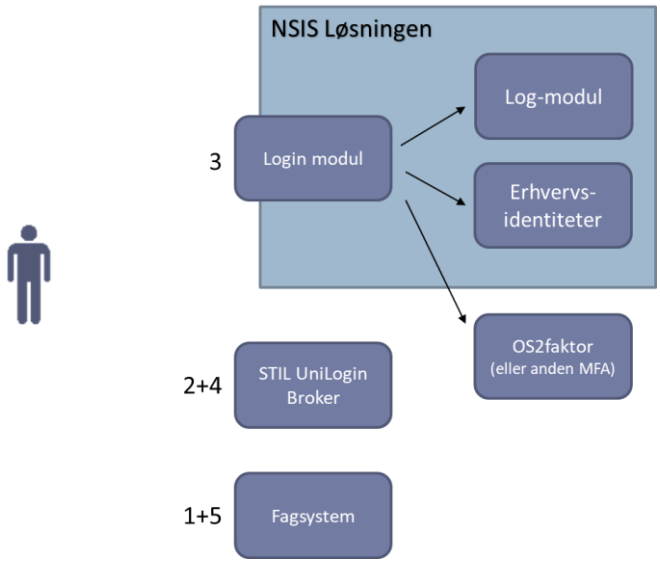


Login flowet til KOMBIT Adgangstyring forløber på samme måde som det gør i dag mod Kommunens AD FS. Det eksisterende login-flow mod KOMBIT, som kører via Kommunens AD FS erstattes af Løsningen, og Kommunens AD FS vil ikke længere være involveret når der foretages login mod KOMBIT.

Login forløber som følger

1. Et fagsystem (SAPA, KY, BBR, ...) der gør brug af KOMBIT Adgangstyring til login, sender en Login forespørgsel til KOMBIT Adgangsstyring
2. KOMBIT Adgangstyring sender forespørgslen videre til Kommunens Lokale Identity Provider (Løsningen)
3. Løsningen gennemfører login processen på det NSIS Niveau som KOMBIT Adgangsstyring efterspørger (Lav eller Betydelig). Ved niveauet Betydelig gennemføres også et 2-faktor login, og ved Lav er det kun et brugernavn/kodeord login der foretages. Endeligt hentes brugerens roller fra OS2rollekatalog, og der udstedes en adgangsbillet til KOMBIT Adgangsstyring med rollerne indlejret. Hele forløbet logges i Log-modulet.
4. KOMBIT Adgangsstyring veksler adgangsbilletten til en adgangsbillet til fagsystemet
5. Brugeren er nu logget ind i fagsystemet

4.7 Login til STIL UniLogin



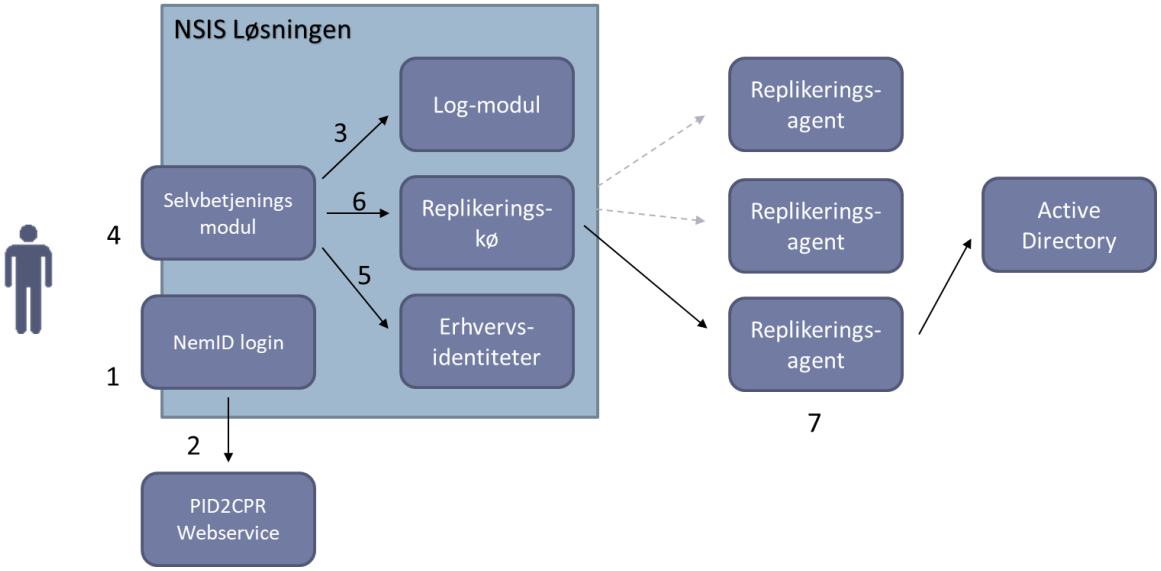
Login flowet til STIL UniLogin Broker forløber på samme måde som det vil gøre hvis der var tale om et login mod Kommunens AD FS. Den største forskel er at det ikke er Kommunens AD FS og underlæggende AD der foretages login mod, men i stedet mod Løsningens Login modul og de udstedte erhvervsidentiteter. Login forløber som følger

1. Et fagsystem på skoleområdet der gør brug af UniLogin til login, sender en Login forespørgsel til UniLogin Brokeren
2. UniLogin Brokeren sender forespørgslen videre til Kommunens Lokale Identity Provider (Løsningen)
3. Løsningen gennemfører login processen på det NSIS Niveau som UniLogin Brokeren efterspørger (Lav, Betydelig og i en overgangsfase også de STIL specifikke niveauer EnFaktor og ToFaktor). Ved niveauet Betydelig (eller ToFaktor) gennemføres også et 2-faktor login, og ved Lav (eller EnFaktor) er det kun et brugernavn/kodeord login der foretages. Hele forløbet logges i Log-modulet, og der udstedes en adgangsbillet til UniLogin Brokeren
4. UniLogin Brokeren veksler adgangsbilletten til en adgangsbillet til fagsystemet

Brugeren er nu logget ind i fagsystemet på skoleområdet.

Step-up håndteres også jf det step-up flow som anvendes i UniLogin.

4.8 Password replikering til Active Directory



Hvis Kommunen har valgt at slå password replikering til, så sker der en synkronisering af kodeordet fra erhvervsidentiteterne, til de AD brugerkonti som er knyttet dertil i det indlæste datagrundlag.

Replikeringen af kodeord sker via en kø-mekanisme, der sikrer at kodeordet replikeres til Active Directory når det er muligt. Fx hvis der er netværksmæssige eller tekniske årsager til at Active Directory ikke kan tilgås, så udføres replikeringen af kodeordet først når adgangen igen er tilgængelig.

For at sikre en høj robusthed af kodeords-replikeringen, er det muligt at installere flere replikerings-agenter on-premise hos Kommunen, og så længe én af disse er aktiv, så vil kodeords-replikeringen fungere.

Replikeringen af kodeord fungerer på følgende måde

1. En bruger logger ind i selvbetjeningsportalen vha NemID (senere MitID)
2. CPR nummeret tilhørende det anvendte NemID hentes via opslag hos Digitaliseringsstyrelsen opslagsservice
3. Login logges i log-modulet
4. Brugeren gennemfører et password skifte via selvbetjeningsmodulet
5. Passwordet skiftes på erhvervsidentiteten
6. Passwordskiftet lægges på replikeringskøen i Løsningen
7. En af de kørende on-premise agenter fanger beskeden fra replikeringskøen, og opdaterer i Active Directory

Hele forløbet, inkl svar tilbage fra Replikerings-agenten, logges til Log-modulet, så kan man se status på password skiftet helt ind til Kommunens Active Directory.

Løsningen overvåger hvor mange replikerings-agenter der er aktive, og hvis antallet af aktive replikerings-agenter falder til 0, går der en alarm i Løsningen, som sendes til driftoperatøren (Digital Identity).

5 Implementeringsforløb

Nedenfor er beskrevet et overordnet implementeringsforløb, som kan give en god ide om hvad det er for en opgave man står overfor i Kommunen.

5.1 Udarbejde strategi for implementering

Kommunen skal starte med at afklare deres målbillede, herunder

- Skal der ske en replikering af kodeord til AD, så brugerne har en oplevelse af af have én brugerkonto, eller skal erhvervsidentiteten opleves at være en særskilt brugerkonto?
- Hvilken MFA løsningen ønskes anvendt, og er der udestående vedrørende revision af denne?
- Hvis ikke OS2rollekatalog skal bruges som rettighedssystem til NemLog-in3 og KOMBIT roller, hvilket rettighedssystem skal så anvendes (bemærk NSIS stiller ikke krav om revision af rettighedsstyring, kun identitetsstyring)

5.2 Valg af kilde til datagrundlag og etablering af udtræk

Hvordan etableres datagrundlaget for de personer som må få udstedt en erhvervsidentitet, og hvordan sikres det at disse fjernes rettidigt fra datagrundlaget i tilfælde af

- Ophør af tilhørsforhold til kommunen
- Dødsfald og/eller længerevarende orlov
- Mistanke om misbrug af erhvervsidentiteten

Kommunen er forpligtiget til at dokumentere og få udført revision af disse processer.

5.3 Teknisk implementering

Gennemførsel af en teknisk implementering, hvor alle nødvendige integrationer sættes op. Det er muligt at sætte integrationen op mod NemLog-in3's integrationstestmiljø hvis dette ønskes.

En integration mod produktionsmiljøet på NemLog-in3 kan først ske når løsningen er anmeldt til Digitaliseringsstyrelsen. Man kan evt overveje at anmelde løsningen på NSIS Lav først, og så ændre anmeldelsen til NSIS Betydelig senere, så man kan gå på produktionsmiljøet tidligt.

5.4 Testforløb

Kommunen bør udarbejde en testplan, og gennemføre denne. Afhængig af hvilke miljøer som den tekniske integration er sat op mod, kan det påvirke omfanget af testforløbet.

5.5 Organisatorisk implementering

Relevant personale skal identificeres og uddannes i brug af Løsningen, herunder blive gjort bekendt med det ansvar de har, og den revision som vil blive udført af deres arbejde.

Der skal udarbejdes dokumentation til de slutbrugere der skal have en erhvervsidentitet, som beskriver hvordan de får, anvender og administrerer en erhvervsidentitet.

5.6 Revision og anmeldelse til Digitaliseringsstyrelsen

Kommunen skal foretage en revision af Løsningen, som kan basere sig delvist på den revisionserklæring som Digital Identity får udarbejdet. Herefter skal Løsningen anmeldes af Kommunen til Digitaliseringsstyrelsen, så Løsningen kan sættes i produktion (eller hvis den allerede er i produktion på NSIS Lav, så ophøjes til NSIS Betydelig).