OS2faktor Login

Lokal Identity Provider

Version: 4.1.0
Date: 19.04.2022
Author: BSG

Indhold

1 Indledning

Dette dokument er en beskrivelse af en OS2faktor Login løsningen 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, og andre infrastrukturer og fagsystemer der stiller krav om overholdelse af NSIS.

1.1 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 dette, er en revisionsrapport af et statsautoriseret revisionsfirma.

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

https://digst.dk/media/25629/nsis-revisionsvejledning-version-205.pdf

Det er altid den ansvarlige brugerorganisation der skal anmelde løsningen, dvs Kommunen, og dermed også Kommunen der skal aflevere en revisionserklæring på deres Lokale Identity Provider.

Denne revision kan dog basere sig på andre revisionserklæringer, fx hvis hele eller dele af løsningen driftes og administreres 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 afløftning af en række af punkterne i den samlede revision som kommunen skal have foretaget.

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

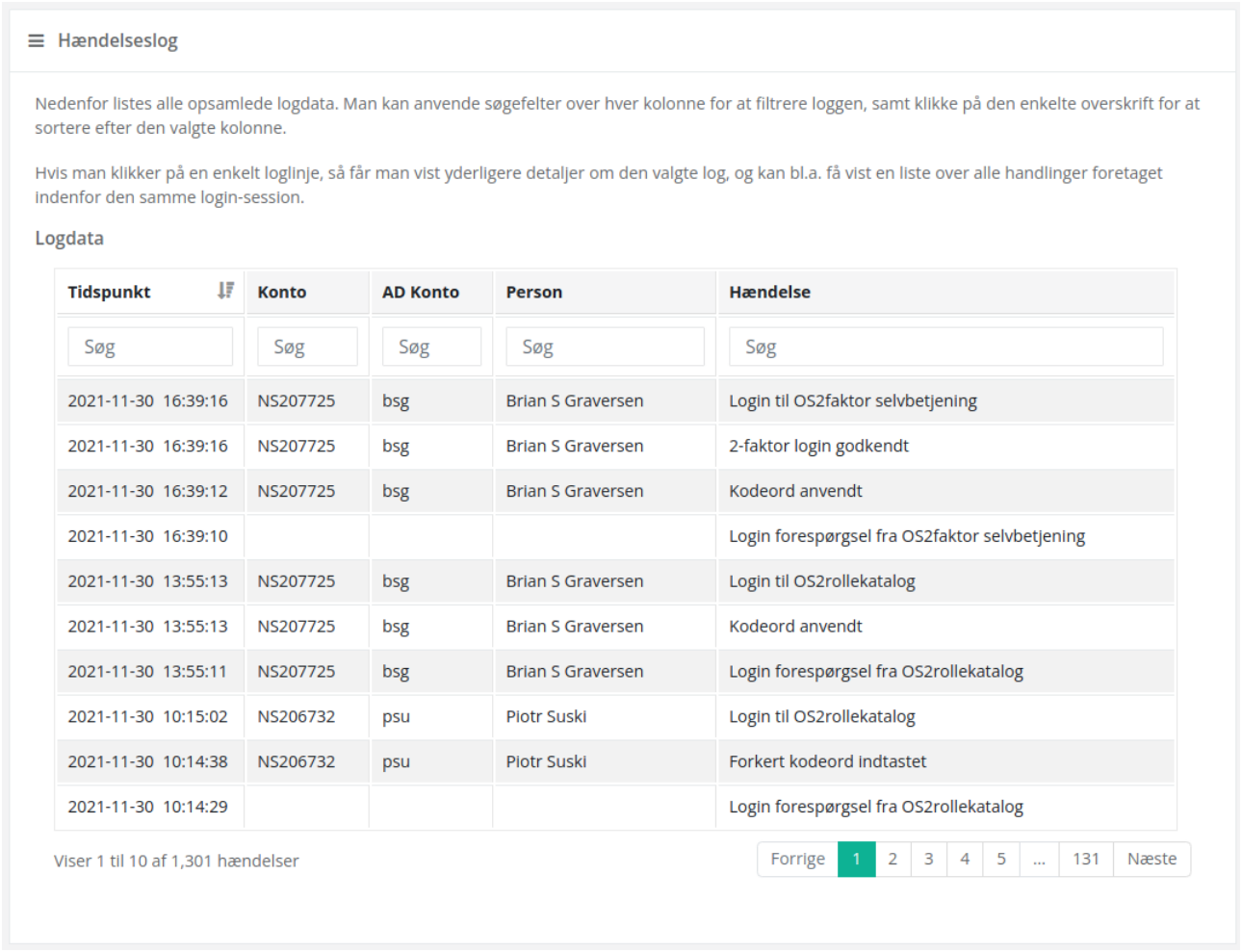
Der udstilles en administrationsportal til Kommunens betroede medarbejdere, hvor de kan konfigurere de enkelte aspekter af Løsningen. Alle konfigurationsvalg falder indenfor rammen af det lovlige jf NSIS kravene, så der vil blot være tale om lokal kommunal tilpasning, herunder

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

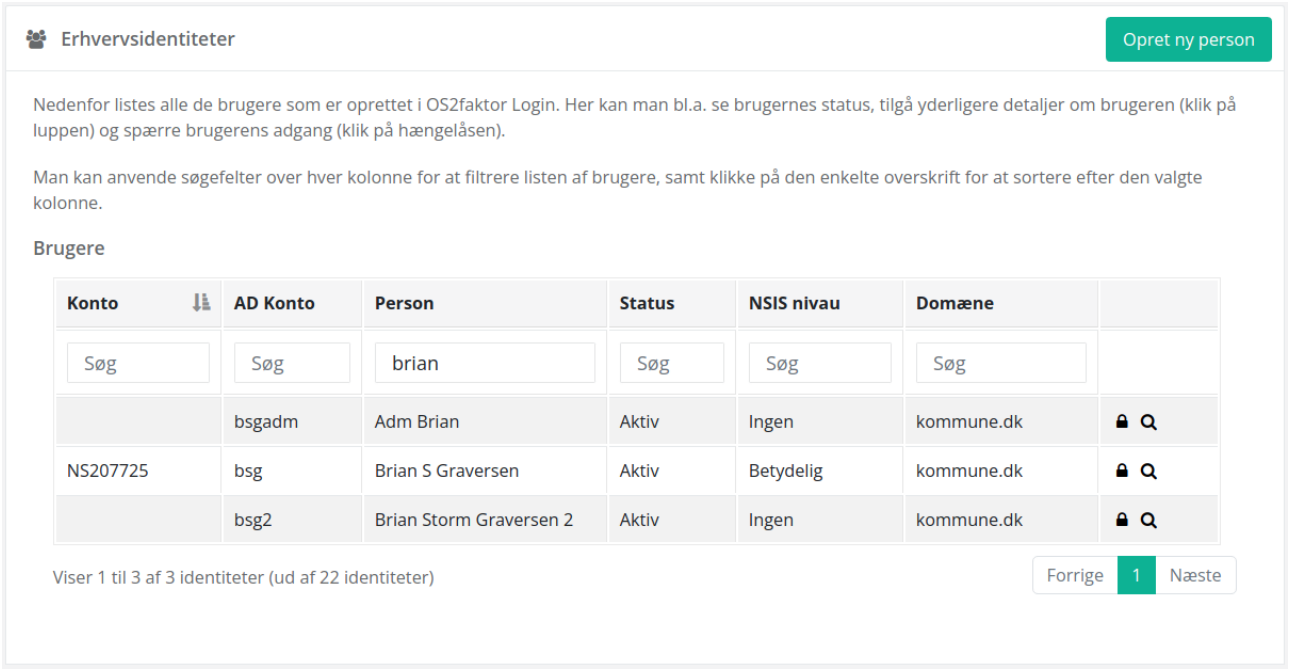
Alle handlinger i administrationsportalen logges via det indbyggede lognings- og rapporteringsmodul beskrevet nedenfor.

Administratorer har adgang til at se en lang række informationer inde i administrationsportalen, og de primære værktøjer er adgang til loggen, samt oplysninger om de indlæste brugere.

Administratorer kan se en lang række oplysninger i loggen, hvor overblikket er illustreret nedenfor



Administratorer kan ligeledes danne sig et overblik over alle personer indlæst i løsningen via administrator-portalen. Her kan de se status på alle personer, samt tilgå detaljer om personen, herunder oplysninger om tilknyttede 2-faktor enheder m.m.



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 foretage login gennem Løsningen. Datagrundlaget består af følgende oplysninger om hver person

- Unikt ID i form af et UUID
- Personnummer
- Navn
- Angivelse af om personen må få en erhvervsidentitet
- Optionelt en brugernavn
- Optionelt en email adresse

Hvis en person indlæses uden et brugernavn, så tildeles personen et af Løsningen. Formålet med at kunne indlæse et brugernavn på personen, er at sikre at personen har samme brugernavn lokalt i Windows (AD brugernavn) samt i Løsningen.

Hvis der medsendes et AD brugernavn, kan Kommunen vælge at passwords fra Løsningen replikeres til kommunens AD, så slut-brugeren har en oplevelse af at have én brugerkonto med ét kodeord.

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 et Active Directory brugernavn 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 personen har gennemført første login vha sit eksisterende AD kodeord, så indrulleres dette i Løsningen, og brugeren behøves ikke vælge et nyt kodeord.
- Hvis brugeren vælger et nyt kodeord, og kommunen har valgt at synkronisere 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)

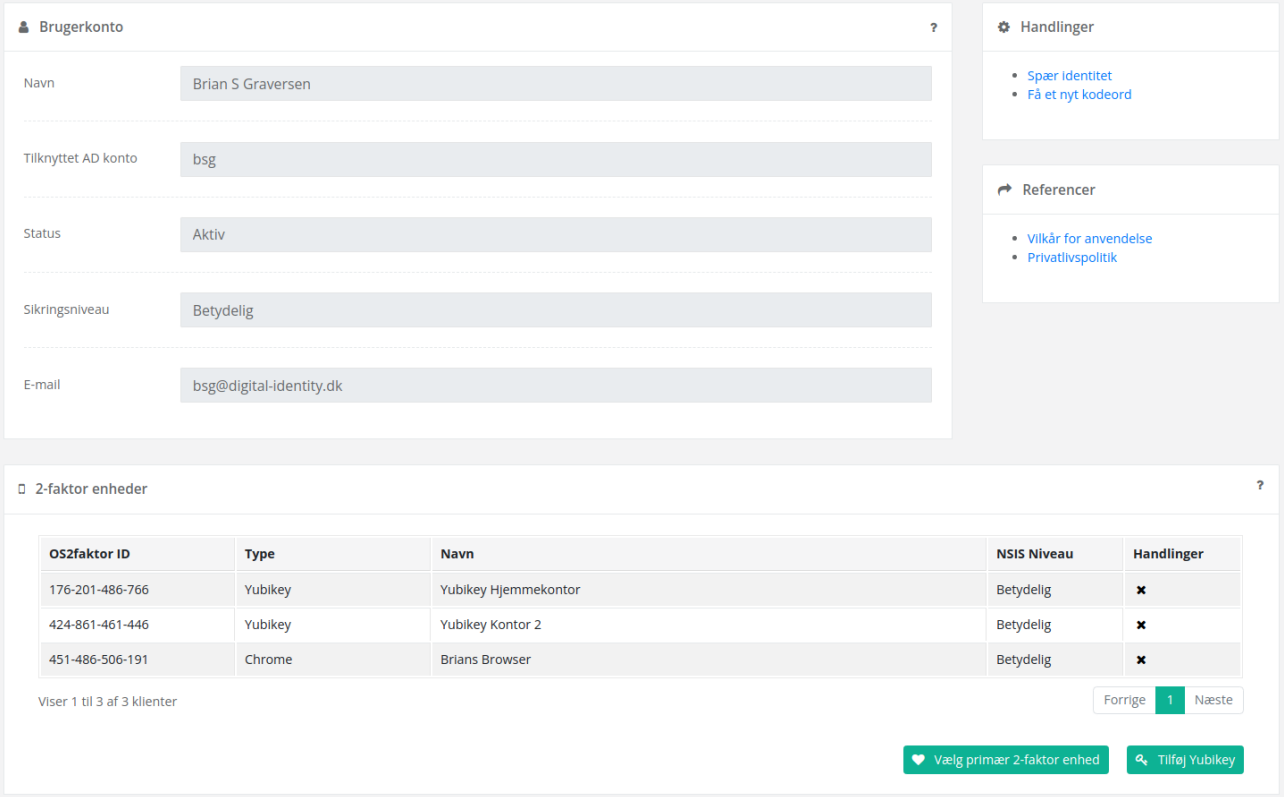
De forskellige spærremetoder sætter forskellige spærre-flag på erhvervsidentiteten, og så længe der er blot ét spærreflag på en erhvervsidentitet, er den funktionelt spærret og kan ikke anvendes.

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

En illustration af selvbetjeningenssiden er vist nedenfor.



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

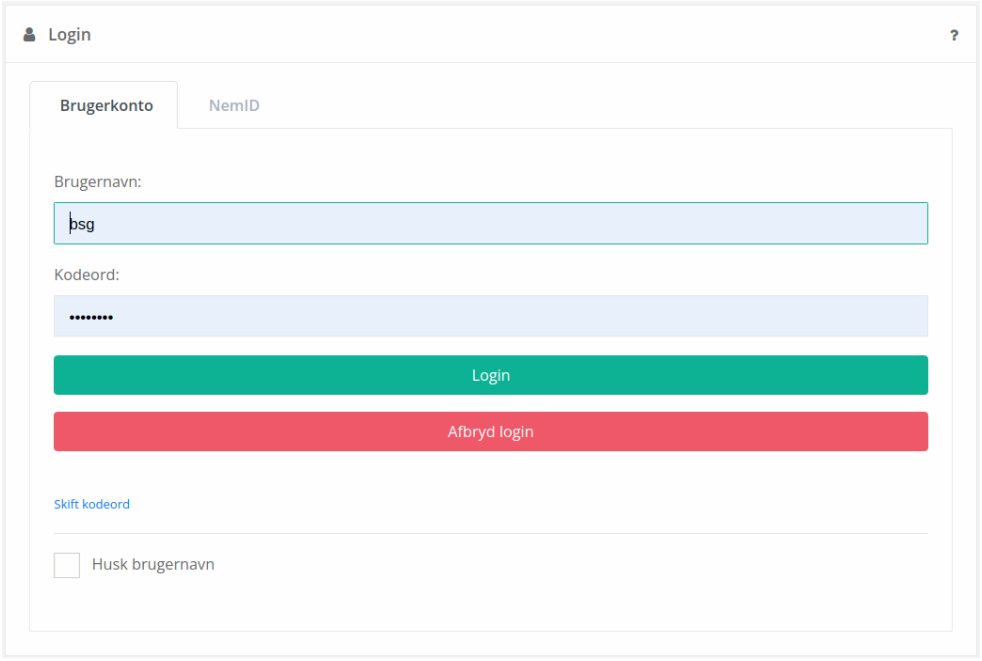
1. En loginforespørgsel modtages fra en af de 3 infrastrukturerer (NemLog-in3, KOMBIT eller STIL)
2. Brugeren foretager login med 1-faktor (brugernavn/kodeord)
3. Det valideres om denne erhvervsidentitet må tilgå den nævnte infrastruktur (jf datagrundlaget leveret af Kommunen)

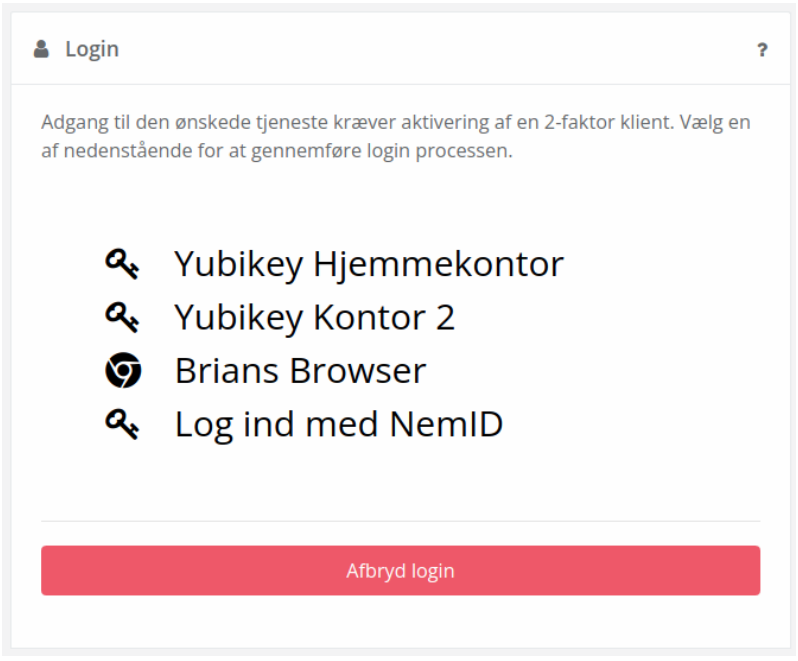
4. Hvis loginforespørgslen stiller krav om 2-faktor login (anmodning om step-up, NSIS Niveau Betydelig eller tilsvarende), så initeres et 2-faktor login forløb
5. Efter login er gennemført, hentes evt roller fra OS2rollekatalog, som medsendes SAML login billetten

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.

Et eksempel på login flowet er vist nedenfor



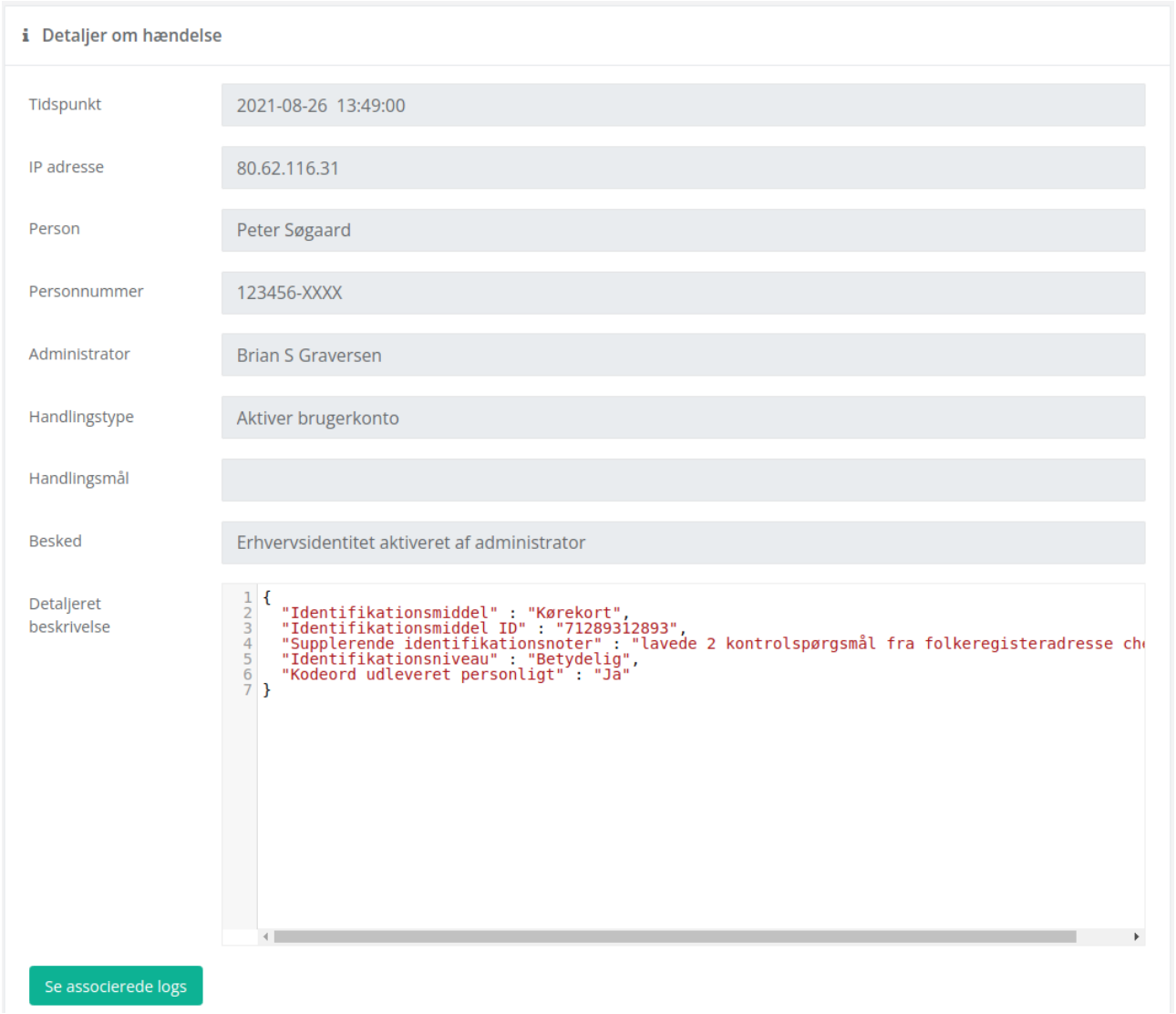


2.4 Lognings- og rapporteringsmodul

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.

Et eksempel på oversigten over loggen er vist længere oppe – der opsamles en række oplysninger om hver hændelse, og der kan tilgås et detaljeret billede af hver loghændelse som vist nedenfor



Logs kan alene læses, men ikke redigeres/slettes via den administrative brugergrænseflade. Det er kun personer med adgang til administratorportalen der kan tilgå loggen, og logindgange gemmes i 13 måneder, hvorefter de slettes fra løsningens database. Logs gemmes i databasen, så de er underlagt backup på lige fod med andre forretningsdata.

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.

Denne integration fungerer både med et on-premise Active Directory, eller et Azure Active Directory.

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

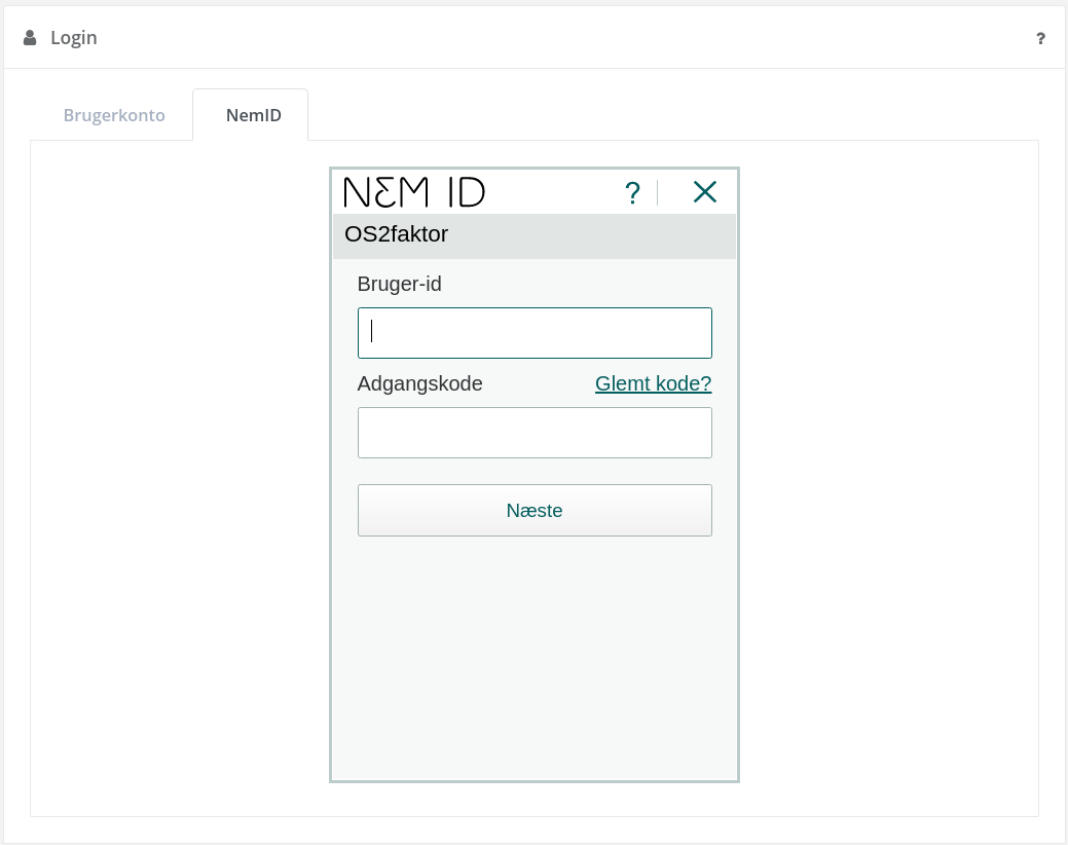
Løsningen udstiller SAML metadata, som kan indlæses direkte i STILs uni-login broker.

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 og MitID

Løsningen integrerer direkte med NemID, som er indlejret i løsningen som illustreret nedenfor. Denne integration fases ud til fordel for en integration med NemLog-in3, som sikrer at både NemID og MitID kan anvendes.

Integrationen til NemLog-in3 som identifikationsmetode, forventes udviklet ved udgangen af 2021.



3.6 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 er designet så den kan hente rettigheder fra andre systemer, herunder indlæsning fra AD via AD grupper. Disse funktioner kan løbende udvides med andre kilder efter behov.

3.7 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).

3.8 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, er der til at starte med kun udviklet en integration til OS2faktor MFA. Løsningen kan løbende udvides med yderligere MFA løsninger efter behov.

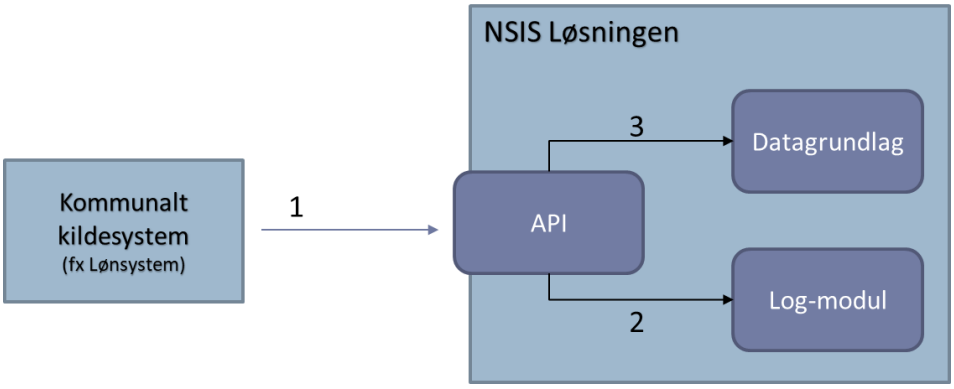
Bemærk at den valgte MFA løsning skal understøtte en registrerings- og spærreproces som lever op til kravene i NSIS, da den vil indgå i den samlede revision.

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

4 Processer, arbejdsgange og dataflow

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 her har løsningen allerede standardintegrationer til en række datakilder, herunder

- Active Directory
- Azure Active Directory
- SOFD Core

Selve integrationen foregår ved at det lokale system leverer data til en REST/JSON snitflade udstillet på løsningen. Snitfladen er dokumenteret og nem at anvende, og kan modtage både fulde loads samt løbende delta opdateringer.

Digital Identity kan assistere med at udvikle lokale integrationer, hvis standardintegrationerne ikke kan finde anvendelse i ens kommune.

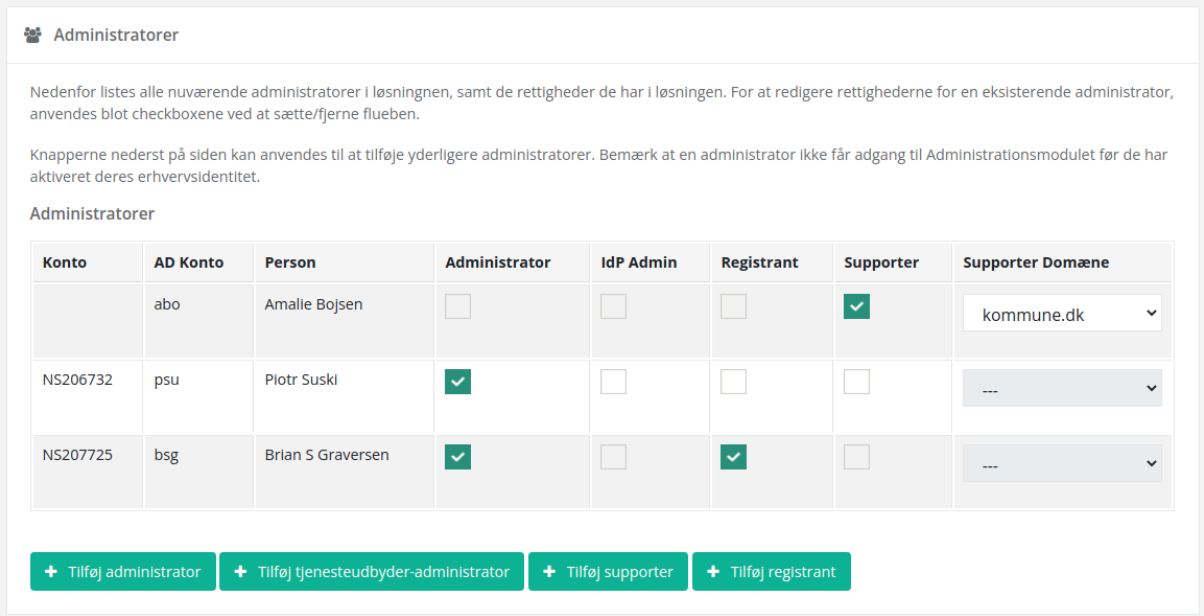
Når data indlæses i Løsningen, sker der følgende

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

Personer der har fået udstedt en erhvervsidentitet kan tildeles adgang til administrationsmodulet. Administrationen af hvem der har administrator-adgange styres inde fra administrationsmodulet (Digital Identity opsætter kommunens første administrator).

Skærmbilledet til administration af administratorer er vist nedenfor. Det er på nuværende tidspunkt at give følgende adgange til administrationsmodulet



- **Supporter**. Denne rolle har læseadgang, og kan afgrænses til ét domæne. Supporteren kan
  - Se hændelsesloggen (indenfor eget domæne)
  - Se alle brugere og deres detaljer (indenfor eget domæne)
  - Trække rapporter og opsætte info-beskeder i login-processen
- **IdP Administrator**. Denne rolle kan administrere integrationer til tjenesteudbydere, samt andre integrationer herunder RADIUS opsætning. Denne rolle giver også samme adgangen som dem en supporter har, men på tværs af alle domæner.

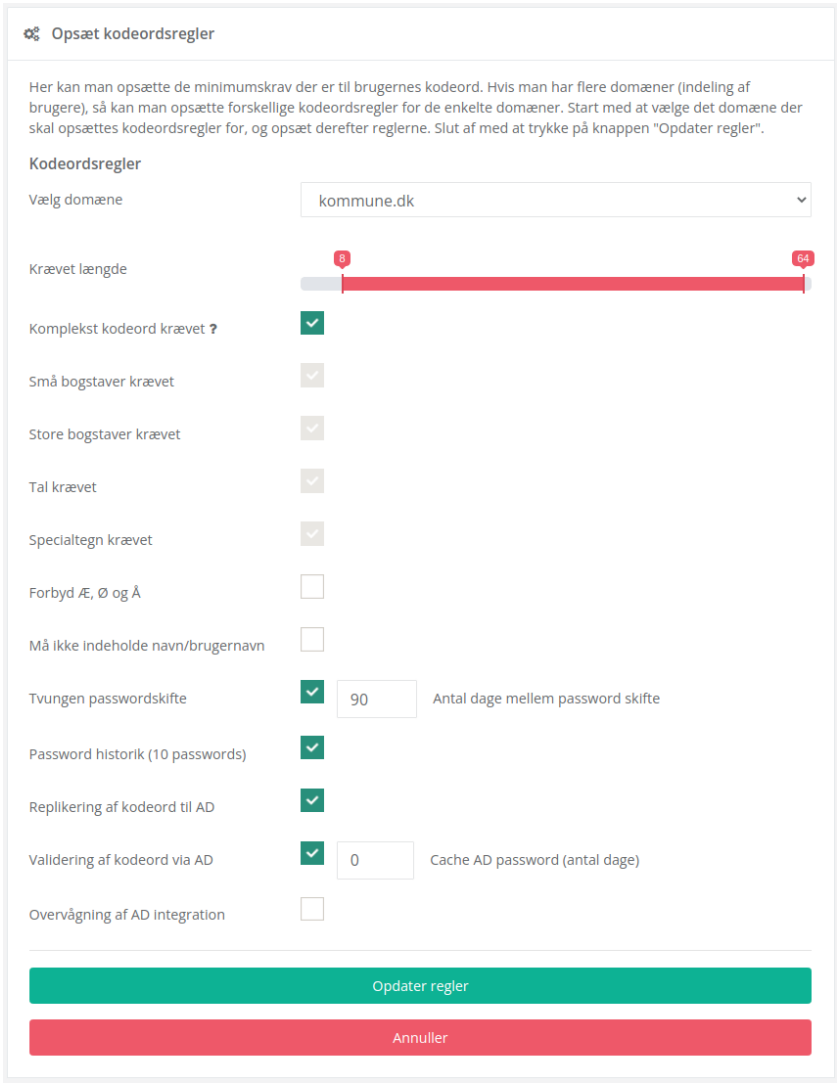
- **Registrant**. Denne rolle gives til betroede medarbejdere der kan udføre aktivering af brugeres erhvervsidentiteter (skal bruges til medarbejdere der ikke vil bruge NemID/MitID til aktivering).
- **Administrator**. Denne rolle kan administrere den tekniske opsætning af løsningen, herunder rolleadministration. Denne rolle giver også samme adgange som Supporter og IdP Administrator rollen, men har ikke adgang til Registrant funktionaliteten (omend en person med denne rolle kan tildele Registrant rollen til sig selv).

Administratorrollen kan udføre en række opgaver som er relevante for anvendelsen af løsningen, herunder

4.2.1 Opsætning af kodeordsregler

Løsningen håndterer kodeordsskifte (beskrevet i detaljer længere nede), og til det formål skal Løsningen kende de regler der gælder for kodeords kompleksitet. Denne opsætning foretages af en administrator ved at udfylde nedenstående formular. Der kan opsættes forskellige regler for kodeordskompleksitet per domæne.

Det er også muligt at opsætte regler for replikering og validering af kodeord op mod kommunens Active Directory (denne validering kan foregå både mod et on-premise AD eller et Azure AD).

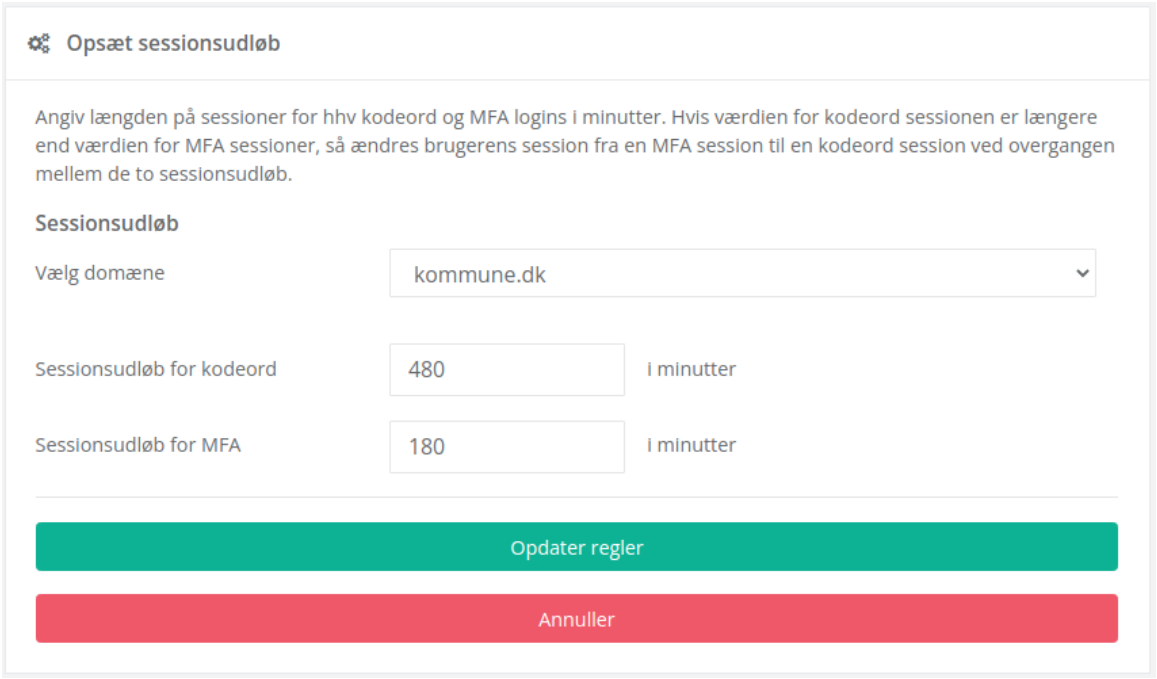


4.2.2 Opsætning af sessionsudløb

En af kravene i NSIS er at sessioner SKAL have et tidsmæssigt udløb. For at understøtte dette, samt sikre den højeste fleksibilitet, kan dette opsættes per domæne, samt per loginmiddel.

I praksis opsættes det via nedenstående skærmbillede, som skal forstås på følgende måde

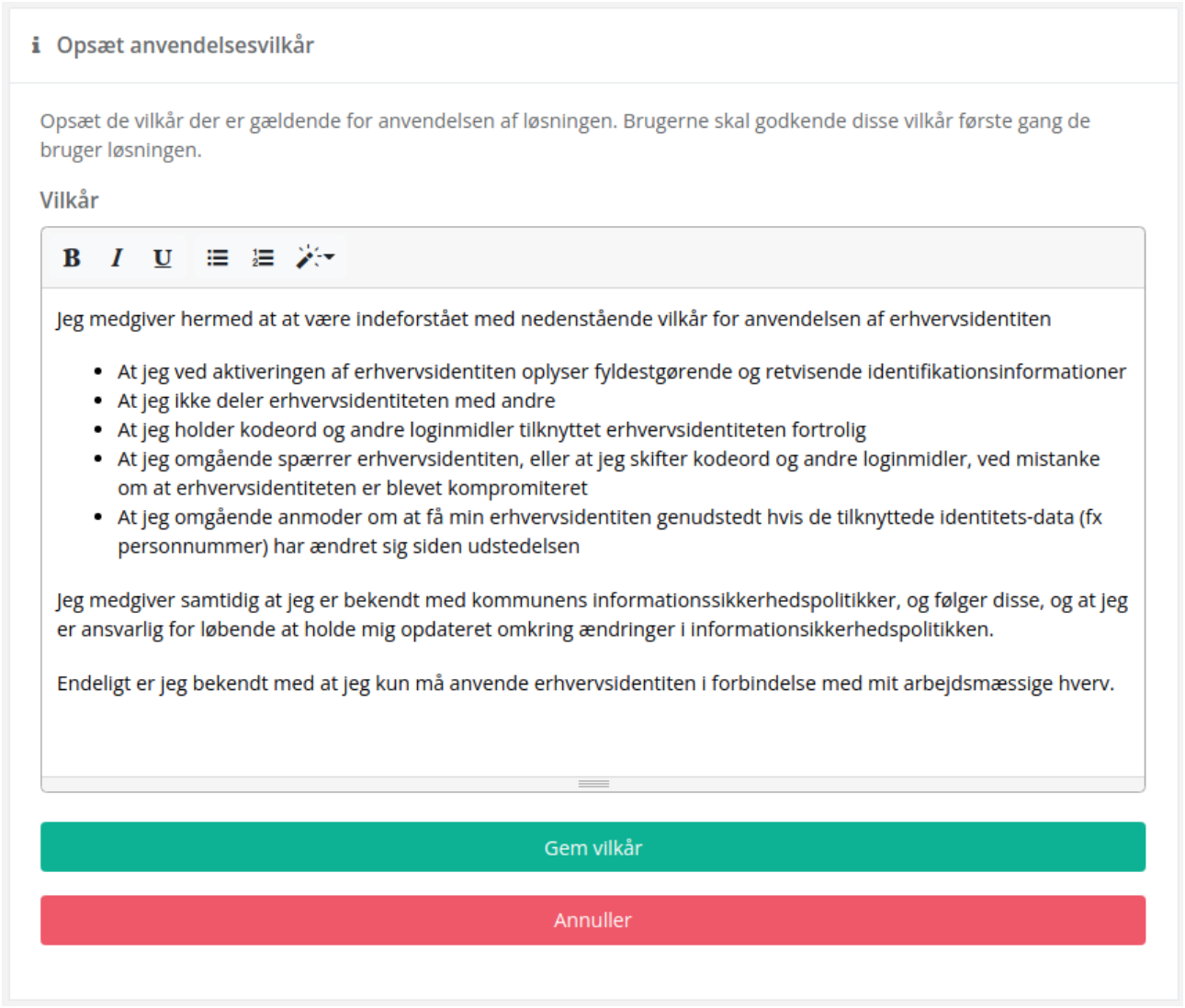
- Sessionsudløbet for kodeord styrer hvor langt tid der går mellem at brugeren SKAL indtaste sit kodeord igen. Hvis man fx sætter det til 480 minutter som vist nedenfor, og brugeren møder ind kl 08:00 om morgenen og logger ind med sit kodeord, så vil kodeords-sessionen udløbe kl 16:00, hvor brugeren så vil blive bedt om kodeord igen (hvis brugeren forsøger et nyt login – brugeren logges ikke ud af systemer som brugeren allerede er logget ind i)
- Sessionsudløbet for MFA (2-faktor) styrer hvor langt tid der går mellem at brugeren skal anvende sin 2-faktor enhed. I eksemplet er den sat til 3 timer



Ved at splitte sessionslevetiden op for hhv kodeord og 2-faktor login'et, giver det en større fleksibilitet i udarbejdelsen af den risikovurdering der vil styre de sessionsværdier man ender med at opsætte.

4.2.3 Opsætning af vilkår

I forbindelse med udstedelsen af en erhvervsidentitet skal brugeren aktivt afkræves en accept af de vilkår som de må anvende deres erhvervsidentitet under. Løsningen er født med et sæt af standardvilkår som overholde de minimumskrav som NSIS stiller til sådanne vilkår, men det er muligt (og anbefalet) at kommunen tilpasser disse vilkår. Dette kan gøres via nedenstående skærmbillede



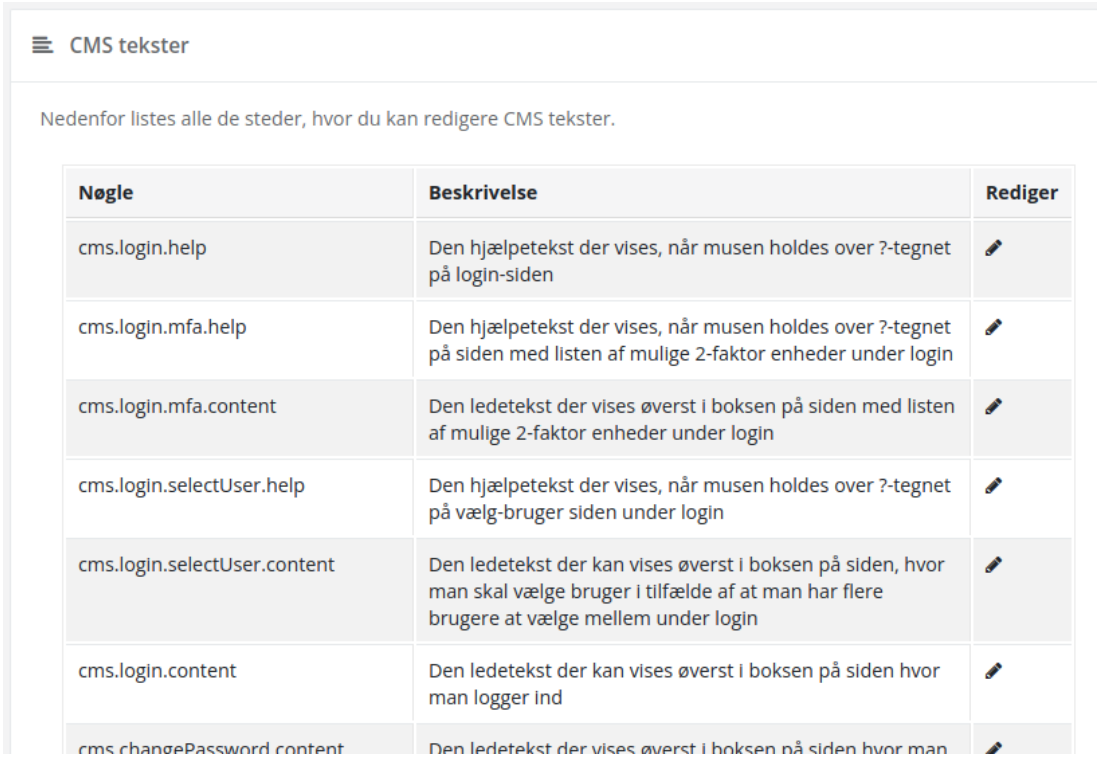
Løsningen sørger for at præsentere disse anvendelses- og privatlivsvilkår for brugeren i forbindelse med aktiveringen, og fører det nødvendige logspor for denne aktivitet.

4.2.4 Redigering af lede- og hjælpetekster i Løsningen

Da Løsningen anvendes af mange forskellige kommuner, kan der være et behov for at tilpasse og målrette den slut-bruger kommunikation der foregår via Løsningen.

Alle skærmbilleder der udstilles til slutbrugerne kan tilpasses, hvor både lede- og hjælpetekster kan redigeres via administrationsmodul.

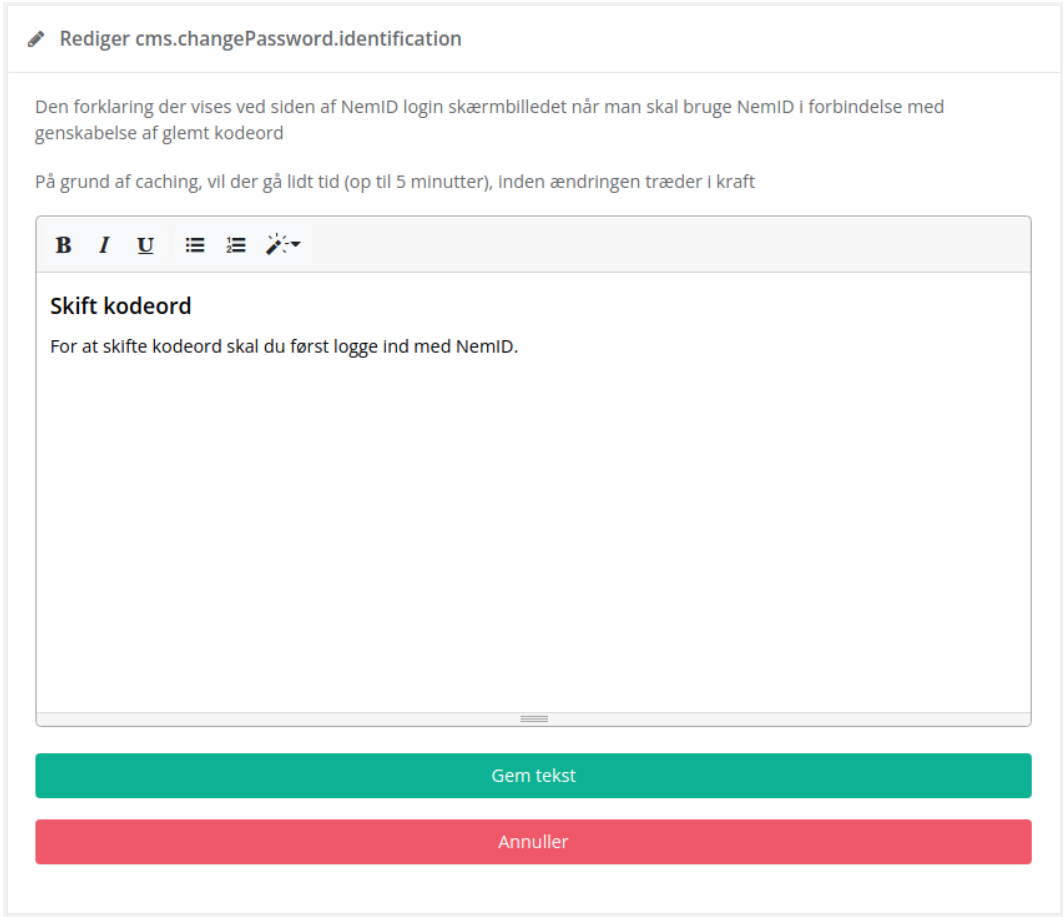
En administrator kan tilgå en liste over alle eksisterende tekster i Løsningen samt redigere disse. En ændring vil slå igennem indenfor få minutter, så effekten kan verificeres med det samme uden involvering af driften.



CMS tekster

Nedenfor listes alle de steder, hvor du kan redigere CMS tekster.

Nøgle	Beskrivelse	Rediger
cms.login.help	Den hjælpetekst der vises, når musen holdes over ?-tegnet på login-siden	
cms.login.mfa.help	Den hjælpetekst der vises, når musen holdes over ?-tegnet på siden med listen af mulige 2-faktor enheder under login	
cms.login.mfa.content	Den ledetekst der vises øverst i boksen på siden med listen af mulige 2-faktor enheder under login	
cms.login.selectUser.help	Den hjælpetekst der vises, når musen holdes over ?-tegnet på vælg-bruger siden under login	
cms.login.selectUser.content	Den ledetekst der kan vises øverst i boksen på siden, hvor man skal vælge bruger i tilfælde af at man har flere brugere at vælge mellem under login	
cms.login.content	Den ledetekst der kan vises øverst i boksen på siden hvor man logger ind	
cms.changePassword.content	Den ledetekst der vises øverst i boksen på siden hvor man	



Rediger cms.changePassword.identification

Den forklaring der vises ved siden af NemID login skærmbilledet når man skal bruge NemID i forbindelse med genskabelse af glemt kodeord

På grund af caching, vil der gå lidt tid (op til 5 minutter), inden ændringen træder i kraft

Skift kodeord

For at skifte kodeord skal du først logge ind med NemID.

Gem tekst

Annuller

4.3 Registreringsproces

Aktivering af erhvervsidentiteter er baseret på selvbetjening. Det er dog muligt for en administrator med rollen "Registrant" at udføre en aktiveringen udenom selvbetjeningsmodulet. Hvis man vælger at gøre brug af den sidste model, skal man være opmærksom på at registranternes arbejdsopgaver I så fald falder ind under den revision som kommunen skal have udført (løsningen sikrer logsporet, men de organisatoriske krav til processen skal løftes af kommunen).

4.3.1 Selvbetjeningsprocessen

En bruger der ønsker en erhvervsidentitet skal tilgå selvbetjeningsmodulet og gennemføre aktiveringssprocessen. Dette håndteres på følgende måde

1. Brugeren identificerer sig selv vha MitID eller NemID
2. Løsningen henter det CPR nummer der er knyttet til brugerens identifikationsmiddel og holder den op mod det datagrundlag som kommunen har indlæst i løsningen. Hvis CPR nummeret ikke eksisterer, eller den indlæste brugere ikke har fået tildelt en erhvervsidentitet (man må gerne indlæse brugere i løsningen som ikke skal have en erhvervsidentitet)
3. Hvis brugeren må få en erhvervsidentitet, præsenteres brugeren for de vilkår der er opsat i Løsningen, og ved accept aktiveres deres erhvervsidentitet
4. Brugeren bliver nu bedt om at vælge et kodeord til deres erhvervsidentitet. Hvis replikering til AD er slået til, vil det valgte kodeord blive synkroniseret til AD, så disse er i sync.
5. Brugeren informeres om at deres erhvervsidentitet er udsted og klar til anvendelse

Hele processen logges undervejs i de enkelte trin, og logsporet kan ses inde i administrationsmodulet.

Alternativt, hvis en bruger er tildelt en erhvervsidentitet som ikke er aktiveret endnu, og brugeren forsøger at gennemføre et login til et fagsystem, så vil brugeren blive spurgt om de ønsker at aktivere deres erhvervsidentitet i forbindelse med login.

Her er processen lidt anderledes, da den sker indlejret i et eksisterende login

1. Brugeren forsøger at logge ind i et fagsystem der er koblet op på Løsningen
2. Løsningen præsenterer login dialogen for brugerne hvor brugeren logger på med sit normale AD brugernavn/kodeord (Løsningen validerer dette mod kommunens AD).
3. Løsningen ser at brugeren har en ikke-aktiveret erhvervsidentitet, og spørger brugeren om denne ønskes aktiveret
4. Hvis brugeren siger ja, bedes brugeren identificere sig vha NemID/MitID – her foretages en kontrol af at det anvendet NemID/MitID er koblet til samme CPR nummer som den AD konto som brugeren forsøge at logge ind med
5. Hvis CPR matcher, vises vilkår for anvendelse af erhvervsidentiteten for brugeren, som skal godkende disse
6. Efter godkendelse, informeres brugeren om at deres erhvervsidentitet er aktiveret og login fortsætter som normalt

I ovenstående model indrulleres det AD kodeord som brugeren loggede ind med, og et password skifte er ikke nødvendigt.

Alle informationstekster der vises for brugeren i disse processer er redigerbare via administrationsmodulet.

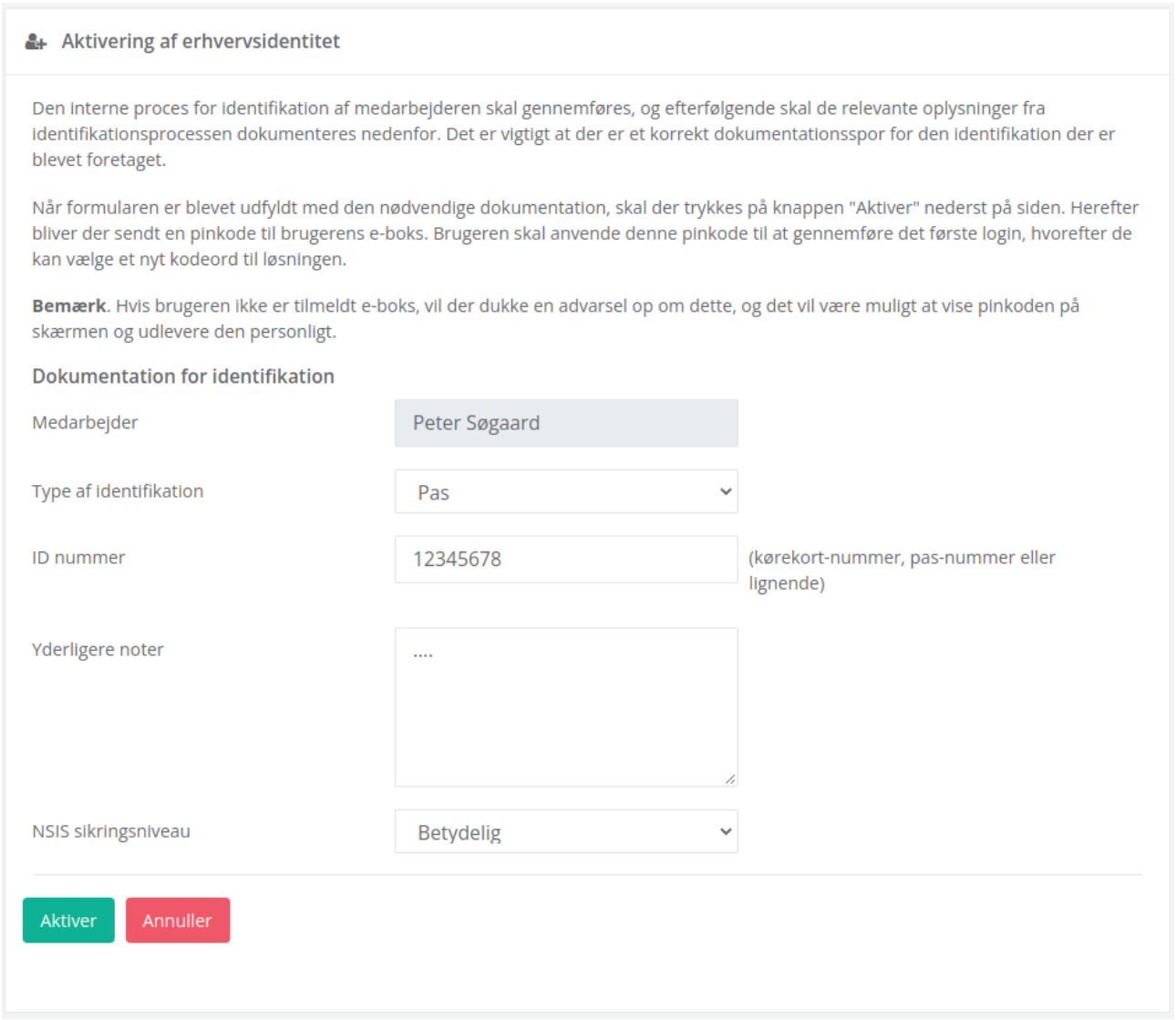
4.3.2 Registrant processen

Hvis en bruger ikke ønsker at anvende sit NemID/MitID til at identificere sig selv under aktiveringsprocessen, kan kommunen vælge at understøtte en manuel aktiveringsproces, hvor brugeren skal møde fysisk op i borgerservice, servicedesk, eller hvad end helpdesk funktion som kommunen udpeger til formålet.

Her skal en betroet medarbejder (kaldet en Registrant), udføre en identifikation af brugeren. Der er en række krav i NSIS til denne identifikationsproces, som registranten skal følge. Løsningen udstiller en webformular til registranter, hvor de kan dokumentere udførslen af denne proces, og afslutte aktiveringen af medarbejderens erhvervsidentitet.

Løsningen sender derefter en pinkode til brugerens e-boks, som skal bruges ved første login for at afslutte aktiveringsprocessen.

Webformularen til aktivering for registranter er vist nedenfor

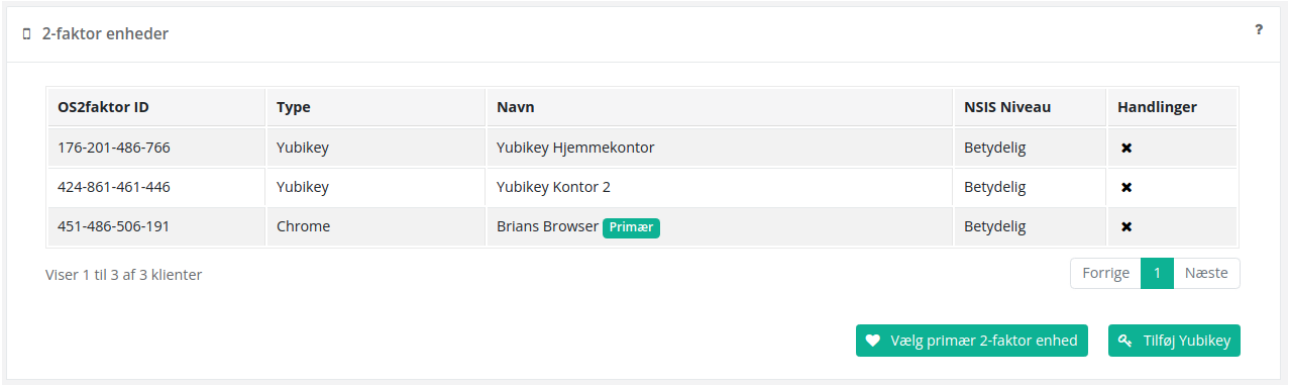


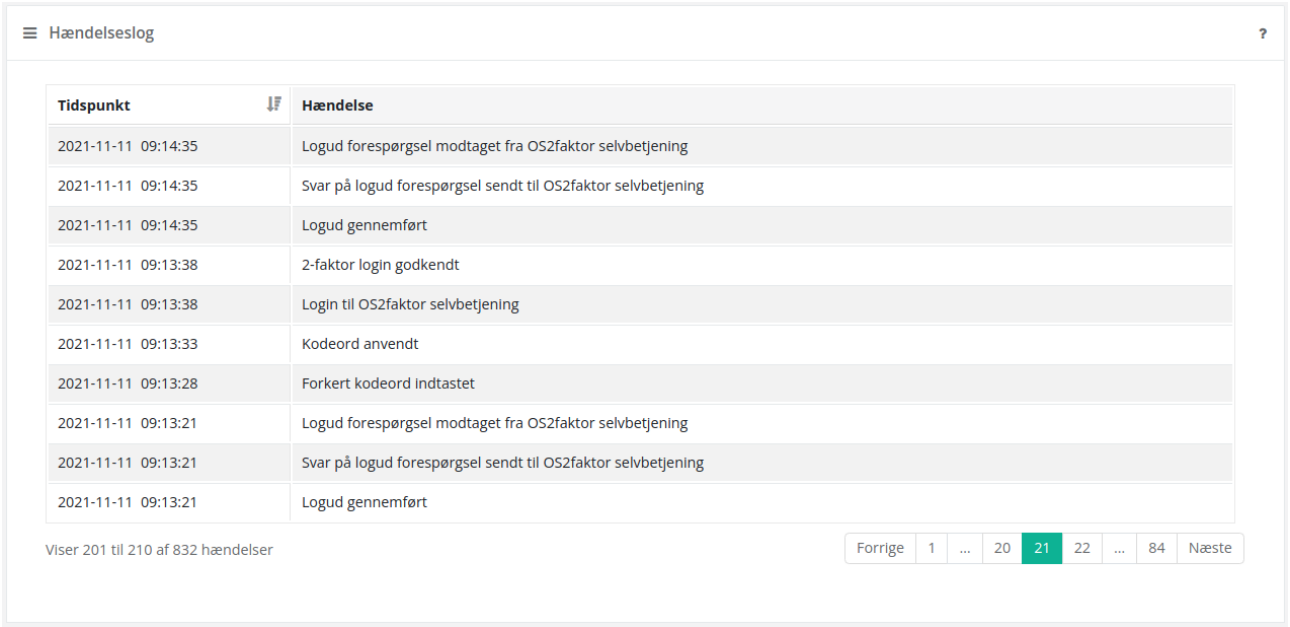
4.4 Selvbetjeningsmodulet

Alle brugere der er registreret i Løsningen, kan logge ind i selvbetjeningsmodulet, hvor de bl.a. har adgang til 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)
- Administrere deres 2-faktor enheder
- Se en fuld log over alt hvad der er sket med deres konto, og hvad den er blevet anvendt til

Nogle af disse funktioner er illustreret nedenfor





4.5 Login til NemLog-in3, KOMBIT Context Handler, osv...

Login flowet til tjenesteudbydere der kræver et NSIS niveau er identisk, og Løsningen kan kobles på alle de tjenesteudbydere og infrastrukturer som det ønskes.

Opsætningen udføres via administrationsmodulet, og selve login for slutbrugerne forløber som beskrevet nedenfor

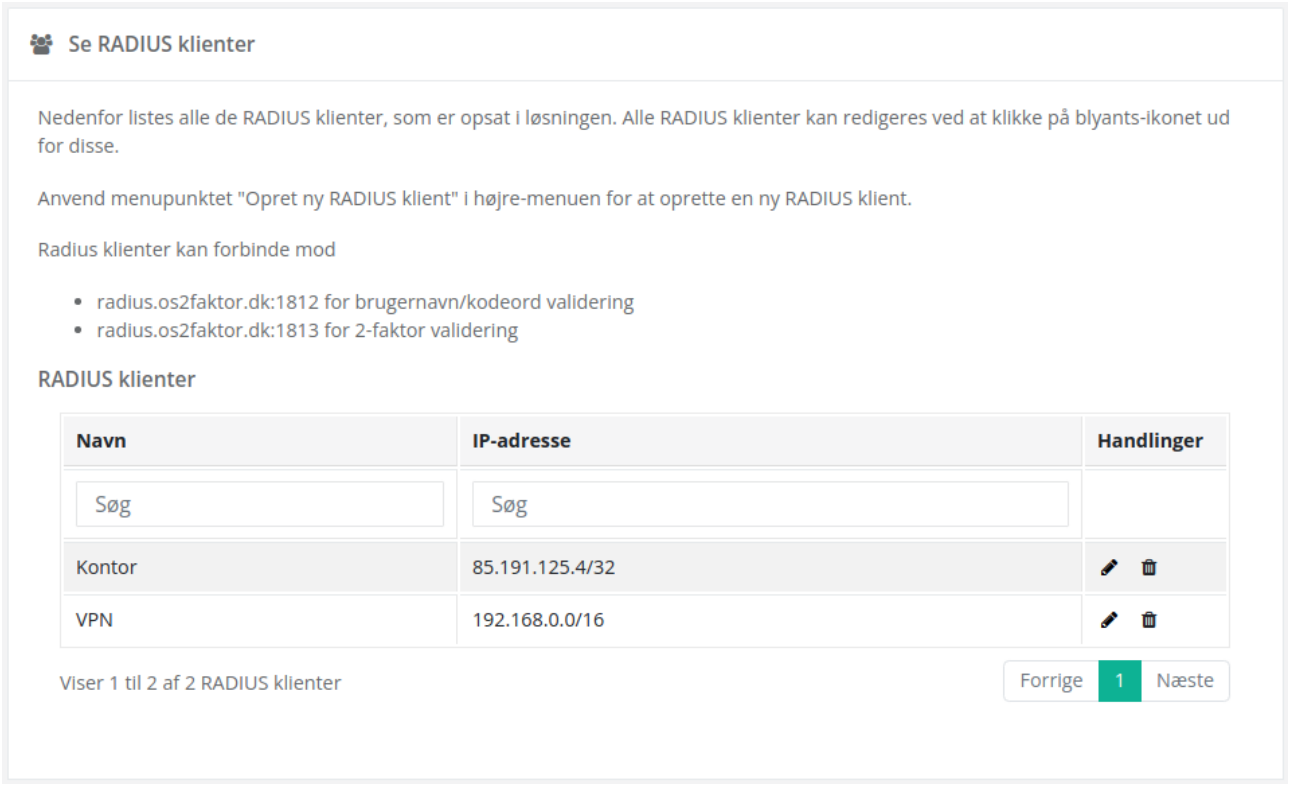
1. Et fagsystem (eller en infrastruktur proxy som NemLog-in3 eller KOMBITs Context Handler) sender en login forespørgsel til Løsningen fordi en bruger har initieret login processen i fagsystemet
2. Løsningen gennemfører login processen på det NSIS Niveau som fagsystemet efterspørger (Lav eller Betydelig). Ved niveauet Betydelig gennemføres også et 2-faktor login, og ved Lav er det kun et brugernavn/kodeord login der foretages. Hvis brugeren allerede har en login session, kan dette reducere loginflowet som beskrevet i nedenstående underbullets
    a. Hvis brugeren har en eksisterende session på samme NSIS niveau som fagsystemet efterspørger, så foretages et login uden bruger-interaktion (single signon oplevelsen)
    b. Hvis brugeren har en eksisterende session på NSIS Lav, og fagsystemet efterspørger NSIS Betydelig, springer Løsningen brugernavn/kodeord dialogen over, og går direkte til 2-faktor login flowet.
3. Løsnigen udsteder en login billet, som sendes til fagsystemet
4. Brugeren er nu logget ind i fagsystemet

Ovenstående er et helt standard SAML login flow, som det er kendt fra andre Identity Provider løsninger. Dog understøttes følgende avancerede SAML funktioner også af løsningen

- **Aktive logins**. Et fagsystem kan efterspørge at en eksisterende session skal tilsidesættes og brugeren SKAL spørges gennemføre et fuldt login flow
- **Passive logins**. Et fagsystem kan spørge om brugeren har en eksisterende session, og kun trigge et login flow hvis den ved det vil resultere i et SSO login uden brugerinteraktion
- **Videregivelse af proxy oplysninger**. Hvis "fagsystemet" er en infrastruktur komponent, der blot viderestiller login'et fra et egentligt fagsystem (dvs den måde KOMBITs Context Handler og NemLog-in3 fungerer på), så kan Løsningen modtage informationer om det bagvedliggende fagsystem, og tilpasse login og logning til denne yderligere information (fx kan Løsningen opsætte individuelle MFA krav per fagsystem i KOMBIT infrastrukturen)
- **Håndtering af step-up**. Step-up forespørgsler fra fagsystemer som allerede har en session med brugeren, håndteres som forventet ved at øge sikkerhedsniveauet med 2-faktor når dette eftespørges

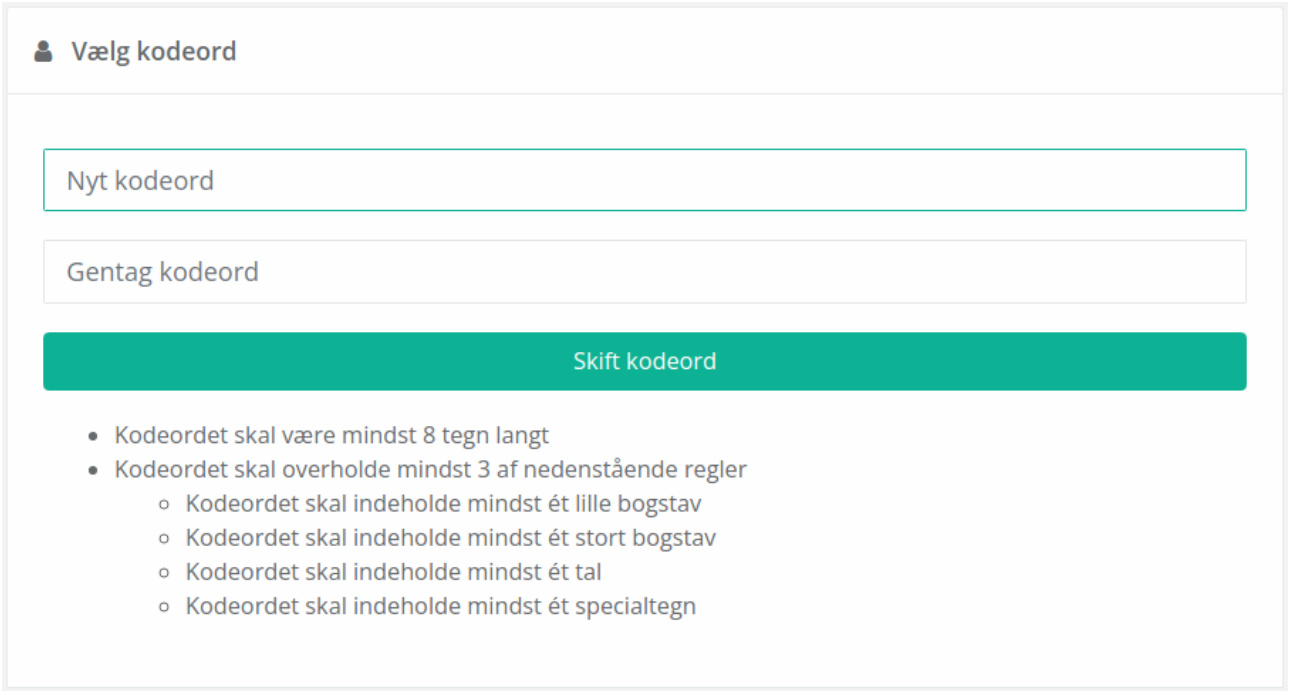
4.6 Login via RADIUS

Løsningen udstiller RADIUS endpoints, der kan anvendes af fx VPN og andre løsninger der understøtter RADIUS som en login mekanisme. I Administrationsmodulet kan man opsætte RADIUS klienter, samt krav til anvendelse (gruppemedlemsskaber, domæne-tilhørsforhold, osv) og login-niveau (brugernavn/kodeord og/eller 2-faktor login)



4.7 Kodeordsskifte

Løsningen udstiller flere snitflader til password skifte, der kan anvendes af slutbrugeren. Når der foretages et password skifte, skal det nye kodeord overholde de krav til password kompleksitet der er opsat i administrationsmodulet, og brugeren hjælpes til at overholde disse krav som illustreret nedenfor



Når brugeren skifter sit kodeord, så replikeres det nye kodeord til kommunens Active Directory (on-premise AD eller Azure AD), så brugeren har en oplevelse af at have ét brugernavn og ét kodeord uagtet hvordan de foretager deres login.

4.7.1 Snitflader til kodeordsskifte

En bruger der ønsker at skifte sit kodeord (eller har glemt sit nuværende kodeord), kan anvende Løsningen til at foretage et kodeorsskifte (eller danne et nyt kodeord) på følgende måder

- Via en web-baseret selvbetjeningsside, hvor man både kan skfite sit nuværende kodeord, eller danne et nyt kodeord hvis man har glemt sit gamle. Hvis man har glemt sit kodeord, skal man identifice sig med NemID/MitID.
- Via windows login skærmen, hvor man kan trykke på "Jeg har glemt mit kodeord", der så åbner et password skifte vindue, hvor man først skal anvende sit NemID/MitID, og så vælge et nyt kodeord
- Via administrationsmodulet, hvor en Registrant kan danne et nyt kodeord til brugeren. Dette kræver fysisk fremmøde og kontrol af nationalt anerkendt billed-id, lige som ved udstedelsen. Løsningen samler det fornødne logspor, og Registranten skal udføre den krævede kontrol af billed-id'et udenfor Løsningen.
- Via Windows indbyggede "skift kodeord" dialog. Hvis en bruger skifter kodeord her, så replikerings kodeordet op til Løsningen (ud over selvfølgelig at blive skiftet i AD'et).

Integrationen til Windows (login skærmen og skift-kodeord dialogen) understøttes ved en såkaldt Windows Credentials Provider, der skal installeres på windows PC'en.

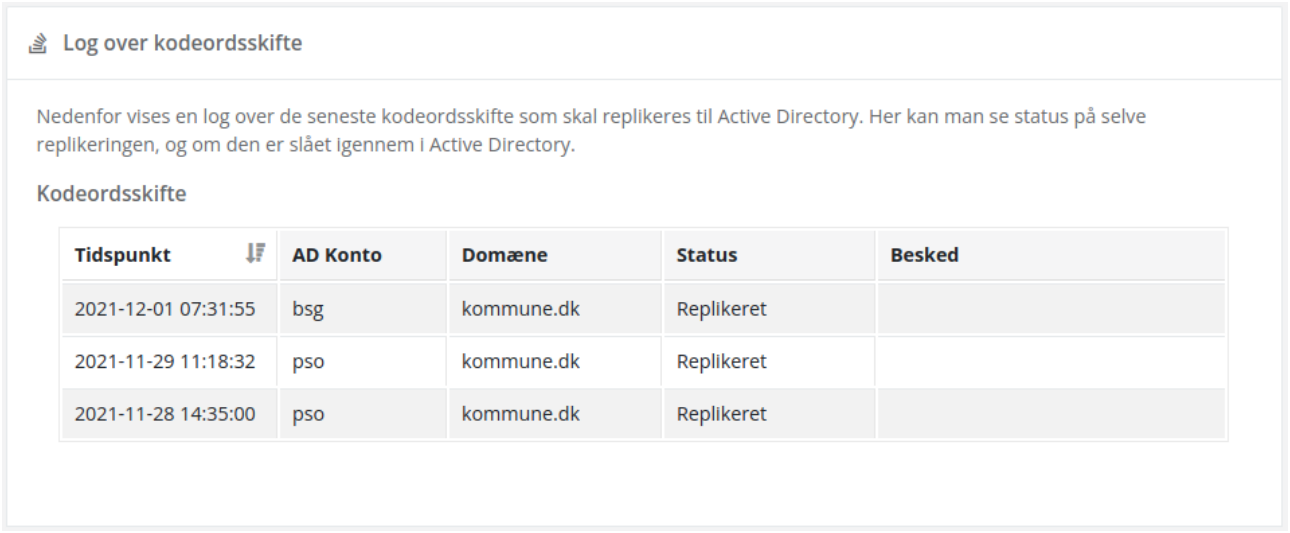
Denne integration sikrer også samtidig at login sessionen etableres ved login til windows maskinen, så brugerne oplever fuld single-signon helt fra første windows login.

4.7.2 Høj-niveau beskrivelse af kodeordsskiftet mod AD

Det forsøges altid at lave en realtidsreplikering af kodeordet, så brugeren får direkte feedback omkring kodeordsskiftet. Hvis forbindelsen til kommunens AD ikke er tilgængelig under kodeordsskiftet, skiftes kodeordet i Løsningen, og der lægges et kodeordsskifte ud på en replikeringskø, som løbende forsøges replikeret til kommunens AD.

Skulle denne replikering ikke kunne lade sig gøre indenfor de næste 10 minutter, går der en alarm på denne fejl. Alarmen går altid til Digital Identity, men man kan vælge at få en kopi af denne alarm tilsendt via opsætning af en overvågnings-email i administrationsmodulet.

Man kan se en status på alle kodeordsreplikeringer i administrationsmodulet som illusteret nedenfor



Hvis der er opstået en fejl, vil alle detaljer om fejlen stå i kolonnen "Besked", som kan bruges til fejlsøgning. De typiske årsager til en fejlet replikering er

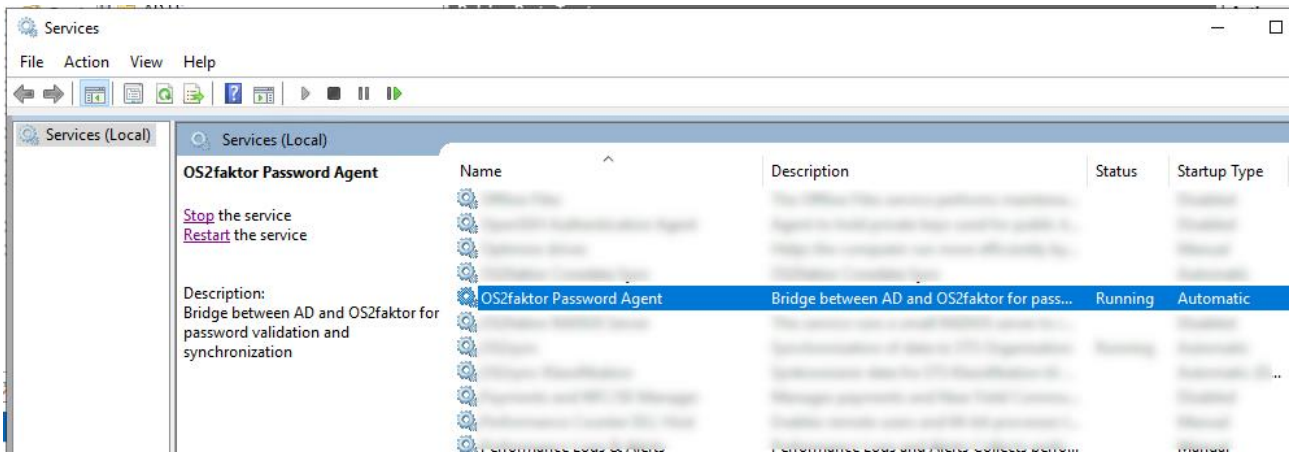
- Ingen forbindelse til kommunens AD
- Manglende rettigheder til at skifte kodeord

Den første imødekommes med et high-availability setup som beskrevet nedenfor, og den sidste skyldes typisk at den servicekonto der bruges til at foretage kodeordsskifte ikke har lov til at skifte kodeordet på den angivne AD konto (fx er det kun domæne administratorer der kan skifte kodeord på andre domæne administratorer).

4.7.3 Teknikken i replikeringen

På mindst 2 servere i kommunens infrastruktur installeres en kodeordsskifte-agent. En Windows Service som håndterer selve kodeords-replikeringen. Så længe mindst én af disse agenter er kørende, vil der være en aktiv replikeringsforbindelse til kommeuns AD, og realtidsreplikering vil være mulig.

Servicen er en standard-service, der kan installeres, startes, stoppes, genstartes, overvåges på lige fod med andre windows services



Agenten indeholder en websocket klient, der konfigureres med en signeringsnøgle. Agenten forbinder til en konfigureret websocket server der udstilles af OS2faktor løsningen, og forbindelsen autentificeres vha signeringsnøglen.

Websocket forbindelsen etableres over HTTPS/443, og er fuld duplex, så 2-vejs kommunikation mellem klient og server er mulig.

Alle beskeder der sendes mellem klient og server er signeret, og begge ender foretager den nødvendige validering. Forbindelsere re-etableres som minimum hver 2. time, men også automatisk ved netværksudfald eller server-genstart.

Hvis der på et tidspunkt er 0 agenter forbundet til et domæne, vil Løsningen smide en alarm. Denne alarm går altid til Digital Identity, men man kan vælge at modtage en kopi af denne alarm via opsætning af en overvågnings-email i administrationsmodulet.

Forsiden af administrationsmodulet viser forskellige metrikker, og her kan man bl.a. se antallet af aktive forbindelser per domæne.