DIGITALISERINGSSTYRELSEN

21. januar 2013
TG

Guide til integration med NemLog-in / Brugeradministration

Denne guide indeholder en kort beskrivelse af, hvorledes man som it-systemudbyder (myndighed eller it-leverandør) kan integrere en it-løsning til NemLog-in's brugeradministrationsløsning (herefter benævnt NemLog-in/Brugeradministration eller FBRS for *fællesoffentligt brugerrettighedsstyringssystem*). Guiden er henvendt til teknisk-orienterede personer, der skal planlægge eller udføre integrationen, og den beskriver de snitflader, som anvendes. Læseren antages således at være bekendt med basal terminologi indenfor føderationer og brugerstyring.

Guiden vil senere blive suppleret med den egentlige, tekniske dokumentation til NemLog-in/Brugeradministration, som offentliggøres i forbindelse med idriftsættelsen.

Baggrund

I januar 2013 blev første del af den nye NemLog-in-løsning sat i drift, og i andet halvår af 2013 er den nye brugeradministrationsløsning på NemLog-in planlagt til at følge efter. Løsningen vil erstatte og udbygge den nuværende brugerrettighedsløsning på virksomhedsportalen Virk.dk (Virk BRS), og eksisterende myndighedsløsninger tilsluttet Virk BRS vil blive migreret over på NemLog-in, hvorefter Virk BRS lukkes ned. Med andre ord vil al Virk's brugerstyring overgå til NemLog-in.

Overblik over grænseflader

Den nye FBRS løsning opererer med to forskellige grænsesnit til myndighedsløsninger:

a) Der findes et legacy grænsesnit, som emulerer de nuværende snitflader på Virk BRS løsningen. Disse kan kun anvendes af de myndighedsløsninger, der på migreringstidspunktet er tilsluttet Virk BRS.
b) FBRS løsningen kommer med en moderniseret grænseflade byggende på OIOSAML profilerne. Nye myndighedsløsninger, der tilsluttes efter migreringen, skal anvende denne grænseflade.

Bemærk at løsninger, der i dag anvender legacy snitfladen (a), skal overgå til den moderniserede snitflade, når løsningen opdateres (eksempelvis ved ændringer i løsningens metadata, skift af certifikat etc.). Dermed vil legacy-snitfladen kunne udfases i fremtiden (tidspunkt ikke fastlagt), når alle myndighedsløsninger er overgået til det nye grænsesnit.

Virk BRS legacy grænseflade

Myndighedsløsninger, der i dag er tilsluttet Virk BRS, integrerer via en eller flere af følgende grænseflader:

- Der anvendes en OIOSAML-baseret snitflade til log-in af og log-out af brugerne (SAML `AuthnRequest` SAML `LogoutRequest`).
- Der anvendes et OIOSAML-baseret `AttributeQuery` til at hente attributter om brugeren, herunder evt. rettigheder som brugeren måtte være blevet tildelt af en brugeradministrator.
- Virk BRS udstiller en SOAP-baseret web service (`LegalUnitService`), som kan anvendes til specielle formål.

Der henvises til Virk's systembeskrivelse [VIRK-SYS] og procesbeskrivelse [VIRK-PRO] for detaljer om disse snitflader.

Den nye FBRS løsning på NemLog-in er bagudkompatibel og viderefører i al væsentlighed Virk's nuværende grænseflader med henblik på, at myndighedsløsninger ikke behøver at blive ændret i første omgang. Der er dog en enkelt undtagelse, idet brugen af SAML Artifact binding ikke understøttes i NemLog-in, da denne ikke er tilladt iflg. OIOSAML.

Dette betyder samlet, at myndigheder som i dag har integreret med Virk BRS ikke forventes at få behov for kodeændringer i deres løsninger, såfremt man ikke anvender SAML Artifact Binding. Dermed er aktiviteterne forbundet med skiftet til NemLog-in reduceret til at importere NemLog-in's metadatafil (dvs. en konfigurationsændring) samt en mindre test af integrationen. Disse aktiviteter forventes at udgøre ganske få timers arbejde.

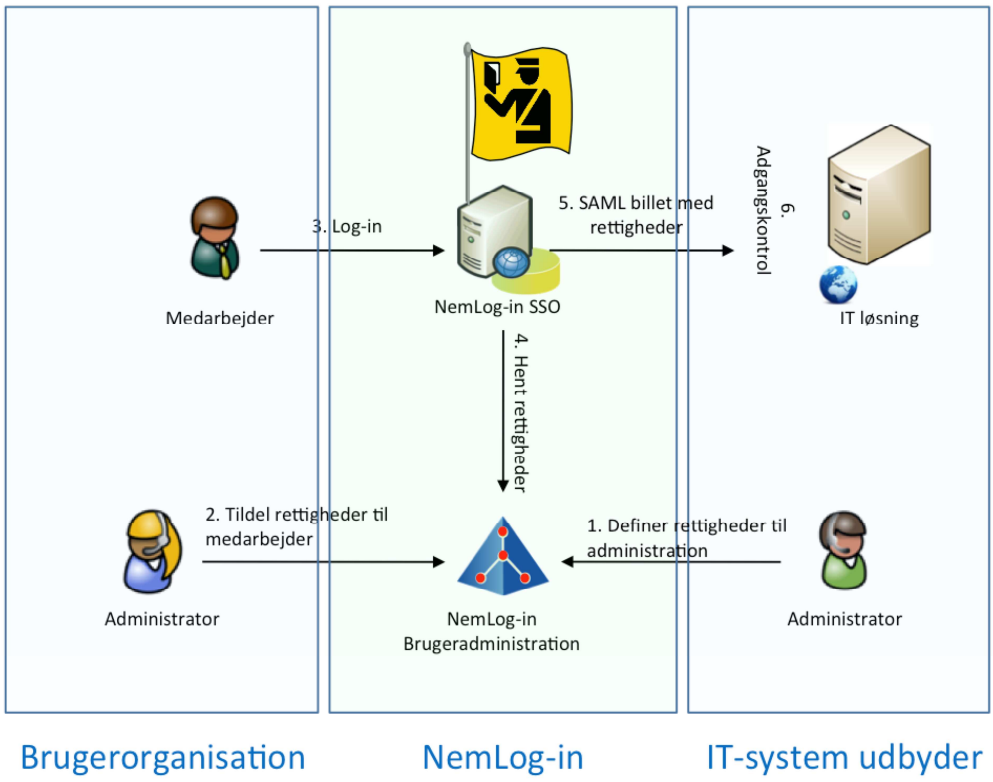
Digitaliseringsstyrelsen vil i god tid inden migreringsdatoen informere nærmere om processen forbundet med skiftet fra Virk BRS til NemLog-in. Processen vil overordnet være en "big-bang" migrering, hvor alle myndigheder og Virk.dk portalen skal skifte samtidigt.

Integration til NemLog-in's brugeradministration

NemLog-in FBRS er som Virk BRS en rollebaseret brugeradministrationsløsning, hvormed virksomheder og myndigheder kan administrere deres medarbejderes rettigheder til offentlige selvbetjeningsløsninger, der er er tilsluttet. Man kan tænke på det som et fællesoffentligt brugerkatalog, hvor hver virksomhed kan udpege et antal brugeradministratorer, der så tildeler medarbejderne i virksomheden de relevante rettigheder. Der er endvidere muligheder for, at rettigheder kan delegeres til andre organisationer (såkaldte erhvervsfuldmagter eller koncernfuldmagter).

Myndighedsløsningerne definerer selv de løsningsspecifikke rettigheder (kaldet *privilegier*), som ønskes administreret via FBRS. Derved slipper myndighedsløsningerne selv for at implementere en løsning til brugeradministration. Privilegierne tilføjes til roller i NemLog-in (af en NemLog-in administrator), som brugeradministratorerne herefter kan tildele til medarbejdere. Det er også muligt at tildele en rolle til mange medarbejdere på én gang ved at samle medarbejderne i en gruppe, som herefter tildeles rollen. Administrationskonceptet er illustreret på figuren nedenfor:

Integrationen fra myndighedsløsninger til NemLog-in FBRS sker via OIOSAML grænsefladen, som i forvejen anvendes til log-in. Når en medarbejder i en virksomhed er tildelt en eller flere roller af sin brugeradministrator, vil de tilhørende privilegier til løsningen fremgå af den SAML Assertion, som udstedes i forbindelse med log-in til løsningen. SAML billetten vil altså udover brugerens identitet være beriget med privilegierne. Den overordnede sammenhæng er illustreret på nedenstående figur:



Dette betyder, at myndighedsløsninger som i forvejen anvender NemLog-in til log-in formål, ikke behøver at integrere til nogle nye snitflader for at begynde at anvende brugeradministrationsløsningen i NemLog-in (FBRS).

For at benytte FBRS til administration af rettigheder skal myndigheden (eller dennes it-leverandør) først definere de (løsningsspecifikke) privilegier, som ønskes administreret (trin 1 på figuren). Disse defineres som et antal URI'er, der indmeldes til FBRS via NemLog-in's tilslutningssystem. Når privilegierne er tildelt en bruger (via en rolle), (trin 2 på figuren) vil de tilhørende URI'er som nævnt optræde i den SAML Assertion, som NemLog-in udsteder (trin 5). Herefter kan privilgierne anvendes i myndighedsløsningens adgangskontrol til at beslutte, hvilken adgang brugeren skal have (trin 6).

Syntaksen for indlejring af privilegier i SAML Assertions er defineret i OIOSAML Basic Privilege Profile [OIO-BPP]. Brugerens privilegier angives i attributten `dk:gov:saml:attribute:Privileges_intermediate` i den udstedte SAML Assertion. Et eksempel på denne er vist nedenfor:

```
<saml:Attribute FriendlyName="Privileges"
   Name="dk:gov:saml:attribute:Privileges_intermediate"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">
      <base64 encoded value>
  </saml:AttributeValue>
</saml:Attribute>
```

Værdien af attributten er en base64 indkodet streng, der kan dekodes til en XML struktur, som indeholder en liste af privilegier som vist i eksemplet nedenfor:

```
<?xml version="1.0" encoding="UTF-8"?>
<bpp:PrivilegeList
   xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
   <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:12345678">
       <Privilege>urn:dk:some_domain:myPrivilege1A</Privilege>
       <Privilege>urn:dk:some_domain:myPrivilege1B</Privilege>
   </PrivilegeGroup>
   <PrivilegeGroup Scope="urn:dk:gov:saml:seNumberIdentifier:27384223">
       <Privilege>urn:dk:some_domain:myPrivilege1C</Privilege>
       <Privilege>urn:dk:some_domain:myPrivilege1D</Privilege>
   </PrivilegeGroup>
</bpp:PrivilegeList>
```

`Scope` attributten på `PrivilegeGroup` elementet angiver den kontekst (afgrænsning), som gælder for de tildelte privilegier (repræsenteret ved `Privilege` elementer), der er indlejret. Disse vil typisk være organisatoriske enheder i form af et CVR nummer, et SE-nummer eller en P-enhed. Dette skal forstås således, at brugeradministratoren har begrænset rettigheden til kun at gælde for den angivne organisatoriske enhed. Til forskel fra modellen i Virk BRS kan brugeradministratorer i FBRS ved tildeling af alle rettigheder frit vælge scope – dvs. myndighedsløsningerne skal være forberedt på at modtage disse. Hvis et konkret scope ikke understøttes af løsningen (f.eks. SE-enheder), kan man ignorere rettigheden og/eller give brugeren en fejlmeddelelse.

Selve brugergrænsefladen til brugeradministratorer er ændret en del fra Virk BRS til NemLog-in FBRS – men dette er helt uafhængigt af snitfladen til myndighedsløsningerne og beskrives derfor ikke yderligere i dette dokument.

NemLog-in's Signeringstjeneste

Samtidig med NemLog-in FBRS lanceres også en ny signeringstjeneste til NemLog-in. Modsat FBRS løsningen er denne af forskellige grunde ikke helt bagudkompatibel med den eksisterende signeringstjeneste på Virk.dk, og derfor

vil myndighederne som anvender denne have en opgave med (mindre) tilretning af integrationen. Det er dog tilstræbt, at den nye tjeneste genbruger en del af den gamle snitflade for at reducere tilretningsarbejdet mest muligt.

Snitfladen til den nye signeringstjeneste findes dokumenteret på NemLog-in's testportal[1], hvor der ligeledes findes en signeringsstub, man kan teste sin integration imod. Stubben er en service, der har samme snitflade som den "rigtige" signeringstjeneste, men som ikke foretager fuld validering af input og blot returnerer statisk output. Det er ikke nødvendigt at tilslutte sig stubben for at anvende den (da den ikke validerer indgående signaturer). Tilslutning til NemLog-in's signeringstjeneste sker via NemLog-in's tilslutningssystem og involverer bl.a. upload af certifikater mm.

Tilslutning til NemLog-in/Brugeradministration

Eksisterende myndighedsløsninger tilsluttet Virk BRS skal ikke gentilsluttes, da de som nævnt migreres over på FBRS. Konkret vil alle tilslutninger, brugere, roller, privilegier og erhvervsfuldmagter blive migreret fra Virk BRS til NemLog-in FBRS.

Nye myndighedsløsninger, som ikke i forvejen anvender Virk BRS, skal tilsluttes ved brug af NemLog-in's tilslutningssystem efter idriftsættelsen. Dette involverer upload af metadata, definition af privilegier etc.

[1] https://test-nemlog-in.dk/testportal/

Eksempel på brug af NemLog-in/Brugeradministration

Herunder beskrives et (fiktivt) eksempel på anvendelse af FBRS, der viser sammenhængen mellem myndighedssiden (løsningen) på den ene side og brugerorganisationen (anvendersiden) på den anden side.

Antag at myndigheden "Acme" har lanceret en ny selvbetjeningsløsning, hvor virksomheder kan indrapportere data – deres "Acme index" for seneste kvartal. Myndigheden har defineret to privilegier for den nye tjeneste, hvor det ene giver adgang til at indberette, mens det andet kun giver mulighed for at se tidligere indberetninger for virksomheden:

- http://acme.org/privileges/indrapporter_acme_index
- http://acme.org/privileges/se_acme_index

Efter disse privilegier er oprettet af Acme via NemLog-in's tilslutningssystem, kan NemLog-in administratoren tilknytte dem nye eller eksisterende roller i FBRS. Antag at FBRS allerede har defineret de to roller:

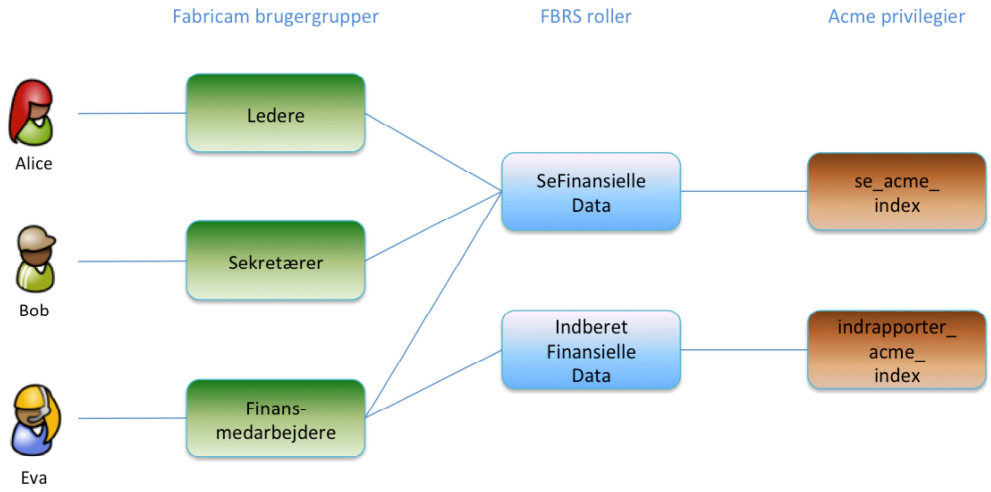
- "IndberetFinansielleData"
- "SeFinansielleData"

NemLog-in administratoren beslutter, at privilegiet "http://acme.org/privileges/indrapporter_acme_index" tilknyttes FBRS rollen " IndberetFinansielleData" og at privilegiet "http://acme.org/privileges/se_tidligere_acme_index" tilknyttes FBRS rollen "SeFinansielleData".

Antag nu at virksomheden Fabricam bliver tilsluttet NemLog-in som brugerorganisation via NemLog-in's tilslutningssystem. Fabricam beslutter, at definere tre brugergrupper for at lette brugeradministrationen. Grupperne er "ledere", "finansmedarbejdere" og "sekretærer". Fabricam tildeler FBRS rollerne "IndberetFinansielleData" og "SeFinansielleData" til brugergruppen "finansmedarbejdere", og FBRS rollen "SeFinansielleData" til brugergrupperne "ledere" og "sekretærer".

Sluttelig udpeger en Fabricam brugeradministrator brugeren "Bob" som medlem af brugergruppen "sekretærer", "Alice" udpeges som medlem af brugergruppen "ledere", og Eva som medlem af brugergruppen "finansmedarbejdere".

Nu vil Alice og Bob kun få privilegiet relateret til at se deres virksomhedens acme index, hvorimod Eva både kan se og indberette virksomhedens acme index (se illustration herunder).



Referencer

[OIO-SAML] ”OIO Web SSO Profile V2.0.9”, Digitaliseringsstyrelsen.
http://digitaliser.dk/resource/2377872

[OIO-BPP] ”OIO Basic Privilege Profile”, Digitaliseringsstyrelsen.
http://digitaliser.dk/resource/2377872

[VIRK-SYS] ”Systembeskrivelse - Brugerrettighedsstyringssystem VIRK”, Cap Gemini, Version 2.2, 2011-08-05.
http://myndighedsnet.virk.dk

[VIRK-PRO] ”Procesbeskrivelse - Brugerrettighedsstyringssystem VIRK”, Cap Gemini, Version 1.3.1, 4-5-2010.
http://myndighedsnet.virk.dk