Løsningsskitse til ny rettigheds-uddelegeringsløsning

Formål med løsningen
Delegeringssystemet har til formål at gøre det nemmere for landmanden at delegere en delmængde af sine rettigheder i en applikation til en ansat, en rådgiver eller en gruppe af medarbejdere på et rådgivningscenter.

Heri ligger som et væsentligt succeskriterie, at landmanden kan foretage delegeringen centralt, via ét login og med en simpel og overskuelig grænseflade.

Funktionalitet for slutbrugeren
Delegeringssystemet laves som en selvstændig web løsning baseret på DLBR Fælles Login (ADFS), hvorfor alle tredjepartsapplikationer på denne login platform ved at linke til uddelegeringsløsningen, kan sende brugeren direkte ind til sin personaliserede delegeringsfunktion.

I delegeringssystemet får brugeren en personaliseret liste over de tredjepartsapplikationer som brugeren har adgang til og som er tilmeldt delegeringsløsningen. Brugeren kan for hver af disse tredjepartsapplikationer delegere en eller flere roller til andre brugere. Dette kan være en anden bruger (brugerdelegering), en medarbejdergruppe under et rådgivningscenter eller et helt rådgivningscenter (gruppedelegering). Brugeren kan se et samlet overblik over sine delegeringer med mulighed for at ændre disse.

De delegeringer som brugeren har modtaget fra andre kan desuden ses:

- Brugerdelegeringer vises på en liste
  Dette er primært af hensyn til landmandens medhjælpere.

- Gruppedelegeringer kan slås op for en bestemt bruger
  Dette er primært af hensyn til konsulenten, der inden en rådgivningsopgave, skal sikre sig at have de fornødne adgange delegeret fra landmanden.

Såfremt en tredjepartsapplikation vil tilbyde delegering udover rolle niveauet, linkes videre til tredjepartsapplikationen, der selv håndterer den videre delegering. Denne vil ikke efterfølgende være synlig i delegeringssystemet.

Administratorfunktioner
Administrationsdelen af delegeringsløsningen leveres som et plug-in til DLIAdmin og kan tilgås af DLIAdmin overadministrator rollen. Administratoren kan oprette (samt redigere og slette) en tredjepartsapplikation og registrere rollerne under denne, samt angive de brugervendte beskrivelser af applikationen og rollerne.

Desuden kan administratoren angive reglen for hvilke brugere der baseret på informationer om brugeren i DLI BrugerDatabasen, skal se applikationen på deres personaliserede delegeringsliste.

Listen over Landbrugscentre som brugerne præsenteres for, skal kunne redigeres af administrator for at kunne frafiltrere testcentre og lignende.

Supportfunktioner
For at kunne servicere brugere der ringer efter support, laves der en funktion hvor VFLs kundeservice på brugerens vegne kan slå op på siden med brugerens delegeringer.

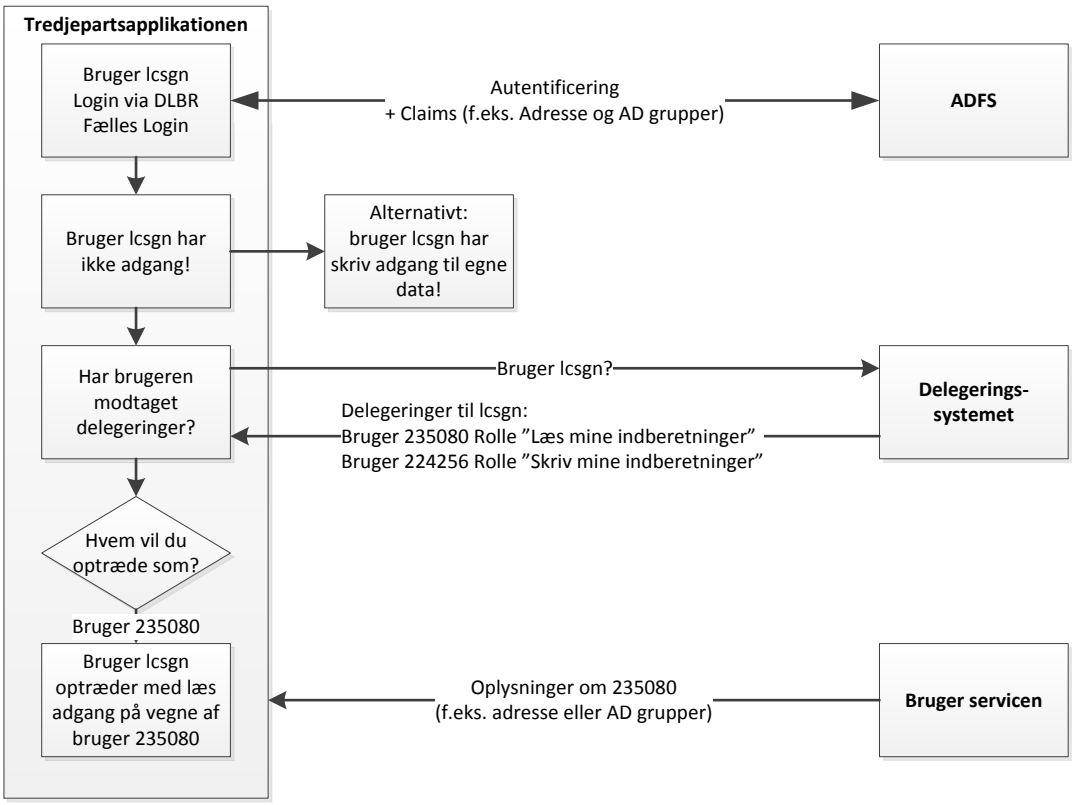
Samspil med tredjepartsapplikationen
Delegeringssystemet holder styr på hvilke roller brugerne har uddelegeret til andre brugere, og udleverer disse oplysninger på anfordring fra en tredjepartsapplikation via et serviceinterface.

Tredjepartsapplikationen skal selv omsætte disse roller til rettigheder for den pågældende bruger, og skal selv præsentere brugeren for den fornødne dialog, hvis eksempelvis brugeren har fået delegeret roller fra flere forskellige brugere, og skal vælge hvem vedkomne vil optræde som. En konsulent kan med gruppedelegering eksempelvis have modtaget delegeringer fra et stort antal landmænd. Eller en landmand kan have egne data i applikationen og samtidig have fået delegeret adgang til andres data.

Tredjepartsapplikationen kan altid identificere den bruger, der udfører arbejdet. Kommunikationen om delegeringer sker uafhængigt af login processen, hvorfor brugeren altid optræder som sig selv – uanset at der arbejdes på andres vegne.

Når en bruger logger på, overføres der brugerinformationer fra ADFS – eksempelvis navn, adresse og AD grupper. Skal brugeren efterfølgende optræde på en anden brugers vegne, skal tredjepartsapplikationen kunne hente de tilsvarende data om de uddelegerede brugere. Dette sker ved at tredjepartsapplikationen kalder en bruger service i DLI BrugerDatabasen.

En skitse over processen er vist nedenfor.



Designprincipper

- Delegeringssystemet er afkoblet fra loginsystemet
  Dette betyder blandt andet at brugeren altid kan identificeres af tredjepartsapplikationen. Det muliggør samtidig gruppedelegeringen, der ellers ville overbelaste login og browser teknologien.

- Rollebaseret delegering
  Den rollebaserede model er en forudsætning for at der kan laves en løsning på tværs, idet delegeringssystemet ikke skal kende rettighedsstrukturen og informationsarkitekturen i hver enkelt tredjepartsapplikation.

Om roller

Rollerne defineres af tredjepartsapplikationen i forbindelse med at denne registreres af administratoren i delegeringssystemet. Rollerne er uden betydning for delegeringsløsningen, der alene formidler dem videre til tredjepartsapplikationen.

Roller skal ikke forstås snævert som en organisatorisk rolle, men kan anvendes som mere brede rettighedsbegreber.

Eksempler på roller

Tredjepartsapplikation	**Roller der kan delegeres**
Min Kalender på landmand.dk	Adgang til at læse min kalender Adgang til at oprette og rette aftaler i min kalender
WebDyr	Adgang til at læse mine data Adgang til at foretage mine indberetninger
E-faktura	Fuld adgang
DBLR arkiv	Alle områder Indbakke Kvæg Ledelse/medarbejdere Mark Miljø Privat Regnskabsbilag Svin Økonomi

Løsningens afgrænsning

Delegeringssystemet kender ikke informationsarkitektur og rettighedsstruktur i tredjepartsapplikationerne.

- Rollerne kan således eksempelvis ikke anvendes til at modellere rettigheder, der er situations- eller databestemte. Eksempelvis at en adgang er afgrænset til 4 af brugerens 6 bedrifter.

- Delegeringssystemet udfører ikke rettighedsgivende handlinger i tredjepartsdatabaser (herunder DLI BrugerDatabasen). Eksempelvis ændrer den ikke en brugers primære landbrugscenter tilhørsforhold, eller melder brugere ind eller ud af AD grupper. Dette skal ske i tredjepartsapplikationen.

Delegeringssystemet kun anvendes af tredjepartsapplikationer, der anvender DLBR Fælles Login. Dette betyder at både modtager og afgiver af delegeringer skal findes i DLI BrugerDatabasen.

Der kan mod delegeringsservicen alene forespørges på én bruger ad gangen.

Funktioner der ikke løses i projektet

- Delegering på anfordring. Der har været diskuteret en løsning, hvor en bruger nemt kan bede en anden bruger om adgang. Eksempelvis kan konsulenten der vil se en brugers data, men får en 'adgang nægtet' i en tredjepartsapplikation, bede brugeren om adgang.

- Fusionering af den nuværende landmand.dk nøgle delegering med det nye delegeringssystem. Løsningsmulighederne har været endevendt, men løsningerne er teknisk inkompatible og derfor meget komplekse at smelte sammen. Tredjepartsapplikationerne under Landmand.dk løsningen bør med tiden lægges om til det nye system. Indtil dette er sket vil begge delegeringssystemer sameksistere.

- Der laves ikke en mobilvenlig udgave af delegeringssystemet.

Øvrige kommentarer

- Serviceinterfacet mod delegeringsløsningen vil være baseret på en REST servicearkitektur.
- Identifikationen af tredjepartsystemet sker ved at dette kalder servicen med en tildelt systemkonto.
- Der bør laves en anvisning til hvordan tredjepartsapplikationer, hvor adgang kræver medlemskab af bestemte AD grupper, kan håndtere dette på en ensartet/standardiseret måde (ikke med i estimatet).

Estimeringsforbehold

- Præsentationen af brugerne, landbrugscentrene og deres organisering er begrænset til de informationer der i dag findes i DLI BrugerDatabasen.
- Estimatet omfatter ikke de ændringer, der skal til i tredjepartssystemer for at anvende løsningen.
- Estimatet omfatter ikke kælderteamets tid forbrugt til at assistere tredjepartsapplikationer med at komme på løsningen.