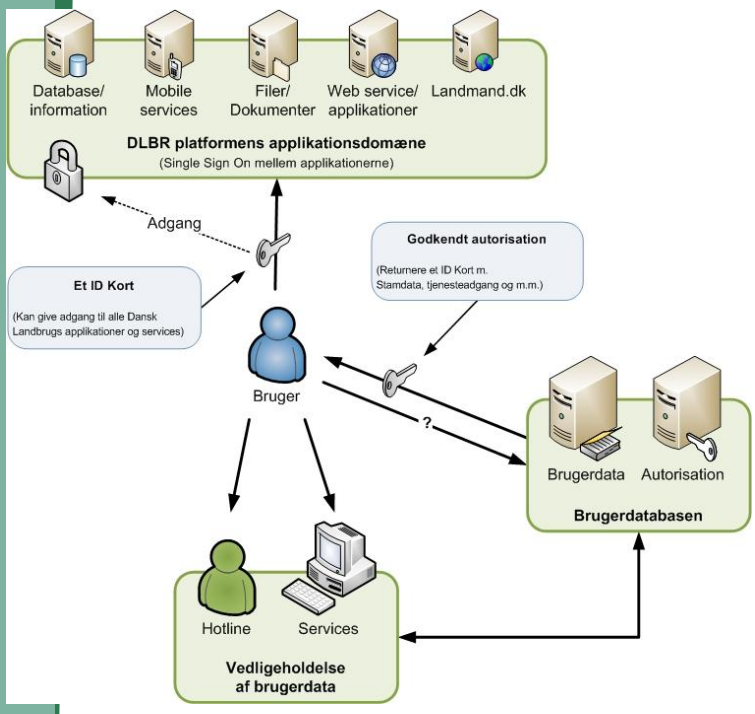
DLI og Single Sign-On

Vejen mod en service enabled arkitektur på Dansk Landbrugs Internetplatform



Dansk Landbrugsrådgivning
Landscentret
Udkærsvej 15, 8200 Århus N · Tlf. 87 40 50 00 · www.landscentret.dk

Indhold

1 Baggrund

Indenfor landbruget opsamles store mængder af data, som er knyttet til den enkelte bedrift. Økonomioplysninger er væsentlige for alle typer af bedrifter, og samtidig følsomme i den forstand, at disse oplysninger ikke skal kunne tilgås af forkerte personer. Omfattende registreringer om arealer, afgrøder, gødskning og planebeskyttelse er også vigtige for de fleste bedrifter. Indenfor husdyrbrug sker der både for kvægbrug og svinebrug en omfattende registrering af de dyr, der indgår i bedriften og de hændelser, som sker over tid. Også for de mindre husdyrgrupper som får, geder, hjorte, heste o.s.v. opsamles vigtige data.

I nogle af de tidligere IT-løsninger, som Dansk Landbrugsrådgivning har udviklet til landmændene og deres rådgivere har disse oplysninger for en stor dels vedkommende været registreret på en lokal computer hos landmanden eller hans rådgiver: Landmanden kunne derved typisk tilgå alle sine data blot ved at åbne de ønskede værktøjer, idet dataadgangen var givet uden yderligere identifikation. For rådgiverens vedkommende skulle den enkelte bedrift identificeres, hvilket typisk kunne ske ved at angive et telefonnummer / medlemsnummer. Herefter var relevante data til rådighed, fordi de var samlet i en database under det enkelte medlemsnummer.

I løbet af de senere år er en stor del af dataregistreringerne flyttet til centrale systemer. Dette har blandt andet baggrund i, at data skal anvendes af flere personer til flere forskellige formål. Eksempelvis er der en række lovkrav, som opfyldes ved at foretage daglige registreringer på bedriften. Disse oplysninger skal naturligt kunne tilgås af myndigheder og andre, som har behov for disse opdaterede oplysninger eksempelvis i forbindelse med et akut sygdomsudbrud.

Med denne struktur følger et behov for at legalisere tilgangen til data på enkeltbrugerniveau, idet ikke alle personer kan se alle data vedrørende den enkelte bedrift. Ligeledes er der individuelle forskelle på, hvad den enkelte bruger kan foretage sig med de registrerede data.

I de centrale systemer, som holder ovennævnte registreringer identificeres brugerne individuelt. Men der er ikke nogen koordinering mellem brugerne i de forskellige systemer. Med andre ord skal en landmand, som ønsker at bruge både kvægdata og økonomidata identificere sig på begge systemer, typisk med forskellige brugernavn og adgangskode.

Dette forhold gør det vanskeligere for slutbrugeren at anvende systemerne, og det vanskeliggør opbygning af applikationer og services, som anvender informationer på tværs af fagområder. Ovenstående forhold begrunder interessen i at udvikle komponenter, som giver mulighed for Single Sign-On (SSO) mellem forskellige systemer, og dermed mulighed for at koble oplysninger fra forskellige systemer på en generisk måde, med andre ord at etablere en Service Orienteret Arkitektur (SOA).

Udover, at det er væsentligt at sikre landmandens og hans rådgiveres adgang til anvendelse af data på tværs af fagområder, er der stadig stigende behov for at kunne dele nogle at informationerne med eksempelvis myndigheder. Dertil kommer at myndighederne selv har systemer med data, som har stor relevans for landmanden, eksempelvis data omkring tilskudsordninger m.v. Derfor er det også en vigtig del af SOA-projektet at forbedre muligheden for udveksling af informationer mellem landbrug og myndigheder.

2 Valg af løsning

Første fase i projektet var at undersøge, om der eksisterer standard løsninger på markedet, som løser de behov, vi har identificeret. Dette arbejde er nærmere beskrevet i særskilte notater (http://wss3.landscentret.dk/websteder/LandbrugsIT/SOA/SSO/Leverandrmdet/ Bilag 171 og Bilag 174). Vi valgte at fokusere på produkter fra 3 leverandører: Ping Identity, IBM og Microsoft. Ping Identity og IBM kunne begge levere "færdige" systemer, med forholdsvis rig funktionalitet. Imidlertid var ingen af løsningerne i stand til at løse de opstillede behov uden supplerende egenudvikling. Microsoft kunne ikke levere en færdig løsning, men præsenterede os for en udvikling, hvor SSO eller Federated Sikkerhed bliver en del af .NET frameworket under det foreløbige navn ADFS version 2 (eller senere Geneva).

Da vi i Dansk Landbrugsrådgivning i forvejen baserer vores egenudvikling på Microsofts produkter faldt valget på at satse på Microsofts kommende produkter og at løse den basale SSO-opgave ved at udvikle egne komponenter baseret på gængse standarder. Væsentlige input til valget var introduktion fra de 3 leverandører, egen udviklingsstrategi og erfaringsudveksling med EMMENTOR, som selv har gennemført et stort integrationsprojekt på vegne af FødevareErhverv. Sidstnævnte fordi vi lægger vægt på at anvende komponenter, som også understøttes af det offentlige.

Nærmere beskrivelse af de udviklede komponenter er samlet i afsnit 7.

3 Brugerdatabasen

Et uundværligt element i en SOA-arkitektur er en fælles bruger database, som giver en entydig identifikation at den enkelte bruger, og som også sikrer, at fælles brugerinformationer vedligeholdes. Dansk Landbrugsrådgivning har etableret en bruger database i DLI (Dansk Internet Platform). Denne bruger database indeholder medarbejdere og kunder fra de lokale centre samt medarbejdere fra Landscentret. Kunderne kan opdeles i 3 undergrupper. Aktive medlemmer og Interesse medlemmer består af landmænd, som betaler et kontingent til og som sådan er medlem af Dansk Landbrug. Den sidste del af kundegruppen består primært af landmænd, som har en berøringsflade med et lokalt landbrugscenter. Ydermere har brugere at portalen Landmand.dk, som ikke hører til de to nævnte grupper kunnet oprette sig som "selvoprettere". DLI-brugerdatabasen er dermed den naturlige fælles brugerdatabase for Dansk Landbrugsrådgivnings SOA.

Der var dog mangler i forhold til at anvende bruger databasen til SOA, hvorfor der i projektet er der løst en væsentlig opgave med at klargøre DLI-brugerdatabasen til at kunne fungere som fundament for en SSO-løsning. Der er gennemført aktiviteter indenfor nedenstående hovedområder:

1. Udvidelse af databasens struktur
2. Datavask, dataflow og mapning af brugerkontekst til eksterne systemer

1 Udvidelse af databasens struktur

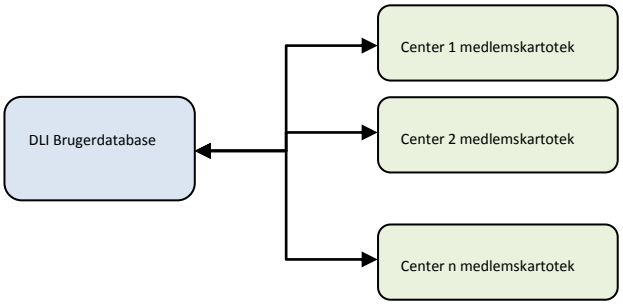
DLI-brugerdatabasen består af et AD og en SQL database med supplerende brugeroplysninger. AD'et har en struktur, der afspejler organisationen Dansk Landbrugsrådgivning og omgivelser. For at kunne anvende DLI brugerdatabasen som fundament for SSO er der gennemført en række tilpasninger med henblik på følgende:

- Det skal være muligt at lave applikationer, der benytter brugerdatabasen til brugerstyring samt overordnet adgangshåndtering via tjenesteadgang. Endvidere etableres mulighed for at håndtere styring af dataadgang for applikationer, som ikke har en intern styring hertil.
- Det skal være muligt at håndtere medarbejder og kunderelationer for store firmaer som f.eks. Arla. Derfor fremtidssikres AD strukturen så det bliver muligt at lave brugerstyring for firmaer, samt tydeligt adskille firmastrukturen fra DLBR strukturen.
- Landbrugene bliver i fremtiden meget større og det bliver nødvendigt at kunne håndtere et stort landbrug som et firma. Derfor fremtidssikres AD strukturen så det bliver muligt at oprette et landbrug som firmaer i firmastrukturen.
- Foreningers medarbejdere og medlems relationer skal kunne håndteres. Da en forening minder meget om et firma håndteres en forening som et firma i firmastrukturen.
- Centrene har brug for at kunne håndtere andre former for kunder end landmænd, f.eks. i forbindelse med salg af økonomiapplikationer og revision til håndværkere. Derfor omdøbes landmands OU'en til "kunder".
- Der benyttes i stigende grad procesudstyr i forbindelse med landbrugene. I dag benyttes landmandens eget login til at autentificere procesudstyret (på prototypeniveau). Dette er på flere måder en problematisk og en yderst usikker fremgangsmåde, som ikke bør anvendes i den endelige løsning. Der skal i stedet benyttes tekniske brugere dedikeret til det pågældende procesudstyr
- Det skal være muligt at benytte udvalg og udvalgsgrupper på en ensartet måde. Udvalgs OU'er skal bygges op på sammen måde som resten af AD strukturen.
- AD strukturen skal være nemmere at vedligeholde og overskue.

2 Datavask og dataflow

Brugerne i brugerdatabasen er en samling af brugere fra de lokale centres administrative systemer. Skematisk kan de illustreres som vist i figur 1.

Figur 1: ***Sammenhæng mellem DLI og Kontorløsning***



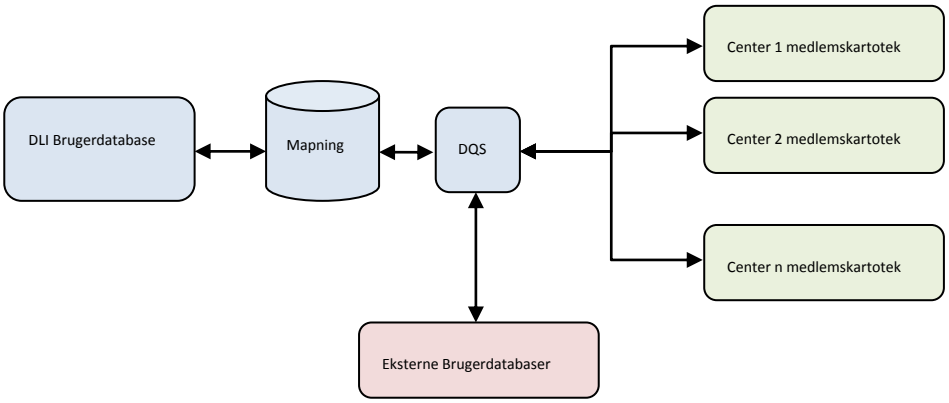
En bruger findes således både i selve DLI og i det administrative system hos et lokalt center. Af forretningsmæssige årsager kan den samme kunde endda være oprettet i det administrative system flere gange eller være til stede i flere centres administrative systemer. Fra starten har der ikke været udviklet en logik, som kunne medvirke til at holde styr på disse sammenhænge. Derfor er der i brugerdatabasen over tid opstået temmelig mange dubletter. Dette er ikke foreneligt med ønsket om at anvende brugerdatabasen som grundlag for SSO. I projektet er der derfor udviklet en vask af brugerdatabasen, som eliminerer dubletterne. Vasken gennemføres ved hjælp af produktet Omikron AdressCenter, som har indbygget funktioner til at håndtere den udfordring, at samme kunde kan være oprettet med navne og adresseoplysninger, som er stavet forskelligt. Dermed kan vi med dette produkt

eliminere væsentlig flere dubletter end med en almindelig tekstsammenligning. Datavasken gennemføres i produktion primo 2009.

For at sikre, at der ikke opstår nye dubletter, implementeres et nyt dataflow mellem centrenes administrative systemer og DLI brugerdatabasen. Kernen i denne styring er OMIKRON Data Quality Server (DQS). DQS er implementeret i miljøet som det skematisk er illustreret i figur 2.

Data Quality Serveren indeholder de samme algoritmer til matchning af navne og adresser m.v. som AdressCenter, der anvendes til vask af brugerdatabasen. Men DQS er et fast element i brugerdatabasen, som løbende sammenligner brugere mellem de lokale centre, selvstændige brugerdatabaser (applikationer med egen brugerstyring) og DLI. Derved anvendes komponenten til at sikre, at der er den rette sammenhæng (mapning) mellem DLI-brugeren og dennes instanser (profiler) i de lokale centre. Endvidere anvendes komponenten til at sikre en mapning mellem DLI-brugeren og samme brugeres identifikation i eksterne brugerdatabaser. Med denne mapning på plads er forudsætningen til stede for at lave SSO mellem DLI og de eksterne systemer, der er mappet til.

Figur 2: *DQS implementeret i DLI-brugerdatabasen*



4 Perspektiver

Perspektiverne i at have federated sikkerhed implementeret er flere.

Set fra bruger side åbner det muligheden for, at brugeren ved at logge på en enkelt central brugerdatabase (DLI), kan få adgang til øvrige applikationer, som er tilpasset til at anvende den federerede sikkerhed. Det giver altså en lidt lettere adgang til de applikationer, som brugeren nu engang har købt adgang til.

Det åbner også mulighed for i de enkelte applikationer at anvende services, som er baseret på andre systemer (andre fagområder) på en standardiseret måde, idet sikkerheden og dermed adgangskontrollen er løst via den federerede sikkerhed. Dette kan ses som en fordel for såvel bruger som applikationsudbyder. Fordelen for brugeren er en applikation med en større brugsværdi, fordi den kan integreres med relevante eksterne systemer. Fordelen for applikationsudbyderen er, at der ikke skal tænkes helt nye løsninger fra bunden hver gang, der ønskes en eller anden form for integration.

Sammenhængen for den enkelte bruger er ikke nødvendigvis begrænset til de applikationer, som ligger indenfor Dansk Landbrugsrådgivnings domæne. Den federerede sikkerhed åbner også mulighed for, at der kan etableres trust til andre firmaer. Dermed kunne man f.eks. forestille sig, at en landmand, der er

logget på DLI vil kunne trække oplysninger direkte fra sit mejeri's interne system, uden eksplicit at skulle logge sig på mejeriets systemer.

Et andet eksempel, som er relevant for landmandens rådgivere kunne være, at der skabes forbindelse mellem rådgiverens medarbejder login og hans DLI-login. Dermed vil det være muligt for brugeren at tilgå DLI-baserede services på baggrund af sin medarbejderlogin. Dvs. brugeren logger på sin arbejdsplads på det lokale center, og kan derefter uden yderligere login tilgå applikationer på DLI blot ved at være logget på centrets netværk.

Endelig er der som tidligere nævnt myndighederne, som på lignende vis på baggrund af et trust forhold vil kunne gives adgang til informationer fra landmandens systemer ligesom et trust modsat vil kunne anvendes til at udveksle informationer den anden vej.

5 Federated sikkerhed

Der benyttes Federated sikkerhed i SOA applikationer på Landcentret. Federated sikkerhed bygger på webserice standarder som giver mulighed for at lave SSO mellem applikationer med forskellige bruger repositories, hvor brugerne kan have forskellige brugernavne og rettigheder.

Brugerne logger på med et DLI-brugernavn og kodeord hvorefter der mappes til brugerens brugernavne i de øvrige systemer. For at kunne lave denne mapning opbygges der en mapning for alle brugerne i DLI-brugerdatabasen, se afsnit 3. I Federated sikkerhed ligger sikkerheden i at der benyttes certifikater til at lave signering og kryptering i stedet for at benytte brugernavn og kodeord hver gang der logges på et nyt system. Dermed er det kun nødvendigt at opretholde en mapning af brugernavnene og ikke kodeordene, hvilket er en stor fordel da kodeord naturligt ændres over tid mens brugernavne er væsentligt mere stabile. Brugerens kodeord gemmes slet ikke i systemet, da det ville forringe systemets sikkerhed væsentligt.

Brugeren logger på via en Security Token Service (STS) som validerer brugeren og udsteder en SAML token indeholdende passende brugerinformationer (claims) om brugeren, som f.eks.: brugernavn(e), om brugeren er landmand, tilhørsforhold til centre, om brugeren har adgang til et givent system osv. De forskellige systemer har behov for forskellige SAML tokens med forskellige claims. Derfor veksles SAML tokens, når der er behov for det.

5.1 Overordnede tjenesteadgange og decentral rettighedshåndtering

DLI-brugerdatabasen indeholder overordnede adgangsgivende tjenesteadgange. En tjenesteadgang angiver om en bruger må benytte et givent system / benytte en webservice. Tjenesteadgangen skal ikke forveksles med detaljerede rettigheder, men derimod ses som et supplement til systemernes eksisterende rettighedsstrukturer. Det enkelte systems nuværende decentrale rettighedshåndtering benyttes derfor også i fremtiden. DLI-brugerdatabasen kan udføre rettighedshåndteringen i de tilfælde hvor det enkelte system måtte ønske det.

Når en webservice kaldes med en SAML token indeholdende blandt andet brugerens tjenesteadgang(e), er det webservicens ansvar at checke, om brugeren har den / de tilstrækkelige adgangsgivende tjenesteadgang(e). Derefter foldes den / de overordnede tjenesteadgang(e) og de øvrige claims i SAML tokenen ud til de finmaskede rettigheder, brugeren har i det enkelte system.

6 Udviklingsprincipper

Selvom vi selv har måttet udvikle komponenter til vores federerede sikkerhed, har det været et mål at basere udviklingen på standarder, så en eventuel senere integration med 3. parts produkter kan ske så smertefrit som muligt.

6.1 Om SOA

Service Orienteret Arkitektur (SOA) er ikke en standard men en arkitekturmæssig tankegang som tilpasses det enkelte firma og løsning. I en SOA benyttes der en række webservice standarder som er kendt som ws-* standarderne. Disse standarder er fastlagt igennem W3C og understøttes af de store spillere på markedet, f.eks. Microsoft, IBM, Oracle osv. Webservice standarderne gør dermed webservice teknologien uafhængig af den teknologiske platform og leverandør, hvilket gør Landscentret uafhængigt og agilt.

6.2 Genbrug

SOA giver store muligheder for genbrug af funktionalitet og data. De enkelte services kan ses som funktionelle byggeklodser, der kan genbruges på tværs af services og applikationer. Funktionalitet og data i eksisterende systemer kan genbruges ved at bygge services, der udstiller funktionalitet og data, der hermed kan genbruges på tværs af Landscentret.
Funktionaliteten placeres kun et sted og benyttes af mange. Det betyder at funktionalitetsændringer og rettelser kun skal laves et sted. Ligeledes gemmes data kun et sted og det er muligt for alle applikationer at have online adgang til konsistente data.

6.3 Løst koblede systemer

I en SOA kalder de forskellige systemer hinanden, hvilket giver afhængighed. Det er derfor vigtigt at afhængigheden minimeres ved at lave løst koblede systemer. Det gøres ved at tilgå data via services med logiske nøgler og ikke tekniske nøgler som er bundet til det underliggende system. En logisk nøgle er f.eks. et CPR nr. i stedet for en database teknisk nøgle der angiver en række. Det skal f.eks. være muligt at skifte en underlæggende database ud med en database fra en anden leverandør eller at skifte et egenudviklet modul af services ud med et standardprodukt.

7 Udviklede komponenter

Den federated sikkerhed er implementeret via server komponenter og en række plumming komponenter til: webservices, web applikationer og Windows klienter. Plumming komponenterne gør det muligt at konfigurere sikkerheden, og de udstiller en række metoder, som understøtter brugen af federated sikkerhed. Her ud over er der implementeret plumming komponenter indeholdende lognings funktionalitet

Sikkerheds server komponenter som implementerer server siden af den federated sikkerhed:

- DLI STS, som er Landscentrets centrale STS.
- DLI web applikations logon.

Plumming komponenter til både webservices, web applikationer og Windows klienter:

- Folder SAML token claims ud og opretter .NET sikkerhedskontekst.
- Sikkerhedskravene konfigureres, incl. hvilken STS der skal udstede SAML tokenen.
- Der udstedes SAML tokens med claims på baggrund af de konfigurerede claims krav.

- Generisk lognings funktionalitet som logger til UptoLog.

Plumming komponenterne til web applikation:

- Cacher SAML tokens for at kunne genbruge SAML tokens og optimere performance.
- Understøtter ASP.NET sikkerhedshåndtering.
- Redirigerer automatisk brugeren til web applikations logon siden ved logon krav, hvis brugeren ikke er logget på eller SAML tokenen er invalid f.eks. hvis SAML tokenen er for gammel.

Plumming komponenterne til Windows klient:

- Cacher SAML tokens for at kunne genbruge SAML tokens og optimere performance.
- Åbner automatisk en logon dialog ved logon krav, hvis brugeren ikke er logget på eller SAML tokenen er invalid.
- Mulighed for SSO fra en web applikation og til en Windows klient at typen ClickOnce.

8 Logning og overvågning

8.1 Logning af fejl, advarsler, trace og tidsmålinger

Et enterprise SOA system breder sig naturligt over et antal servere og klienter. Det betyder at en fejl på f.eks. en server også får betydning for andre servere og / eller klienter i SOA applikationen. Det kan også være at en fejl kun opstår, når en specifik klient kalder en webservice eller at en fejl opstår, når nogle webservices kaldes i en speciel rækkefølge.

Når en fejl logges er det derfor ikke kun vigtigt, hvilken server eller klient fejlen er opstået på, men også i hvilken sammenhæng fejlen er opstået. Sammenhængen ses som en aktivitet, der starter når brugeren f.eks. trykker på en knap og afsluttes når handlingen er afsluttet. Plumming komponenterne sørger for at sende et aktivitets ID med i webservice kaldene, sådan at aktivitetsinformationen vedligeholdes på tværs af serverne og klienterne.

Fejl logges i et centralt logningssystem som gemmer fejl informationerne samt fejlens aktivitets sammenhæng. Logningssystemet kan herefter visualisere en fejlsituation og den sammenhæng fejlen er opstået i.
Udover fejl kan også trace og tidsmålinger logges. Der kan f.eks. laves en tidsmåling fra det tidspunkt hvor brugeren trykker på en knap og starter en aktivitet til brugeren får resultatet tilbage. I en sådan tidsmåling kan det ses hvor lang tid, de enkelte funktioner har taget og tidsmæssige sammenhænge mellem server og klient.

UptoLog benyttes som logningssystem.

8.2 Overvågning

SOA applikationens samlede oppetid er afhængig af de enkelte elementers (servere / systemer) oppetid. Det vil sige at oppetiden bliver dårligere jo større systemet er. Problemet løses ved at benytte redundant drift, og overvåge de enkelte elementer i systemet hvorved den ønskede oppetid kan opnås. Overvågningen foretages på to niveauer: element og applikation.

- Overvågningen på element niveau foretages via is alive sider. Hvert element har en is alive side, som tester om det enkelte element er fejlfrit. Ved fejl informerer is alive siden om fejlsituationen.
- Overvågningen på applikations niveau foretages via check af forretningsprocesser. Der indspilles et mindre antal vigtige forretningsprocesser for den enkelte applikation, som afspilles med jævne mellemrum. Det checkes om forretningsprocessen kan gennemføres fejlfrit.

I begge overvågnings situationer logges fejl i logningssystemet, det er hermed muligt at overskue fejlsituationen. Det er især nødvendigt at benytte logningssystemet til at overskue fejlsituationen når en forretningsproces fejler, da flere elementer aktiveres under forretningsprocessen og den detaljerede fejlinformation bliver logget, men ikke vist i brugerdialogen.

9 Implementering

9.1 Systemer med Federated sikkerhed

De basale komponenter i federated sikkerhed implementeres i produktion primo 2009. I implementeringen sikres det, at Landmand.dk (med tilhørende applikationer) og CMS-platformen fungerer sammen med federated sikkerhed, altså at der er SSO mellem disse eksisterende og nye produkter, som logger på via federated sikkerhed.

Primo 2009 implementeres et nyt system, som realkreditrådet skal anvende til at opsamle oplysninger om ejendomsværdier. Systemet er udviklet af Dansk Landbrugsrådgivning, Web&IT, og anvender federated sikkerhed til adgangskontrol.

Primo 2009 implementerer Dansk Kvæg sine DFC-services, som er webservices, der understøtter opsamling af data til og distribution af data fra Kvægdatabasen fra forskellige samarbejdsparter. Det kan være dataopsamling fra procesudstyr på landmandens bedrift eller opsamling af data fra inseminører. DCF-services benytter federated sikkerhed.