

Deltagelse i DEF-nøglen realiseret via LDAP-projektet

Opsætning og vedligeholdelse

Indhold

1	Indledning.....	3
1.1	LDAP-projektet.....	3
1.2	Serviceaftaletilbud til forskningsbibliotekerne	3
2	Funktionaliteten i LDAP- og proxyløsningen	4
2.1	Rolledefinition	4
2.2	Brugsscenarium af LDAP-proxy løsningen	5
2.3	Første udgave	5
2.4	Fælles logon	6
2.5	Adgang afhængig af brugeren og ikke maskinen.....	6
2.6	Lokal vedligeholdelse af data	6
3	Support	8
3.1	Opsætning	8
3.2	Drift.....	8
3.3	Support.....	8
4	Krav til datalevering.....	9
4.1	Dataindhold.....	9
4.2	Dataformater	10
4.3	Levering og sikkerhed.....	10
4.4	Opdateringer.....	11
5	Kontaktpersoner.....	12
5.1	Tilmelding til tjenesterne	12
5.2	På det enkelte bibliotek	12
5.3	Henvendelser angående opsætning og drift	12

1 Indledning

Fra starten af DEF-samarbejdet har der været et behov for at realisere fælles adgang til ressourcer på nettet samt at tilbyde adgang til visse ressourcer baseret på brugerens identitet snarere end på brugerens fysiske placering (ip-nummer). Dette har været omtalt som *DEF-nøglen*, dvs. som den tekniske facilitet, der betyder, at en låner ved et forskningsbibliotek kan få adgang til elektroniske ressourcer på samme bibliotek og evt. på andre biblioteker eller informationsudbydere ved at benytte en fælles login til alle disse services.

I LDAP-projektet er der realiseret en løsningsmodel på DEF-nøglen, som kan anvendes til at give brugernavnsstyret adgang til visse elektroniske ressourcer (pt. især elektroniske tidsskrifter) uafhængigt af, hvor brugeren befinder sig. Specifikt giver dette deltagernes brugere adgang til de elektroniske tidsskrifter hjemmefra, blot de oplyser et gyldigt brugernavn/kodeord til systemet og de i er tilknyttet en institution, som har adgang til disse tidsskrifter.

1.1 LDAP-projektet

I perioden fra slutningen af 2001 og gennem 2002 har det såkaldte LDAP-projekt været gennemført, som et DEF-projekt med deltagelse af IT-12-bibliotekerne. I dette projekt er der defineret en distribueret virtuel netværksdatabase baseret på LDAP-protokollen, som indeholder oplysninger om de deltagende institutioners brugere og deres adgangsrettigheder.

Da erfaringerne fra tidligere undersøgelser har vist, at det er vanskeligt at definere en sådan brugerdatabase (herunder beskrivelsen af adgangsrettigheder til vilkårlige ressourcer), har LDAP-projektet fokuseret kraftigt på at lave en løsning, som har en betydelig generalitet i brugerdata-basen, men som til gengæld er mere målrettet mod at sikre, at i hvert fald adgang til én type ressourcer bliver understøttet: Adgang til elektroniske tidsskrifter for autoriserede brugere, der ønsker adgang til tidsskrifterne fra andre steder end selve deres institution, f.eks. hjemmefra eller på rejser. Denne adgangskontrol baserer sig på at LDAP-databasen indeholder oplysninger om hvilke(n) institution(er), hver enkelt bruger er tilknyttet (som ansat, studerende osv.).

Selve adgangen til de elektroniske tidsskrifter er realiseret i en såkaldt proxy-løsning. I LDAP-projektet driver IT-12 partnere selv deres LDAP- og proxy-servere.

1.2 Serviceaftaletilbud til forskningsbibliotekerne

Som udløber af LDAP-projektet er der indgået to aftaler mellem DEF og Statsbiblioteket, der betyder, at Statsbiblioteket på basis af aftaler med de enkelte deltagere tilbyder at overtage konfiguration og drift af en LDAP-, hhv. en proxyservice for de biblioteker, som måtte ønske at indgå i LDAP-/proxynetværket, men ikke ønsker at drive disse services selv.

I dette dokument vil vi beskrive indholdet og funktionalitet i disse tilbudte services og opridse de ting, som de deltagende biblioteker skal levere for at komme med og for at holde deres del af servicen up-to-date.

- Statsbiblioteket: Institutionen, der er serviceudbyder af det aktuelle produkt, som kan anskaffes af biblioteker. Dvs. at SB står for de tekniske og driftmæssige dele, som ikke kræves af det enkelte bibliotek.
- Biblioteket: Aftageren af den udbudte service. Der stilles krav til vedligeholdelse af data fra disses side for at opretholde nutidige informationer.
- Brugeren: Den aktuelle person, som benytter denne service, som det tilknyttede bibliotek har anskaffet. Dvs. en låner eller bibliotekar, som vil tilgå ressourcer gennem denne løsning.

2.2 Brugsscenarium af LDAP-proxy løsningen

Brugeren, som på figur 1 er vist som personen ved arbejdsstationen til venstre åbner portalen (P) i sin browser. Portalen giver en forside, hvor der skal indtastes login informationen. Denne information, som skal bruges til at lave en autentifikation af brugeren, sendes via LDAP'en til en LDAP-server (I), der er henvist til i portalen. Autentifikationen foregår ved kontrol af alt brugerdata i systemet, som kan ligge flere forskellige steder. Derfor er der mulighed for, at der er flere forskellige LDAP-servere involveret i denne autentifikation, hvilket er vist med klyngen af I'er. Efter en godkendt autentifikation har brugeren nu adgang til systemet. Portalen kan derfor præsentere en side med tilgængelige ressourcer, eller det er muligt for brugeren at lave en søgning blandt materialet. Næste trin er en autorisation via serveren (A), hvorved brugeren får adgang til specifikke ressourcer. Brugeren er autoriseret til at tilgå de ressourcer, som er indeholdt i både de nationale og lokale licenser alt efter tilknytning. Autorisationen er ligeledes distribueret, hvilket giver mulighed for at kontrollere alle de licenser, som findes indenfor samarbejdet, i forhold til den aktuelle bruger. I den første version, der er beskrevet nedenfor i næste afsnit, er autorisationen indflettet i proxyen, så der vil ikke være særskilte servere, der står for dette.

Selve ressourcerne, som brugeren ønsker vist, ligger ved de forskellige forlag (D), og denne kontakt foregår via proxy'en. Dette skyldes, at forlagene laver deres egen autorisation af hver forespørgsel, som i de fleste tilfælde betyder en kontrol af den aktuelle IP-adresse. Med proxy løsningen gives, der adgang til brugere, som har rettighed til ressourcen ud fra licensen, men under andre omstændigheder ikke ville kunne få adgang pga. forkert IP-adresse. Dette kunne f.eks. være en forsker, som laver en forespørgsel fra sin hjemmearbejdsplads. Proxy'en sender dataene direkte tilbage til brugeren, så portalen ikke belastes af denne trafik.

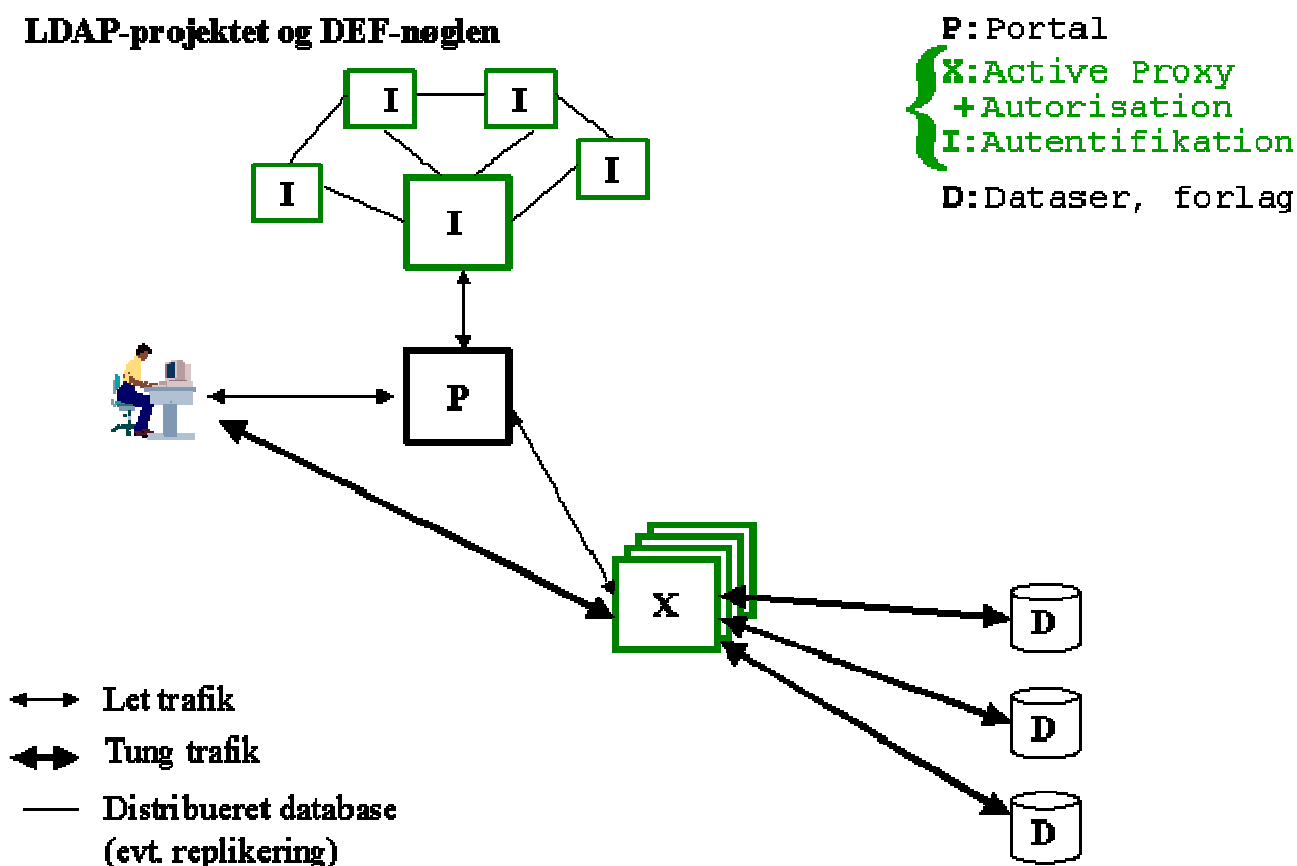
Ved siden af fremvisningen af ressourcen for brugeren, kan der føres en registrering af forbruget, som kan bruges i forbindelse med betaling og statistik. Dette er vist i figuren ved kassen (C).

2.3 Første udgave

Den første udgave, der kommer til at køre, ser lidt anderledes ud end den generelle løsning. Ligesom adgangen i første omgang er begrænset til elektroniske tidsskrifter, så er modellen blevet simplificeret noget. Den aktuelle model er vist i figur 2, hvor den største forskel ses i sammenfletning af autorisationen og bibliotekets proxy.

Tilbudet i serviceløsningen giver hvert bibliotek sin egen virtuelle LDAP-server og proxy. Disse er gengivet som henholdsvis en af knuderne (I) og en fra stakken (X). Funktionelt betyder det, at biblioteket blot skal vedligeholde dataene, der beskrevet i afsnit 4, mens software og maskiner varetages af Statsbiblioteket, som aftalen er lavet med.

LDAP-projektet og DEF-nøglen



Figur 2: Første versions arkitektur

2.4 Fælles logon

En af de store fordele ved DEF-nøglen i LDAP-projektet er brugen af standardiseret brugerdata. De præcise parametre for disse data beskrives i afsnit 4.

Ved udnyttelse af denne facilitet og standarden for LDAP-serverne er det information nok, at en bruger blot er oprettet et sted i systemet. Den server, som den aktuelle login forespørgsel henvendes til, har nemlig mulighed for at kontrollere brugerens identitet ved samtlige brugerdata i systemet. Den samme funktionalitet bruges ved adgangen til andres ressourcer i systemet. Det betyder, at det er nok at logge på en gang og ikke hos hver enkelt af bibliotekerne, som brugeren vil benytte.

2.5 Adgang afhængig af brugeren og ikke maskinen

Ved brug af en proxy for hvert bibliotek, kan brugerne benytte bibliotekets ressourcer, som om de brugte en arbejdsstation fysisk på biblioteket. De kan altså arbejde fra et vilkårligt sted i verden, hvis de blot har det rette login. Metoden til dette ligger i at proxy'ens IP-adresse ligger indenfor det område, som forlagene kender til. Når der kontrolleres hos forlagene om adgang er tilladt, ser de på IP-adressen fra den maskine, som henvendelsen kommer fra. I dette tilfælde den aktuelle proxy. Ved at have enkelte proxyer for hvert bibliotek, kan der tegnes licenser, som kun giver adgang til netop dette bibliotek.

2.6 Lokal vedligeholdelse af data

Et stort problem med adgang til flere forskellige ressourcer har været distribution af brugerdata. Der findes systemer, hvor man kan tilgå alle tidsskrifterne, men udbyderne af systemet skal have en

komplet opdateret brugerdatabase, før det virker tilfredsstillende. Dette er ikke noget problem for biblioteker, som ikke særlig ofte har ændringer i deres database, men disse er efterhånden et fåtal. Ved at benytte lokal vedligeholdelse af data kan man nøjes med at synkronisere sin eksisterende database med LDAP-databasen, og alle i samarbejde vil derefter kunne tilgå dataene. Det betyder, at en opdatering lokalt vil have gennemslags kraft globalt uden ekstra arbejde.

3 Support

Som en del af den indgående serviceaftale mellem Statsbiblioteket og biblioteket er der mulighed for at få hjælp til løsning af problemer, som opstår undervejs.

3.1 Opsætning

Den proxy, som tilordnes det enkelte bibliotek, skal kende de tidsskriftdatabaser, som skal kunne tilgås af det pågældende biblioteks brugere. På forhånd er den konfigureret til at formidle adgang til de udbydere, der indgår i nationale licenser administreret af DEF. Såfremt det enkelte bibliotek har licenser herudover, skal konfigurationen heraf konfigureres specifikt i proxy'en efter aftale mellem SB og det pågældende bibliotek.

3.2 Drift

LDAP- og proxytjenesterne afvikles på servere, som i udgangspunkt er tilgængelige i 24-timers drift ugen rundt. Kortere driftsafbrydelser i forbindelse med opdatering af systemerne vil kunne forekomme. Sådanne afbrydelser vil i videst muligt omfang blive annonceret over for bibliotekerne i forvejen.

3.3 Support

Hvis der er spørgsmål til driften eller opsætningen af LDAP- og proxytjenesterne, kan de deltagende biblioteker sende henvendelser til Statsbibliotekets helpdesk som beskrevet i afsnit 5.

4 Krav til datalevering

Det reelle arbejde for det enkelte bibliotek, der gerne vil med i samarbejdet, kommer til at ligge i dataleverancer. Det er derfor meget vigtigt allerede ved tilslutningen til projektet at gøre sig klart, hvilke krav, der skal overholdes nu, og hvilke krav, der kan komme senere. Kravene til data skal tilgodeses, hvilket betyder, at alt, hvad der leveres til systemet, skal være i samme format, og de påkrævede felter skal være udfyldt.

4.1 Dataindhold

I den første version, der er skitseret på figur 2, er der ikke brug for ret mange informationer for at få systemet til at virke. Der er dog nogle ekstra felter, som kan udfyldes allerede nu, da der senere vil blive brug for dem, efterhånden som antallet af forskellige ressourcer tilbydes.

ISO-latin-1 tegnsættet skal benyttes og tabulatortegnet må ikke indgå i feltværdierne.

Kravene til indholdet af brugerdatafilen er således:

1. Fulde navn (cn) angives som: <fornavn> <mellemlnavn> <efternavn>
Mellemlnavnsdelen kan indeholde 0 eller flere navne.
2. Bruger-id (uid)
Unikt login navn. Dvs. det er unikt for det enkelte bibliotek.
3. Kodeord (userPassword)
Kode, som enten kan være ukrypteret eller være krypteret med en af følgende algoritmer: Crypt, md5, sha, ssha eller smd5. Dette kan gøres nemt med /usr/sbin/slappasswd. Hvis dette program ikke benyttes, skal der laves en test af krypteringstypen.
4. Bruger institution (brugerInstitution)
Den eller de institutioner, som brugeren er tilknyttet. Der kan angives 0 eller flere som adskilles med tegnet ”|”. Koden for institutionen angivet ud fra den/de tildelte OID. Denne ser ud som følgende og er bestemt centralt: 1.3.6.1.4.1.11356.2.3.#, hvor # er institutionens tildelte nummer. Det er muligt at angive en videre hierarkisk underopdeling. Denne kode benyttes til autorisation af brugeren. Det er vigtigt at disse koder tilknyttes brugerne i forhold til licensaftalerne og ikke bibliotekstilknytningen.
Et eksempel kunne være en Statsbiblioteks låner, som er tilknyttet Århus Universitetet, hvor dette felt vil indeholde koden for Århus Universitet.

Ud over disse påkrævede felter kan de følgende udfyldes efter behov. Det er dog nødvendigt at alle felterne forekommer, disse kan blot være tomme.

5. Postadresse (postalAddress)
Brugerens fysiske postadresse, der kan benyttes til f.eks. hjemkaldelser. Denne skal gives som: <vejnavn> <husnummer> <etage> <interntnummer/placering>”|” <postnummer> <by>
6. E-mailadresse (mail)
Brugerens egen e-mailadresse i kompletform.

Navnene, som står i parentes, er de reelle LDAP-navne, som feltet indeholder. Det skal altså være muligt at opfylde punkterne 1 – 4 for at en person kan oprettes i databasen.

Biblioteket bliver tildelt et IP-nummer ved oprettelse i projektet. Denne IP-adresse, som er nummeret på proxy'en, skal behandles, som om det er en af institutionens egne. Dvs. at der til alle udbydere indenfor institutionens licenser skal oplyses denne nye adresse. Dette sikrer, at der er adgang til de ressourcer, som institutionen har. Denne adresse ændrer sig ikke, og det vil derfor være en en-gangsopgave.

4.2 Dataformater

Indholdet af brugerdatafilen, der er beskrevet i forrige afsnit, skal leveres i et fastlagt format. Dette er nødvendigt, da der skal kunne opdateres jævnlige, og disse skal kunne foregå automatisk.

Leverancerne af filen vil oftest være et udtræk fra en eksisterende database, og derfor er der blevet valgt et meget generelt format, som alle burde kunne generere uden problemer.

Filen skal være en tabulator separeret tekstfil, hvor hvert felt er adskilt af et tabulator tegn. Dette format er direkte kompatibelt med de fleste database systemer samt Excel og Access. Den første linie i filen skal indeholde LDAP-navnene i den ovenstående rækkefølge, så der senere kan ændres på formatet uden, at det vil have indflydelse på det gamle format. De efterfølgende rækker skal bestå af en bruger pr. række, hvor dataene står i samme rækkefølge som titellinien. Hver række skal indeholde præcis 5 tabulator tegn. Der er her vist et eksempel på en brugerdatafil:

Først ses brugerdataene i tabelform og derefter som tabulatorsepareretfil.

cn	uid	userPassword	brugerInstitution	postalAddress	mail
Thomas Koch Rasmussen	ral	vreG34g3	1.3.6.1.4.1.11356.2.3.6 1.3.6.1.4.1.11356.2.3.1.1	Sandagervej 2 8240 Risskov	tkr@statsbiblioteket.dk
Jens Hansen	jh	{SSHA}a6kSovaXBtBPFoXkxBuURMtAu+wkbdAi	1.3.6.1.4.1.11356.2.3.4.1	Roskildevej 45B 4.th.l 2000 Frederiksberg	jh@teol.ku.dk

```

cn          uid          userPassword          brugerInstitution          postalAddress
mail
Thomas Koch Rasmussen ral          vreG34g3  1.3.6.1.4.1.11356.2.3.6|
1.3.6.1.4.1.11356.2.3.1.1          Sandagervej 2|8240 Risskov
tkr@statsbiblioteket.dk
Jens Hansen          jh          {SSHA}a6kSovaXBtBPFoXkxBuURMtAu+wkbdAi
1.3.6.1.4.1.11356.2.3.4.1          Roskildevej 45B 4.th.l|2000 Frede-
riksberg          jh@teol.ku.dk

```

4.3 Levering og sikkerhed

Da der skal leveres informationer som brugernavn og kodeord, er det vigtigt at sikkerheden er god. Samtidig skal leveringen kunne foregå nemt og automatisk. I det medfølgende dokument *brugervejledning.pdf*, bliver proceduren beskrevet trin for trin. I det nedenstående bliver hovedpunkterne beskrevet.

- Man modtager en zip-fil fra Statsbibliotekets helpdesk. Udpak filen i en mappe og køre batch filen *setup.bat*
- Send *public.txt* filen i keys-undermappen til Statsbiblioteket på mailadressen: ldap-tech@statsbiblioteket.dk, hvor emnet på mailen er: Public key fra <biblioteksnavn>

- Efter modtagelsen af jeres fil, vil der blive returneret en mail om, at biblioteket er oprettet som bruger.
- Nu kan brugerdatabasefilen leveres ved at køre batchen: `brugerdatabase_update <brugerdatabasefilnavn>`.

Biblioteker, som benytter Linux/Unix, skal i stedet gøre følgende:

- Installer OpenSSH_3.4 og lav en nøgle med kommandoen: `ssh-keygen -t rsa -f key`.
- Den offentlige nøgle (`key.pub`) sendes til mailadressen: ldap-tech@statsbiblioteket.dk, hvor emnet på mailen er: Public key fra <biblioteksnavn>
- Efter modtagelsen af jeres nøgle, vil der blive returneret et script (`brugerdata_update`), der bruges til leveringerne.
- Nu kan brugerdatabasefilen leveres ved at køre scriptet: `brugerdatabase_update <brugerdatabasefilnavn>`.

IP-nummeret på proxyen og brugerinstitutionskoden sendes til bibliotekets kontaktperson, efter Statsbiblioteket har modtaget dennes e-mailadresse.

4.4 Opdateringer

Det er vigtigt, at brugerdatabase bliver opdateret løbende, så informationerne hele tiden er korrekte. Derfor kan det være en stor fordel at få automatiseret leverancerne af disse informationer. Hvordan dette gøres er op til det enkelte bibliotek, men med metoden til levering beskrevet i forrige afsnit, skulle mulighederne for automatisering være nemme. Det er vigtigt, at alle brugerinformationerne leveres hver gang, da de gamle oplysninger overskrives ved indsendelse af en ny fil.

5 Kontaktpersoner

I forbindelse med base13 og proxytjenesterne er kan følgende kontaktadresser anvendes.

5.1 Tilmelding til tjenesterne

Henvendelser angående tilmelding til tjenesten og vilkårene herfor rettes til

Danmarks Elektroniske Fag- og Forskningsbibliotek

Styrelsen for Bibliotek og Medier

H.C. Andersens Boulevard 2, 5

1553 København V

att. Lotte Sterup

Telefon: 33 73 33 25

E-mail: lst@bibliotekogmedier.dk

5.2 På det enkelte bibliotek

I forbindelse med tilmelding til tjenesten skal det enkelte bibliotek udpege en kontaktperson. Denne kontaktperson kan foretage henvendelser til helpdesken og vil modtage driftsmeddelelser og eventuelle øvrige henvendelser angående driften af tjenesterne.

5.3 Henvendelser angående opsætning og drift

Support i forbindelse med driftsafviklingen og konfigurationen fås ved henvendelse til Statsbibliotekets helpdesk-funktion. Denne support er et tilbud til de deltagende biblioteker, som selv må håndtere henvendelser fra slutbrugerne.

Henvendelsen bør ud over de ønskede spørgsmål også henviser til base13/proxy-aftalerne. Den foretrukne fremsendelseform for henvendelsen er elektronisk post.

Helpdeskfunktionen er bemanded mandag-fredag kl. 8.00-15.30, og behandlingen af henvendelser modtaget i dette tidsrum vil normalt blive besvaret inden for en halv time. Henvendelser modtaget uden for den bemandede periode blive behandlet, når bemanningen igen er til stede.

Helpdesk modtager henvendelserne på:

email: helpdesk@statsbiblioteket.dk

telefon: 8946 2020

post: Statsbiblioteket, att. helpdesk, Universitetsparken, 8000 Århus C