Generell Feide-arkitektur

Introduksjon

Feide er i stor grad innført i universitets- og høgskolesektoren, og blir nå innført i grunnopplæringen. Samtlige fylkeskommuner er enten ferdige eller godt i gang med å innføre Feide for sine videregående skoler, og i disse dager setter mange kommuner i gang med det samme for sine grunnskoler. Kommuner oppfordres til å innføre en identitetsforvaltning basert på Feide fra flere hold, blant annet i et brev fra kunnskapsministeren til alle landes kommuner [1] og i eKommune 2012 [2].

En elektronisk identitetsforvaltning som Feide medfører en rekke fordeler for Skole-Norge [3]. Blant annet fordi opplysninger om personer lagres kun ett sted i skoleeiers organisasjon, og fordi alle digitale tjenester benytter samme informasjon.

Dette dokumentet beskriver den generelle Feide-arkitekturen på et overordnet nivå. En grundigere beskrivelse av arkitekturen finnes i Feides systemarkitektur [4].

Identitetsforvaltning og Feide

I takt med at stadig flere tjenester og ressurser gjøres tilgjengelige i elektronisk form, øker behovet for å kunne tilby digitale tjenester med personalisert innhold. For å realisere personaliserte tjenester kreves det at man sikkert kan fastslå hvem en person er og hvilke roller han er assosiert med, for å kunne gi personen riktig tilgang. Slik sikker identifisering forutsetter en god elektronisk identitetsforvaltning, og er aktuelt i utdanningssektoren som så mange andre steder. Sikker identifisering er for eksempel nødvendig når skolene tar i bruk læringsplattformer, nasjonale prøver og digital eksamen.

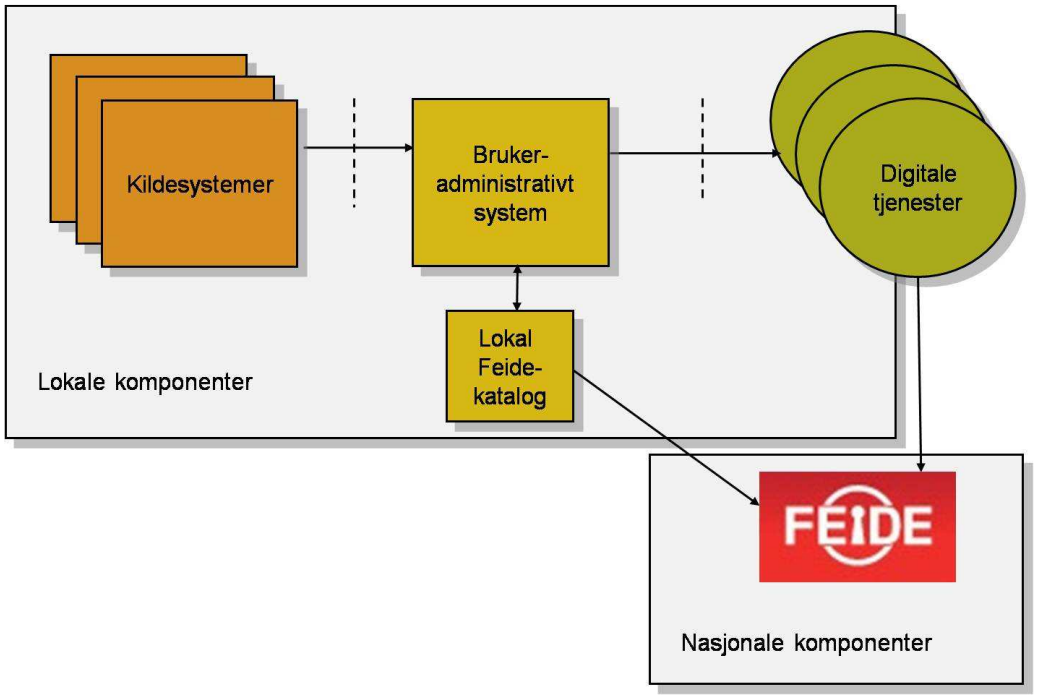
Feide (Felles elektronisk identitet) er Kunnskapsdepartementets satsing på en enhetlig identitetsforvaltning i utdanningssektoren. Feide innebærer at alle elever og ansatte får én elektronisk identitet, i form av ett brukernavn og passord som kan brukes ved en rekke tjenester. Feide lar personer tilknyttet norske utdanningsinstitusjoner identifisere seg via en felles innloggingstjeneste, og stiller krav til hvordan personopplysninger skal håndteres ved den enkelte organisasjon. Feide bygger på at samtlige tilknyttede institusjoner har tillit til hverandres data, ved at Feide har tillit til at hver institusjon hele tiden leverer korrekte og oppdaterte data. Organisasjonen holder selv orden på persondata om egne brukere, og den største jobben med Feide-innføringen er derfor å rydde i personregistre og innføre rutiner som sikrer god datakvalitet. Siden all personinformasjon ligger lokalt og hver personopplysning er knyttet til en autoritativ

[1] http://www.uninettabc.no/content.ap?thisId=8617
[2] http://ksikt-forum.no/temaer/ekommune
[3] http://www.uninettabc.no/content.ap?thisId=1096
[4] http://docs.feide.no/guide-0004-1.1-no.pdf

kilde må hver opplysning vedlikeholdes kun ett sted og det er lettere å sørge for korrekt og oppdatert informasjon.

Generell Feide-arkitektur

Den generelle Feide-arkitekturen hos skoleeier består av ett eller flere kildesystemer, et brukeradministrativt system og en lokal Feide-katalog. I tillegg kommer Feides nasjonale innloggingstjeneste og en eller flere digitale tjenester, lokale eller nasjonale. Figuren under viser hvordan de ulike komponentene i Feide henger sammen. Figuren er uavhengig av teknologivalg, og gir rom for lokale tilpasninger ut i fra hvilke løsninger skoleeier allerede har.



Generell Feide-arkitektur med lokale og nasjonale komponenter

Hver komponent er en del av en kjede informasjonsbehandlende komponenter. Kvalitetssikrete data fra administrative systemer fører til opprettelse av unike elektroniske identiteter i det brukeradministrative systemet. Det brukeradministrative systemet legger dessuten til ny informasjon om brukeren, for eksempel brukernavn, passord og aggregerte grupper. Informasjon om brukeren kan deretter overføres til tjenester etter behov, men tjenestene kan også selv lagre ytterligere informasjon om brukeren, for eksempel hvilke ressurser brukeren har tilgang til, eller brukerens preferanser på nyheter og farger. Under beskrives de enkelte komponentene i arkitekturen nærmere.

Kildesystemene

Kildesystemene er kilden for all informasjon i et identitetsforvaltningssystem. All administrasjon av en organisasjons personinformasjon gjøres i disse systemene, her registreres, vedlikeholdes og slettes informasjon som det brukeradministrative systemet i neste omgang benytter seg av. Informasjon som typisk ligger i kildesystemene er navn, adresser, fødselsnummer, elevnummer, telefonnummer, e-postadresser, klassetilhørighet, fag, og så videre.

Hver personopplysning vedlikeholdes i ett bestemt kildesystem. Samme informasjon kan lagres også i andre systemer, men skal kun endres i det bestemte systemet. Systemene skal altså ikke være i konflikt med hverandre, det skal ikke være mulig å registrere forskjellig informasjon om en person i to ulike kildesystemer. På denne måte sikres korrekte, konsistente og oppdaterte data.

Alle vertsorganisasjoner i Feide, det vil si institusjoner eller skoleeiere tilknyttet Feide, må ha ett eller flere kildesystemer. Disse vil typisk være:

- Et skoleadministrativt system (SAS), som inneholder informasjon om elever, lærere, fag og skoler. Produkter i bruk i dag er blant annet SATS [5], Extens [6], Oppad [7], TP-systemet [8], WIS Skole [9] og Unique Skole [10].
- Et lønns- og personalsystem (LP), som inneholder informasjon om lærere og andre ansatte.
- Andre katalogtjenester [11], for eksempel Active Directory, NIS og lignende.

Det brukeradministrative systemet

Det brukeradministrative systemet (BAS) er IT-avdelingens støttesystem, som mottar oppdaterte personopplysninger fra ett eller flere kildesystemer, sammenstiller personinformasjon fra de ulike systemene, oppretter brukere med tilhørende brukernavn og passord, og vedlikeholder informasjon om brukerne. Ved at alle brukere opprettes i det brukeradministrative systemet og herfra synkroniseres ut til andre brukerdatabaser får brukere samme brukernavn og passord ved alle tilknyttede systemer, og når brukeren bytter passord vil dette kunne gjelde i alle systemene.

Mange digitale tjenester behøver opplysninger om for eksempel navn, skole- og klassetilhørighet, og kan få dette fra det brukeradministrative systemet. Det brukeradministrative systemets viktigste oppgave er nettopp å videreformidle personopplysninger fra kildesystemene til digitale tjenester, og klargjør blant annet opplysninger som kreves av Feides nasjonale innloggingstjeneste. Ved at de digitale tjenestene henter

[5] http://ist.biz
[6] http://ist.biz
[7] http://www.oppad.no
[8] http://barman-hanssen.no
[9] http://www.wis.no
[10] http://vismacultus.no
[11] http://www.uninettabc.no/content.ap?thisId=689

nødvendig informasjon fra det brukeradministrative systemet sikres at tjenestene har korrekte, konsistente og oppdaterte personopplysninger.

Digitale tjenester

Noen eksempler på digitale tjenester kan være e-post, nettverkspålogging, læringsplattformer, digitale læremidler, portaltjenester, bibliotektjenester, administrative tjenester, opptakssystemer og digitale prøver.

Mange tjenester ønsker å kontrollere hvilke brukere de gir tilgang til, og krever innlogging med brukernavn og passord. Feide gjør det enkelt å gi elever og lærere tilgang til digitale tjenester. Med Feide kan skoleeiere gi sine elever og ansatte et Feide-navn og et tilhørende passord som de kan bruke for å logge inn på digitale webtjenester tilpasset Feide.

Flere digitale tjenester har dessuten behov for opplysninger om personen som logger inn. For eksempel kan en tjeneste ønske å vite personens navn, klasse og fag, slik at tjenesten kan presentere riktig og tilpasset informasjon. Feide-arkitekturen sørger for at tjenesten får korrekt og oppdatert informasjon om brukeren. Informasjonsformidlingen er kontrollert, slik at tjenesten ikke får tilgang til informasjon uten at dette er avtalt på forhånd. Dette for å ivareta brukerens personvern.

Lokal Feide-katalog og nasjonal innloggingstjeneste

En skoleeier som ønsker å bli vertsorganisasjon i Feide må sette opp en lokal Feide-katalog, som skal ha en kobling mot Feides nasjonale innloggingstjeneste. Innloggingstjenesten autentiserer brukere tilhørende en gitt organisasjon mot organisasjonens egne lokale Feide-katalog.

Den lokale Feide-katalogen er en standard LDAP-katalogtjeneste. All informasjon i katalogen kommer fra det brukeradministrative systemet, noe som sikrer at informasjonen er korrekt, konsistent og oppdatert. Informasjon i Feide-katalogen skal automatisk oppdateres minst en gang i døgnet. Feides LDAP-spesifikasjon [12] definerer hvilken person- og organisasjonsinformasjon som skal ligge i katalogen, en del attributter er obligatoriske, noen er anbefalte og andre er frivillige. Den lokale Feide-katalogen kobles mot Feides nasjonale innloggingstjeneste, Moria [13].

Når en Feide-bruker skal logge inn på en digital tjeneste vil tjenesten videresende brukeren til innloggingstjenesten. Brukeren oppgir Feide-navn og passord, som valideres mot brukerens lokale Feide-katalog. Dersom brukeren har oppgitt riktig brukernavn og passord vil tjenesten få beskjed om dette, og brukeren får tilgang til tjenesten. Personopplysningene ligger i den enkelte organisasjons lokale Feide-katalog, og ikke i den sentrale innloggingstjenesten.

[12] http://docs.feide.no/spec-0001-1.1-en.pdf
[13] http://docs.feide.no/fs-0002-2.0-no.html

Enkelte tjenester kan ha inngått avtale om å få overført personopplysninger fra innloggingstjenesten, og får dette sendt tilbake etter vellykket innlogging. Innloggingstjenesten henter disse personopplysningene fra den lokale Feide-katalogen, men kun om dette er avtalt på forhånd. På denne måten bevarer brukeren kontroll over sine egne personopplysninger.

Grensesnitt

I tillegg til de allerede nevnte komponentene trengs grensesnitt for overføring av data. For å importere data fra kildesystemene inn i det brukeradministrative systemet trengs grensesnitt for import, og for å eksportere data fra det brukeradministrative systemet trengs grensesnitt for eksport.

I enkelte tilfeller kan allerede eksisterende grensesnitt benyttes, i andre tilfeller må nye koblinger lages. For datautveksling mellom skoleadministrative og brukeradministrative systemer er det definert et XML-basert grensesnitt ved navn ABC Enterprise [14], som gjør det enkelt å hente data om personer, organisasjoner, grupper og relasjoner på et bestemt format uavhengig av hvilket skoleadministrativt system som brukes. ABC Enterprise er i utstrakt bruk i dag, men vil fases ut og erstattes av en ny norsk standard for personrelatert informasjonsflyt i utdanning (PIFU) [15].

For å overføre data mellom brukeradministrative systemer og digitale tjenester benyttes ofte IMS Enterprise [16], et internasjonalt XML-basert grensesnitt for utveksling av informasjon mellom administrative tjenester i utdanning. Både ABC Enterprise og IMS Enterprise er anbefalte grensesnitt, og på sikt vil ABC Enterprise erstattes av PIFU. LDAP-grensesnittet mellom lokal Feide-katalog og den nasjonale innloggingstjenesten er påkrevd for organisasjoner som skal kobles opp mot Feide.

Ulike implementeringer

Organisasjoner som skal innføre en identitetsforvaltning har ofte ulike utgangspunkt. Hvilken løsning de velger avhenger blant annet av hvilke systemer og tjenester de allerede bruker, samt hvilken plattform som kjøres og hvilken kompetanse og erfaringer de allerede har. Det som skiller de ulike løsningene fra hverandre rent teknologisk er hvilke produkter det brukeradministrative systemet består av. Følgende teknologier er brukt for å realisere brukeradministrative systemer i eksisterende Feide-løsninger:

- Cerebrum (PostgreSQL og Python-script)
- Novell (eDirectory og Identity Manager)
- Microsoft (SQL-server, ILM og ADAM)

Cerebrum er basert på programvare med åpen kildekode, og er utviklet ved Universitetet i Oslo. Cerebrum brukes blant annet av Østfold fylkeskommune og Giske kommune. Rogaland fylkeskommune er ett av fylkene

[14] http://www.uninettabc.no/content.ap?thisId=1080
[15] http://www.uninettabc.no/pifu
[16] http://www.imsglobal.org/enterprise

som har valgt å gå for en Novell-basert løsning, med eDirectory som sentral katalogtjeneste og Identity Management som synkroniseringsmotor. I Hedmark fylkeskommune er det utviklet en gjenbrukbar Feide-løsning basert på programvare fra Microsoft, denne omtales som Buddy-løsningen og bygger på SQL-server, ADAM og ILM. I dag er det etablert et samarbeid rundt bruk og videreutvikling Buddy-løsningen. Flere andre aktører har produkter med tilsvarende funksjonalitet, dette gjelder for eksempel IBM, Oracle og Sun. Det ventes at flere aktører vil levere Feide-løsninger i løpet av kort tid.

I praksis spiller det liten rolle hvilken teknologi som benyttes, og det er fullt mulig å blande produkter fra de ulike teknologiene. Som regel velger organisasjoner imidlertid å satse på den teknologi og de produkter de allerede kompetanse på og erfaringer med.

Tekniske beskrivelser av Feide-løsninger:

- Identitetsforvaltning basert på Cerebrum
  – Med eksempler fra Østfold fylkeskommune og Giske kommune [17]
- Identitetsforvaltning basert på Novell-produkter
  – Med eksempel fra Rogaland fylkeskommune [18]
- Identitetsforvaltning basert på Microsoft-produkter
  – Buddy-løsningen og eksempel fra Hedmark fylkeskommune [19]

[17] http://www.uninettabc.no/content.ap?thisId=925
[18] http://www.uninettabc.no/content.ap?thisId=924
[19] http://www.uninettabc.no/content.ap?thisId=923