Feide systemarkitektur

Januar 2011

Versjon 2.0

UNINETT

Document History

Version	Date	Initials	Comments
2.0	Januar 2011	HV	Dokumentet er oppdatert ihht gjeldende arkitektur.

UNINETT
Abels gate 5 – Teknobyen
NO-7465 Trondheim
telephone: +47 73 55 79 00
fax: +47 73 55 79 01
e-mail: info@uninett.no
web: www.uninett.no

Innholdsfortegnelse

1 Innledning

Dette dokumentet beskriver Feides arkitektur.

1.1 Målgruppe

Primær målgruppe er IT-ledere som har behov for å identifisere aktører og komponenter som inngår i Feide, og samspillet mellom dem på overordnet nivå. Det forutsettes ikke detaljert teknisk bakgrunn for å lese dokumentet, men generelt kjennskap til IT-systemer er en fordel.

1.2 Hva menes med en arkitektur

Med en arkitektur mener vi:

- En modell av komponenter, informasjon og begreper
- Spesifikasjon og tekstlig beskrivelse av komponentene som fungerer sammen
- Spesifikasjon og tekstlig beskrivelse av grensesnittene mellom komponenter
- Avtaler, bestemmelser og retningslinjer som aktørene er bundet av

1.3 Symboler brukt i figurene

I figurene brukes følgende symboler for komponentene i arkitekturen:

Brukere: Elever, studenter og ansatt

Tjenester: Læresystemer, biblioteker, informasjonleverandører etc.

Vertsorganisasjoner: Undervisnings- og forskningsorganisasjoner og lignende

Feides innloggingstjeneste

Andre føderasjoner: eduroam, Kalmar, MinSide

2 Oversikt

2.1 Feide som identitetsleverandør (Identity Provider)

Feides innloggingstjeneste formidler informasjon om brukere til tjenesteleverandører.

Å bekrefte at en bruker er den vedkommende gir seg ut for å være, kalles autentisering. En person som benytter tjenester koblet til Feide autentiserer seg én gang ved innlogging gjennom Feide i starten av en arbeidsøkt. Deretter kan Feide garantere brukerens identitet overfor ulike tjenesteleverandører; Feide er en tiltrodd tredjepart.

Feide tilbyr også kontrollert formidling av informasjon om en autentisert bruker. En tjeneste kan derfor avlastes for oppgavene med å administrere grunnleggende brukerdata, spesielt ansvaret for å holde brukerdata oppdatert.

Autentiseringen bekrefter brukerens identitet, uavhengig av hvilke tilgangsrettigheter brukeren har. Tjenesten kan selv foreta tilgangskontroll basert på den informasjon som er sendt av Feide.

Feides tilbud om autentisering og brukerinformasjon er basert på web, og kan kun benyttes av tjenester som tilbys over web.

2.2 Vertsorganisasjoner og tjenesteleverandører

Feide håndterer utveksling av informasjon mellom aktører som administrerer Feide-brukere, vertsorganisasjoner, og aktører som tilbyr tjenester til brukerne, tjenesteleverandører. Samme organisasjon, f.eks. et universitet, kan opptre både som vertsorganisasjon og som tjenesteleverandør. Vertsorganisasjoner, tjenesteleverandører og Feide utgjør til sammen en føderasjon, illustrert her i figur 1.

Figur 1: Oversikt over aktørene i Feide

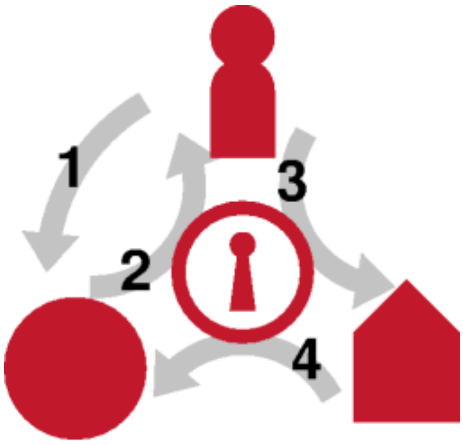
Brukeren benytter en nettleser for kommunikasjon med et sett web-baserte tjenester. Tjenestene mottar autentiseringsinformasjon og attributter gjennom Feide. Slik informasjon lagres ikke i Feides innloggingstjeneste, men i en LDAP-katalog hos den vertsorganisasjon brukeren tilhører. Attributter

leses med de adgangsrettigheter brukeren selv er gitt til LDAP-katalogen, og Feide videreformidler attributtene til tjenester med behov for dem. Før første gangs innlogging til en tjeneste må brukeren godkjenne at attributter videresendes til tjenestene brukeren benytter, i henhold til Feides avtale med tjenesteleverandøren. Hvis brukeren ikke ønsker dette kan innloggingen avbrytes.

2.3 Feide-innlogging

En vellykket Feide-autentisering foregår i følgende steg:

1. Brukeren forsøker å åpne en web-side for den tjenesten han ønsker å benytte.
2. Tjenesten sender en autentiseringsforespørsel til Feide, som åpner et innloggingsskjema for brukeren.
3. Brukeren skriver inn sitt Feide-navn og passord i innloggingsskjemaet og returnerer det til Feide. Feide sender navn og passord til brukerens vertsorganisasjon for kontroll.
4. Vertsorganisasjonen returnerer til Feide en bekreftelse på at brukeren er autentisert, samt de attributter vertsorganisasjonen har lagret for denne brukeren. Feide videreformidler til tjenesten bekreftelse på brukerens autentisering, samt de brukerattributtene som tjenesten har avtale om at skal utleveres.



Hvis brukeren allerede har spesifisert sitt Feide-navn og passord for en annen tjeneste, kan denne sekvensen forkortes: Når Feide mottar forespørselen i steg 2, kan en bekreftelse på brukerens identitet og aktuelle attributter returneres til tjenesten uten at brukeren behøver å oppgi navn og passord på nytt, og uten å måtte kontakte vertsorganisasjonen.

2.4 Informasjon formidlet av Feide vs. lokal informasjon

En vertsorganisasjon håndterer et standardsett attributter for hver bruker, definert av norEdu* Object Class Specification [norEdu], samt Feides formkrav [formkrav_go, formkrav_uh]. Dette er en nordisk tilpasning av de internasjonale standard-skjemaene eduPerson og eduOrg [eduPerson].

Disse attributtene lagres i en LDAP-katalog hos vertsorganisasjonen til brukeren. Når en bruker autentiseres, henter Feide informasjon fra vertsorganisasjonens LDAP-katalog. De attributter tjenesten på forhånd har avtalt å få av Feide, blir så sendt til tjenesten. Fordelen med dette er:

- Tjenesteleverandøren slipper å håndtere informasjon om individuelle brukere: I stedet for å selv lagre attributtene,ber tjenesten Feide om å skaffe den til veie. F.eks. behøver ikke et bibliotek lagre lånernes e-postadresser; når en bruker bestiller en bok, får biblioteket vite fra Feide hvor melding skal sendes (brukerens e-post-adresse) så snart boka blir tilgjengelig.
- Tjenesten er sikret å alltid få oppdaterte opplysninger. En del tjenester har likevel behov for å bevare mer informasjon om brukeren enn Feide kan tilby, og håndterer denne selv, lokalt

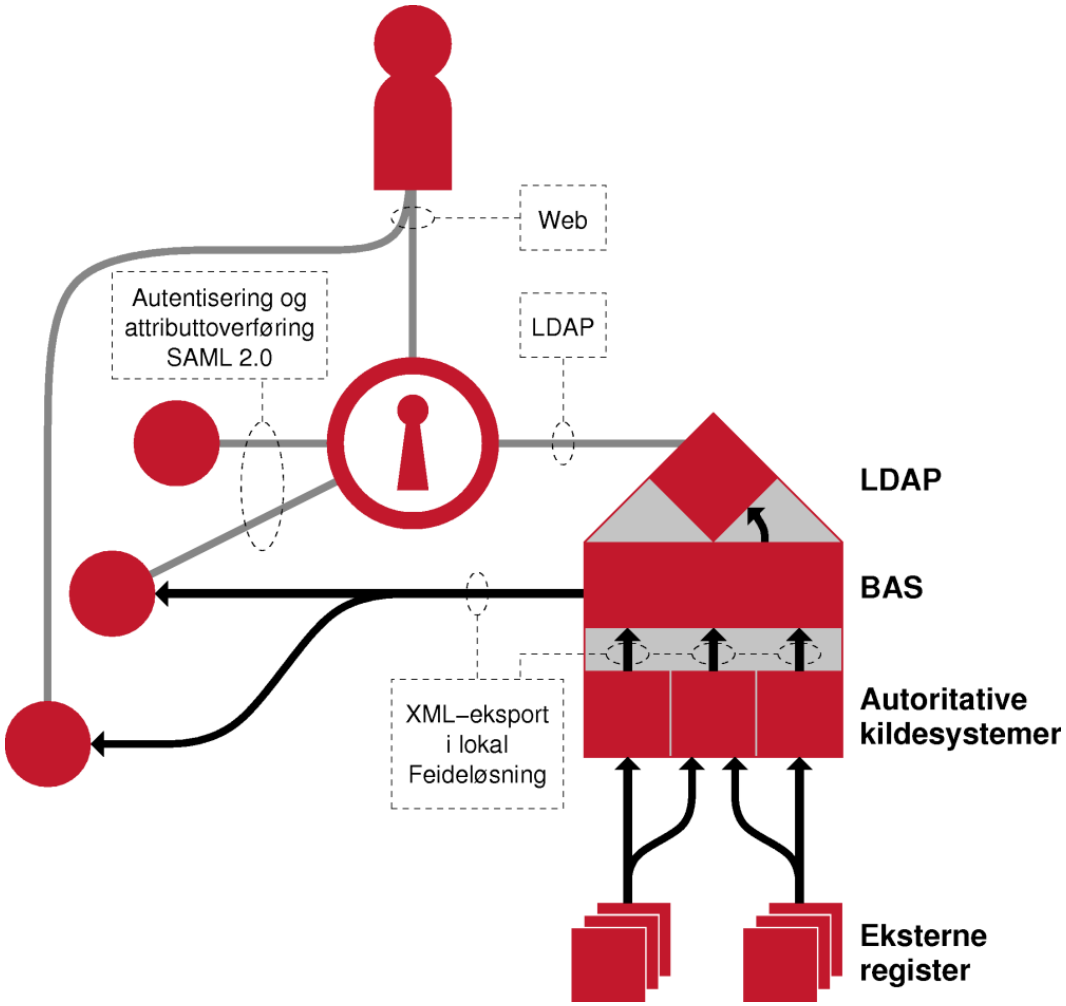
lagret. Det kan for være fordelaktig om brukeravhengig informasjon som lagres lokalt av tjenesten er tillegg til informasjonen Feide formidler, slik at man unngår lokal lagring av kopi av informasjon som likevel kan hentes gjennom Feide. Det sikrer at tjenesten ikke benytter seg av foreldet informasjon.

Feide inngår en avtale med hver enkelt tjenesteleverandør om hvilke attributter tjenesten skal få via Feide. Attributter utleveres bare i den grad det er nødvendig for å utføre tjenesten. Feide lagrer ikke attributter, ut over mellomlagring så lenge en Feide-sesjon er aktiv.

Enkelte attributter, f.eks. fødselsnummer, identifiserer en person unikt, og kan brukes til å koble informasjon fra ulike kilder. Feide er restriktiv med hensyn på å gi tilgang til for eksempel fødselsnummer, og tjenesteleverandører må vise til et reelt behov for å få utlevert dette gjennom Feide.

3 Feides informasjonsmodell

Informasjonsflyten i Feide løper fra vertsorganisasjoner, via Feide, til tjenesteleverandører som vist i figur 2. Eventuell informasjon fra tjenesteleverandører tilbake til vertsorganisasjonene går utenom Feide, og er ikke definert i denne arkitekturen.



Figur 2: Kildesystemer og brukeradministrativt system

Feide stiller visse krav til identitetsforvaltningen i vertsorganisasjoner som er koblet til Feide, og vertsorganisasjonen forplikter seg til å følge retningslinjer spesifisert i kontrakten med Feide.

3.1 LDAP-katalog hos vertsorganisasjonen

Vertsorganisasjonen håndterer informasjon, hentet fra autoritative kilder, om brukere i organisasjonen. Eksempler er navn, kontaktinformasjon, tilknytning til organisasjonen, autentiseringsinformasjon og lignende.

Feide krever at hver vertsorganisasjon stiller til disposisjon et standardsett attributter om organisasjonens brukere i en LDAP-katalog. Semantikk og struktur til informasjonen er spesifisert i Feides formkrav [norEdu, formkrav_go samt formkrav_uh].

LDAP-katalogen har følgende egenskaper:

- LDAP-katalogen brukes for å autentisere brukere.
- LDAP-katalogen inneholder beskrivende attributter for alle autentiserte brukere.
- Informasjonen i LDAP-katalogen holdes til enhver tid så korrekt og oppdatert som det er mulig.
- Detaljerte krav er angitt i retningslinjer spesifisert i kontrakten mellom Feide og vertsorganisasjonen.
- Innloggingstjenesten henter brukerinformasjon fra LDAP-katalogen hos brukerens vertsorganisasjon.

Følgende krav stilles til alle LDAP-kataloger:

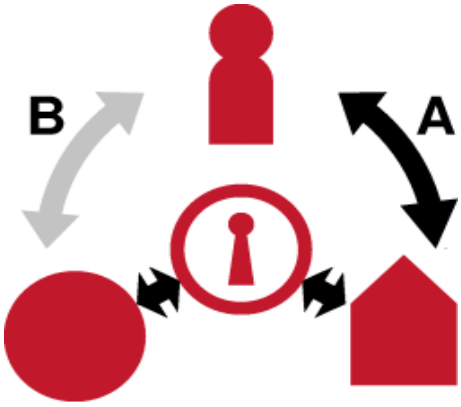
- Kommunikasjonen mellom katalog og Feide er pålitelig og sikret mot avlytting.
- Katalogen er tilgjengelig gjennom standard LDAP-protokoll.
- Informasjonen i katalogen fylles inn fra et system for identitetsforvaltning (et brukeradministrativt system) hos organisasjonen.
- Innloggingstjenesten må kjenne startpunktets DN («Distinguished Name») for Feide-delen av katalog-treet, og må ha rettighet til å søke opp en brukers DN ut fra vedkommendes Feide-navn.

3.2 Provisioning

I den grad det er ønskelig og nødvendig kan det overføres informasjon til en tjeneste på forhånd om et antall brukere på gjennom såkalt *provisioning*. Vertsorganisasjonen overleverer da informasjon om for eksempel alle nye studenter dette semesteret. Dette gjøres utenfor Feide.

Når brukeren logger inn på tjenesten første gang, leverer Feide tilstrekkelig informasjon til at tjenesten kan identifisere den riktige (forhåndsregistrerte) kontoen. Provisioning er særlig aktuelt der tjenesten har behov for informasjon som ikke er omfattet av brukerattributtene i Feides LDAP-skjema.

4 Feides tillitsnettverk



Figur 3: Implisitte og og eksplisitte tillitsrelasjoner

Feides tillitsnettverk er uttrykt ved et sett avtaler, kontrakter, implementasjoner og retningslinjer. Betegnelsen "tillitsnettverk" indikerer at parter må kunne stole på hverandre i tilstrekkelig grad slik at Feide kan fungere på tvers av organisasjonsgrenser. I dagens utgave av Feide opereres det med ett felles tillitsnivå.

Brukerne i Feide administreres av sine vertsorganisasjoner. Feide krever at brukerne holdes ansvarlig for alle sine handlinger i bruk av datasystemer og tjenester, og at godtatte regler for akseptabel bruk blir håndhevet.

Krav til beskyttelse av data og til personvern er regulert av norsk lov. Dersom Feide-autentisering benyttes i forbindelse med vertsorganisasjoner og/eller tjenester utenfor Norge kan tilsvarende lovgiving i andre land komme til anvendelse. Feides arkitektur er utviklet for å tilfredsstille kravene i personopplysningsloven [popl], særlig med hensyn til sikkerhet og personvern.

4.1 Tillit mellom flere parter

Pilene i figur 3 ovenfor viser hvor det eksisterer tillitsforhold.

4.1.1 Tillit mellom brukere og vertsorganisasjonene

Ansatte, studenter og andre som tilhører en organisasjon har et forhold til sin vertsorganisasjon, representert ved pil "A". Endring av disse forholdene over tid håndteres av vertsorganisasjonen selv. Siden Feides kontakt med brukere går via vertsorganisasjonene, vil krav og forpliktelser overfor Feide bare indirekte ha betydning for brukere.

4.1.2 Tillit mellom brukere og tjenester

Tillitsforholdet mellom brukere og tjenester, merket "B", er et implisitt forhold som brukere kan velge om de vil akseptere ved Feide-innlogging. Tilliten er basert på sikkerhetsmekanismene i Feide, avtale mellom tjenesteleverandøren og vertsorganisasjonen, Feides avtale med disse to, og mellom brukeren og vedkommendes vertsorganisasjon.

4.2 Kontrakter og retningslinjer

Nedenfor redegjøres for hvilke forhold som er regulert i kontrakts form, og det identifiseres områder der samarbeidet er basert på tillit til oppfølging av kontrakten.

4.2.1 Kontrakt mellom Feide og en vertsorganisasjon

Kontrakten mellom Feide og en vertsorganisasjon regulerer følgende forhold:

- tekniske detaljer om vertsorganisasjonens LDAP-katalog
- juridiske ansvarsforhold mellom Feide og vertsorganisasjonen
- prosedyrer for å sikre konfidensialitet og personvern
- tilgjengelighet, format og kvalitet på attributter som formidles til Feide
- ansvar for brukerstøtte og support

Partenes forpliktelser	
Feide	**Vertsorganisasjonen**
• yte andrelinje-kundestøtte • kontinuerlig overvåke at innloggingstjenesten er i drift • legge til rette for overvåking av tilgang til LDAP-katalog	• yte førstelinje-brukerstøtte til egne brukere • tilby autentisering av egne brukere gjennom organisasjonens LDAP-katalog • tilby attributter i samsvar med Feides skjema med hensyn til syntaks og semantikk • levere konsistente og oppdaterte data til Feides innloggingstjeneste

Tillit mellom partene	
Feide	**Vertsorganisasjonen**
• korrekt identifisere en tjenesteleverandør som mottar attributter gjennom Feide • beskytte persondata, inkludert passord, mot uautorisert tilgang, og ikke bruke denne informasjonen til annet formål enn autentisering av Feide-brukere og formidling av attributter til tjenesteleverandører i henhold til avtale	• korrekt bekrefte eller avkrefte at en bruker som tilhører organisasjonen har spesifisert korrekt passord, på forespørsel levere korrekte attributter i den grad det er spesifisert i avtale • avvise autentisering av brukere som ikke lenger har tilknytning til organisasjonen

4.2.2 Kontrakt mellom Feide og en tjenesteleverandør

Kontrakten mellom Feide og en tjenesteleverandør regulerer følgende forhold:

- tekniske detaljer om tjenesten
- juridiske ansvarsforhold mellom Feide og tjenesteleverandøren
- en liste over vertsorganisasjoner som skal tillates tilgang til tjenesten; tjenesten kan også være åpen for alle vertsorganisasjoner eller kun for egen/intern organisasjon
- hvilke attributter tjenesten etterspør for autentiserte brukere
- kontaktpunkter for administrative spørsmål og driftsspørsmål

Partenes forpliktelser	
Feide	**Tjenesteleverandøren**
• muliggjøre Feide-innlogging til lokale tjenester for organisasjonens egne brukere • varsle alle vertsorganisasjoner når en ny tjeneste innføres • sørge for at brukere fra vertsorganisasjoner som har åpnet for en tjeneste blir oppkoblet til tjenesten	• registrere alle tjenester med Feide-autentisering hos UNINETT • skal ha en personvernerklæring som skal være lett tilgjengelig for Feide-brukere

Tillit mellom partene	
Feide	**Tjenesteleverandøren**
• formidle korrekt informasjon om autentiserte brukeres identitet	• avstå fra å permanent lagre attributter innhentet gjennom Feide når dette ikke er både spesifisert i avtalen og en nødvendig forutsetning for å utføre tjenesten

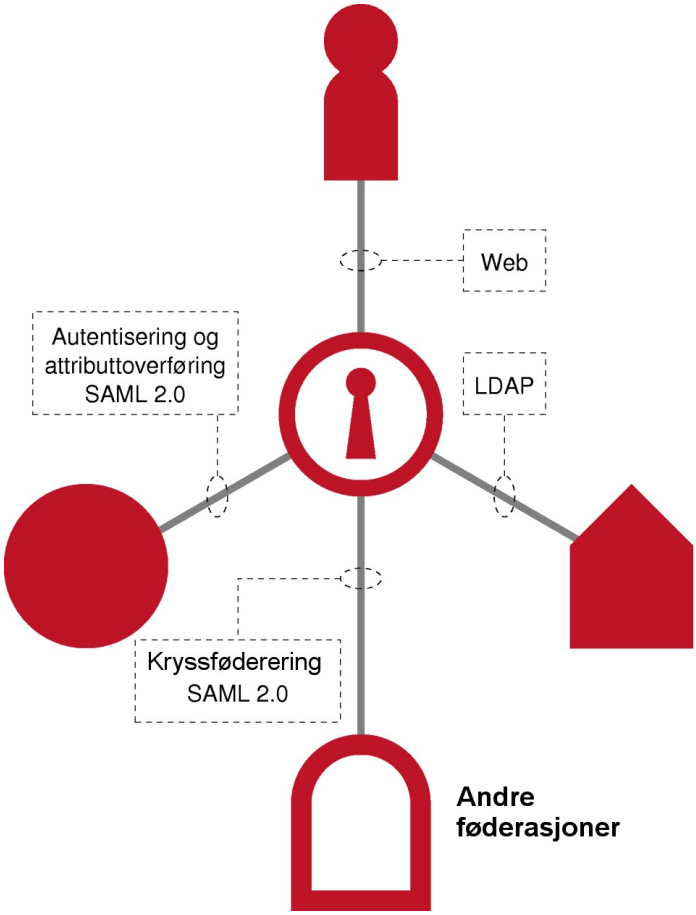
4.3 Kryssføderering

Feide kan også kobles sammen med tilsvarende føderasjoner i andre land eller i Norge. Dette kalles kryssføderering, og skjer gjennom avtaler som regulerer følgende forhold:

- Retning på fødereringen: Om eksternt autentiserte brukere skal tillates tilgang til tjenester koblet til Feide, og om brukere logget inn via Feide skal gis tilgang til tjenester i den andre føderasjonen.
- Juridisk ansvarlige personer som representerer hver føderasjon.

- Tekniske standarder som fødereringen er basert på.
- Kontaktpunkter for administrative spørsmål og driftsspørsmål.
- Retningslinjer for utveksling av attributter: Hvilke attributter kan utveksles (avhenger av retning på fødereringen) og hvordan attributter i andre føderasjoner kobles med Feide-attributter. Feide vil kun foreta kryssføderering med andre føderasjoner som foretar autentisering på et sikkerhetsnivå som er sammenlignbart med Feides egne prosedyrer.

5 Grensesnitt



Figur 4: Komponenter og grensesnitt i Feide

Følgende grensesnitt er vist i figuren over:

- Web: Mellom brukere og Feides innloggingstjeneste.
- Autentisering og attributtoverføring: Mellom tjenester og innloggingstjenesten
- Kryssføderering: Mellom Feide og eksterne partnere (andre føderasjoner).
- LDAP: Mellom innloggingstjenesten og vertsorganisasjonene.

Hvert grensesnitt forklares i avsnittene nedenfor. Grensesnittene er beskrevet ved logisk informasjonsflyt. Meldingsflyten på fysisk nivå kan avvike fra dette, noe som kan ha betydning for kravene til sikkerhetstiltak rundt kommunikasjonslinjene.

5.1 Mellom brukere og innloggingstjenesten

Dette grensesnittet brukes primært for brukerens dialog med innloggingstjenesten og er basert på web-protokoller. Dialogen aktiveres dersom brukeren ikke allerede har en Feide-sesjon, eller tjenesten krever ny innlogging (som regel av hensyn til sikkerhet).

Brukerne skal informeres om følgende:

- at innloggingsforsøk håndteres av Feides innloggingstjeneste
- navnet på den tjenesten brukeren kobler seg til
- hvilke attributter tjenesten kan få overført gjennom Feide

Første gang brukeren logger seg på en tjeneste, vil brukeren få opp en side hvor alle brukerattributtene tjenesten vil motta blir listet opp. Brukeren må gi sitt samtykke til at disse opplysningene blir sendt til tjenesten. Dersom brukeren ikke ønsker å samtykke til dette, blir innloggingen avbrutt.

5.2 Mellom tjenester og innloggingstjenesten

Grensesnittet er basert på web-mekanismer for redirigering av brukeren. Disse mekanismene er i henhold til SAML 2.0 [saml] og er nærmere beskrevet i Feide Integration Guide [intguide] og Feide Technical Guide [techguide].

Feide gir tjenesten en bekreftelse på at brukeren er autentisert, og i tillegg får tjenesten oversendt attributter om brukeren i henhold til avtale inngått med Feide.

5.3 Mellom innloggingstjenesten og andre føderasjoner

Den konkrete utformingen av dette grensesnittet på protokollnivå kan variere, avhengig av hvilken teknologi det andre føderasjonen benytter. Verken brukere, vertsorganisasjoner eller tjenesteleverandører er påvirket av løsningene valgt for dette grensesnittet. Aktuelle alternativer omfatter:

- krysskobling i henhold til Liberty Alliance-standarder [liberty]
- web-redirigering etter mønster av kommunikasjonen mellom tjenesteleverandør og Feide
- LDAP-oppslag etter mønster av kommunikasjon mellom Feide og vertsorganisasjon
- andre, eventuelt proprietære, autentiseringsprotokoller, for eksempel Shibboleth [shibboleth]

5.4 Mellom innloggingstjenesten og vertsorganisasjonene

Grensesnittet benytter LDAP:

- Innloggingstjenesten formidler brukernavn og passord til vertsorganisasjonen, og får i retur svar på om passordet er korrekt oppgitt for denne brukeren.
- Innloggingstjenesten får utlevert attributter for autentisert bruker.
- Feides arkitektur er utformet for å være uavhengig av autentiseringsmetode, men i dagens utgave brukes alltid brukernavn/passord overført over en kryptert kommunikasjonskanal.

5.5 Mellom brukere og tjenester

Kommunikasjonen mellom brukere og tjenester går direkte mellom partene uten at Feide på noen måte er koblet inn.

Feide-autentisering er derimot en essensiell del av etablering av dialogen. Fordi mekanismene for autentisering er basert på web-protokoller, benytter også dialogen mellom bruker og tjeneste web-protokoller. Tjenesten kan i tillegg ta i bruk andre protokoller i dialog med brukeren, men dette ligger utenfor Feide.

En bruker kobler seg opp mot en tjeneste, ikke direkte mot Feide. Tjenester som ikke er allment tilgjengelig vil kreve innlogging eller autentisering av brukeren før det blir gitt tilgang.

Tjenesten kan tilby brukeren et valg mellom flere innloggingsalternativer som

- lokal innlogging uavhengig av Feide
- Feide-innlogging
- autentisering ved andre autentiseringstjenester via Feide (kryssføderering)
- andre eksterne autentiseringstjenester uavhengig av Feide

Hvis brukeren blir gitt et valg, er det ønskelig at Feide-innlogging vises med Feides logo på tjenestens innloggingsside. Velger brukeren Feide-innlogging eller autentisering ved kryssføderering gjennom Feide, settes autentiseringen over til Feides innloggingstjeneste.

Hvis brukeren allerede er Feide-innlogget, blir autentiseringen basert på den eksisterende Feide-sesjonen i stedet for å kreve ny innlogging fra brukerens side. Det er dette som kalles *single sign on* (SSO). En tjeneste kan, av sikkerhetshensyn, velge å alltid kreve ny innlogging, selv om brukeren allerede har en aktiv Feide-økt.

Når brukeren ønsker å logge ut av en tjeneste, får brukeren spørsmål om han/hun ønsker å logge ut av Feide (single log out) eller bare ut av tjenesten:

- *Single log out* (SLO) betyr avslutning av Feide-sesjonen og utlogging av alle tjenester brukeren har logget på gjennom Feide. Hvis en tjeneste etter dette ber om autentisering, må brukeren foreta en ny Feide-innlogging.
- Dersom brukeren bare logger ut av den ene tjenesten, har brukeren fortsatt en aktiv Feide-sesjon og kan fortsette å bruke andre tjenester som før. Dersom brukeren ønsker å logge inn på en ny tjeneste, vil han/hun komme rett inn så lenge tjenesten aksepterer *single sign-on*.

6 Vertsorganisasjoner

En vertsorganisasjon administrerer en gruppe brukere og gir ut brukernavn, passord og attributter for alle brukere som tilhører vertsorganisasjonen. Feide lagrer ikke brukernavn, passord eller attributter, men forutsetter at vertsorganisasjonen tar hånd om dette.

I kontrakten med Feide forplikter vertsorganisasjonen seg til å oppfylle et antall krav slik at Feide kan være i stand til å utføre autentiseringen. Det forutsettes at data om brukere lagres sikkert, og tilbys Feide på et standard format.

LDAP-katalogene til vertsorganisasjonene kan samlet betraktes som en distribuert database, med Feide som et sentralt kontaktpunkt. Det er flere prinsipielle grunner for at dette er valgt framfor en sentralisert database med all brukerinformasjon kontrollert av Feide:

- Sentralisert datalagring medfører økt sikkerhetsrisiko, og medfører ofte større kostnader til lagring og vedlikehold.
- Endringer i en sentralisert database involverer et større apparat. Ofte etableres prosedyrer der oppdatering gjøres sjeldnere, og informasjonen kan derfor være mindre oppdatert og pålitelig.
- Tjenesteleverandører slipper å forholde seg direkte til hver enkelt vertsorganisasjon og å håndtere akkreditiver (som f.eks. passord). Dette ivaretas gjennom sentralisert innlogging.
- Når tjenester tilbys informasjon (attributter) om brukere er korrekt bruk avhengig av en klart definert semantikk for disse dataene. Dette ivaretas gjennom Feides LDAP-skjema, som spesifiserer innhold, syntaks og semantikk for attributtene, om de er obligatoriske, og om det kan finnes flere verdier av samme attributt for en gitt bruker.

Fordi autentisering direkte avhenger av informasjon fra vertsorganisasjonene, er det viktig at opplysningene er så oppdatert som mulig. Det vil si at alle endringer, tillegg og slettinger i kildesystemene må reflekteres i data som gjøres tilgjengelig for Feide, og som eventuelt videreformidles av Feide.

Følgende krav stilles til en vertsorganisasjon	
Kildesystem	• Rutiner for håndtering av hvert autoritative kildesystem må, om nødvendig, tilpasses slik at det bevares og leveres data av best mulig kvalitet. Dette er en kontinuerlig pågående prosess. • Underlagsdata for LDAP-katalogen må være på elektronisk form. Det vanlige er at kildene for personinformasjon er skoleadministrative systemer, lønningsregistre og regnskapssystemer. Slike systemer kalles kildesystemer. • Organisasjonen definerer ett kildesystem som autoritativt for hvert personattributt: For hvert attributt, f.eks. "navn" eller "telefonnummer" finnes én definert autoritet. Alle andre steder der samme attributtverdi benyttes betraktes som kopier. Oppstår det tvil om korrekt verdi for et attributt, er verdien fra den autoritative kilden bestemmende. I organisasjoner med ulike

	grupper brukere, f.eks. studenter og ansatte, kan autoritativ kilde være ulik for hver gruppe, men for en gitt person skal autoritativ kilde være entydig bestemt.
Brukeradministrativt system (BAS)	• Det må benyttes et system for identitetsforvaltning, et brukeradministrativt system (BAS). • BAS håndterer data fra alle autoritative kildesystemer. Rutiner for håndtering av hvert kildesystem må, om nødvendig, tilpasses slik at det bevares og leveres data av best mulig kvalitet.
LDAP	• Organisasjonen må tilby en LDAP-katalog for Feides innloggingstjeneste. • LDAP-katalogen må levere informasjon i samsvar med Feides formkrav og norEdu*-spesifikasjonen[norEdu, formkrav_go og formkrav_uh]. • LDAP-katalogen har i sitt katalogtre definerte inngangspunkter som er kjent av Feides innloggingstjeneste. • Det må være etablert kanaler slik at data automatisk og feilfritt kan flyte fra kildesystemene til LDAP-katalogens grensesnitt mot Feides innloggingstjeneste. Dette inkluderer en avbilding av kildesystemets semantikk på semantikken i Feides LDAP-skjema. De automatiske prosedyrene skal holde informasjonen tilgjengelig for Feide så oppdatert som mulig i forhold til kildesystemet.
Roller	• De roller og former for tilknytning som brukere kan ha til organisasjonen må være klart definerte. Organisasjonen må sikre at interne prosedyrer tildeler og bruker roller/tilknytning konsistent. • Alle Feide-brukere har en eller flere tilknytninger til sin vertsorganisasjon, valgt fra et lite, men fleksibelt sett. En av tilknytningene skal være identifisert som den primære. Eksempler på slike tilknytninger er "student" og "ansatt".

Følgende steg må gjennomføres for å bli godkjent vertsorganisasjon i Feide	
1	Installere et BAS og en LDAP-katalog som kan levere informasjon om brukere til Feide i henhold til de kravene som stilles av Feide.
2	Gjøre nødvendig opprensking i data i kildesystemene, f.eks. fjerne utgåtte poster og dupliserte innslag, og kontrollere at viktige datafelter har konsistent semantikk.
3	Verifisere at prosedyrer for håndtering av persondata sikrer konstant høy datakvalitet.
4	Sørge for at brukere får passord generert i henhold til gitte kriterier for sikre passord. Verifisere at alle brukernavn er unike, og at de følger navneregler som vil være uforandret

	over en viss tid.
5	Verifisere at både autoritative data om hver bruker, som navn og adresse, og genererte data, som lokale brukernavn og krypterte passord, er tilgjengelig i LDAP-katalogen.
6	Sende en søknad til Feide om å få bli en vertsorganisasjon, med dokumentasjon på at punktene ovenfor er oppfylt.
7	Inngå kontrakt med Feide. Hvis organisasjonen planlegger å også tilby Feide-tjenester, reguleres dette av samme kontrakt.
8	Gi Feides innloggingstjeneste adgang til organisasjonens LDAP-katalog.

7 Brukere

Feide stiller bare indirekte krav til brukere; Feide og brukerens vertsorganisasjon har opprettet en avtale, og brukerens forpliktelser retter seg mot vertsorganisasjonen.

Feides arkitektur og design er utformet for å beskytte persondata fra misbruk og for å gi brukere innsynsrett i deres egne data, rett til å bli informert om hvilke attributter Feide-tjenester kan motta, og rett til å godkjenne utlevering av attributter.

Vertsorganisasjonen definerer og håndhever retningslinjer for bruk av datasystemene. Feide krever at organisasjonen har retningslinjer for identitetsforvaltning.

Retningslinjene bør blant annet angi:

- hvem som skal tildeles (elektroniske) identiteter i organisasjonens IT-infrastruktur (f.eks. elever, lærere, andre ansatte, andre personer som er tilknyttet)
- hvordan identiteten skal opprettes
- hvordan identiteten skal vedlikeholdes
- hva identiteten skal brukes til
- når identiteten skal termineres

Feide-navn kan og vil bli brukt utenfor vertsorganisasjonen. Feide krever at vertsorganisasjoner holder sine brukere ansvarlig for å respektere retningslinjer for akseptabel bruk av IKT-utstyr. Retningslinjene defineres av organisasjonen selv, men Feide kan bistå ved etablering eller oppdatering av disse.

Senter for IKT i utdanningen tilbyr en standard mal for slike retningslinjer i undervisningssektoren [IKT-regl].

Det er vertsorganisasjonens ansvar å identifisere, med en rimelig grad av sikkerhet, de personer som skal opptre som brukere knyttet til organisasjonen. Dersom en person gir uriktige opplysninger til organisasjonen, f.eks. ved bruk av falske identifikasjonspapirer, er dette en sak mellom vertsorganisasjon og bruker; ansvaret for å hindre at slikt skjer ligger hos organisasjonen.

Feide antar ubetinget at informasjon i LDAP-katalogen er korrekt og gyldig, i henhold til de avtaler og kontrakter som regulerer Feides bruk av LDAP-katalogen.

8 Feide-tjenester

En tjeneste er et tilbud om å utføre en avgrenset oppgave for en bruker, f.eks. utføre søk i en database, produsere en utskrift, overføre en epost eller presentere informasjons- og læremateriell.

Feide-tjenester kan være lokale, tilgjengelig kun for brukere i samme organisasjon som tjeneste- leverandøren (f.eks. et universitet som tilbyr tjenester til egne studenter), eller tjenester som kan gjøres tilgjengelig også for Feide-autentiserte brukere i andre organisasjoner.

Tjenesteleverandøren kan stille krav til de som vil benytte tjenesten, f.eks. at det er etablert et kundeforhold. Dette gjelder særlig for kommersielle tjenester. Tjenesten må selv håndheve slike begrensinger.

8.1 Etablering av en Feide-tjeneste

En tjeneste som får utført autentisering av brukere gjennom Feide er en Feide-tjeneste. For å bli en Feide-tjeneste må tjenesteleverandøren, eieren av tjenesten, godkjennes av Feide. Dette starter med en søknad til Feide, og fører fram til en kontrakt for en tjeneste som kommuniserer med Feides innloggingstjeneste for autentisering og tilgang til attributter. Kontrakten regulerer forpliktelsene mellom Feide og tjenesteleverandøren, og regulerer følgende forhold:

- hvilke attributter tjenesten får tilgang til for autentiserte brukere
- kontaktpersoner for tekniske og administrative forhold, samt en liste over personer som har myndighet til å forhandle endringer i avtalen mellom tjenesteleverandøren og Feide, samt forhandle endringer i Feides konfigurasjonsdata for tjenesten
- prosedyrer for rapportering av endring i tjenester eller nye fellestjenester
- krav til behandling av personopplysninger

8.2 Protokoller

Feide-tjenester tilbys brukere gjennom et web-grensesnitt. Kommunikasjonen går direkte mellom tjeneste og bruker; kun under autentiseringen redirigeres brukeren til Feides innloggingstjeneste.

Under autentiseringen kommuniserer tjenestene med Feide gjennom SAML 2.0-protokollen [saml]. Kravene til dette grensesnittet er definert i Feide Integration Guide [intguide] og Feide Technical Guide [techguide]. Tjenesteleverandøren kan benytte vilkårlig programvare som fyller disse kravene.

9 Innlogging

En stegvis beskrivelse av en typisk Feide-innlogging er beskrevet i kapittel 2.3. I dette kapittelet gir vi en mer detaljert beskrivelse av hendelsesforløpet når en bruker logger seg på en tjeneste gjennom Feide.

Kortfattet beskrivelse av innloggingsprosessen:

- Når en bruker sender en forespørsel til en tjeneste koblet til Feide, og brukeren har en aktiv og gyldig tjenestesesjon, blir ikke Feide kontaktet; forespørselen behandles uten ytterligere autentisering.
- Hvis brukeren ikke har en aktiv og gyldig tjenestesesjon, holder tjenesten midlertidig tilbake responsen, og setter brukeren over til Feides innloggingstjeneste for autentisering.
- Hvis brukeren allerede er innlogget gjennom Feide, får tjenesten i retur en bekreftelse på autentiseringen, samt aktuelle attributter for brukeren, uten at det er åpnet noen brukerdialog. Tjenesten behandler deretter forespørselen fra brukeren.
- Hvis brukeren ikke er innlogget gjennom Feide, men har valgt autentisering gjennom en ekstern autentiseringstjeneste (kryssføderering), setter Feides innloggingstjeneste brukeren videre over til den andre autentiseringstjenesten, som (hvis ikke brukeren allerede er autentisert) åpner en brukerdialog. Feide mottar bekreftelse på autentiseringen, og videreformidler denne til tjenesten, som så kan behandle brukerens forespørsel.
- Hvis brukeren ikke er innlogget gjennom Feide, og har valgt Feide-autentisering, åpner Feides innloggingstjeneste en brukerdialog for innlogging. Innloggingstjenesten formidler brukernavn og passord fra brukeren til vertsorganisasjonens LDAP-katalog. Når passordet er bekreftet korrekt, henter innloggingstjenesten brukerens attributter fra vertsorganisasjonens LDAP-katalog. Deretter sender innloggingstjenesten til Feide-tjenesten bekreftelse på autentisering, samt de attributter tjenesten har avtale om å få tilgang til. Tjenesten behandler deretter brukerens forespørsel.
- Tjenesten kan be Feide om å åpne en autentiseringsdialog med brukeren selv om brukeren allerede har en aktiv og gyldig Feide-sesjon. Dette benyttes av tjenester som krever et høyere sikkerhetsnivå for å forhindre at en Feide-innlogget arbeidsstasjon som er midlertidig forlatt misbrukes av uvedkommende.

10 Referanser

[eduPerson] eduPerson Object Class Specification (200806)
http://middleware.internet2.edu/eduperson/

[formkrav_go] Feide formkrav til grunnopplæringa – Bruk av norEdu* Object Class Specification v.1.5 for grunnopplæringa:
http://www.feide.no/sites/feide.no/files/documents/go_attributter.pdf

[formkrav_uh] Feide formkrav til høgere utdanning – Bruk av norEdu* Object Class Specification v.1.5 for høgere utdanning:
http://www.feide.no/sites/feide.no/files/documents/uh_attributter.pdf

[IKT-regl] Senter for IKT i utdanningen: IKT-reglement for grunnopplæringen:
http://www.uninettabc.no/content.ap?thisId=11465

[intguide] Feide Integration Guide
http://www.feide.no/sites/feide.no/files/documents/Feide_integration_guide.pdf

[liberty] Liberty Alliance homepage:
http://www.projectliberty.org/

[norEdu] norEdu* Object Class Specification, version 1.5:
http://www.feide.no/sites/feide.no/files/documents/norEdu_spec.pdf

[popl] Lov om behandling av personopplysninger (personopplysningsloven):
http://www.lovdata.no/all/nl-20000414-031.html

[saml] SAML Specifications, OASIS Security Services Technical Community:
http://saml.xml.org/saml-specifications

[shibboleth] Shibboleth homepage:
http://shibboleth.internet2.edu/

[techguide] Feide Technical Guide
http://www.feide.no/sites/feide.no/files/documents/Feide_technical_guide.pdf

11 Ordliste

attributt

En egenskap som kan assossieres med et objekt, f.eks. etternavnet til en person. Attributtet er identifisert ved et attributtnavn, og har en attributtverdi for hvert objekt. Et attributt kan være obligatorisk eller valgfri for en gitt klasse objekter, f.eks. er etternavn obligatorisk for en person, mens mellomnavn er valgfritt. Det kan være tillatt med flere verdier av et attributt for samme objekt, f.eks. kan en person ha flere fornavn. Attributtverdien kan være sammensatt, f.eks. kan en adresse bestå av gatenavn, husnummer, postnummer og sted. Attributtnavn, tillatte verdier, om verdien kan repeteres osv. spesifiseres i et skjema.

autentisering

Å bekrefte at en person er den vedkommende utgir seg for å være. En vanlig metode er kontroll av brukernavn med tilhørende passord, som i Feide. Andre metoder kan være basert på f.eks. engangspassord, digitale sertifikater eller fingeravtrykklesere.

autorisasjon

Den adgang en bruker har til informasjon eller tjenester hos en tjenestetilbyder. "Å autorisere" brukes både om å tildele en bruker adgang, og om å identifisere en brukers adgangsrettigheter. Autorisering forutsetter normalt at brukeren er autentisert. Feide tilbyr autentisering, men overlater til tjenestene å gjøre autorisering basert på denne autentiseringen.

Feide

Forkortelse for: Felles Elektronisk IDEntitet, Federated Electronic IDEntity. Utdanningssektorens system for identitetsforvaltning og single sign on.

Feide-navn

Identifikasjon av en Feide-bruker. Består av to deler, et lokalt brukernavn og (en av) vertsorganisasjonens navn (<brukernavn>@<vert>). Navnet er tildelt av vertsorganisasjonen, og skal være unikt. Feide-navn gjenbrukes ikke. Feide-navnet er internt knyttet til et fødselsnummer, og derfor alltid knyttet til én enkelt person. En person kan i prinsipp ha flere Feide-navn, f.eks. ved skifte av utdanningsinstitusjon, men Feide har ingen bevissthet om at ulike navn representerer samme person.

single sign on (SSO)

En innlogging som lar en bruker få benytte flere uavhengige tjenester, som alle krever autentisering, uten å behøve å gå gjennom en eksplisitt autentiseringsprosedyre for hver tjeneste så lenge en tiltrodd autentiseringstjeneste som Feide eller tilsvarende kan verifisere brukerens autentisitet.

føderasjon

En samling av vertsorganisasjoner og tjenesteleverandører som har felles retningslinjer og avtaleverk rundt identitetsforvaltning.

identitetstjeneste (engelsk term: identity provider)

Feides tjeneste for å levere informasjon om vilkårlig Feide-bruker til en tjenesteleverandør. Dette kan avlaste tjenesten for å selv administrere informasjon knyttet til den enkelte bruker. Feide realiserer identitetstjensten ved å innhente data fra en LDAP-katalog til vertsorganisasjon brukeren

tilhører. Feide har egen kontrakt med hver enkelt tjeneste om hvilke attributter tjenesten skal få tilgang til. Denne informasjonen utleveres fra Moria ved vellykket innlogging (autentisering).

innlogging

En interaktiv prosedyre der en bruker autentiserer seg ved å oppgi et brukernavn og et passord.

kryssføderering (Engelsk term: cross federation, confederation)

Sammenkobling av Feide med annen autentiseringstjeneste. Tilbyr Feide-brukere tilgang til tjenester fra andre føderasjoner eller tilbyr brukere fra andre føderasjoner tilgang til fellestjenester.

LDAP-katalog

Katalogsystem for registrering av og tilgang til vilkårlig informasjon om personer, institusjoner, fysiske objekter osv. Kan også brukes f.eks. for lagring av brukerens passord. Data i en LDAP-katalog er beskrevet i et skjema som definerer hvilken informasjon som blir lagret i katalogen. LDAP er protokollen som brukes for å registrere eller hente informasjon i katalogen.

norEdu*-spesifikasjonen

Feides LDAP-skjema for informasjon om personer og organisasjoner i utdanningssektoren. norEdu*-spesifikasjonen er basert på eduOrg/eduPerson utviklet i regi av internasjonale aktører som Internet 2 og EDUCAUSE. norEdu er utviklet i nordisk regi, under ledelse av Feide.

SAML

Forkortelse for: Security Assertion Markup Language. En standard utviklet av OASIS for utveksling av informasjon som angår brukerens identitet og andre attributter mellom en autentiseringstjener og en tjenesteleverandør. SAML 2.0 benyttes i Feide.

tiltrodd tredjepart

En uavhengig instans som gir pålitelig informasjon til to parter om motparten, f.eks. om motpartens identitet, og som begge parter har tillit til. Begge kan da være sikker på at mottatt informasjon faktisk kommer fra den de tror de kommuniserer med - spesielt viktig når informasjon utveksles mellom to parter som ikke kjenner hverandre. Uttrykket brukes også i andre sammenhenger, som f.eks. en pålitelig tjeneste for opplysning om en brukers offentlige nøkkel i PKI.

tjenesteleverandør (engelsk term: service provider)

En organisasjon som yter tjenester til personer i utdanningssektoren, og benytter Feide for autentisering. En tjenesteleverandør må ha en avtale med Feide, og er derfor en Feide-organisasjon (som også kan opptre som vertsorganisasjon for Feide-brukere).

vertsorganisasjon

Utdanningsorganisasjon som har tatt i bruk Feide og tildelt Feide-navn til sine elever, studenter, ansatte og andre tilknyttede personer. En gitt institusjon kan opptre både som vertsorgansisasjon og som tjenesteleverandør; f.eks. kan et universitet både være vertsorganisasjon for sine studenter, og samtidig tilby elektroniske læringsressurser til studentene. I Feide behandles disse to funksjonene uavhengig av hverandre, også når samme institusjon tilbyr begge funksjoner.