

Saksdokument

Porteføljestyre for data og infrastruktur

Til	Porteføljestyre for data og infrastruktur
Dato	09.11.2023
Saksnummer	14/23
Sakstype	O/D-sak
Saksansvarlig	Hildegunn Vada
Saksbehandler	Hildegunn Vada

Feide produktstrategi og framtidsscenarier

Som for alle produktområder i Sikt skal det utarbeides en produktstrategi for Feide. I denne saken presenterer vi produktområdet Feide, ulike problemstillinger eller strategiske valg som har utfordret oss i prosessen med å utarbeide en produktstrategi, samt framtidsscenario-modellen som vi har brukt som hjelpemiddel i prosessen. Til slutt presenterer vi tre ulike framtidsscenarier vi har utviklet for Feide. Det er ønskelig med porteføljestyret sine innspill på hvilken verdi Feide skal skape for sektoren og hvilken posisjon/rolle Feide bør ta i de ulike scenariene.

Produktområdet Feide

Produktområdet Feide inneholder tre produkter:

- Feide
- IntArk
- Feide-hotell

Feide

Av disse tre er Feide det største produktet med 700 kunder og 2000 tilknyttede tjenester. Feide etablerte seg rundt år 2000 som UH-sektorens felles innloggingstjeneste – der man med ett brukernavn og passord kunne få tilgang til flere digitale tjenester. Fra ca år 2010 ble Feide også tatt i bruk av grunn- og videregående skoler – og man har i ettertid sett at utbredelsen av Feide ble viktig for digitaliseringen av grunnopplæringen.

Det mest utbredte har vært Feide-innlogging med brukernavn og passord, men det har de siste 10 årene vært et tilbud om sterk autentisering i Feide. En sterk Feide-autentisering har hatt krav om både 2-faktor og at Feide-identiteten har vært utstedt til legitimerede brukere.

Feide sender over et gitt sett med brukerdata om den innloggede brukeren i forbindelse med at brukeren logger inn på en tjeneste. Dette er data som navn, tilknytning til universitet/skole, rolle etc. Hvilke data som sendes over, avtales med den enkelte tjeneste, og skal være regulert i databehandleravtalen mellom tjenesteleverandøren og universitet/skoleeieren.

Fra år 2015 økte etterspørselen etter andre typer data enn det som var registrert i organisasjonenes Feide-kataloger og regulert i Feides informasjonsmodell, og Feide ble utvidet med det som da het Dataporten. Her kunne «hva som helst» av data utveksles mellom datakilde og tjeneste uten at Sikt (tidl. Uninett) var involvert i standardisering av disse dataene. Den viktige funksjonaliteten som Feide (Dataporten) bidro med, var tilgangsstyring –at kun de tjenester som skulle ha tilgang, fikk tilgang til datakilden. For å oppnå dataminimering, var det også et viktig poeng at datautleveringen mellom tjeneste og datakilde var koblet til en innlogget bruker. Med andre ord: at tjenesten kun fikk tilgang til



data om den innloggede brukeren. Eksempel på data som ble utvekslet på denne måten var hvorvidt brukeren hadde betalt semesteravgift eller ikke.

Den nye funksjonaliteten for datautveksling (Dataporten) ble tatt stadig mer i bruk, og fra 2020 fikk vi ny finansiering fra Utdanningsdirektoratet (Udir) for å slå sammen Dataporten med Feide, og til å videreutvikle Feide til å kunne utveksle data mellom tjeneste og datakilde uten en innlogget bruker (såkalt maskin-til-maskin). Det ble også besluttet – i samråd med Udir – å videreutvikle administrasjonsgrensesnittet (Feides kundeportal), for å få på plass bedre støtte for prosessen med å ta i bruk nye digitale tjenester, som f.eks. å inngå databehandleravtale, tilgjengelighetserklæring og støtte til risikovurderinger. Dette er pågående arbeid.

I 2023 utgjør brukerfinansiering 50% av inntektene til Feide. Av dette er om lag 25% fra høyere utdanning og forskning og 75% fra grunnopplæringa (hovedsakelig kommuner og fylkeskommuner). De resterende 50% av Feides inntekter kommer fra Udir.

Hovedleveranser fra Feide i 2023 er:

- Innlogging, med overføring av et standardisert sett med brukerdata
- Tilgangsstyring til datakilder (API-er), både med og uten kontekst av innlogget bruker
- Administrasjonsportal hvor man kan administrere tilgang til tjenester og datakilder og prosessene rundt å ta i bruk tjenester.

IntArk

IntArk er en tjeneste som ble utviklet av UiO og tatt i bruk av BOTT og enkelte andre institusjoner før 2021. Tjenesten ble høsten 2021 vedtatt som fellestjeneste for UH-21 av Digitaliseringsstyret. Vedtaket slo også fast at Sikt skulle ta over som leverandør av tjenesten fra januar 2022 med UiO som underleverandør. Det var et samarbeid mellom den tidl. Unit, Uninett og UiO som førte frem til dette vedtaket. Det er per i dag 14 UH-institusjoner som aktivt bruker IntArk. Denne tjenesten tilbys ikke til grunnopplæringa foreløpig.

IntArk består av tre hovedkomponenter:

- **Styringsregler:** Beste praksis og arkitekturprinsipper for hvordan UH-sektoren bør dele data mellom datakilder og tjenester.
- En **meldingskø** som varsler tjenester om at data i en datakilde er endret, slik at tjenesten kan hente dataene på nytt. Dette er spesielt nyttig for tjenester som trenger å få data i forkant av at brukeren logger inn, og som har nytte av å bli raskt oppdatert med nye data. For eksempel når brukerne forventer at data er oppdaterte tilnærmet umiddelbart, og ikke dagen etterpå.
- En **API gateway** som står foran datakildene (API-ene) og kontrollerer at kun de tjenester som har riktige "nøkler" får tilgang til datakilden (API-et). I tillegg tilbys en del administrativ støtte for drift av API-et, som logging av trafikk til og fra, statistikk over bruk, mulighet for å sette opp ratebegrensning etc.

Feide-hotell

Feide-hotell er en skytjeneste som leverer en hostet Feide-katalog. Feide-katalogen er den lokale brukerkatalogen som hver organisasjon (universitet, skoleeier etc) må ha for å være tilkoblet Feide og la sine brukere logge inn på Feide. Det er her de standardiserte brukerdataene som kan utleveres til tjenester i forbindelse med en Feide-pålogging, ligger lagret.

Produktstrategi – utfordringer

Vi har et tydelig bilde av hvilken verdi produktområdet leverer i dag:

- Trygg tilgang: Alle i kunnskapssektoren har enkel og trygg tilgang til digitale tjenester.
- Tilgang til data gir bedre tjenester: Leverandører kan lage bedre og mer skreddersydde tjenester når de får enklere tilgang til relevante brukerdata. Dette gir bedre læring, undervisning og forskning.
- Forenkling og oversikt: Virksomheter i kunnskapssektoren kan enkelt holde oversikt over hvilke digitale tjenester de benytter og hvilke data tjenestene mottar.
- Kompetent leverandør: Feide leverer på behovene i kunnskapssektoren, er en robust tjeneste som er enkel å bruke, og henger godt sammen med øvrige nasjonale felleskomponenter.



Men hvilken verdi trenger sektoren at Feide leverer i tiden som kommer? Da vi skulle utarbeide en produktstrategi for produktområdet, havnet vi raskt inn i noen utfordrende diskusjoner/problemstillinger, som for eksempel:

- Vi har allerede begynt å delegere autentiseringen til eksterne parter som organisasjonenes egne skyløsninger (eks Azure AD/Entra ID), Helse-ID, TSD-innlogging og ID-porten – skal vi fortsette videre langs dette sporet? Flere personer har eID i alle disse løsningene - hvor god er brukeropplevelsen for disse?
- Vi er opptatt av at Feide tilbyr sterk autentisering og ikke “bare” 2-faktorinnlogging og forholder oss strengt til EU-rammeverk for autentisering. Er dette viktig for våre kunder? Blir det mer eller mindre viktig fremover?
- Skal Feide forbedre sin egen innloggingsløsning og jobbe i retning av sikrere innlogging enn brukernavn og passord, f.eks. passordløse løsninger?
- Hvilke eID-løsninger vil komme på plass på nasjonalt nivå (fra Digdir/ID-porten)? Vi kjenner den nye eID-strategien, men hvor raskt vil det utvikle seg og hvordan vil omverden respondere? Hvilke behov i kunnskapssektoren vil disse løsningene dekke?
- Hva med utenlandske brukere, i Norge, i EU? Hvordan vil eIDAS 2.0 / Digital lommebok påvirke Feide?
- Hva med utenlandske brukere som befinner seg utenfor EU, men som norsk kunnskapssektor trenger å samarbeide med? Hvor trygge trenger sektoren å være på hvem man samarbeider med, og hvem man slipper inn i sine systemer?
- Hvordan skal Feide bidra inn i å etablere autentisering med høyere sikkerhetsnivå for barn fra 12 år og oppover? Hva med barn under 12 år?
- Hvordan vil sektorens bruk av store skytjenester som M365 og Google utvikle seg og hvordan påvirker det oss? Hvordan kan vi balansere organisasjonenes ønske om sikre og brukervennlige løsninger for sin organisasjon, med enkeltpersoners behov for livslang læring og studentmobilitet på tvers av etablerte organisasjonsgrenser?
- Skal vi standardisere mer data på samme måte som vi har gjort og hatt suksess med i Feides informasjonsmodell?
- Skal vi kun tilby de tekniske løsningene for å tilgangsstyre tilgang til data, eller skal vi aktivt gå inn og rådggi organisasjoner og tjenesteleverandører?
- Skal vi dytte enda mer på for å få tjenester og datakilder til å ta i bruk brukerstyrt datadeling?

Alle disse spørsmålene er vanskelig å svare på i dag, fordi vi vet ikke hvordan omverdenen vår utvikler seg langs disse ulike aksene.

Vi trenger å forstå mer om fremtiden og våre kunders behov i fremtiden for å utvikle en oppdatert og robust produktstrategi for Feide.

Framtidsscenario-modellen

Det kan kjennes utfordrende å satse fullt og helt langs en akse når vi ikke har en klar oppfatning av hvordan omverdenen og våre kunder og samarbeidspartnere vil utvikle seg. Vi har derfor tatt i bruk en metode vi kaller framtidsscenario-modellen og som innebærer å se på **hvilke eksterne endringer som vil påvirke oss i tiden fremover**. Med bakgrunn i kartlagte eksterne drivere og trender, utvikler man ett eller flere framtidsscenarier som sier noe om vår omverden i fremtiden. For et gitt scenario prøver vi å svare på:

1. Hvilken verdi skal Feide skape for våre brukere i fremtiden?
2. Hva er forretningsverdien for Feide i fremtiden?
3. Hvordan må vi jobbe og rigge oss for fremtiden?

Etter dette ser vi nærmere på hvordan vi må endre oss for å kunne levere ønsket verdi. «Hvis vi skal levere denne verdien om 4 år, hvor må vi være om 3 år? Om 2 år? Om 1 år? Og hvilke endringer må vi gjøre allerede i morgen?»

Denne øvelsen ønsker vi å gjøre for flere ulike framtidsscenarier, og vi kan da oppnå to mål:

- Å gjøre retningsvalg og sette i verk tiltak som vil være riktige i flere ulike scenarier. Dette vil gi en mer robust produktstrategi fordi det vi velger å gjøre vil skape verdi i flere scenarier.
- Om verden viser seg å utvikle seg en annen retning enn det vi trodde, kan vi raskere endre oss fordi vi har jobbet med ulike scenarier.



Framtidsscenarier utviklet for Feide

Vi har valgt å utvikle tre framtidsscenarier for produktområdet Feide, som vi har gitt følgende titler:

- Fremragende offentlig medborger
- Dominerende globale storaktører
- Sentrale suksesser

Fremragende offentlig medborger

- Vi har en velfungerende offentlig infrastruktur for autentisering som dekker flere brukergrupper enn i dag og er mer utbredt enn i dag. Barn fra 12 år og oppover har tilgang på offentlig autentisering på middels/høyt sikkerhetsnivå. Løsningen dekker de aller fleste utenlandske personer i Norge og EU-borgere, og det er standardiserte prosesser og rutiner for utlevering av eID til alle disse målgruppene.
- Ansatt-porten benyttes til innlogging for ansatte på universitetene og i kommunene.
- Digital suverenitet: Økt trusselnivå i verden fører til høyt sikkerhetsfokus i Norge og i kunnskapssektoren, og økt fokus på sikring av data og personvern.
- Det er lagt til rette for studentmobilitet og livslang læring gjennom at vi tar vare på studenters digitale identitet gjennom hele deres læringslivsløp, uavhengig av deres tilknytning til enkeltorganisasjoner.
- Leverandører av både tjenester og datakilder har begynt å realisere verdiene som ligger i bruk og gjenbruk av data. Det er godt datadriv mellom datakilder og tjenester, og det gjøres mye innovasjon basert på eksisterende data.

Dominerende globale storaktører

- Økonomiske nedgangstider preger norsk offentlig sektor, også på digitaliseringsfeltet. Dette fører til at det nasjonale eID-tilbudet er omtrent på dagens nivå og ikke utvidet til å dekke flere brukergrupper.
- Vi ser stor bruk av de dominerende globale skytjenestene og økosystemene rundt disse. Skytjenestene retter seg først og fremst rettet mot enkeltorganisasjoner. Flere organisasjoner bruker disse etablerte skytjenestene til flere formål enn i dag (eks LMS).
- Skytjenestenes gode AI-tilbud styrker posisjonen til disse tjenestene. Det viser seg at sky muliggjør AI-skapt verdi, og alt blir mer AI-drevet med skytjenester.
- Vi er ikke kommet nærmere å realisere visjonen om studentmobilitet og livslang læring.
- Det er et lite attraktivt edTech-marked: Krav om effektivisering gjør at globale skytjenester som Microsoft og Google stadig blir viktigere for norske kommuner og UH-institusjoner, og edTech-markedet for øvrig er lite.

Sentrale suksesser

- Vi har en velfungerende offentlig infrastruktur for autentisering som dekker flere brukergrupper enn i dag og er mer utbredt enn i dag. Barn fra 12 år og oppover har tilgang på offentlig autentisering på middels/høyt sikkerhetsnivå. Løsningen dekker de aller fleste utenlandske personer i Norge og EU-borgere, og det er standardiserte prosesser og rutiner for utlevering av eID til alle disse målgruppene.
- Vi ser stor bruk av de dominerende globale skytjenestene og økosystemene rundt disse. Skytjenestene retter seg først og fremst rettet mot enkeltorganisasjoner og ikke samarbeid på tvers av organisasjoner. Mange organisasjoner bruker disse etablerte skytjenestene til flere formål enn i dag (eks LMS).
- Det offentlige ønske om og tilrettelegging for "en innbygger, en eID" står i motsetning til de globale aktørenes strategi om innlåsing.
- Ansatt-porten benyttes ikke til innlogging for ansatte på universitetene og i kommunene.
- Skytjenestenes gode AI-tilbud styrker posisjonen til disse tjenestene. Det viser seg at sky muliggjør AI-skapt verdi, og alt blir mer AI-drevet med skytjenester.
- Det er lagt til rette for studentmobilitet og livslang læring gjennom at vi tar vare på studenters digitale identitet gjennom hele deres læringslivsløp, uavhengig av deres tilknytning til enkeltorganisasjoner.
- Leverandører av tjenester kobler seg direkte til organisasjonens skytjenester, og har begynt å realisere noe av verdien som ligger i gjenbruk av organisasjonens data. Det er godt datadriv mellom organisasjonens skytjeneste og tredjepartsaktører.