NTNU
Det skapende universitet

En systemanalyse av storskala identitetsforvaltning for aksesstyring

Annette Grande

Master i kommunikasjonsteknologi
Oppgaven levert: Juni 2006
Hovedveileder: Stig Frode Mjølsnes, ITEM
Medveileder(e): Ingrid Melve, Uninett

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Oppgavetekst

Foreta en analyse på systemnivå av to forslag til storskala (nasjonale) arkitekturer for brukerautorisasjon og -autentisering, FEIDE og Sikkerhetsportalen.

Utarbeid relevante kriterier og gjør en sammenlignende analyse, for eksempel med hensyn til sikkerhetsantakelser, meldingskompleksitet, robusthet mot feilsituasjoner, anvendelsesområder, standardisering, organisering, implementerings- og driftskostnader, brukervennlighet, mobilitet. Underbygg evalueringskonklusjonen med en nærmere definert eksperimentell del der dette synes naturlig.

Oppgaven gitt: 16. januar 2006
Hovedveileder: Stig Frode Mjølsnes, ITEM

Sammendrag

Internettdekningen her i landet blir stadig bedre, og mange velger å ta i bruk nettbaserte tjenester. Dette er i tråd med regjeringens ønske om å effektivisere offentlig og privat sektor ved å anvende IKT der det er mulig. Flere og flere tjenester legges på nett, og en økende mengde av disse er knyttet til brukerens identitet. Personaliserte tjenester stiller krav til en god elektronisk identitetsforvaltning, som innebærer autentisering av brukeren og autorisasjon for spesifikke ressurser. Med en god identitetsforvaltning kan den som tilbyr tjenestene være sikker på at man har med riktig person å gjøre. Noen mulige former for autentisering er brukernavn og passord, digitale sertifikater og biometri. Brukernavn og passord er en mye brukt løsning, men mange tjenester foretrekker også digitale sertifikater.

Denne rapporten ser på to systemer for storskala identitetsforvaltning, nemlig Sikkerhetsportalen og FEIDE. Begge systemene autentiserer sine brukere med utgangspunkt i brukernes elektroniske identitet, og gjør det mulig å tilby sikre tjenester på nett. Oppgaveteksten nevner en rekke aspekter systemene kan sammenlignes med hensyn til, en viktig del av denne rapporten er derfor å avgrense aspektene og å utarbeide analysekriterier i form av spørsmål som besvares for hvert av de to systemene. De aspektene som særlig vektlegges i rapporten er organisering og sikkerhetsantakelser, meldingskompleksitet og robusthet. Til sammen beskriver disse aspektene systemenes oppbygning og virkemåte, hvor systemene brukes og hvilke tjenester de tilbyr, hvordan meldingene går og hvordan disse er sikret, hva systemene gjør for å sikre robusthet mot feilsituasjoner, og mye mer. Kriteriene gir informasjon som er nødvendig for å forstå systemene, og de danner grunnlag for en evaluering og sammenligning av systemene. De mindre tekniske aspektene kostnadsfaktorer og brukervennlighet er inkludert for å gjøre analysen mest mulig komplett, men disse vies liten oppmerksomhet i diskusjonsdelen.

I forbindelse med oppgaven er en eksperimentell del utført. Sertifikater som utstedes for bruk med Sikkerhetsportalen studeres i det første av to eksperimenter, et eksperiment som er ment å skulle bidra til forståelse av sertifikatenes sentrale funksjon i Sikkerhetsportalsystemet, og til å se hvor brukervennlig Sikkerhetsportalen er for sine sluttbrukere. I et andre eksperiment foretas en integrasjon mot FEIDE, som illustrerer hvordan man kan integrere FEIDE-innlogging i egne tjenester. Eksperimentet er ment å bidra til forståelse rundt hvilke integrasjonsmuligheter som finnes, hvordan kommunikasjonen går i FEIDE og hvordan bruk av billetter gjør autentisering og attributthenting mulig på en sikker måte.

Sikkerhetsportalen tilbyr et sett av sikkerhetstjenester, og skal gjøre det lettere for det offentlige å tilby sikre elektroniske tjenester. Bruk av Sikkerhetsportalen vil være obligatorisk for alle statlige virksomheter med behov for elektronisk ID og signatur, og anbefalt også for kommunene. Sikkerhetsportalen bygger på PKI, og bruker offentlig-nøkkel sertifikater for identifisering av sine brukere. Hvert brukersted tilknyttet Sikkerhetsportalen har et grensesnitt mot en sentral sikkerhetsserver, som tar seg av all kommunikasjon mot Sikkerhetsportalen. Sluttbrukere trenger derfor kun å forholde seg til brukerstedet de ønsker å benytte en tjeneste fra, og ikke til selve Sikkerhetsportalen. Sikkerhetsportalen på sin side bruker tjenester fra ulike leverandører av PKI-tjenester, og skjuler disse leverandørene for brukerstedene. Sluttbrukere av Sikkerhetsportalen har et sertifikat, som i tillegg til å brukes for autentisering også kan brukes for signering og kryptering.

Utdanningssektoren har òg et økende behov for å kunne identifisere sine studenter og ansatte på en sikker elektronisk måte. FEIDE er et system som autentiserer brukere tilknyttet norske

utdanningsinstitusjoner via en sentral innloggingstjeneste, med en målsetning om å få organisasjonenes lokale identitetsforvaltning på en felles form. I likhet med Sikkerhetsportalen er FEIDE et desentralisert system, informasjonen om FEIDEs brukere ligger ikke i den sentrale delen av systemet, men ute hos den enkelte organisasjon. I Sikkerhetsportalen ligger informasjon om brukere derimot i brukernes egne sertifikater. Når en FEIDE-bruker ønsker å logge på en FEIDE-tjeneste sendes han til den sentrale innloggingstjenesten hvor han oppgir brukernavn og passord. Opplysningene sjekkes mot brukerens lokale organisasjon, og hvis de stemmer autentiseres brukeren. Den sentrale innloggingstjeneren utfører altså autentiseringen via brukerens lokale FEIDE-løsning, og kan på forespørsel hente ut nødvendig informasjon om brukeren.

Mens Sikkerhetsportalen er knyttet til bruk av offentlig-nøkkel sertifikater, er FEIDE uavhengig av autentiseringsløsning. For FEIDE er PKI en av flere muligheter, men i dag er det brukernavn og passord som er utbredt. Begge systemene har rutiner og mekanismer på plass som ivaretar et godt personvern, og i begge systemene er personlig og sikkerhetsrelatert informasjon sikret under sending. Systemene er designet for å være robuste og motstandsdyktige mot at utenforstående skal kunne utilgjengeliggjøre tjenesten eller skaffe seg uautorisert tilgang til informasjon eller utstyr.

Forord

Denne hovedoppgaven er utført ved NTNU våren 2006, ved institutt for telematikk.

Jeg vil gjerne takke min veileder fra UNINETT, Ingrid Melve, for god hjelp og nyttige råd underveis. Jeg vil også takke faglærer fra institutt for telematikk, Stig Frode Mjølsnes, for gode innspill.

Trondheim, juni 2006
Annette Grande

Innhold

Figurer og tabeller

Akronymer

ASCII – American Standard Code for Information Interchange
AT – Autentiseringstjener
BAS – Brukeradministrativt system
BBS – Bankenes Betalingssentral
CA – Certification Authority
CAPI – Crypto API
CRL – Certificate Revocation List
DoS – Denial of Service
FEIDE – Felles Elektronisk Identitet
HTML – Hypertext Markup Language
HTTP – Hypertext Transfer Protocol
HTTPS – Secure HTTP
ID – Identitet
ID-FF – Identity Federation Framework
ID-WSF – Identity Web Service Framework
IKT – Informasjons- og kommunikasjonsteknologi
IPSec – IP Security
JAAS – Java Authentication and Authorization Service
LDAP – Lightweight Directory Access Protocol
MD5 – Message Digest Algorithm #5
MMS – Multimedia Message, multimediemelding
NTNU – Norges Teknisk- Naturvitenskapelige Universitet
NTP – Network Time Protocol
OASIS – Organization for the Advancement of Structure Information Standards
PGP – Pretty Good Privacy
PKCS – Public Key Cryptography Standard
PKI – Public Key Infrastructure
RA – Registration Authority
RFID – Radio Frequency Identity
RSA – Offentlig-nøkkel krypteringsalgoritme, etter Rivest, Shamir og Adleman
SAML – Security Assertion Markup Language
SEID – Samarbeid om Elektronisk ID og signatur
SET – Secure Electronic Transactions
SIM – Subscriber Identity Module
S/MIME – Secure Multipurpose Internet Mail Extensions
SMS – Short Message Service, tekstmelding
SOAP – Simple Object Access Protocol
SPKI – Simple Public Key Infrastructure
SSL – Secure Sockets Layer
SSO – Single SignOn
TLS – Transport Layer Security
URL – Uniform Resource Locator
WSDL – Web Services Description Language
X.509 – En ITU-T standard for PKI
XML – eXtensible Markup Language

1 Introduksjon

Nordmenn flest har i dag god tilgang til Internett, både privat, ved skole og arbeidsplass. Norske internettbrukere har så langt vært ivrige etter å ta i bruk nye elektroniske Internettjenester som nettaviser og e-post. Banktjenester utføres nå i nettbank, varer og tjenester bestilles og betales for over nett. Digitale filer utveksles på øyeblikket, og man holder kontakt med venner og kjente ved hjelp av chatting. Mange av alle de elektroniske tjenester som finnes er upersonlige. For eksempel nettavisene, der hvem som helst kan gå inn og lese gratis nyheter uten at man må oppgi hvem man er. Men det finnes også personlige tjenester, som krever at personer identifiserer seg før de får tilgang til tjenestene. Man får ikke tilgang til sin webbaserte e-postkonto før man har bevist at man er den rette eieren av kontoen, for eksempel ved å oppgi brukernavn og passord. Man får heller ikke kjøpt flybilletter på nett uten å oppgi personopplysninger og betalingsinformasjon. Å realisere sikre personlige tjenester setter krav til en god identitetsforvaltning, slik at tjenestetilbydere sikkert kan vite at de har å gjøre med riktig person, samt hvilke rettigheter denne personen har.

1.1 Bakgrunn

Denne hovedoppgaven er skrevet ved institutt for telematikk ved NTNU (Norges Teknisk-Naturvitenskapelige Universitet), som en del av en fordypning i emnet informasjonssikkerhet. Oppgaven tar utgangspunkt i at svært mange nordmenn i dag har tilgang til Internett og tar i bruk elektroniske tjenester, og at den norske regjering ønsker å anvende IKT (Informasjons- og Kommunikasjonsteknologi) innen alle sektorer for økt effektivisering og verdiskapning. Offentlige etater og kommuner, samt kommersielle og private aktører, tilbyr i dag et utvalg elektroniske tjenester over Internett. En del av disse tjenestene er personlige og krever sikkerhetsmekanismer på plass i bakgrunn. Før en bruker får tilgang til informasjon om seg selv eller til personlige tjenester må han bevise at han er den han utgir seg for, altså autentisere seg. Dette kan gjøres på ulike måter, men brukernavn og passord er et alternativ som er særlig mye brukt. Alternativer er fødselsnummer og engangskoder, eller digitale sertifikater. Hvilken autentiseringsmekanisme som benyttes er avhengig av hvor stor sikkerhet tjenesten krever. Skal det utveksles informasjon mellom bruker og tjenestetilbyder må det i tillegg sikres at informasjon ikke endres på veien, og at informasjonen kommer fra riktig avsender. Dette kan gjøres ved hjelp av digital signatur. Ønsker man at ingen andre enn mottaker skal kunne lese innholdet i informasjonen benyttes også kryptering. For å kunne tilby sikre tjenester må altså brukere av disse tjenestene ha sin egen elektroniske identitet, og bak tjenestene må det være gode systemer for autentisering av personer på grunnlag av denne identiteten.

Oppgaven tar for seg to forslag til nasjonale arkitekturer for brukerautentisering og brukerautorisasjon, nemlig Sikkerhetsportalen og FEIDE (Felles Elektronisk Identitet). Dette er to systemer som gjør det mulig å tilby sikre tjenester på nett, og brukes i henholdsvis offentlig sektor og utdanningssektoren. Sikkerhetsportalen og FEIDE er begge systemer for identitetsforvaltning, hvor brukere først identifiseres og deretter får tilgang til tjenester de har autorisasjon for.

1.2 Formål

Etter som flere tjenester gjøres tilgjengelige fra Internett blir behovet for identitetsforvaltning stadig større, i offentlig sektor så vel som i privat sektor. Alle som ønsker å tilby sine kunder sikre personlige tjenester over nett krever at kundene har en elektronisk identitet samt at mekanismer er på plass for håndtering av denne. Først når kundenes elektroniske identitet er verifisert vil kundene få aksess til sine ressurser og tjenester.

Formålet med denne rapporten er å foreta en systemanalyse av storskala identitetsforvaltning for aksesstyring. Det eksisterer flere identitetsforvaltningssystemer i Norge i dag, blant annet BankID fra bankene, Buypass fra Norsk Tipping og Mobil PKI fra Telenor og Netcom. Dette er infrastrukturer for elektronisk legitimasjon og signatur, og alle kunne inngått i en systemanalyse av storskala identitetsforvaltning. Men en analyse av alle eksisterende identitetsforvaltningssystemer ville blitt meget omfattende, i stedet er to systemer plukket ut for en sammenlignende analyse. Det første av disse systemene er den nye Sikkerhetsportalen som skal tilby sikker innlogging og sikker informasjonsutveksling mellom norske borgere og det offentlige. Sikkerhetsportalen skal være et overbygg over ulike leverandører av PKI-tjenester, slik at brukere av Sikkerhetsportalen ikke trenger å forholde seg til den enkelte PKI-leverandør. Det andre systemet er FEIDE, et godt etablert system som muliggjør sikker identifisering av elever, studenter, lærere og andre ansatte i utdanningssektoren.

Rapporten setter fokus på ulike løsninger for organisering av identitetsforvaltningssystemer. At nettopp Sikkerhetsportalen og FEIDE er valgt er ikke helt tilfeldig. FEIDE er særlig interessant fordi den er mer enn en PKI (Public Key Infrastructure), i FEIDE-løsningene som har vært i bruk frem til i dag har ikke PKI vært brukt i hele tatt. Sikkerhetsportalen på sin side er fullstendig sertifikatbasert, og er en viktig aktør innen norsk identitetsforvaltning da alle statlige etater med behov for sikkerhetstjenester pålegges å bruke Sikkerhetsportalen, i tillegg oppfordres kommunene til det samme.

1.3 Antagelser og begrensninger

I forhold til at oppgavetittelen lyder ”en systemnivå analyse av storskala identitetsforvaltning”, kunne alle de store identitetsforvaltningssystemene i Norge vært gjenstand for analyse og diskusjon i denne rapporten. Da ville imidlertid omfanget på oppgaven bli veldig stort, og det ville ikke være mulig å gå i dybden på de enkelte systemene. Av den grunn er oppgaven avgrenset til å se på kun to systemer for identitetsforvaltning, og systemer som BankID, Buypass og Mobil PKI vil ikke studeres nærmere.

To storskala arkitekturer for identitetsforvaltning analyseres, nemlig Sikkerhetsportalen og FEIDE. Sikkerhetsportalen er opprettet for å realisere sikre elektroniske fra det offentlige, FEIDE for å realisere sikre elektroniske tjenester fra utdanningsinstitusjoner. Systemene analyseres på et systemnivå, med vekt på arkitektur og oppbygging, og et særlig fokus på hvor sikkerheten ligger. Meldingskompleksitet og robusthet er interessante aspekter, sammen med andre momenter som angår systemets sikkerhet. For å avgrense oppgaven noe vil mindre tekniske aspekter som brukervennlighet, kostnader og gevinster vies forholdsvis liten plass. Disse aspektene vil uansett drøftes kort for å gjøre analysen så komplett som mulig. Oppgaven legger heller ikke stor vekt på det juridiske rundt systemene og på personvern, men noen av de viktigste lover og forskrifter systemene forholder seg til nevnes.

1.4 Metode

Oppgaven foretar en sammenlignende analyse på systemnivå av to forslag til storskala identitetsforvaltning. FEIDE er i stor grad rullet ut ved høyskoler og universiteter, og har vært operativ i lengre tid. Sikkerhetsportalen ble lansert 15.desember 2005, og er i dag tatt i bruk av næringslivsportalen Altinn samt av en pilotgruppe for MinSide. Både Sikkerhetsportalen og FEIDE er omtalt og beskrevet i en rekke dokumenter og spesifikasjoner tidligere. Disse dokumentene begrunner i stor grad innføringen av systemene, legger føringer for utrullingen og beskriver systemenes funksjonalitet. Det finnes også detaljerte tekniske systemspesifikasjoner, dette gjelder spesielt for FEIDE hvor all kode og dokumentasjon er åpent tilgjengelig.

Det denne rapporten gjør som tidligere dokumenter ikke gjør, er at den identifiserer likheter og ulikheter ved de to arkitekturene, med tanke på organisering, kompleksitet, sikkerhet, robusthet og brukervennlighet. Oppgaven er i hovedsak teoretisk, hvor rapporten i seg selv er sluttproduktet. Der det synes naturlig og overkommelig gjennomføres imidlertid også en eksperimentell del. Det som er gjøres av eksperimenter er å sette opp en testtjeneste som benytter FEIDE-innlogging, og å teste sertifikatene som i dag utstedes for bruk med Sikkerhetsportalen. Bortsett fra den eksperimentelle delen går arbeidet med oppgaven ut på å samle inn og strukturere informasjon om de to systemene, tilgjengelig fra skriftlige og muntlige kilder.

1.5 Eksperimentell del

Oppgaveteksten nevner at oppgaven skal inkludere en eksperimentell del, og to eksperimenter er foretatt i forbindelse med arbeidet på denne oppgaven. I utgangspunktet var ønsket å få satt opp et brukersted for hvert av de to systemene, og sette opp en testtjeneste som benyttet henholdsvis Sikkerhetsportalen og FEIDE for sikker innlogging. En slik integrasjon ble gjennomført for FEIDE, eksperimentet er nærmere beskrevet i kapittel 6.2. Da Sikkerhetsportalen og BBS ikke har en åpen testtjeneste tilgjengelig ble det vanskelig å få gjennomført en integrasjon med Sikkerhetsportalen. I stedet ble et eksperiment gjennomført med de sertifikatene som per i dag utstedes for bruk med Sikkerhetsportalen, dette er nærmere beskrevet i kapittel 6.1.

Eksperimentet med Sikkerhetsportalens sertifikater går ut på å bestille og installere slike sertifikater, og å utforske hva de kan brukes til og ikke. Eksperimentet bidrar til forståelse av sertifikatenes viktige funksjon i Sikkerhetsportalsystemet, i tillegg til å demonstrere hvordan sluttbrukere kan komme i gang med tjenester fra Sikkerhetsportalen. Eksperimentet med FEIDE-integrasjon går ut på å integrere FEIDE-innlogging i en egen testtjeneste. Eksperimentet er inkludert for å bidra til forståelse rundt hvordan FEIDE foretar autentisering, og særlig til å forstå betydningen av den billettbaserte løsningen.

1.6 Oppbygning

Kapittel 1 fungerer som en introduksjon for oppgaven, og beskriver kort bakgrunn for oppgavens tema, formålet med rapporten samt hvordan arbeidet har foregått med rapporten og med den eksperimentelle delen. Kapittel 2 inneholder bakgrunnsinformasjon for resten av oppgaven, og ser på de krav som i dag stilles til sikker elektronisk identifisering. Ulike typer identitetsforvaltning beskrives, og forskjellen på autentisering og autorisasjon forklares.

Single SignOn beskrives også kort. Kapittel 2 introduserer videre Sikkerhetsportalen og FEIDE, bakgrunnen for deres opprettelse og en overordnet beskrivelse av hvordan systemene fungerer.

Kapittel 3 går gjennom de kriteriene som nevnes i oppgaveteksten, og vurderer i hvilken grad hvert av disse skal være sentralt i analysen. Med utgangspunkt i en kort diskusjon identifiseres noen viktige aspekter systemene skal sammenlignes med hensyn til, en rekke spørsmål grupperes og kriterier stilles opp.

Kapittel 4 og 5 besvarer spørsmålene definert i kapittel 3. Kapittel 4 besvarer spørsmålene for Sikkerhetsportalen, kapittel 5 besvarer de samme spørsmålene for FEIDE. Den første gruppen av spørsmål går på organisering og sikkerhetsantakelser. Dette er den klart mest omfattende av gruppene, men også den klart viktigste. Her skisseres blant annet systemarkitektur og anvendelsesområder, hvilke standarder systemene bruker, hvilke autentiseringsløsninger som er valgt, hvordan personvernet ivaretas, og så videre. Alt dette er viktig og nødvendig bakgrunnsinformasjon for å forstå systemene og kunne ta fatt på en drøftende sammenligning.

Kapittel 6 beskriver de to eksperimentene som er utført i forbindelse med oppgaven, og bidrar til bedre forståelse av sentrale deler av de to foregående kapitlene.

Kapittel 7 diskuterer og sammenligner resultatene fra kapittel 4 og 5. Mens kapittel 4 og 5 inneholder organiserte faktaopplysninger om systemene er det her i kapittel 7 sammenligningen finner sted, og likheter og ulikheter identifiseres.

Etter diskusjonen kommer kapittel 8 som konkluderer rapporten, og kapittel 9 med en oversikt over referansene brukt i arbeidet.

2 Krav om sikker elektronisk identifisering

Sikkerhetsportalen og FEIDE er begge resultater av et ønske om å kunne foreta sikker elektronisk identifisering. Kan man tilby dette finnes det nesten ikke grenser for hvilke tjenester som kan legges på Internett. Et mål er å erstatte alle papirskjema som i dag benyttes for kommunikasjon med det offentlige, med elektroniske tjenester. Kan man stole på at tjenestene bygger på sikre mekanismer for identifisering, signering og kryptering kan dette snart være en realitet. Hele det norske velferdssamfunnet vil dra nytte av at den tidkrevende papiradministrasjonen vi kjenner erstattes med elektronisk behandling, på denne måten kan viktige ressurser frigjøres til verdiskapning.

Med stadig flere elektroniske tjenester blir elektronisk identitetsforvaltning bare mer og mer nødvendig, og det stilles krav til gode systemer for elektronisk identifisering. Kapittel 2.1 vil kort presentere noen vanlige løsninger for identitetsforvaltning. Videre vil kapittel 2.2 se på hva autentisering og autorisasjon er, på hvordan disse to operasjonene henger sammen. Kapittel 2.2 introduserer også prinsippet med Single SignOn. Deretter vil kapittel 2.3 og 2.4 introdusere henholdsvis Sikkerhetsportalen og FEIDE.

2.1 Identitetsforvaltning

Identitetsforvaltning går ut på å kunne fastslå hvem en gitt person er, samt å fastslå hvilken rolle denne personen har. En person som skal identifiseres elektronisk legger fram digitalt bevis på hvem han er, en elektronisk ID (identitet) som sier hvem han er uten at han trenger å være personlig tilstede. Elektronisk ID er egnet for en rekke personaliserte tjenester, blant annet innsyn i personlig informasjon, søknadsbehandling, tilgangskontroll for nettverksressurser og så videre.

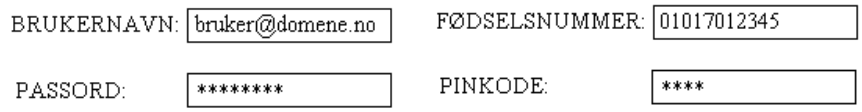
2.1.1 Brukernavn og passord/pinkode

Den vanligste formen for identifisering innebærer at man oppgir brukernavn og passord for å få tilgang til en tjeneste. I enkelte tilfeller får man velge brukernavn selv, andre ganger får man et tildelt. Det er heller ikke uvanlig at e-postadresse, fødselsnummer eller mobiltelefonnummer benyttes som brukernavn. Sammen med brukernavnet som forteller hvem man hevder å være må man oppgi en hemmelighet som beviser at man virkelig er denne personen. Denne hemmeligheten kan være et passord eller en kode, selvvalgt eller tilfeldig tildelt. Eventuelt kan det være en engangskode fra et kodekort, en kodegenerator, en SMS eller et bilde sendt som MMS. Koder fra en kodegenerator er generert av en algoritme inne i generatoren, og er kun gyldig i et kort tidsintervall. At passord og koder holdes hemmelig er en nødvendig forutsetning for at dette skal være en sikker løsning. Passord bør også være konstruert slik at de er umulig å gjette for utenforstående.

Sikkerhetsnivå for passord og koder varierer svært mye, fra lavt til veldig høyt. Hvilket nivå en kode har avhenger av hvordan den genereres og distribueres, hvordan den oppbevares og om den brukes flere ganger. En engangskode sendt via en sikker kanal vil gi stor grad av sikkerhet, mens et passord skrevet på en post-it lapp festet til maskinen den gir tilgang til vil gi liten grad av sikkerhet. Mange tjenester tilbyr et passordbasert innloggingsskjema, med varierende grad av sikkerhet på passord og koder. En type tjenester som ofte benytter passord for identifisering er e-posttjenester, hvor man typisk velger sitt eget passord idet man

oppretter kontoen, et passord som gjenbrukes ved hver eneste pålogging. Før innføringen av BankID har også bankene typisk brukt koder for innlogging i nettbank. De kodene bankene bruker for identifisering av sine kunder er allikevel av en helt annen art en passordene e-posttjenester bruker. Bankene benytter engangskoder fra for eksempel kodekort eller kodegenerator, og for å logge inn i nettbanken må man ha tilgang til eierens kodekort eller kodegenerator. Andre tjenester som benytter passord for identifisering er for eksempel tjenester for eksamensoppmelding ved universiteter og høyskoler, og tjenester med informasjon om lån og tilbakebetaling i Lånekassen. Disse tjenestene krever at man oppgir fødselsnummer sammen en fast kode, som antas å være mindre sikker enn bankenes engangskoder siden de gjenbrukes mange ganger.

Figur 2.1 viser til venstre et innloggingsvindu hvor bruker må oppgi brukernavn og passord og til høyre et innloggingsvindu hvor bruker må oppgi fødselsnummer og en pinkode. Koden kan være en fast kode, eller en engangskode fra et kodekort, en kodegenerator, en SMS eller et MMS-bilde.



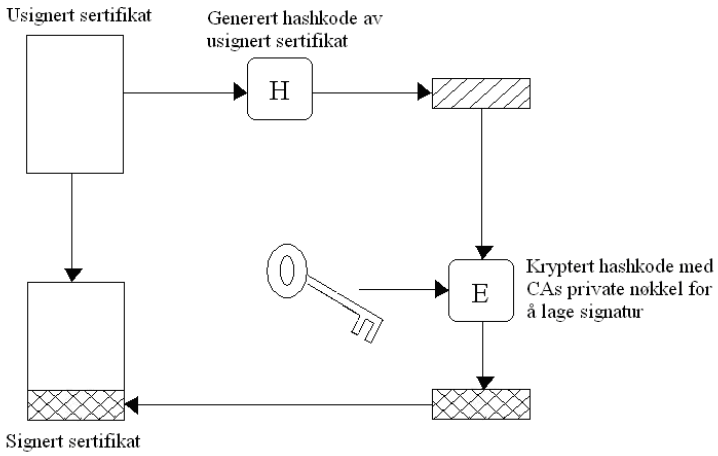
Figur 2.1: Innlogging med brukernavn og passord, eller med fødselsnummer og pinkode.

2.1.2 Digitale sertifikater

Et alternativ til identifisering med brukernavn og passord er digitale sertifikater, enten lagret på brukers datamaskin eller integrert i et smartkort. Et digitalt sertifikat er legitimasjon i elektronisk form som benyttes for å vise at man er den man utgir seg for, eller for å kontrollere at en digital signatur er gyldig. Dette innebærer bruk av PKI (Public Key Infrastructure), altså at kryptografi tas i bruk for autentisering og elektronisk signatur. I en PKI har brukeren en hemmelig krypteringsnøkkel som ingen andre kjenner, og tjenesten kan verifisere at brukeren er den han hevder ved å sjekke mot en tilhørende offentlig nøkkel. Koblingen mellom en bruker og hans nøkkel finnes i et digitalt sertifikat, signert av en tiltrodd tredjepart. En brukers sertifikat og private nøkkel kan for eksempel være lagret i et smartkort, det vil si et plastkort med en elektronisk chip. Smartkortet er beskyttet med en pinkode, og i tillegg trengs det en kortleser for å lese innholdet på kortet.

Kohnfelder introduserte i 1978 konseptet med signerte datastrukturer for å overbringe en offentlig nøkkel til en tiltrodd part [1]. Offentlig-nøkkel sertifikater er siden benyttet for å binde en entitets navn og eventuelle andre attributter til en korresponderende offentlig nøkkel. Motivasjonen for å bruke sertifikater er å sikre integritet, det vil si å forhindre at nøkler endres, samt å sørge for autentisering, altså å sikre at nøkkelen tilhører den faktiske eieren. Det finnes en rekke ulike digitale sertifikattyper, blant annet X.509 offentlig-nøkkel sertifikater, SPKI-sertifikater, PGP-sertifikater og attributtsertifikater. Disse sertifikatene har ulike formater som kan eksistere i flere versjoner, og en enkelt versjon kan instansieres på ulike måter. I mange sammenhenger er et digitalt sertifikat synonymt med et X.509 offentlig-nøkkel sertifikat, fordi X.509 standarden er et universelt akseptert skjema for offentlig-nøkkel sertifikater. X.509 sertifikater brukes i mange applikasjoner for nettverkssikkerhet, blant annet i IPSec (IP Security), SSL (Secure Sockets Layer), SET (Secure Electronic Transactions) og S/MIME (Secure Multipurpose Internet Mail Extensions) [2].

Et offentlig-nøkkel sertifikat består av en offentlig nøkkel og en brukeridentitet, signert av en tiltrodd tredjepart. Denne tredjeparten er typisk en sertifiseringsautoritet, ofte omtalt som CA (Certification Authority), som alle brukere stoler på, for eksempel en bank de alle tilhører. En bruker kan presentere sin offentlige nøkkel til autoriteten på en sikker måte, og få et sertifikat. Sertifikatet publiseres til alle som trenger brukerens offentlige nøkkel, og de kan selv verifisere sertifikatets gyldighet ved hjelp av den tiltrodde signaturen. Figur 2.2 illustrerer bruken av offentlig-nøkkel sertifikater, figuren er rekonstruert fra [2]. Av det usignerte sertifikatet som inneholder eierens brukeridentitet og offentlige nøkkel, genereres en hashkode. Videre krypteres denne hashkoden med CAs private nøkkel, og slik oppstår sertifikateierens signatur. Signaturen legges ved sertifikatet og et signert sertifikat foreligger. Mottaker kan enkelt verifisere signaturen ved å bruke CAs offentlige nøkkel.



Figur 2.2: Bruk av offentlig-nøkkel sertifikat.

PKI kan også benyttes på mobiltelefoner, såkalt mobil PKI. Mobil PKI brukes på samme måte som annen PKI, for autentisering og digitale signaturer, og fordelen med denne formen for identitetsforvaltning er at man kun behøver en vanlig mobiltelefon. I mobil PKI ligger den private nøkkelen lagret i brukerens SIM-kort (Susbscriber Identity Module), mens en tiltrodd tredjepart administrerer den offentlige nøkkelen. Mobiltelefonen kan også benyttes til identifisering uten at PKI ligger på SIM-kortet. For eksempel som en del av en totrinns autentisering, der man mottar en kode på SMS eller MMS som må oppgis for å få tilgang til en tjeneste eller til neste autentiseringssteg. På Altinn kan man enten logge inne med smartkort fra Buypass, via Sikkerhetsportalen, eller med mobiltelefon. I tilfellet for mobiltelefon må man på Altinns hjemmeside oppgi fødselsnummer og passord, deretter får man tilsendt en engangskode fra Sikkerhetsportalen i form av en SMS. Brukeren oppgir denne koden når han blir bedt om det i nettleseren sin, og hvis koden godkjennes autentiseres brukeren.

I likhet med passord og koder kan også sikkerhetsnivået på sertifikater variere stort. Ofte antas sertifikater å være sikrere enn passord, noe som ikke nødvendigvis er tilfelle. For at et sertifikat skal ha høy grad av sikkerhet knyttet til seg må det genereres og oppbevares på en sikker måte. Et sertifikat installert på en datamaskin kan være lett å misbruke for andre som har tilgang til samme maskin, mens en kodegenerator kan være vanskelig å misbruke dersom man ikke kjenner koden man må ha for å få tilgang til lagret informasjon. Sertifikater med ulike krav til sikkerhet genereres, distribueres og oppbevares på ulike måter. For eksempel vil

sertifikater som ligger på smartkort være sikrere enn sertifikater som ligger som ubeskyttede filer i programvare. Og det er større sikkerhet for at sertifikater og nøkler kommer frem til riktig eier dersom de utleveres ved personlig fremmøte fremfor nedlastning fra Internett.

2.1.3 Biometri

En tredje klasse av identifiseringsmetoder benytter biometri. Biometri handler om metoder som gjør det mulig å måle og sjekke biologiske mønstre [3], og er mye omdiskutert. For å identifisere en person sjekkes dennes kjennetegn mot en forhåndslagret database, og for å kontrollere at en person er den han utgir seg for sjekkes data lagret i for eksempel pass eller smartkort mot det mønsteret personen viser frem. I et pass eller smartkort er kjennetegnene gjerne lagret i en RFID-brikke (Radio Frequency Identity). Ulike former for biometri inkluderer gjenkjenning av fingeravtrykk, ansiktstrekk, stemme, blodårer og andre biologiske mønstre som unikt identifiserer mennesker. Gjenkjenning av den fargede delen rundt øynene, irisgjenkjenning, går for å være den form for biometri som gir minst risiko for feil. Ved fingeravtrykk er det lettere å få like mønstre, for eksempel for eneggede tvillinger.

Det eksisterer datamaskiner og annet elektronisk utstyr som krever at man avgir fingeravtrykk før man får tilgang til det, og enkelte bedrifter har allerede innført biometrisk adgangskontroll. I Norge har Datatilsynet vært skeptiske til å ta i bruk biometri, da det er store utfordringer knyttet til personvern når man må identifisere seg med biologiske data. Datatilsynet har fått en rekke henvendelser om å ta i bruk biometri, og har fattet vedtak i mange av sakene. Med hjemmel i et strengt norsk lovverk har de kommet frem til at på grunn av personopplysningslovens § 12 [4] kan entydige identifikasjonsmidler bare nyttes der det er saklig behov for sikker identifisering og der metoden er nødvendig. Biometriske kjennetegn faller inn under definisjonen av entydige identifikasjonsmidler, og Datatilsynet har ikke funnet metodene nødvendige i noen av sakene behandlet til nå. Blant bedriftene som har fått avslag fra datatilsynet etter å ha søkt om bruk av biometrisk gjenkjenning for kunder og ansatte er Bunnpriskjeden som ønsket å ta i bruk fingeravtrykkgjenkjenning for inn- og utstempling av ansatte, og SAS Braathens som ønsket å bruke fingeravtrykk for å sikre at samme person sjekker inn på flyet som faktisk går om bord [5]. Diskoteket Tiger Tiger ønsket fingeravtrykkgjenkjenning i garderoben for å sikre at rett person får rett jakke, og ESSO ønsket å kontrollere tilgangen til tankanlegg ved hjelp av fingeravtrykk.

Flere land tar i bruk biometri i pass, visum, nasjonale identitetskortkort og andre identitetsdokumenter [6]. Også i Norge jobbes det med å utstede pass med fingeravtrykk, men Datatilsynet er kritisk til bruk av biometriske pass [5]. Justisdepartementet og Datatilsynet arbeider for tiden med å endre lovverket, slik at det kan bli mulig å ta i bruk biometriske hjelpmidler også i Norge. Det er imidlertid usikkert når den nye loven er klar og hvordan den vil se ut. Figur 2.3, hentet fra [7], illustrerer noen muligheter for identifisering ved hjelp av biometri. Fra venstre mot høyre ser vi fingeravtrykk, ansiktsgjenkjenning, håndgjenkjenning, irisskanning og stemmegjenkjenning.

Figur 2.3: Noen mulige løsninger for identifisering av mennesker ved bruk av biometri.

Sikkerhetsportalen og FEIDE er to systemer for nasjonal identitetsforvaltning, hvor enhver bruker har sin egen unike ID. Sikkerhetsportalen bruker digitale sertifikater for å identifisere sine brukere, FEIDE har så langt brukt brukernavn og passord. Det er ikke umulig at også biometri tas i bruk noen år frem i tid, men da må altså det norske lovverket endres først.

2.2 Autentisering og autorisasjon

Identitetsforvaltning innebærer som nevnt håndtering av opplysninger om hvem en person er og hvilke rettigheter han har. Identitetsforvaltning inkluderer derfor både autentisering og autorisasjon. I de følgende underkapitlene kommer en nærmere beskrivelse av autentisering og autorisasjon, samt av felles pålogging eller såkalt Single SignOn (SSO).

2.2.1 Autentisering

Autentisering dreier seg om hvem en entitet er, om forbindelsen mellom en identitet og en entitet [1]. Med andre ord er autentisering prosessen med å bestemme om noen eller noe faktisk er hva det hevder å være, prosessen med å identifisere et individ, et program eller en prosess.

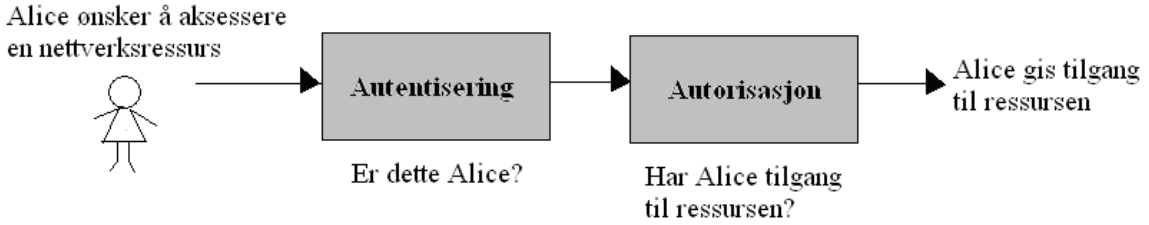
Autentisering er basert på at det som skal identifiseres har et bevis for sin identitet. Et slikt bevis kan være noe man fysisk har, eksempelvis et førerkort, et bankkort eller et forsikringsbevis. Eller det kan være noe man kan, som et selvvalgt passord, sitt eget fødselsnummer eller telefonnummer. Beviset kan også være noe man er, representert ved et fingeravtrykk, irisskanning, stemmegjenkjenning eller andre biometriske kjennetegn. Den mest brukte form for bevis på identitet er nok brukernavn og passord, hvor det faktum at en bruker kjenner korrekt passord antas å garantere at brukeren er den han utgir seg for. Digitale sertifikater og digitale signaturer er en annen form for autentisering som er nokså utbredt. Mens autentisering forsikrer at et individ er den han hevder å være, sier det derimot ingenting om dets aksessrettigheter. Det gjør imidlertid autorisasjonsprosessen.

2.2.2 Autorisasjon

Autentisering går altså ut på å verifisere forbindelsen mellom en identitet og en entitet, mens autorisasjon dreiser seg om hva identiteten er tillatt å se og gjøre [1]. Autorisasjon går med andre ord ut på å verifisere hvilke aksessrettigheter en bruker har, hvilke aktiviteter som er tillatt. Autorisasjon er som regel nødvendig i forbindelse med autentisering, etter at en bruker er autentisert må han gjerne også få autorisasjon for spesifikke tjenester og aktiviteter. Hvilken form for autorisasjon en bruker får kan være situasjonsavhengig, for eksempel kan tidspunkt, fysisk lokasjon og kredittgrense være av betydning for hva en bruker får lov til å se og gjøre.

Anta at Alice ønsker tilgang til en aksessbeskyttet nettverksressurs hun har rettigheter til å bruke. Først må Alice autentisere seg, hun må legge frem bevis på at hun virkelig er Alice. Dette kan gjøres ved å oppgi brukernavn og passord, ved å presentere et digitalt sertifikat, et fingeravtrykk, en stemmeprøve eller hvilken som helst annen informasjon som unikt identifiserer henne i systemet. Når det er klart at det faktisk er Alice som ber om å få bruke nettverksressursen, foretas det videre en autorisasjon som bekrefter at Alice har rett til å

benytte ressursen. Forutsatt at Alices identitet på forhånd er bekreftet bør hun få den tilgangen hun står oppført med. Figur 2.4 illustrerer forskjellen og sammenhengen mellom autentisering og autorisasjon. Ved autentisering avgjør man om dette virkelig er Alice, og ved autorisasjon avgjør man om Alice har tilgang til den forespurte ressursen gitt at det faktisk er Alice som spør. Sikkerhetsportalen og FEIDE foretar autentisering av sine brukere, deretter må det gis autorisasjoner til spesifikke ressurser.



Figur 2.4: Autentisering og autorisasjon for å få tilgang til beskyttet ressurs.

Et system for elektronisk identitetsforvaltning krever at samtlige brukere har en elektronisk ID som unikt identifiserer de i systemet. Elektronisk ID er et system for elektronisk legitimasjon og signatur [8], og gjør en rekke funksjoner mulige. Et system for elektronisk identifisering muliggjør blant annet sikker pålogging til nettverk og tjenester, samt signering og kryptering av informasjon for å sikre integritet og konfidensialitet.

2.2.3 Single SignOn

Noen ganger har man behov for å logge inn på flere tjenester, i samme domene eller på tvers av domener. Å måtte autentisere seg for hver enkelt tjeneste blir fort tungvint, og det ville vært mye enklere om man kunne ha en felles påloggingstjeneste slik at én enkelt pålogging var gyldig for alle tjenester. Det er nettopp dette Single SignOn (SSO) realiserer, en felles pålogging som gjør at brukere kan logge inn én gang og få aksess til flere applikasjoner. SSO innebærer at hver bruker har en identitet som er gyldig i flere systemer, for eksempel et passord eller et sertifikat, og hvis en bruker logger på en tjeneste med sin vanlige identitet kan han senere bruke andre tjenester hvor han har samme identitet uten å logge inn på nytt.

Den store fordelen med SSO er at brukeren slipper å oppgi passord eller vise sertifikat for hver tjeneste han ønsker å bruke, en enkelt autentisering og autorisasjon er nok til å gi brukeren aksess til alle systemer han har tillatelse for. Når en bruker er autentisert for en tjeneste som støtter SSO kan autentiseringsdata deles med andre tjenester brukeren ønsker å bruke, og de andre tjenestene aksepterer autentiseringsinformasjonen uten å selv foreta en autentisering. Man unngår altså redundans, og det eneste som kreves er at de to applikasjonene har tillit til hverandres autentiseringsdata. SSO kan realiseres ved hjelp av SAML (Security Assertion Markup Language), en XML-basert standard for utveksling av autentiserings- og autorisasjonsinformasjon over Internett. Når en bruker som er autentisert for en tjeneste ønsker å bruke en annen tjeneste, sender den første tjenesten informasjon om brukerens autentisering og autorisasjon til den nye tjenesten.

2.3 Sikkerhetsportalen

2.3.1 Bakgrunn

De siste årene har stadig flere nordmenn fått tilgang til Internett. Internett brukes til nyhetslesing, innhenting av faktastoff, e-post, chatting, banktjenester, annonsering, bestilling av varer og billetter, samt en rekke andre tjenester. Flertallet av norske husstander har Internett privat, mange har også tilgang til Internett fra arbeidsplass eller skole. I tillegg tilbyr biblioteker og enkelte andre institusjoner nettilgang. Dette resulterer i at både skoleungdom, yrkesaktive og eldre i større eller mindre grad har tilgang til Internett, og i løpet av det siste tiåret har en svært stor andel av befolkningen fått Internettilknytning. Ifølge en undersøkelse gjennomført av Transportøkonomisk institutt og TNS Galllup i 2005, bruker 69 prosent av befolkningen Internett daglig, mens det er 23 prosent som aldri bruker Internett [9]. I følge denne undersøkelsen bruker altså mer enn to tredeler av befolkningen Internett daglig. Regjeringen har en målsetning om at alle som ikke selv har tilgang til Internett, i løpet av 2007 skal ha tilbud om å få utført tjenester på nett i sitt nærmiljø [10]. I takt med at stadig flere norske borgere tar i bruk Internett, dukker det hele tiden opp nye elektroniske tjenester. Ikke bare fra kommersielle aktører, men også fra offentlige etater og kommuner. For eksempel kan man på Skatteetatens nettsider levere selvangivelsen og bestille nytt skattekort, og Lånekassen har gjort det mulig å søke om lån og stipend fra sine nettsider. Enkelte kommuner har gjort det mulig å søke på nett om for eksempel barnehageplass, leie av kommunale bygg, bytte av fastlege og så videre. Det kommer stadig flere nettjenester, og i de kommende årene vil det bli mange flere.

Regjeringen la i juni 2005 ut to handlingsplaner for en enklere hverdag for henholdsvis borgere og næringsliv, ”eNorge 2009” fra Moderniseringsdepartementet [10] og ”Et enklere Norge 2005-2009” fra Nærings- og handelsdepartementet [11]. I ”eNorge 2009” fastlegger regjeringen en overordnet IT-politikk for perioden 2005-2009, med et mål om en enklere hverdag for folk flest og trygghet for fremtidens velferd. Disse målene skal man forsøke å nå ved hjelp av informasjonsteknologi anvendt på riktig måte. ”eNorge 2009” grupperer sine mål i tre hovedområder. Det første målområdet er enkeltmennesket i det digitale Norge. Regjeringen ønsker at alle skal ha mulighet til å delta i informasjonssamfunnet, og på denne måten unngå digitale skiller. Dette forutsetter god Internettilgang, at digitale tjenester er tilpasset den enkeltes behov, og at hele befolkningen innehar en god digital kompetanse. I tillegg forutsettes et godt forbruker- og personvern, og en god kultur for IT-sikkerhet. Det andre målområdet er innovasjon og vekst i næringslivet. Regjeringen ønsker at det offentlige og privat næringsliv bedre skal utnytte mulighetene som informasjonsteknologien skaper, at Norge i større grad skal skape verdier fra kunnskapsbaserte virksomheter. Det tredje målområdet er en samordnet og brukertilpasset offentlig sektor. Ved hjelp av informasjonsteknologi ønsker regjeringen at borgerens møte med det offentlige skal gjøres enklere, i tillegg å frigjøre ressurser for å styrke velferdstilbudet.

Bruken av elektroniske tjenester som krever at kommunikasjonsparter identifiserer seg, binder seg til kommunikasjonens innhold på en måte som kan spores, eller som trenger konfidensialitetsbeskyttelse; er økende. Dette forutsetter elektronisk ID og elektronisk signatur [10]. Offentlige og private tjenestetilbydere har frem til i dag dekket sine sikkerhetsbehov ved hjelp av svært ulike løsninger. Resultatet er at brukere må holde styr på en mengde brukernavn, passord og koder. Mange velger derfor å benytte samme passord ved flere tjenester, de velger passord som er lette å huske og dermed lette å gjette, og passord skrives gjerne ned. Alt dette svekker naturligvis sikkerheten ved systemene. Ved å ta i bruk en

standardisert elektronisk signatur kan én og samme ID gjenbrukes mot mange tjenester, og en rekke offentlige tjenester vil enkelt kunne digitaliseres. Regjeringen ønsker at alle relevante statlige, kommunale og fylkeskommunale tjenester skal kunne tilbys digitalt senest i 2009, gjennom innbyggerportalen MinSide [10]. For store volumtjenester skal minst 75 prosent av målgruppen benytte de elektroniske tjenestene innen 2009, og 80 prosent av brukerne av offentlige digitale tjenester skal være fornøyd eller meget fornøyd med tjenestene.

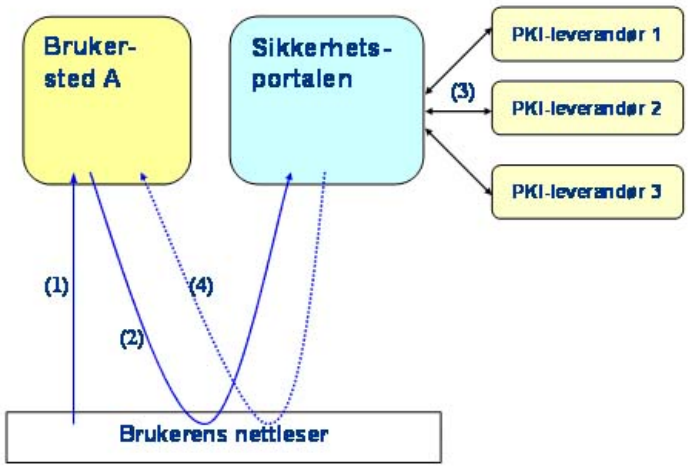
2.3.2 Kort fortalt

Når etater og kommuner tilbyr elektroniske tjenester er det naturlig at disse ønsker sikker innlogging og overføring av dokumenter. Tjenestene krever derfor ofte autentisering, kryptering og signering. Eksempler på tjenester som krever sikker innlogging og informasjonsoverføring er de nyopprettede portalene Altinn og MinSide, for henholdsvis næringsliv og borgere. En bruker må autentisere seg for brukerstedet før han får tilgang til sine tjenester, i tillegg kan det være behov for signering og kryptering for å sikre at informasjon er undret og kommer fra riktig avsender, samt at kun mottaker kan lese innholdet. Om etater og kommuner med behov for autentisering, signering og kryptering skal lage funksjonalitet for dette selv vil hvert brukersted få unødvendig store kostnader og samme arbeid vil utføres mange ganger.

Derfor tok Moderniseringsdepartementet sammen med Næringsdepartementet initiativ til å opprette en felles sikkerhetstjeneste for offentlig sektor, kjent som Sikkerhetsportalen [12]. Sikkerhetsportalen skal levere kostnadseffektive PKI-tjenester, og sørge for autentisering av brukere som ønsker å kommunisere med det offentlige via Internett. 15. februar 2005 fikk Brønnøysundregistrene oppdraget med å utlyse, inngå og forvalte en rammeavtale for Sikkerhetsportalen. BBS (Bankenes Betalingssentral AS) ble 17. juni 2005 valgt som leverandør av Sikkerhetsportalen. 1. juli 2005 ble kontrakten signert, og utviklingen av løsningen satt i gang.

Sikkerhetsportalen tilbyr et standardisert grensesnitt som gjør det enklere for brukerstedene å integrere sikkerhetstjenestene autentisering, signering og kryptering i løsningene sine. Sikkerhetsportalen håndterer all kommunikasjon mot de ulike PKI-leverandørene og hvert brukersted forholder seg kun til én part, nemlig den sentrale delen av Sikkerhetsportalen. En vanlig bruker forholder seg til nettsider og dialoger fra brukersteder, og kan aldri se eller kommunisere direkte med Sikkerhetsportalen. Men selv om det er usynlig for brukeren er Sikkerhetsportalen alltid involvert når autentisering, signering og kryptering benyttes.

Figur 2.5, hentet fra [12], illustrerer et eksempel på bruk av Sikkerhetsportalen. En bruker prøver å få tilgang til et aksessbeskyttet område på en offentlig nettside, her kalt brukersted A (1). Han videresendes til Sikkerhetsportalen (2), og om han ikke allerede har en etablert sesjon mot Sikkerhetsportalen vil han presenteres for en påloggingsside. Brukerens autentiseringsopplysninger bekreftes mot riktig PKI-leverandør (3), og brukeren sendes tilbake til det offentlige brukerstedet A (4).



Figur 2.5: Bruk av Sikkerhetsportalen.

Kapittel 4 går mye mer detaljert inn på hvordan Sikkerhetsportalen er organisert og realisert.

2.4 FEIDE

2.4.1 Bakgrunn

Internett får flere og flere anvendelsesområder, også innen det norske utdanningssystemet. Nyere læreplaner legger stor vekt på IKT som et redskap for læring i skolen. Dagens unge skal forstå de samfunnsmessige gevinstene med IKT, og kunne dra nytte av teknologien i sin studiehverdag gjennom informasjonssøking og kommunikasjon. Internett er en unik kilde til informasjon fra hele verden, og med denne teknologien er svarene aldri langt unna. Langt unna er heller ikke andre mennesker og kulturer, og samarbeid og fjernkontakt kan brukes på en helt ny måte. Et av regjeringens mål for de neste årene er at alle skal ha mulighet til å delta i informasjonssamfunnet, noe som blant annet forutsetter at hele befolkningen innehar en god digital kompetanse [10]. For å sørge for en god digital kompetanse i den norske befolkningen er det særlig viktig med god IKT-opplæring i grunnskolen og i videregående skoler. Slik vil dagens unge få en god forståelse for og kunnskap om IKT, og bidra til å trygge velferden i Norge de neste tiårene.

Som en naturlig konsekvens av at IKT er på full fart inn i norske skoler er det også vokst frem et behov for personaliserte tjenester i utdanningssektoren, hvor brukere må kunne identifisere seg elektronisk. Stadig flere digitale ressurser og tjenester i utdanningssektoren baserer seg på elektronisk identifikasjon som tilgangskontroll [13], derfor er det viktig med et godt system for identitetsforvaltning i utdanningssektoren.

2.4.2 Kort fortalt

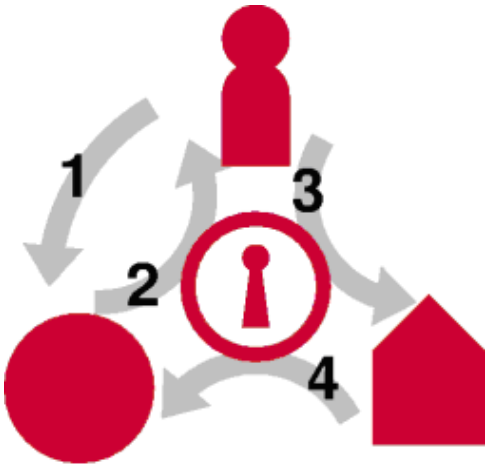
Å kunne gi elever og lærere riktig tilgang til digitale ressurser og tjenester skaper et behov for sikker identifisering, og det kreves en enhetlig elektronisk identitetsforvaltning. Her kommer FEIDE inn i bildet, som et system som autentiserer personer tilknyttet norske utdanningsinstitusjoner via en innloggingstjeneste [14]. Systemet er basert på et samarbeid mellom organisasjoner i utdanningssektoren og deres leverandører av IT-baserte tjenester. Målet er å få organisasjonenes lokale identitetsforvaltning på en felles form, slik at hver

organisasjon kan bekrefte identiteten til sine egne studenter, elever eller ansatte på samme måte.

Arbeidet med FEIDE i universitets- og høykolesektoren har pågått siden 2000 i regi av UNINETT [14]. Prosjektet gjennomføres i samarbeid med oppdragsgiver Kunnskapsdepartementet. I dag er FEIDE innført for rundt halvparten av brukerne i høyere utdanning, og det arbeides med lokale FEIDE-løsninger. Departementet har besluttet at FEIDE også skal innføres i grunnskoler og videregående skoler, et arbeid som drives av UNINETT ABC. FEIDE som løsning for identitetsforvaltning i utdanningssektoren omtales i flere nasjonale styringsdokumenter, blant annet i "Program for digital kompetanse 2004-2008" [15]. Her står det at alle institusjoner i universitets- og høyskolesektoren skal ha et nasjonalt brukernavn innen 2006, og alle i grunnopplæringen innen 2008. Det poengteres at FEIDE-teknologien skal spille en sentral rolle i dette arbeidet.

FEIDEs sentrale funksjon er identitetskontroll eller autentisering [16]. Programvaren som utfører autentiseringen er en viktig del av mellomvaren FEIDE etablerer ved utdanningsorganisasjonene. I tillegg til autentisering tilbyr FEIDE formidling av informasjon om brukeren, informasjon som kan brukes til å kontrollere tilgang til ressurser, selv om FEIDE i seg selv ikke tilbyr autorisasjon.

Figur 2.6, hentet fra [14], illustrerer hvordan FEIDEs sentrale innloggingstjeneste Moria fungerer. Figuren viser en bruker (stilisert person) i kontakt med sin vertsorganisasjon (stilisert hus) og en tjeneste (sirkel). I kommunikasjonen mellom brukere, vertsorganisasjoner og tjenester griper FEIDE inn, illustrert ved et nøkkelhull i midten. Brukeren henvender seg til en aksessbeskyttet elektronisk tjeneste (1). Deretter videresender tjenesten brukeren til FEIDEs innloggingsside Moria, og Moria ber om brukerens FEIDE-navn og passord (2). Moria videresender påloggingshenvendelsen til autentiseringstjeneren ved brukerens vertsorganisasjon (3), og Moria videresender svaret fra autentiseringstjeneren til tjenesten (4). Når autentiseringstjeneren har godkjent oppgitt FEIDE-navn og passord, vil tjenesten be Moria om brukerdata. Tjenesten får den informasjonen FEIDE har avtalt at den kan få, og som brukeren har gitt sitt samtykke til under innloggingen.



Figur 2.6: Bruk av FEIDEs sentrale innloggingstjeneste Moria.

Kapittel 5 går mye mer detaljert inn på hvordan FEIDE er organisert og realisert.

3 Kriterier for en sammenlignende analyse

Denne oppgaven tar for seg Sikkerhetsportalen og FEIDE, to storskala arkitekturer for identitetsforvaltning. Systemene realiserer elektronisk identifikasjon, og brukes til å autentisere og autorisere brukere som søker tilgang til sikre elektroniske tjenester via Internett. Målet med rapporten er å påpeke forskjeller og likheter mellom arkitekturene, og å trekke noen konklusjoner. Fokus ligger på organisatoriske og tekniske aspekter, særlig på aspekter som angår sikkerhet. En rekke systemaspekter nevnes i oppgaveteksten, og kapittel 3.1 drøfter hvilke av disse som er mest interessante i forhold til en analyse av Sikkerhetsportalen og FEIDE. Analysekriterier defineres i form av spørsmål for de mest relevante systemaspektene, disse er samlet i en tabell i kapittel 3.2.

3.1 Vektlegging av systemaspekter

Siden oppgaven er en del av et fordypningsemne i informasjonssikkerhet er det et naturlig at den i hovedsak fokuserer på de tekniske løsningene, og særlig på sikkerhetsmekanismer. Dette kapitlet tar stilling til hvilke systemaspekter som er mest interessante å studere nærmere, og avgrenser i så måte oppgaven. Underveis i diskusjonen av de ulike aspektene defineres også kriterier på spørsmålsform.

Oppgaveteksten nevner en del systemaspekter, og det første som nevnes er *sikkerhetsantakelser*. Systemene bygger på en rekke forutsetninger, som påvirker systemenes sikkerhet og pålitelighet. Særlig viktig er organiseringen av systemkomponenter, autentiseringsløsninger som er valgt, og sikkerhetstjenester som tilbys. Disse aspektene er helt nødvendige å se på, fordi uten at man forstår hva systemene gjør og hvordan de er sammensatt blir det vanskelig å diskutere noe som helst rundt systemenes sikkerhet. Før man tar fatt på en systemnivå analyse er det spesielt nødvendig å ha oversikt over systemenes *organisering*. Tre punkter som går på arkitektur er sammen med en rekke andre spørsmål om sikkerhetsantakelser samlet i en seksjon kalt organisering og sikkerhetsantakelser. Informasjonen disse spørsmålene får frem om systemenes organisering er viktig informasjon som kreves på plass før man begir seg ut på en analyse. Følgende tre spørsmål knyttet til arkitektur er inkludert.

Arkitektur:

a) Hvilke delsystemer eksisterer?
b) Hvilke av disse kommuniserer med hverandre?
c) Hvor i systemet er sikkerheten realisert?

For å forstå et system er det viktig å ha oversikt over hva det kan brukes til, hvilke *anvendelsesområder* det har. Likheter og ulikheter ved systemene på andre områder kan muligens forklares ved å se på forskjeller i hvor og hvordan systemene anvendes. Det å kartlegge anvendelsesområder er ikke en viktig del av selve analysen, men nyttig bakgrunnsinformasjon som forutsettes for å kunne analysere systemene. To punkter om anvendelsesområder er inkludert under seksjon for organisering og sikkerhetsantakelser. Det første svarer på hvor systemene brukes, det andre på hvilke sikkerhetstjenester de realiserer.

Anvendelsesområder:

a) Hvor brukes systemet i dag, og i morgen?
b) Hvilke sikkerhetstjenester tilbys?

Et annet aspekt som nevnes er *Standardisering.* Standardisering kan blant annet omfatte hvilke kjente standarder systemene bygger på, noe som har mye å si for kompatibilitet med andre løsninger. Kanskje er systemene også i ferd med selv å bli de facto standarder innen visse bransjer eller samfunnsområder. To punkter om standardisering er tatt med i beskrivelsen av systemene, det første ser på hvilke åpne standarder systemene bruker, det andre på i hvilken grad systemene selv er i ferd med å bli en standard. Spørsmålene er plassert under seksjon for organisering og sikkerhetsantakelser, og er viet liten plass da de ikke direkte angår teknisk systemsikkerhet.

Standardisering:

a) Hvilke åpne standarder er systemet basert på?
b) Er systemet i ferd med å bli en standard innen visse sektorer?

Et av de aller viktigste valgene som ligger bak de to systemene er valget om autentiseringsløsning. Hvordan systemene foretar autentisering av sine brukere er veldig viktig i forhold til hvor sikkert systemet er og hva som kreves for å integrere løsningen i egne tjenester. Først og fremst er det viktig å skissere hvilken autentiseringsløsning som benyttes, videre beskrives også hvilke krav som stilles til brukernes elektronisk identitet.

Autentisering:

a) Hvilke autentiseringsløsninger benyttes?
b) Hvilke krav stilles til brukernavn og passord / nøkler og sertifikater?

I et system for identitetsforvaltning er det viktig med gode rutiner for behandling av personopplysninger, viktig å ivareta brukernes personverninteresser. Et godt personvern er en forutsetning for et godt identitetsforvaltningssystem, og noen punkter om personvern inngår i systembeskrivelsen. Hvilke personopplysninger som lagres om brukerne er inkludert som et punkt, samt hvilke rutiner som er på plass for å sikre et godt personvern, om transaksjoner logges i systemet og om personopplysningsloven oppfylles.

Personvern:

a) Hvilke personopplysninger lagres, og hvor lagres de?
b) Hvilke rutiner og mekanismer er på plass?
c) Logges transaksjoner, er de i så fall sikret mot endringer?
d) Ivaretas personverninteresser generelt, og oppfylles personopplysningsloven?

Autentisering kan foregå på mange nivå, og ulike tjenester stiller gjerne ulike krav til sikkerhet. Et eget punkt ser på hva som antas om sikkerhetsbehov for ulike tjenester. Dette punktet beskriver også systemenes evne til å tilby løsninger på ulike sikkerhetsnivå, noe som i høy grad går på teknisk systemsikkerhet.

Sikkerhetsbehov:

a) Hva antas om grad av nødvendig sikkerhet for ulike tjenester?

Et system er ikke sterkere enn sitt svakeste ledd, og systemer kan svikte dersom alle antakelser ikke er oppfylt. For eksempel antas det i denne oppgaven at systemleverandører ikke er korrupte, at de som jobber med å utvikle og drive systemene følger sine plikter og ikke misbruker sin tilgang til informasjon, samt at sluttbrukere ikke låner bort sin identitet til andre. Veldig mange sikkerhetsantakelser kan i teorien slå feil, og alle disse vil ikke diskuteres i denne rapporten. Det som er av interesse for oppgaven er de antakelser som går på teknisk sikkerhet, derfor antas det i resten av oppgaven at systemleverandører og

mennesker som behandler informasjonssystemer og sikkerhetsrelatert informasjon oppfyller aller krav som stilles til de og at de har tilfredsstillende sikkerhetsrutiner på plass. Det som da kan gå feil er at de tekniske løsningene svikter, for eksempel at inntrengere lykkes i å finne hull i sikkerhetsløsningene. Et punkt som ser på konsekvenser om slike sikkerhetsantakelser ikke slår til er inkludert i seksjon for organisering og sikkerhetsantakelser.

Systemsvikt:

a) Hva er konsekvensene om sikkerhetsantakelsene ikke slår til?

Brukernes mulighet for *mobilitet* kan virke inn på systemenes utbredelse, altså i hvilken grad man kan forflytte seg mellom ulike brukerterminaler og lokasjoner og fremdeles få tilgang til de tjenestene man vanligvis har tilgang til. Man skal for eksempel kunne levere sin selvangivelse fra hvilken som helst lokasjon og hvilken som helst maskin. Et punkt er inkludert som ser på hvor lett det er å benytte tjenester fra nye lokasjoner og med nytt utstyr, men siden punktet ikke går direkte på tekniske sikkerhetsaspekt er punktet viet liten plass.

Mobilitet:

a) Hvor lett er det å benytte tjenester fra nye lokasjoner og med nytt utstyr?

Alle spørsmål nevnt så langt samles i en seksjon kalt organisering og sikkerhetsantakelser, som altså inneholder mye teori om hvordan systemene er realisert, hvilke løsninger som er valgt og hvordan de tilbyr sikkerhet. Seksjonen er ment å skulle gi den bakgrunnsinformasjon som er nødvendig for å forstå systemene og for å kunne drøfte løsningene nærmere.

Videre i oppgaveteksten nevnes *meldingskompleksitet*. Systemenes meldingskompleksitet er interessant å studere nærmere, og kan omfatte blant annet hvordan meldinger utveksles ved autentisering og annen kommunikasjon, hva de inneholder og hvordan de beskyttes under sending. Hvordan meldingsutvekslingen ser ut er fullstendig avhengig av valgt autentiseringsløsning, og vil være ulik for systemene. Kanskje har det ene systemet en mer optimal eller sikrere meldingsutveksling enn det andre, kanskje ikke. Spørsmål som går på meldingskompleksitet er samlet i en seksjon kalt nettopp meldingskompleksitet, to punkter ser på meldingenes gang og to på sikring av meldingene.

Meldingenes gang:

a) Hvordan går meldingene ved autentisering?
b) Hvordan går meldingene ved kommunikasjon med brukersted?

Sikring av meldingene:

a) Kan sensitiv informasjon leses ut av meldinger på avveie?
b) Hvilke mekanismer sikrer meldingene?

Et annet viktig aspekt er *robusthet mot feilsituasjoner*. Et identitetsforvaltningssystem bør ikke bryte sammen hver gang en feilsituasjon inntreffer, men bør ha mekanismer som håndterer i alle fall de vanligste feilsituasjonene. Et robust system må være skalert for det antall brukere og transaksjoner det kan komme til å oppleve, og flaskehalser bør identifiseres og tas hensyn til. Mulige situasjoner som kan oppstå bør identifiseres og det bør vurderes hva systemene gjør for å sikre robusthet, samt hvilken tilgjengelighet systemene vil ha. Et system som ikke er robust mot de vanligste feilsituasjoner er et ustabilt system, og robusthet er derfor et viktig kriterium i en systemanalyse. Spørsmål som går på systemrobusthet er samlet i en seksjon kalt robusthet mot feilsituasjoner. Seksjonen inneholder punkter om feilsituasjoner, tilgjengelighet og flaskehalser.

Feilsituasjoner:

a) Er det mulig å gjøre systemet utilgjengelig ved diverse angrep?
b) Hvor mange brukere, brukersteder eller transaksjoner er systemet designet for å håndtere?
c) Hva skjer om forbindelsen brytes eller systemet av andre grunner går ned?

Tilgjengelighet:

a) Hvor stor tilgjengelighet forventes systemet å ha?
b) Hva gjøres for å sikre høy tilgjengelighet?

Flaskehalser:

a) Finnes det deler av systemet som har stor innvirkning på den totale ytelsen?

Avgjørende for om systemene tas i bruk er blant annet *implementerings- og driftskostnader* assosiert med systemene, både for brukersteder og sluttbrukere. Hvilke kostnader som er assosiert med systemene er viet forholdsvis liten plass i denne oppgaven, men er omtalt i en egen seksjon kalt implementerings- og driftskostnader for å gjøre systembeskrivelsen mer fullstendig. Tre spørsmål er inkludert, men er ikke gjenstand for videre diskusjon i rapporten.

Kostnader til implementering og drift:

a) Hvilke kostnader ha man sentralt?
b) Hvilke kostnader har brukerstedene?
c) Hvilke kostnader har sluttbrukere?

En annen avgjørende faktor for om systemene tas i bruk er *brukervennlighet*. Altså hvor lett det er å ta i bruk systemene for sluttbrukere og for brukersteder som ønsker å tilby sikre tjenester. Til tross for at denne rapporten har hovedvekt på organisering, meldingsutveksling og sikkerhet er noen spørsmål knyttet til brukervennlighet inkludert, siden brukervennlighet er et avgjørende moment for systemenes popularitet. Spørsmålene er samlet i en egen seksjon, og går på krav til brukerutstyr, hvordan man kommer i gang med bruk av systemene, samt hvor godt brukergrensesnittet er. Punktet er viet forholdsvis liten plass og er ikke gjenstand for en grundigere analyse.

Krav til brukerutstyr:

a) Er løsningen plattformuavhengig med hensyn til operativsystem og nettleser?
b) Stilles det krav til brukerens maskinvare/brukerterminal?

Å ta i bruk systemet:

a) Hvordan kommer brukersteder i gang?
b) Hvordan kommer sluttbrukere i gang?

Brukergrensesnitt:

a) Er menyene intuitive?
b) Får brukeren tydelig beskjed om hva som skjer?

Med utgangspunkt i denne drøftingen settes det opp en tabell med kriterier, organisert i fem seksjoner og en rekke underpunkter som inneholder ett eller flere spørsmål. Kriteriene er utformet som spørsmål, de samme spørsmålene som er identifisert i dette avsnittet. Disse skal besvares for hvert av de to identitetsforvaltningssystemene, og videre er resultatene gjenstand for sammenligning og drøfting. De mest belyste områdene i resten av denne rapporten er organisering og sikkerhetsantakelser, meldingskompleksitet og robusthet mot feilsituasjoner. Hvert av disse områdene er viet en egen seksjon, og det er også temaene implementerings- og driftskostnader samt brukervennlighet, selv om disse anses som mindre sentrale temaer.

3.2 Kriterier

I tabell 3.1 følger en samlet oversikt over spørsmålene definert i kapittel 3.1, gruppert i seksjoner etter tema. Disse spørsmålene skal i de kommende kapitlene skal besvares for Sikkerhetsportalen og FEIDE.

1) ORGANISERING OG SIKKERHETSANTAKELSER
1) Arkitektur a) Hvilke delsystemer eksisterer? b) Hvilke av disse kommuniserer med hverandre? c) Hvor i systemet er sikkerheten realisert?
2) Anvendelsesområder a) Hvor brukes systemet i dag, og i morgen? b) Hvilke sikkerhetstjenester tilbys?
3) Standardisering a) Hvilke åpne standarder er systemet basert på? b) Er systemet i ferd med å bli en standard innen visse sektorer?
4) Autentisering a) Hvilke autentiseringsløsninger benyttes? b) Hvilke krav stilles til brukernavn og passord / nøkler og sertifikater?
5) Personvern a) Hvilke personopplysninger lagres, og hvor lagres de? b) Hvilke rutiner og mekanismer er på plass? c) Logges transaksjoner, er de i så fall sikret mot endringer? d) Ivaretas personverninteresser generelt, og oppfylles personopplysningsloven?
6) Sikkerhetsbehov a) Hva antas om grad av nødvendig sikkerhet for ulike tjenester?
7) Systemsvikt a) Hva er konsekvensene om sikkerhetsantakelsene ikke slår til?
8) Mobilitet a) Hvor lett er det å benytte tjenester fra nye lokasjoner og med nytt utstyr?
2) MELDINGSKOMPLEKSITET
1) Meldingenes gang a) Hvordan går meldingene ved autentisering? b) Hvordan går meldingene ved kommunikasjon med brukersted?
2) Sikring av meldingene a) Kan sensitiv informasjon leses ut av meldinger på avveie? b) Hvilke mekanismer sikrer meldingene?
3) ROBUSTHET MOT FEILSITUASJONER
1) Feilsituasjoner a) Er det mulig å gjøre systemet utilgjengelig ved diverse angrep? b) Hvor mange brukere, brukersteder eller transaksjoner er systemet designet for å håndtere? c) Hva skjer om forbindelsen brytes eller systemet av andre grunner går ned?
2) Tilgjengelighet a) Hvor stor tilgjengelighet forventes systemet å ha? b) Hva gjøres for å sikre høy tilgjengelighet?

3) Flaskehalser a) Finnes det deler av systemet som har stor innvirkning på den totale ytelsen?
4) IMPLEMENTERINGS- OG DRIFTSKOSTNADER
1) Kostnader til implementering og drift a) Hvilke kostnader har man sentralt? b) Hvilke kostnader har brukerstedene? c) Hvilke kostnader har sluttbrukere?
5) BRUKERVENNLIGHET
1) Krav til brukerutstyr a) Er løsningen plattformuavhengig med hensyn til operativsystem og nettleser? b) Stilles det krav til brukerens maskinvare/brukerterminal?
2) Å ta i bruk systemet a) Hvordan kommer brukersteder i gang? b) Hvordan kommer sluttbrukere i gang?
3) Brukergrensesnitt a) Er menyene intuitive? b) Får brukeren tydelig beskjed om hva som skjer?

Tabell 3.1: Momenter som inngår i en sammenlignende analyse.

4 Sikkerhetsportalen

Sikkerhetsportalen ble lansert 15. desember 2005, og skal på sikt tilby et sett av sikkerhetstjenester som gjør det enklere for det offentlige å benytte funksjonalitet for autentisering, signering og kryptering i egne løsninger. Per i dag tilbys støtte for autentisering samt en registreringstjeneste, fra 1.7.2006 planlegges støtte for signering og tiltrodd arkivering, senere også støtte for kryptering. Sikkerhetsportalen er basert på PKI, en infrastruktur som realiserer sikker kommunikasjon ved hjelp av private og offentlige nøkler.

For å besvare spørsmålene i tabell 3.1 benyttes først og fremst informasjon fra Brønnøysundregistrenes hjemmesider om Sikkerhetsportalen [12]. I tillegg benyttes informasjon fra andre dokumenter og føringer på hvordan Sikkerhetsportalen skal tas i bruk i offentlig sektor. Kravspesifikasjonen for felles Sikkerhetsportal i offentlig sektor produsert av Brønnøysundregistrene er ikke et offentlig tilgjengelig dokument, og er derfor ikke en del av kildegrunnlaget for denne rapporten. Denne kravspesifikasjonen bygger imidlertid sterkt på kravspesifikasjonen for PKI i offentlig sektor [17], som benyttes som kilde under en rekke punkter. Siden Sikkerhetsportalen oppfyller kravspesifikasjonen for PKI i offentlig sektor vil alle krav som stilles i denne også være oppfylt av Sikkerhetsportalen. I enkelte tilfeller vil Sikkerhetsportalen stille strengere krav enn kravspesifikasjonen for PKI, og enkelte steder utdype kravene noe mer.

Her følger spørsmål og svar om Sikkerhetsportalen, kategorisert i fem seksjoner og med en rekke underpunkter. Først betraktes organisering og sikkerhetsantakelser, deretter følger meldingskompleksitet, robusthet mot feilsituasjoner, implementerings- og driftskostnader og til slutt brukervennlighet. Figur 4.1 [12] viser Sikkerhetsportalens logo.

Figur 4.1: Sikkerhetsportalens logo.

4.1 Organisering og sikkerhetsantakelser

Denne seksjonen inneholder spørsmål som går på hvordan Sikkerhetsportalen er organisert og realisert. Svarene på spørsmålene er ment å gi nødvendig bakgrunnsinformasjon om Sikkerhetsportalen for å kunne ta fatt på en systemanalyse. Første punkt går på systemarkitektur, nærmere bestemt hvordan Sikkerhetsportalen er bygd opp, hvilke systemkomponenter som kommuniserer med hverandre, og hvor sikkerheten er realisert. Punkt nummer to tar for seg anvendelsesområder, samt hvilke tjenester som tilbys. Tredje punkt ser på standarder og standardisering, og fjerde punkt på autentiseringsløsninger. Punkt fem besvarer spørsmål knyttet til personvern og behandling av personopplysninger, punkt seks ser på muligheter for å dekke ulike tjenesters krav til sikkerhet. Punkt sju drøfter muligheten for at sikkerhetsantakelser og rutiner kan svikte, og punkt åtte vurderer Sikkerhetsportalen med tanke på mobilitet.

4.1.1 Arkitektur

a) Hvilke delsystemer eksisterer?

Brukersted
Et brukersted representerer en offentlig etat eller en kommune som ønsker å tilby sikre elektroniske tjenester til sine brukere. Hvert brukersted har et grensesnitt mot den sentrale Sikkerhetsportalen, en programvaremodul som integreres ved brukerstedet for å få tilgang til tjenester fra Sikkerhetsportalen. Denne modulen kalles for en *integrasjonsmodul*, og kan bestå av en "eFactory Security Client" fra SPAMA og en "SAML Affiliate Agent" fra Computer Associates. Klienten støtter autentisering og signering, og kommuniserer med en "eFactory Security Server" hos BBS. Andre typer programvare kan også brukes, men løsningen nevnt her er en ferdigpakke. Sluttbrukerne trenger kun å forholde seg til det aktuelle brukerstedet, siden integrasjonsmodulen tar seg av all kommunikasjon mot Sikkerhetsportalen. For brukerstedene finnes det også en *kundeweb*, hvor brukeradministrator kan administrere ulike forhold og få tilgang til rapporter og driftsstatistikker, fakturainformasjon og mye mer.

Bruker
En sluttbruker av Sikkerhetsportalens tjenester er en person som ønsker å benytte sikre elektroniske tjenester fra det offentlige, det vil si som har behov for autentisering, signering eller kryptering. En sluttbruker av Sikkerhetsportalens må ha tilgang til en datamaskin med tilhørende programvare. Han må også være i besittelse av et digitalt sertifikat utstedt av en PKI-leverandør, som gjør han i stand til å identifisere seg for tjenesten. Dette sertifikatet kan enten befinne seg på brukerens datamaskin, eller det kan være integrert i et smartkort. Hvis sertifikatet befinner seg i et smartkort kreves det at brukeren også har en smartkortleser som kobles til datamaskinen.

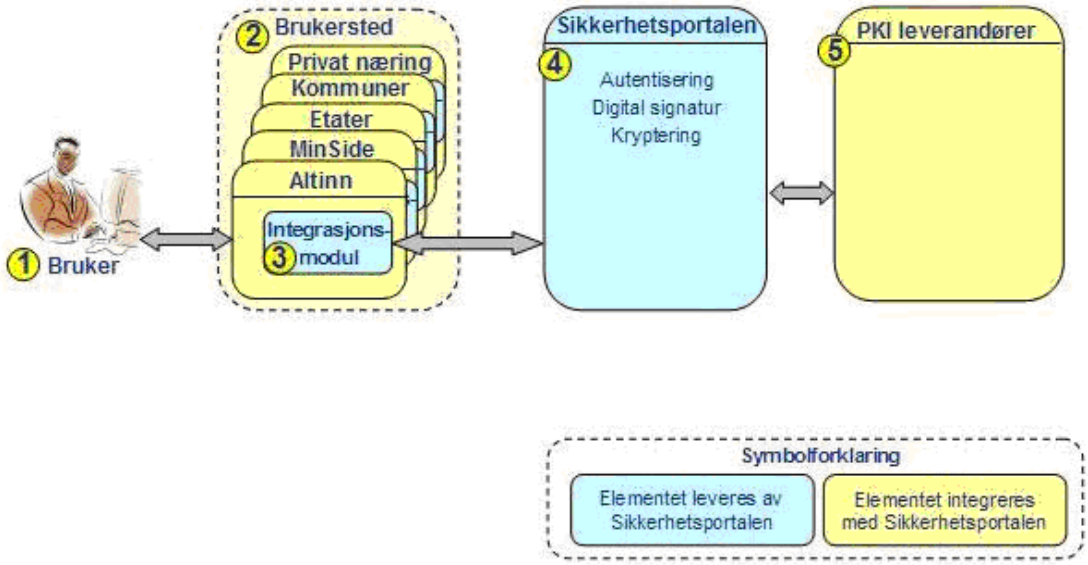
Sikkerhetsportalen
Den sentrale Sikkerhetsportalen tilbyr et sett av sikkerhetstjenester som gjør det enklere og billigere for brukersteder å integrere autentisering, signering og kryptering i egne tjenester. Sikkerhetsportalen har en standardisert integrasjonsmodul hos hvert brukersted, som kommuniserer med den sentrale sikkerhetsserveren hos BBS. Sikkerhetsserveren består av en "eFactory Security Server" fra SPAMA, og en "eTrust SiteMinder" fra Computer Associates. Sikkerhetsserveren har støtte for standard metoder for brukerautentisering og SSO, samt innebygd støtte for SAML. Sikkerhetsportalen har et eget *tiltrodd digitalt arkiv* hvor viktige dokumenter og annen informasjon lagres, signert og tidsstemplet.

PKI-leverandør
Sikkerhetsportalen bruker tjenester fra ulike PKI-leverandører for å kunne tilby autentisering, kryptering og digital signatur til sine brukersteder. Disse leverandørene må være godkjente i den forstand at de støtter bruk av digitale sertifikater i henhold til kravspesifikasjon for PKI i offentlig sektor [17]. PKI-leverandører utsteder sertifikater for brukere, og tilbyr i den forbindelse en registreringstjeneste. På forespørsel henter de også brukeres offentlige nøkler i egne eller offentlige kataloger, og sender disse til Sikkerhetsportalen. Brukere velger selv hvilken PKI-leverandør de vil bestille sertifikat fra, basert på hvilket sertifikat de har behov for. Det skal finnes en webbasert oversikt over tilgjengelige PKI-leverandører, hvilke sertifikattyper de støtter og linker til leverandørene. Avhengig av sikkerhetsnivå på sertifikatet mottar man det ved

personlig oppmøte, i posten, eller ved å laste det ned elektronisk. Commfides Norge AS har inngått avtale med BBS om leveranse av PKI-tjenester til Sikkerhetsportalen, en avtale som innebærer at Commfides Norge vil utstede digitale sertifikater som kan brukes i Sikkerhetsportalen [18]. Sikkerhetsportalen har også en avtale med Siemens Business Services om å levere sertifikater til Sikkerhetsportalen [19], og det forhandles visstnok med flere PKI-leverandører, deriblant Buypass og Bank-ID. Løsningen Siemens Business Services tilbyr benytter sertifikater fra ZebSign.

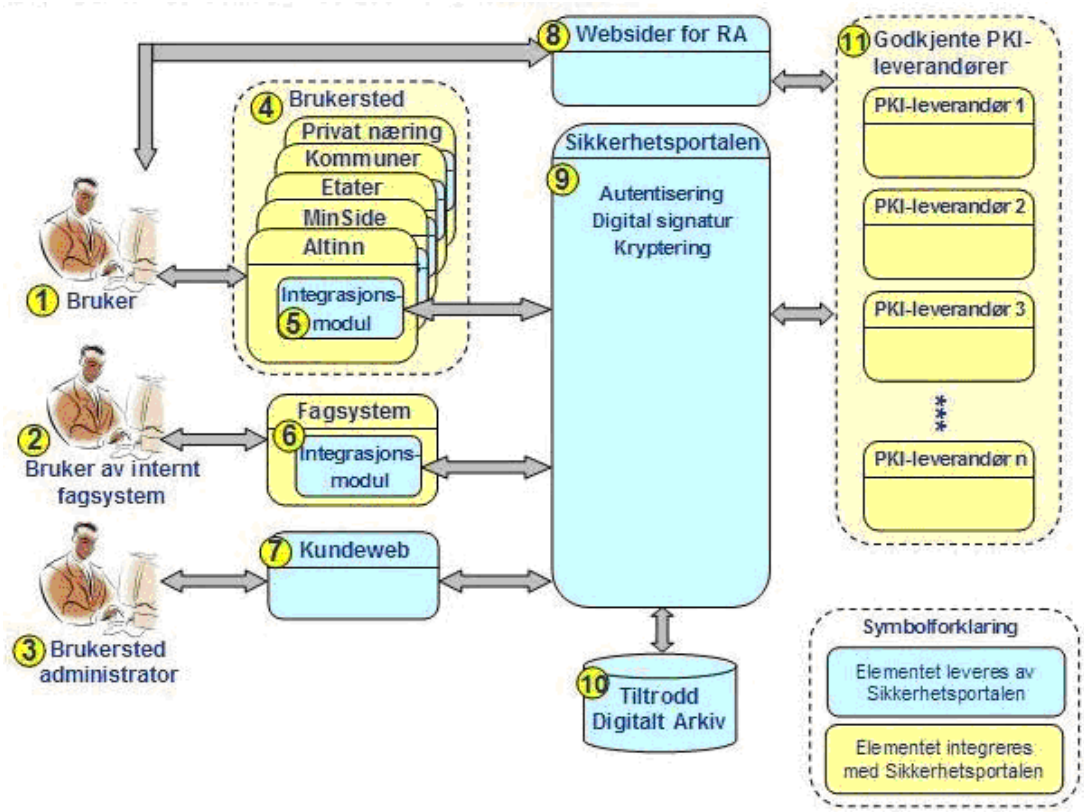
b) Hvilke av disse kommuniserer med hverandre?

Figur 4.2 [12] viser hovedelementene i systemet rundt Sikkerhetsportalen, og hvor den viktigste kommunikasjonen går. En bruker går til et brukersted på nett, og bes om å bevise sin identitet. Det foregår altså kommunikasjon mellom brukeren og brukerstedet. Brukerstedet på sin side kommuniserer også med Sikkerhetsportalen via integrasjonsmodulen. Sikkerhetsportalen på sin side kommuniserer med ulike PKI-leverandører for å verifisere sertifikater. Altså kommuniserer brukeren kun med brukerstedet, og slipper å forholde seg til Sikkerhetsportalen eller tilgjengelige PKI-leverandører. I noen tilfeller kan det imidlertid være interaksjon mellom brukere og PKI-leverandører, for eksempel ved bestilling av sertifikater. Brukerstedet har kun direkte kontakt med Sikkerhetsportalen, og slipper å forholde seg til PKI-leverandører som står bak og bistår med tjenester. Det går aldri informasjon direkte mellom to brukersteder, det er sikkerhetsserveren som overfører informasjon til brukerstedene. Ved SSO mellom to brukersteder er det teknisk sett kun SSO mellom sikkerhetsserveren og brukerstedet.



Figur 4.2: Elementer i Sikkerhetsportalen.

Figur 4.3 [12] viser litt flere detaljer i organiseringen av Sikkerhetsportalen. Her ser man også Sikkerhetsportalens kopling mot tiltrodd digitalt arkiv for arkivering av informasjon, og hvordan en sluttbruker også kan være en bruker av et internt fagsystem eller en administrator med tilgang til en kundeweb. Websider for RA (Registration Authority)er en oversikt over tilgjenglige PKI-leverandører med informasjon om sertifikattyper og lenker for bestilling av sertifikater.



Figur 4.3: Elementene i Sikkerhetsportalen med litt flere detaljer.

c) Hvor i systemet er sikkerheten realisert?

For å benytte tjenester som krever innlogging via Sikkerhetsportalen må en sluttbruker legge frem et sertifikat som viser hvem han er og hvilke rettigheter han har. Brukerstedets integrasjonsmodul sjekker sertifikatet mot Sikkerhetsportalen, som benytter tjenester fra riktig PKI-leverandør for å verifisere sertifikatets gyldighet.

Sikkerheten er fordelt på flere deler av Sikkerhetsportalsystemet. Mye av den er naturlig nok realisert i den sentrale Sikkerhetsportalen, og i brukerstedets integrasjonsmodul. I tillegg er systemet avhengig av at tjenestene fra PKI-leverandørene er til å stole på, blant annet må man være fullstendig sikker på at sluttbrukers sertifikat inneholder en korrekt forbindelse mellom den aktuelle bruker og hans offentlige nøkkel. Dette skal ikke være noe problem da godkjente PKI-leverandører for Sikkerhetsportalen skal oppfylle kravspesifikasjon for PKI i offentlig sektor [17].

4.1.2 Anvendelsesområder

a) Hvor brukes systemet i dag, og i morgen?

Bruk av Sikkerhetsportalen skal være obligatorisk for alle statlige virksomheter med behov for elektronisk ID og signatur [10]. I tillegg er det sterkt anbefalt for kommuner å benytte løsningen. Innen utgangen av 2006 skal det utarbeides ordninger som bidrar til at offentlige brukersteder tar i bruk Sikkerhetsportalens tjenester og integrerer disse i digitale tjenester. Leverandøren av Sikkerhetsportalen står også fritt til å selge Sikkerhetsportalens tjenester på det private markedet, så i utgangspunktet er det åpent for alle aktører både i offentlig og privat sektor å benytte Sikkerhetsportalen.

Alle norske borgere er potensielle sluttbrukere av tjenester fra Sikkerhetsportalen. Derfor er det viktig at sluttbrukere av Sikkerhetsportalen ikke trenger å vite hva Sikkerhetsportalen gjør, hvordan den fungerer eller hvilke avtaler som ligger til grunn. All interaksjon foregår mellom brukeren og det enkelte brukerstedet, og Sikkerhetsportalen er ikke synlig for brukeren.

Næringslivsportalen Altinn er pilotbruker for Sikkerhetsportalen, og representerer det første brukerstedet. Altinn er et felles nettsted for dialog med det offentlige, man skal blant annet kunne levere offentlige skjemaer over Internett. Næringslivet skal også kunne sende data direkte fra sine økonomi- og regnskapssystemer som Altinn videresender til statens saksbehandlingssystemer. Siden 3.2.2006 har brukere av Altinn kunnet logge inn ved hjelp av Sikkerhetsportalen.

Borgerportalen MinSide, som i utgangspunktet skulle vært lansert i desember 2005, vil også benytte tjenester fra Sikkerhetsportalen. MinSide skal gi norske borgere enkel tilgang til offentlige elektroniske tjenester. I første omgang vil et begrenset utvalg statlige elektroniske tjenester være tilgjengelige, men etter hvert vil MinSide utvides med flere statlige og kommunale tjenester. I følge en pressemelding fra Fornyings- og administrasjonsdepartementet blir MinSide allikevel ikke lansert i løpet av første kvartal 2006 [20], men ingen ny dato for lansering er publisert. Så langt er det bare en mindre forsøksgruppe som har tatt i bruk tjenestene fra MinSide.

b) Hvilke sikkerhetstjenester tilbys?

Sikkerhetsportalen skal tilby autentisering, signering og kryptering. Autentisering vil si å identifisere en bruker, noe Sikkerhetsportalen gjør ved hjelp av digitale sertifikater. Signering brukes for å knytte en persons elektroniske identitet til informasjon som skal sendes, og kryptering brukes for å hindre at andre enn mottaker kan lese innholdet i informasjon som sendes. Brukerstedenes integrasjonsmodul håndterer autentisering av brukere, digital signering og SSO mot andre brukersteder.

En viktig forutsetning for disse sikkerhetstjenestene er at hver bruker har en elektronisk identitet, et digitalt sertifikat som unikt knytter sammen person og nøkler. I en PKI, det vil si i en infrastruktur basert på offentlig-nøkkelkryptografi, har hver bruker en privat nøkkel som kun denne brukeren kjenner og som skal være minst like sikker som brukerens fysiske håndsignatur. En tilsvarende offentlig nøkkel er tilgjengelig for allmennheten, og brukes for å dekryptere meldinger kryptert med brukerens private nøkkel.

Sikkerhetsportalen støtter SSO, som gjør at man trenger å logge på kun én gang selv om man ønsker å benytte flere ulike tjenester som bruker Sikkerhetsportalen. Sikkerhetsportalen autentiserer brukeren ved førstegangs pålogging, og utsteder samtidig et bevis som andre brukersteder senere kan akseptere.

Sikkerhetsportalen tilbyr en registreringstjeneste for digitale sertifikater, per i dag kun for sertifikater av typen ”Person-Standard”, men fra 31.12.2006 også for sertifikater av typen ”Person-Høyt” og ”Virksomhet”. Det finnes en webtjeneste hvor man kan få informasjon om PKI-leverandører og deres sertifikater, samt søke om å få utstedt digitale sertifikater.

Sikkerhetsportalen har et såkalt tiltrodd digitalt arkiv, hvor kryptert tidsstemplet informasjon arkiveres sammen med nødvendige metadata. Arkivet sikrer konfidensialitet, sporing og sikkerhet, og opptrer som en tiltrodd tredjepart mellom brukersted og bruker. En bruker som leverer selvangivelsen sin via Altinn godkjenner og signerer selvangivelsen, deretter lagres den i det tiltrodde digitale arkivet.

Brukerstedene har en kundeweb hvor brukeradministrator kan administrere og finne informasjon fra Sikkerhetsportalen. Dette kan være rapporter, driftstatistikker, fakturainformasjon, kundeservicerapporter, søk mot tiltrodd digitalt arkiv, og mye annen informasjon knyttet til driften av systemet.

4.1.3 Standardisering

a) Hvilke åpne standarder er systemet basert på?

Åpne standarder er viktig for å sikre grensesnitt for kobling mot andre tjenester. EUs definisjon for åpenhet setter fire minimumskrav for at en standard skal betraktes som en åpen standard [21]. Først av alt må standarden være anerkjent og vedlikeholdes av en ikke-kommersiell organisasjon. Standarden må være publisert med tilgjengelig dokumentasjonen, gratis eller mot en ubetydelig avgift, og det må være tillatt å kopiere, distribuere og bruke standarden. Videre må den intellektuelle rettighet knyttet til standarden være gjort ugjenkallelig tilgjengelig uten royalty, og det må ikke være noen forbehold om gjenbruk av standarden. I praksis anses standarder utviklet av offisielle standardiseringsorganisasjoner som åpne standarder.

Sikkerhetsportalen støtter flere åpne standarder. Blant annet bruker Sikkerhetsportalen ID-FF (Identity Federation Framework) og ID-WSF (Identity Web Service Framework) som rammeverk for elektronisk identitet til brukere og webtjenester [12]. Spesifikasjonene for ID-FF og ID-WSF er utviklet av Liberty Alliance [22], en sammenslutning av globale organisasjoner som jobber med utfordringer knyttet til elektronisk identitet og identitetsbaserte webtjenester. I tillegg støttes SAML fra OASIS, et rammeverk basert på XML (eXtensible Markup Language) for utveksling av autentiserings- og autorisasjonsinformasjon.

Brukerstedenes integrasjonsmodul tilbys for både .NET og Java, og den kommuniserer med sikkerhetsserveren hos leverandøren via Web Services og HTTPS. En Web Service er en plattformuavhengig standard for informasjonsutveksling basert på XML. HTTPS (Secure HTTP) er standard HTTP (Hypertext Transfer Protocol) utvekslet over en SSL-kryptert sesjon.

b) Er systemet i ferd med å bli en standard innen visse sektorer?

Ja, Sikkerhetsportalen er i ferd med å bli en standard i offentlig sektor, det vil si i statlige og kommunale virksomheter. Bruk av Sikkerhetsportalen vil være obligatorisk for alle statlige virksomheter med behov for elektronisk ID og elektronisk signatur, og er anbefalt også for kommuner.

4.1.4 Autentisering

a) Hvilke autentiseringsløsninger benyttes?

Sikkerhetsportalen benytter digitale sertifikater for å autentisere sine brukere, som er en kobling mellom brukerens identitet og dens offentlige nøkkel, signert av en tiltrodd sertifiseringsautoritet. Alle som kjenner sertifiseringsautoritetens offentlige nøkkel kan verifisere at koblingen er signert av denne, og vil ha tillit til brukerens offentlige nøkkel. Sertifikatene kan installeres på brukerens datamaskin, eller de kan integreres i smartkort.

Sikkerhetsportalen skal på sikt støtte tre ulike sertifikater, tilpasset ulike sikkerhetsnivå. De tre typene er "Person-Standard", "Person-Høyt" og "Virksomhet", og er definert i kravspesifikasjon for PKI i offentlig sektor [17]. Sertifikatene kan benyttes til autentisering, signering og kryptering. Det som skiller sertifikater av de ulike typene er i hvilken grad man kan ha tillit til de, og i hvilke sammenhenger de kan benyttes. "Person-Standard" brukes der det er behov for rimelig grad av sikkerhet om identiteten til den man kommuniserer med eller der skaden ved kompromittering er middels stor. "Person-Høyt" og "Virksomhet" brukes der det er behov for stor grad av sikkerhet om identiteten til den man kommuniserer med eller der skaden ved kompromittering er stor. "Person-Standard" og "Person-Høyt" er ment for privatpersoner, mens "Virksomhet" er ment for virksomheter. De tre typene har ulike praksiser for identifisering og registrering av sertifikateier, og for hvordan private nøkler og sertifikater utleveres. Det kan være forskjeller i hvilke algoritmer og nøkkellengder som brukes, hvordan nøkkelgenerering foregår, antall nøkkelpar som benyttes og hvordan nøklene kan brukes, hvordan de private nøklene beskyttes, og hvordan sertifikater trekkes tilbake.

Når en privat nøkkel ligger lagret i et smartkort beskyttet med pinkode er det relativt sikkert at bare eieren kan benytte nøkkelen. Private nøkler som ligger lagret som en fil på en datamaskin beskyttes også med pinkode eller passord, men det er større risiko for at slike nøkler kompromitteres, og de gir derfor ikke samme tillit.

b) Hvilke krav stilles til nøkler og sertifikater?

I følge kravspesifikasjon for PKI i offentlig sektor [17] skal en utsteder av et *"Person-Standard"* sertifikat oppfylle aktuelle krav i lov om elektronisk signatur [23] og forskrift om krav til utsteder av kvalifiserte sertifikater mv [24]. Ved registrering skal det verifiseres at personen finnes i det norske folkeregisteret, og det skal sikres at utlevering av nøkler, koder, passord og sertifikater skjer til riktig person, ved utsendelse per post til folkeregistrert adresse eller ved like sikker elektronisk utsendelse. Et sertifikat av typen *"Person-Høyt"* skal være et kvalifisert sertifikat og sertifikatutsteder skal oppfylle registrerings- og utleveringsprosedyrer for kvalifiserte sertifikater, blant annet krav om personlig fremmøte. En utsteder av et *"Virksomhet"* sertifikat skal oppfylle aktuelle krav i lov om elektronisk signatur [23] og forskrift om krav til utsteder av kvalifiserte sertifikater mv [24]. Virksomheten skal entydig kunne identifiseres ved at sertifikatet utstyres med organisasjonsnummer fra Enhetsregisteret i henhold til SEID-prosjektets sertifikatprofil [25]. Det skal videre sikres at utlevering av nøkler med tilhørende passord og sertifikat skjer til en person som har rett til å motta dette på vegne av virksomheten, ved personlig oppmøte.

Samtlige sertifikater skal kunne inneholde de norske tegnene æ, ø og å. Sertifikatene bør støtte brukerspesifiserte utvidelser, og nødvendige rotsertifikater for verifisering skal distribueres på en sikker måte. Algoritmer og nøkkellengder skal spesifiseres av leverandøren. Asymmetriske nøkler bør være basert på RSA, og de bør ha minimum 1024 bits lengde. Samtlige signerings- og krypteringsalgoritmer må være av god kvalitet. For asymmetriske krypteringsalgoritmer skal det være umulig å utlede den private nøkkelen fra den offentlige nøkkelen, for symmetriske krypteringsalgoritmer skal det være umulig å finne nøkkelen ved å analysere den forvrengte teksten, og for hashalgoritmer skal det være veldig usannsynlig at to ulike dokumenter genererer samme resultat. Nøkkellengde og oppbygging av krypteringsalgoritmen har mye å si for kvaliteten på krypteringen.

Private nøkler og sertifikater kan genereres av en PKI-leverandør, eller av programvare eller utstyr levert av en slik leverandør. Nøkler generert av brukeren selv lagres i en kryptert fil på brukerens datamaskin. Hos en sertifikatutsteder kan nøkler genereres i et beskyttet system og så plasseres for eksempel på et smartkort eller i en datafil som overleveres eieren. Nøkler kan også genereres direkte på smartkortet, slik at den private nøkkelen aldri forlater dette kortet. Nøkkeleieren bør selv få bestemme passord og pinkoder, og det bør brukes kontrollprogramvare som sørger for at kodene er av tilfredsstillende kvalitet. Et og samme nøkkelpar kan brukes for både autentisering, signering og kryptering. Eventuelt kan brukere ha flere separate nøkkelpar, for eksempel en for hver av de tre sikkerhetsfunksjonene. Dette gir større trygghet for at ens nøkler ikke blir misbrukt, som ved at man uten å være klar over det signerer et dokument i det man autentiserer seg for et ukjent system.

Private nøkler må beskyttes i henhold til kravspesifikasjon for PKI i offentlig sektor [17]. Tilgang til nøkler av sikkerhetsnivå ”Person-Standard” skal kreve autentisering, og brukeren skal selv ha mulighet til å velge om hver operasjon som involverer private nøkler skal godkjennes. Private nøkler tilhørende ”Person-Standard” må som et minimum lagres kryptert. Tilgang til nøkler av sikkerhetsnivå ”Person-Høyt” skal kreve minimum tonivå autentisering, hvor det ene nivået er noe brukeren er i fysisk besittelse av og som ikke er elektronisk kopierbart. Brukeren skal videre godkjenne hver operasjon som involverer private nøkler ved å autentisere seg. Private nøkler må aldri finnes i klartekst i registre som kan kompromitteres eller på annen måte gi opphav til misbruk. For private nøkler av sikkerhetsnivå ”Virksomhet” skal det være mulig å realisere tilgangskontroll, og virksomheten skal selv godkjenne operasjoner som involverer private nøkler.

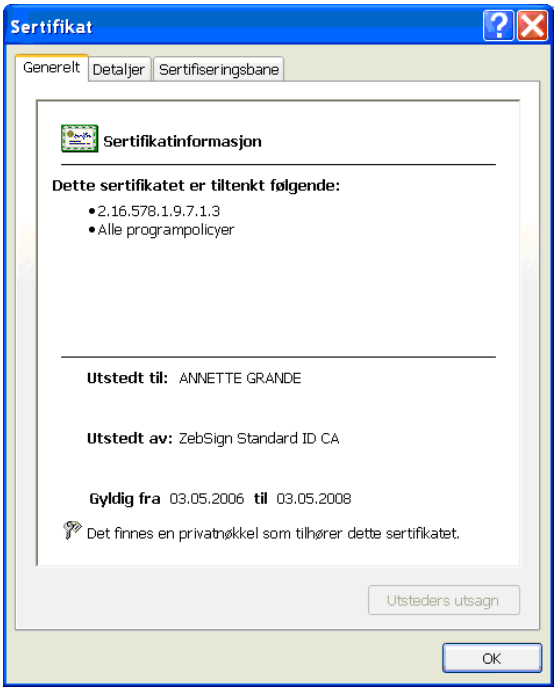
Selv om ingen andre enn eieren skal kjenne passord og private nøkler kan det skje at de kommer på avveie. Når en nøkkel eller et passord kompromitteres må sertifikater utstedt av den tapte nøkkelen ikke godtas lenger, og det må utstedes nye sertifikater. Videre må det gamle sertifikatet knyttet til den kompromitterte private nøkkelen tilbakekalles. Tilbakekalling av sertifikater kan forekomme når man mistenker uautorisert tilgang til private nøkler uten å ha konkrete bevis, eller når man kjenner til at et sertifikat misbrukes. Andre tilfeller som medfører tilbakekalling av sertifikater kan være at sertifikatholder skifter navn eller status, at han ikke lenger er berettiget til å ha sertifikatet, eller at sertifikatets gyldighetsperiode er gått ut. Ved melding om behov for tilbakekalling sperrer sertifikatutstederen sertifikatet ved å utstede signerte og tidsstemplete tilbaketrekkingslister. Dersom passord eller pinkoder som brukes for å få tilgang til private nøkler mistenkes kompromittert må disse endres umiddelbart.

Sertifikatene ZebSign i dag utsteder for bruk med Sikkerhetsportalen er gyldige i to år, og i følge kravspesifikasjon for PKI er minimum levetid for alle sertifikattyper 13 måneder [17].

4.1.5 Personvern

a) Hvilke personopplysninger lagres, og hvor lagres de?

Data om brukere av Sikkerhetsportalen ligger lagret i deres sertifikater, utstedt fra den enkelte PKI-leverandør. Dette kan eksempelvis være informasjon som navn, adresse, e-postadresse og fødselsnummer. Brukere som ønsker å logge inn på Altinn via Sikkerhetsportalen må besøke nettsiden https://webra.bbs.no og bestille en engangskode som sendes i posten. Ved hjelp av denne engangskoden kan brukere bestille et sertifikat, en såkalt elektronisk ID, og en lenke til sertifikatet mottas på e-post. Sertifikatet lastes ned og installeres, og er deretter klart til bruk. Dagens sertifikater er utstedt av ZebSign som en ZebSign Standard ID i samsvar med kravspesifikasjon for PKI i offentlig sektor [17]. Figur 4.4 viser et slikt sertifikat, og tabell 4.1 viser hvilke felter sertifikatet inneholder.



Figur 4.4: Et ZebSign Standard ID sertifikat, utstedt for bruk med Sikkerhetsportalen.

Felter i sertifikatet	**Forklaring**
Versjon	X.509 versjonsnummer (V3)
Serienummer	Sertifikatets serienummer
Signaturalgoritme	Algoritme for signering (sha1RSA)
Utsteder	Navn på sertifikatutsteder (ZebSign Standard ID CA)
Gyldig fra	Start på gyldighetsperiode
Gyldig til	Slutt på gyldighetsperiode
Emne	Sertifikatemne

Fellesnøkkel	Brukerens offentlige nøkkel (1024 bits RSA nøkkel)
Hovedbegrensninger	Begrensninger
Nøkkelidentifikator for emne	Nøkkel-ID for emne
Sertifikatkriterier	Policy for sertifikatet
Alternativt navn for emne	Alternativt navn i form av e-postadresse
Nøkkelidentifikator for instans	Nøkkel-ID for instans
Informasjonstilgang for instans	Tilgang til sertifiseringsinformasjon
CRL-distribusjonspunkt	URL til hvor revokeringslistene distribueres
Bruk av nøkler	Spesifiserer hva nøklene kan brukes til
Avtrykksalgoritme	Algoritme for avtrykk (sha1)
Avtrykk	Avtrykk
Egendefinert navn	Brukerens navn

Tabell 4.1: Felter i et ZebSign Standard ID sertifikat utstedt for bruk med Sikkerhetsportalen.

En ZebSign Standard ID utstedt for Sikkerhetsportalen inneholder altså navn på sertifikatutsteder, samt navn, e-postadresse og unik identifikator for sertifikateieren, sertifikatets gyldighetsperiode, data nødvendig for fremstilling og verifisering av digital signatur og sertifikatets serienummer [26]. ZebSign oppbevarer relevante opplysninger om utstedelse og bruk av ZebSign Standard ID i 10 år, fra tidspunktet hvor levetiden på sertifikatet opphører eller trekkes tilbake. Sertifikatet legges i et eget register for sperrede ID'er. Sertifikater utstedt av ZebSign inneholder ikke sertifikateiers personnummer, men sertifikatene inneholder en unik identifikator som gjør det mulig for ZebSign å finne personnummeret til sertifikateieren på forespørsel fra brukersteder som har behov for dette [27].

Når begrepet personvern brukes innen informasjonssikkerhet snakkes det om at personlig identifiserbar informasjon og sensitiv informasjon samles og brukes kun for de bruksområder de opprinnelig var tiltenkt [28]. Personlig identifiserbar informasjon er informasjon som kan spores tilbake til et individ, som navn, personnummer, postadresse og e-postadresse. Sensitiv informasjon er informasjon som under visse omstendigheter krever spesiell beskyttelse, som finansiell og medisinsk informasjon, eller informasjon om religiøs og politisk oppfatning. Bekymringer knyttet til personvern er en av de mest betydningsfulle i forbindelse med digital identitetsforvaltning. Et økt omfang av personopplysninger og muligheten for samkjøring av ulike datakilder gjør det nødvendig med et godt personvern. Det må finnes begrensninger for innsamling av personopplysninger, og de opplysninger som benyttes må være av god kvalitet, beskyttes godt og behandles med ansvarlighet.

b) Hvilke rutiner og mekanismer er på plass?

Datatilsynet har laget en veiledning i informasjonssikkerhet for kommuner og fylker, som påpeker en rekke viktige momenter som angår sikkerhet [29]. Disse er også veldig aktuelle for Sikkerhetsportalen.

Angående personellsikkerhet må det stilles et krav til at de som arbeider med informasjonssystemene skal ha nødvendig kompetanse til å utføre sine oppgaver. Alle

medarbeidere med tilgang til sensitive personopplysninger eller informasjon om sikring av slike opplysninger skal ha taushetsplikt, og autorisasjon skal kun gis der det er nødvendig for å utføre pålagte oppgaver i henhold til gjeldende strategi.

Når det gjelder fysisk sikkerhet må virksomheten sørge for at lokaler og utstyr som brukes er forsvarlig sikret, særlig de rom hvor det er plassert utstyr for behandling av sensitive personopplysninger eller sikring av slike. Tjenermaskiner, kommunikasjons- og nettverksenheter må sikres godt. Adgangskontroll bør innføres på kritiske lokaler og utstyr, og fysisk områdeinndeling av lokaler må vurderes.

Systemteknisk sikkerhet går på tilgang til tjenester og informasjon i nettverk. Slik tilgang skal kun gis ved behov, og som et utgangspunkt skal alle tjenester være sperret. Mulig sikkerhetsarkitektur omfatter enkle løsninger med et fysisk skille mellom risikoutsatte tjenester og sensitive personopplysninger, og mer omfattende løsninger der det er behov for en integrert nettverksløsning for bruk av ulike opplysninger. Informasjonssystemet kan deles i soner, eller tilgangskontroll kan realiseres i form av nettverkskontroll, applikasjonskontroll, brannmur eller viruskontroll. Slike sikkerhetsbarrierer kan bidra til å redusere virkningen av DoS-angrep (Denial of Service) for uautorisert utilgjengeliggjøring av tjenester. Det er også et viktig prinsipp at intern datakommunikasjon kun skjer via medier virksomheten har fysisk kontroll med, og at sensitive personopplysninger via ekstern datakommunikasjon krever ende-til-ende kryptering mellom to sikrede soner.

Det er viktig for Sikkerhetsportalen at et godt system for informasjonssikkerhet er på plass. Beskyttelsesmekanismer som forhindrer fysiske innbrudd og tyveri må eksistere, inkludert adgangskontroll for systempersonell. Sikkerhetsrelaterte tiltak som forhindrer uautorisert tilgang til informasjon skal være på plass, for eksempel SSL og kryptering av beskjeder. Videre er det kun PKI-leverandørene som skal ha den informasjonen som trengs for å verifisere et brukersertifikat. Sikkerhetsportalen får på forespørsel en gitt brukers offentlige nøkkel, og kan selv verifisere brukerens identitet. Det må også eksistere sikkerhetsprosedyrer som sørger for at arkiverte data ikke kan gå tapt eller endres.

c) Logges transaksjoner, er de i så fall sikret mot endringer?

Transaksjoner i Sikkerhetsportalen logges i sikkerhetsserveren hos BBS. All aktivitet fra et brukersted sender over en bruker som skal autentiseres og til brukeren er ferdig autentisert og sendt tilbake til brukerstedet, logges [12]. Loggene kan ved en tvist mellom bruker og brukersted benyttes som uavhengig bevis. For å støtte ikke-benektning finnes en tidsstemplingstjeneste som med nøyaktighet kan fortelle når en gitt transaksjon fant sted. Dette forutsetter korrekte og synkroniserte klokker i hele systemet. Tidsstemplingstjenesten benyttes ved logging av transaksjoner, og kan i neste omgang benyttes for å spore eventuelle sikkerhetsbrudd.

d) Ivaretas personverninteresser generelt, og oppfylles personopplysningsloven?

Sikkerhetsportalen skal oppfylle personopplysningsloven [4], dermed ivaretas brukernes personverninteresser. Personopplysningsloven er ment å beskytte den enkelte mot at personvernet krenkes gjennom behandling av personopplysninger. Den skal bidra til at personopplysninger behandles i samsvar med grunnleggende

personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og høy kvalitet på personopplysninger. Den behandlingsansvarlige skal sørge for at personopplysninger er korrekte, at de ikke lagres lenger enn nødvendig, og at de kun brukes til angitt formål. Fødselsnummer og andre entydige identifikasjonsmidler kan i følge personopplysningslovens § 12 bare benyttes når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering. Den behandlingsansvarlige skal gjennom systematiske tiltak sørge for tilfresstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet, og dokumentasjon om sikkerhetstiltakene skal være tilgjengelig. Retten til innsyn gir enhver som ber om det rett til å vite hva slags behandling av personopplysninger den behandlingsansvarlige foretar. Behandling av sensitive personopplysninger som ikke er avgitt uoppfordret forutsetter konsesjon fra Datatilsynet.

I følge personopplysningsforskriften [30] skal det føres oversikt over hvilke personopplysninger som behandles, og en risikovurdering skal gjennomføres for behandling av disse. Klare ansvars- og myndighetsforhold skal etableres for bruk av informasjonssystemet, medarbeidere skal kun bruke systemet for å utføre pålagte oppgaver de er autoriserte for, og de er pålagt taushetsplikt for personopplysninger og sikkerhetsrelatert informasjon. Videre skal det iverksettes tiltak mot uautorisert adgang til utstyr og informasjon, det skal være umulig å foreta uautorisert endring av opplysninger, og det skal treffes tiltak mot ødeleggende programvare. Kommunikasjon av personopplysninger skal sikres, lagringsmedier med slike opplysninger skal merkes, og opplysninger som ikke lenger er i bruk skal slettes. For å sikre tilgjengelighet skal personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk kopieres.

4.1.6 Sikkerhetsbehov

a) Hva antas om grad av nødvendig sikkerhet for ulike tjenester?

Sikkerhetsportalen skal benyttes for tjenester med ulike sikkerhetsbehov, og grad av nødvendig sikkerhetsbehov må vurderes for hver enkelt tjeneste. For tjenester med et normalt sikkerhetsbehov vil sertifikater av typen ”Person-Standard” tilby tilstrekkelig sikkerhet. Eksempler på bruk av sikkerhetsnivå ”Person-Standard” kan være autentisering av brukere mot tjenester som selvangivelse eller innrapportering fra næringsliv når dette ikke omfatter særlig følsomme opplysninger, endring av bostedsadresse, tilgang til transaksjoner med økonomiske konsekvenser opp til et visst nivå eller andre søknader og henvendelser til offentlig virksomhet som krever trygghet for at avsenders identitet er korrekt [31].

For tjenester med veldig høye krav til sikkerhet vil man kunne benytte kvalifiserte sertifikater. Dette kan være sertifikater av typen ”Person-Høyt” eller ”Virksomhet”, for henholdsvis enkeltpersoner og virksomheter. Et eksempel på bruk av sikkerhetsnivå ”Person-Høyt” kan være å autentisere ukjente brukere mot webbaserte tjenester som gir tilgang til dokumenter som inneholder særlig følsomme opplysninger, som helseopplysninger og saksopplysninger i trygdeetaten [31]. Andre eksempler kan være å sende søknad til Lånekassen om betalingslettelse eller rentefritak, eller å autentisere avsender ved innsending av elektroniske resepter eller sykemeldinger.

4.1.7 Systemsvikt

a) Hva er konsekvensene om sikkerhetsantakelsene ikke slår til?

En rekke forutsetninger om systemsikkerhet ligger til grunn for Sikkerhetsportalen. For eksempel antas det at leverandører og driftspersonell ikke har skjulte hensikter, at disse følger gjeldende reglement og at fysiske barrierer er på plass for å hindre at uvedkommende får uautorisert tilgang til systemet. Sikkerheten i Sikkerhetsportalen settes på spill dersom personer eller systemer som håndterer sensitive opplysninger svikter, da dette kan resultere i at utenforstående får tilgang til informasjon de ikke skulle hatt tilgang til, som personopplysninger eller annen informasjon som angår systemets informasjonssikkerhet.

Sannsynligheten for en systemsvikt skal være liten, da rutiner er på plass for å hindre uautorisert adgang til områder, utstyr og systemer. Kryptering av kommunikasjon og fysiske barrierer skal gjøre det vanskelig å bryte seg inn i systemer og å fange opp sensitiv informasjon under sending og oppbevaring.

Å misbruke en annen persons identitet skal i teorien være vanskelig, men risikoen avhenger av hvilken type sertifikater som benyttes. Der private nøkler ligger lagret på brukers private datamaskin er det særdeles viktig at passord eller koder som trengs for å få tilgang til nøklene holdes hemmelig. Om noen får tilgang til slike koder kan de bruke den tilhørende nøkkelen og utgi seg for å være nøkkelens eier. Det er noe vanskeligere å få uautorisert tilgang til private nøkler som befinner seg i et smartkort. Man må da ha tilgang både til smartkortet og til koden som gir tilgang til nøkkelen lagret i kortet.

4.1.8 Mobilitet

a) Hvor lett er det å benytte tjenester fra nye lokasjoner og med nytt utstyr?

Det er i dag lett for brukere av Sikkerhetsportalen å benytte tjenester fra nye lokasjoner og med nytt utstyr for å oppnå mobilitet. Brukere kan på en enkel måte flytte nøkler og sertifikater mellom ulike systemer og terminaler. De filene som ZebSign i dag utsteder for brukere av Sikkerhetsportalen inneholder privat nøkkel og sertifikat, og kan enkelt kopieres til andre maskiner og installeres på nytt der. Der sertifikater ligger i smartkort må også smartkortleser og programvare for denne medbringes til det nye systemet.

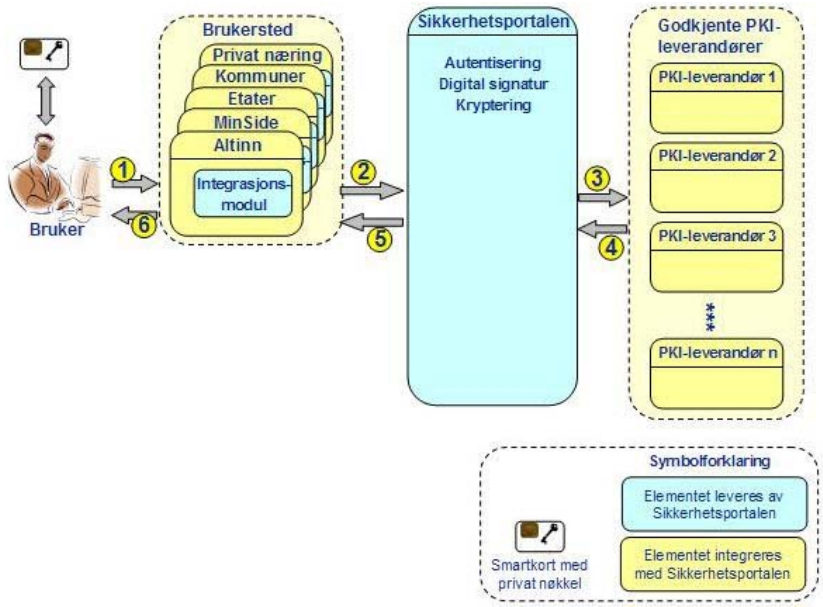
4.2 Meldingskompleksitet

Denne seksjonen inneholder spørsmål om hvordan meldingsutvekslingen foregår i Sikkerhetsportalen. Første punkt ser på hvor de ulike meldingene går, andre punkt ser på hvilke mekanismer som sikrer meldingene under sending.

4.2.1 Meldingenes gang

a) Hvordan går meldingene ved autentisering?

Figur 4.5 [12] illustrerer hvordan autentisering av en bruker med digitalt sertifikat kan foregå ved bruk av Sikkerhetsportalen. Videre følger en nærmere beskrivelse av trinnene i autentiseringen.



Figur 4.5: Autentisering ved bruk av Sikkerhetsportalen.

En bruker ønsker å benytte en tjeneste fra en offentlig etat, og logger inn på deres nettside med sitt digitale sertifikat (1). Brukeren må velge hvilken PKI-leverandør som skal benyttes for autentisering, en PKI-leverandør han tidligere har mottatt et digitalt sertifikat fra. Sertifikatet kan for eksempel ligge i et smartkort som kobles til brukerens datamaskin. Brukeren setter i så fall smartkortet i kortleseren, og oppgir en hemmelig pinkode som gir tilgang til det digitale sertifikatet lagret i kortet. Brukerens private nøkkel hentes ut fra sertifikatet, og brukes til å kryptere en melding som skal sendes til Sikkerhetsportalen.

Integrasjonsmodulen hos brukerstedet kommuniserer med Sikkerhetsportalen og oversender den krypterte meldingen via en Web Service eller HTTPS (2). Når Sikkerhetsportalen tar i mot den krypterte meldingen benyttes egne integrasjoner mot de ulike PKI-leverandørene. Den krypterte meldingen fra brukerstedet sendes videre til riktig PKI-leverandør (3).

Videre kontrolleres innloggingsinformasjonen (4). Meldingen fra brukerstedet ble kryptert med brukerens private nøkkel, og må derfor dekrypteres med brukerens offentlige nøkkel. PKI-leverandøren henter denne fra en katalog, offentlig eller lokalt, og dekrypterer meldingen. Om den dekrypterte meldingen er lesbar er brukeren den han utgir seg for, hvis ikke er det en uoverensstemmelse mellom den påståtte identiteten til brukeren og sertifikatet han bruker. Dersom innloggingen er vellykket sender PKI-leverandøren en melding om dette til Sikkerhetsportalen, sammen med en beskrivelse av hvilket sikkerhetsnivå brukeren er autentisert for. Når

Sikkerhetsportalen får melding fra PKI-leverandøren om hvordan autentiseringen gikk, sender Sikkerhetsportalen tilbakemeldingen om dette videre til brukerstedets integrasjonsmodul (5).

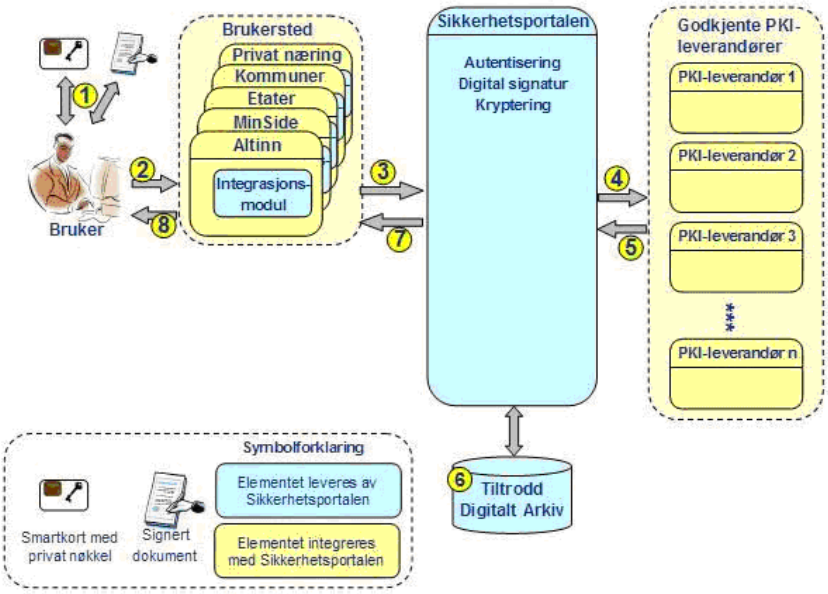
Om innloggingen er vellykket vil brukerstedet gjennom integrasjonsmodulen få tilgang til informasjonen som ligger lagret i brukerens sertifikat; det kan være navn, adresse, sertifikat-ID, fødselsnummer og lignende. Brukeren logges så inn på brukerstedets system og får tilgang til de tjenester som tilbys for sikkerhetsnivået han er innlogget på (6). Om autentiseringen ikke er vellykket vil brukerstedet ikke få tilgang til informasjon om brukeren, og brukeren logges ikke inn på brukerstedet.

Sikkerhetsportalen støtter SSO, som gjør at brukere som ønsker å benytte flere tjenester med innlogging fra Sikkerhetsportalen kun trenger å logge inn for den første tjenesten. Dette er mulig fordi sikkerhetsserveren utsteder en informasjonskapsel til brukeren ved første pålogging som angir at han er autentisert for et gitt sikkerhetsnivå. Ved pålogging sjekkes det om brukeren allerede har en sesjon mot Sikkerhetsportalen, altså om han har en gyldig informasjonskapsel. Har han det er alt greit og han er allerede autentisert. Har han ikke det presenteres han for en påloggingsside hvor han oppgir påloggingsopplysninger som sendes til riktig PKI-leverandør for verifisering. Andre tjenester som stoler på utstederen av kapselen vil senere kunne akseptere denne. Innholdet i informasjonskapselen må være kryptert, og overføres i HTTP eller XML.

b) Hvordan går meldingene ved kommunikasjon med brukersted?

Punkt a) så på hvordan kommunikasjonen går mellom de ulike komponentene i Sikkerhetsportalen ved autentisering av en bruker. Dette punktet ser på den kommunikasjon som foregår etter at brukeren er autentisert. En bruker vil kunne motta informasjon fra brukerstedet som ikke stiller spesielle krav til sikkerhet, for eksempel generelle opplysninger og upersonlig informasjon. For slik informasjonsutveksling kan meldingene gå mellom bruker og brukersted uten at Sikkerhetsportalen bistår med tjenester. Det mest interessante er imidlertid å se på den kommunikasjonen som finner sted etter at en bruker er autentisert og som stiller krav til digital signatur eller kryptering. Her kommer en gjennomgang av hvordan signering og kryptering foregår.

Digital signering realiserer en unik kobling mellom digital informasjon og en person eller en virksomhet [12]. Signerte skjemaer og digital signatur kan lagres i Sikkerhetsportalens tiltrodde digitale arkiv for fremtidig bruk, for eksempel i eventuelle juridiske tvister. Figur 4.6 [12] viser hvordan signering kan foregå i Sikkerhetsportalen. Under følger en nærmere forklaring av de ulike trinnene.



Figur 4.6: Signering ved bruk av Sikkerhetsportalen.

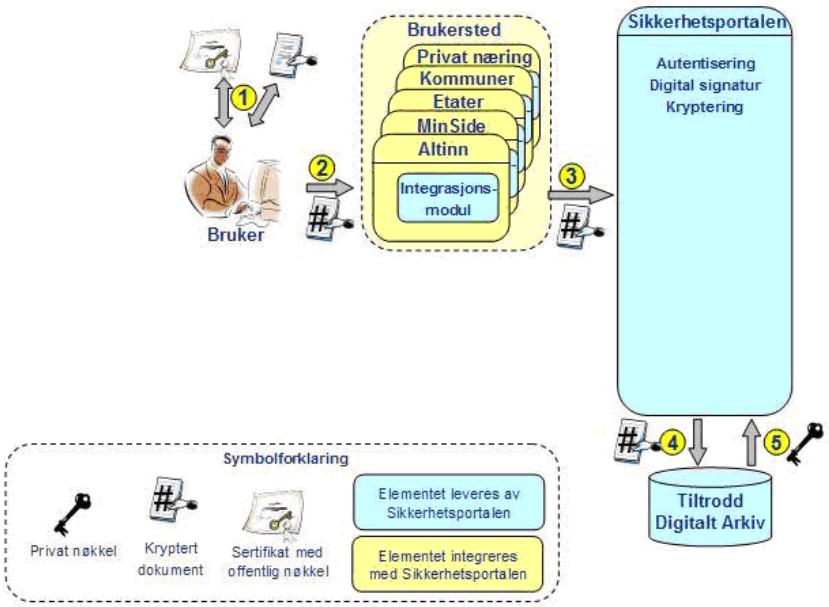
Anta at en bruker benytter en tjeneste fra en offentlig etat og skal sende inn et skjema som krever signatur (1). Brukeren setter smartkortet i kortleseren og oppgir en pinkode som gir tilgang til den private nøkkelen lagret i kortet. En kryptert melding genereres, en digital signatur som kobler skjema og bruker. Når skjemaet er signert gjøres signaturen tilgjengelig for brukerstedet (2), og integrasjonsmodulen hos brukerstedet sender skjema og signatur til Sikkerhetsportalen (3).

Sikkerhetsportalen kontakter PKI-leverandøren som utstedte brukerens sertifikat og nøkkelpar, og ber om brukerens offentlige nøkkel (4). Sikkerhetsportalen får nøkkelen fra PKI-leverandøren, og dekrypterer signaturen med denne (5). Om signaturen lar seg dekryptere stemmer brukerens identitet, og skjema og signatur kan lagres i Sikkerhetsportalens tiltrodde arkiv (6). Skjema og signatur er juridisk bindende, og Sikkerhetsportalen fungerer som en uavhengig tiltrodd tredjepart ved en juridisk tvist.

Dersom signaturen var korrekt får brukerstedet beskjed om dette og kan være trygg på at skjemaet er signert av en bruker med bekreftet identitet (7). I neste omgang får brukeren beskjed om at signeringen var vellykket (8).

Esignaturloven legger til rette for en sikker og effektiv bruk av elektronisk signatur, ved å fastsette krav til kvalifiserte sertifikater, til utstederne av disse sertifikatene og til sikre signaturfremstillingssystemer [23]. Sikkerhetsportalen skal kun støtte tjenester fra godkjente PKI-leverandører som oppfyller kravspesifikasjon for PKI i offentlig sektor, disse leverandørene antas også å oppfylle esignaturloven.

Kryptering skal sørge for at informasjon kun er tilgjengelig for mottaker. Kryptering forutsetter at avsender har tilgang til mottakers krypteringssertifikat og kan bruke hans offentlige nøkkel for kryptering av informasjon. Mottaker kan være Sikkerhetsportalens tiltrodde digitale arkiv, en annen bruker eller et fagsystem. Det som skal sendes kan være et dokument, en e-post eller et elektronisk webskjema. Figur 4.7 [12] illustrerer gangen i krypteringen, og under følger en beskrivelse av prosessen.



Figur 4.7: Kryptering ved bruk av Sikkerhetsportalen.

En bruker ønsker å kryptere informasjon som skal sendes til en mottaker, her et tiltrodd digitalt arkiv. Brukeren har tilgang til mottakers krypteringssertifikat, og krypterer informasjonen med mottakers offentlig nøkkel (1). Slik er det kun mottaker som kan dekryptere informasjonen med sin tilhørende private nøkkel. Selve krypteringen kan foregå på flere måter. Kryptering av e-post støttes av de fleste PKI-leverandører, og Microsoft har definert et standard grensesnitt for kryptografi- og PKI-tjenester i Windows, nemlig CAPI (Crypto API). Om informasjonen befinner seg i nettleseren må det finnes en modul som kan kryptere denne informasjonen, for eksempel i Java. Om det er et fagsystem som skal kryptere vil integrasjonsmodulen ha funksjonalitet for dette.

Den krypterte informasjonen sendes fra bruker til det aktuelle brukerstedet (2), og videre til Sikkerhetsportalen for lagring i tiltrodd digitalt arkiv (3). Om den krypterte informasjonen allerede er tilgjengelig på brukerstedet, for eksempel dersom det var et fagsystem som sto for krypteringen, trengs ikke steg (2). Informasjonen lagres i tiltrodd digitalt arkiv (4), sammen med tidsstempel og annen metadata. For at den krypterte informasjonen skal kunne dekrypteres må mottakers private nøkkel benyttes(5). I dette eksempelet lagres informasjonen i tiltrodd digitalt arkiv, og den private nøkkelen i Sikkerhetsportalens eget krypteringssertifikat brukes for dekryptering.

4.2.2 Sikring av meldingene

a) Kan sensitiv informasjon leses ut av meldinger på avveie?

Nei, all trafikk som inneholder sikkerhetsrelatert informasjon skal krypteres. Om noen skulle lykkes i å fange meldinger med slik informasjon under sending vil disse være meningsløse for den som får tak i dem.

b) Hvilke mekanismer sikrer meldingene?

Meldinger som inneholder personlige opplysninger og sikkerhetsrelatert informasjon skal krypteres. Personlige opplysninger kan for eksempel være unike ID'er, fødselsnummer, passord og koder. Sikkerhetsrelatert informasjon er all informasjon som kan svekke systemets sikkerhet hvis den kommer på avveie.

Videre skal det ikke være mulig å bryte seg inn eller på annen måte skaffe seg uautorisert tilgang til personopplysninger eller sikkerhetsrelatert informasjon. Alle forsøk på innbrudd skal aller helst oppdages og unngås. Dette krever fysiske hindringer, kryptering av lagret informasjon og adgangskontroll til systemer, informasjon og områder. Det må også eksistere mekanismer som sørger for at uvedkommende ikke kan overta etablerte sesjoner.

4.3 Robusthet mot feilsituasjoner

Denne seksjonen ser på Sikkerhetsportalens robusthet. Første punkt identifiserer mulige trusler for systemets tilgjengelighet og ser på systemets dimensjonering, andre punkt ser på hva som gjøres for å sikre høy tilgjengelighet. Punkt nummer tre identifiserer mulige flaskehalser i systemet.

4.3.1 Feilsituasjoner

a) Er det mulig å gjøre systemet utilgjengelig ved diverse angrep?

Ingen systemer er fullstendig beskyttet mot angrep som utilgjengeliggjør dets tjenester, heller ikke Sikkerhetsportalen. Angrep mot den sentrale delen av Sikkerhetsportalen vil nok være det mest effektive, ved å gjøre innloggingstjenesten utilgjengelig. Sikkerhetsportalen må være godt beskyttet mot innbrudd og endring av informasjon. Den sentrale sikkerhetsserveren må være særlig robust og vanskelig å få uautorisert tilgang til. All kommunikasjon som inneholder personopplysninger eller annen sikkerhetsrelevant informasjon må være kryptert slik at det er umulig for uvedkommende å få noe fornuftig ut av informasjonen som sendes.

Datatilsynet anbefaler i sin veiledning i informasjonssikkerhet [29] tekniske sikkerhetsbarrierer som hindrer utførelse av program som automatisk overføres fra eksternt datanett, for eksempel ActiveX og Java-komponenter. Brannmur og operativsystem skal ha de siste oppdateringer, og sikkerhetsbarrieren skal være motstandsdyktig mot DoS-angrep. Alle innkommende filer og flyttbare lagringsmedier må virussjekkes for å forhindre at ødeleggende programmer får gjøre skade i systemet.

b) Hvor mange brukere, brukersteder eller transaksjoner er systemet designet for å håndtere?

Sikkerhetsportalen bør skalere til en brukermasse som er minst like stor som antall innbyggere i Norge. Det må forventes at antall brukersteder vil kunne vokse betraktelig de neste få årene, og at tjenestene blir tatt i bruk minst i samme grad som tilsvarende papirbaserte tjenester brukes i dag. Sikkerhetsportalen må skalere slik at alle innbyggere kan utføre all kommunikasjon med det offentlige via Sikkerhetsportalen.

c) Hva skjer om forbindelsen brytes eller systemet av andre grunner går ned?

Om systemet går ned bør alle tjenester utilgjengeliggjøres, og brukere bør presenteres for en feilmelding som informerer om situasjonen, mulig feilårsak og når man kan forvente systemet oppe igjen. Eventuelle halvveis utførte transaksjoner bør rulles tilbake, og brukeres autentiseringssesjoner ugyldiggjøres.

4.3.2 Tilgjengelighet

a) Hvor stor tilgjengelighet forventes systemet å ha?

Som en følge av at Sikkerhetsportalen skal oppfylle kravspesifikasjon for PKI i offentlig sektor [17] skal dens tjenester være tilgjengelig 24 timer i døgnet, alle dager året rundt. Løsninger for autentisering og signering skal ha en oppetid på 99,9 % i snitt over et år, og planlagt nedetid i forbindelse med oppdateringer og periodisk drifting skal være minimal. Ved behov for oppdateringer og vedlikehold av tjenester skal dette avtales med kunden i rimelig tid før gjennomføring. Slikt arbeid skal fortrinnsvis foregå mellom 01:00 til 04:00 lørdag, søndag eller mandag. Avtalt nedetid regnes ikke som manglende oppetid. Periodiske driftsprosedyrer som for eksempel sikkerhetskopiering skal ikke kreve avtalt nedetid.

b) Hva gjøres for å sikre høy tilgjengelighet?

Sikkerhetsportalen er designet og organisert på en slik måte at den skal ha en veldig høy tilgjengelighet. Det finnes også alternative anlegg parate til å ta over hvis det opprinnelige anlegget går ned.

4.3.3 Flaskehalser

a) Finnes det deler av systemet som har stor innvirkning på den totale ytelsen?

Sikkerhetsportalen har vært operativ kun i noen få måneder, for autentisering av brukere fra Altinn med sertifikater av typen ”Person-Standard”. Sikkerhetsportalen har derfor så langt ikke vært ute for de helt store ytelsesproblemene. Den største flaskehalsen vil kanskje kunne vise seg å bli det lokale brukerstedet. For tjenester med svært mange brukere vil man for eksempel måtte fordele lasten på et sett av tjenere, slik at man ikke risikerer at hele tjenesten går ned på grunn av stor pågang.

4.4 Implementerings- og driftskostnader

Denne seksjonen identifiserer kostnader knyttet til implementering og drift av Sikkerhetsportalen; sentralt, for brukersteder og for sluttbrukere.

4.4.1 Kostnader til implementering og drift

a) Hvilke kostnader har man sentralt?

Bruk av Sikkerhetsportalen fører med seg en del kostnader. Det er direkte kostnader relatert til inngåelse av avtale med Sikkerhetsportalen, samt kostnader forbundet med bruk av Sikkerhetsportalens tjenester [12]. Gammel maskinvare, programvare og

nettverk må oppgraderes, problemer og egeninnsats gir tapt fortjeneste, opplæring og kompetansebygging kreves og organisasjonsutvikling i forbindelse med nye arbeidsprosesser vil koste.

Det finnes to alternative prismodeller for bruk av Sikkerhetsportalen, en transaksjonsbasert og en brukerbasert. I en transaksjonsbasert modell belastes brukerstedet for antall transaksjoner mot Sikkerhetsportalen, mens i en brukerbasert modell belastes brukerstedet for antall brukere over en gitt periode. Sikkerhetsportalen vil utføre veldig mange flere autentiseringstransaksjoner enn signeringer, og utfordringen er å prise en felles pålogging til Sikkerhetsportalen. Mange velger å benytte blandingsmodeller, dette gjelder blant annet Altinn hvor sertifikatinnehaver og sertifikatmottaker deler på kostnadene. Sertifikatinnehaver betaler for en etableringspakke som dekker smartkort, kortleser og programvare, sertifikatmottaker betaler for signeringstransaksjonene [8].

Offentlige tjenester benyttes relativt sjelden og det er normalt ønskelig med en transaksjonsmodell. Men trenden er at stadig flere offentlige brukersteder ønsker mer fastlagte utgiftsmodeller for å få mindre usikkerhet i forhold til kostnadsnivå. Offentlige tjenester kan deles i to grupper. Det finnes noen tjenester som alle bruker en sjelden gang, for eksempel innlevering av selvangivelsen, og så finnes det andre tjenester for grupper med spesielle behov, for eksempel tjenester for arbeidsledige. Den første gruppen har en stor brukermasse, men brukes sjelden. Her er det normalt sett best med en transaksjonsbasert modell. Den andre gruppen har færre brukere, men brukergruppen endres stadig. Her vil det lønne seg med en modell med fast brukergruppe.

Sikkerhetsportalen sentralt har utgifter knyttet til sikkerhetsserveren, samt til annen maskinvare, drift og utvikling, og til personell for brukerstøtte og administrativt arbeid.

b) Hvilke kostnader har brukerstedene?

Ved brukerstedene må eksisterende arbeidsprosesser erstattes av prosesser kompatible med Sikkerhetsportalen. Utgifter knyttet til manuell papirflyt og postgang erstattes av utgifter til maskinvare, programvare og nettverk. Brukerstedene trenger en integrasjonsmodul for kommunikasjon med sikkerhetsserveren hos BBS, og de trenger en eller flere tjenester som skal bruke innlogging via Sikkerhetsportalen. Kostnadene knyttet til klargjøring av et brukersted for tjenester fra Sikkerhetsportalen dekkes av det enkelte brukerstedet.

Brukestedet har videre kostnader knyttet til selve bruken av Sikkerhetsportalens tjenester, hvor det betales for antall transaksjoner eller for antall brukere. Mer sammensatte betalingsmodeller er også mulige.

BBS skal ha to personer fast tilgjengelig for bistand ved integrasjon av brukersted mot Sikkerhetsportalen, samt at en ressursbase på 22 årsverk skal kunne bidra ved stort påtrykk [12]. Ved hvert brukersted bør det finnes en prosjektgruppe med juridisk, økonomisk og teknologisk kompetanse.

c) Hvilke kostnader har sluttbrukere?

Sluttbrukere som ønsker å ta i bruk tjenester fra Sikkerhetsportalen må laste ned programvare og dokumentasjon [12]. De sertifikatene av typen ZebSign standard ID som i dag utstedes for bruk med Sikkerhetsportalen er gratis, og medfører ingen kostnad for brukeren.

4.5 Brukervennlighet

Denne seksjonen ser på Sikkerhetsportalens brukervennlighet. Første punkt ser på brukerutstyr, andre punkt på hvordan brukersteder og sluttbrukere kommer i gang med Sikkerhetsportalen, og tredje punkt vurderer brukergrensesnittet.

4.5.1 Krav til brukerutstyr

a) Er løsningen plattformuavhengig med hensyn til operativsystem og nettleser?

Det er viktig at Sikkerhetsportalen ikke binder brukeren til én plattform med hensyn til for eksempel operativsystem eller nettleser. Derfor skal ulike nettlesere støttes, som et minimum Internet Explorer5.0, Netscape 8.0.3.3, Mozilla 1.7.11, Firefox 1.06, Opera 6.0 og Safari 1.2 [12]. Også nyere versjoner av disse skal støttes, og det kreves at nettleseren støtter informasjonskapsler. Hvis dette ikke er tilfelle kan den ikke brukes mot Sikkerhetsportalen for autentisering eller SSO.

Videre skal ulike operativsystem kunne benyttes, blant annet Windows, Unix, Linux og Mac. Både nyere og eldre versjoner bør støttes. Sikkerhetsportalen krever ikke installasjon av annen programvare, kun en smartkortleser og programvare for denne dersom kvalifiserte sertifikater i smartkort benyttes.

b) Stilles det krav til brukerens maskinvare/brukerterminal?

Det kreves at brukerens operativsystem og nettleser er støttet, samt at nettleseren støtter informasjonskapsler. For kvalifiserte sertifikater av typen ”Person-Høyt” og ”Virksomhet” kreves i tillegg en smartkortleser og tilhørende programvare.

4.5.2 Å ta i bruk systemet

a) Hvordan kommer brukersteder i gang?

Offentlige etater som ønsker å ta i bruk Sikkerhetsportalen kontakter Brønnøysundregistrene, som sender prismodell, abonnementsavtale og teknisk informasjon. Mye av denne informasjonen er konfidensiell på grunn av sikkerhets- og forretningsmessige forhold [12]. Etater som ønsker informasjon må derfor undertegne en avtale om utlevering og behandling av konfidensiell informasjon knyttet til Sikkerhetsportalen. Brønnøysundregistrene videresender henvendelsen til BBS for teknisk bistand og tilpasninger av abonnementsavtalen til brukerstedeierens behov. Når avtalen med BBS er inngått får brukerstedet tilgang til et nettsted med informasjon og veiledning for å ta i bruk Sikkerhetsportalen. Her finnes også integrasjonsmodul og nødvendig programvare. Brukerstedet får samtidig tilgang til en kundeweb med mye nyttig driftsinformasjon.

Før et brukersted kan ta i bruk sikkerhetstjenester fra Sikkerhetsportalen må det klargjøres for kommunikasjon med sikkerhetsserveren over et SAML-grensesnitt. Det finnes tre hovedalternativer for hvordan integrasjonen med Sikkerhetsportalen kan gjøres [12]. Den ene er bruk av en Affiliate Agent-modul fra Sikkerhetsportalen, den andre er bruk av en .NET modul, og den tredje er bruk av egen programvare som oppfyller SAML. Webbaserte brukersted som kun skal benytte elektronisk identitet eller som støtter ID-FF 1.1/SAML 2.0 trenger ikke integrasjonsmodul, disse overlater innlogging til Sikkerhetsportalen [32]. Brukersteder som ikke støtter ID-FF/SAML 2.0 eller som vil ha lokal innlogging trenger imidlertid integrasjonsmodul.

I følge kravspesifikasjon for PKI i offentlig sektor skal det finnes tilstrekkelig dokumentasjon til at en programmerer med generell kompetanse skal kunne benytte grensesnittet [17]. Videre skal det finnes kompilerbar eksempelkode som viser bruk av alle funksjoner i applikasjonens programmeringsspråk. Sikkerhetsportalen skal også tilby brukerstøtte for sine brukersteder, via telefon eller e-post. Behandlingstiden på henvendelser bør være kort innenfor normal kontortid.

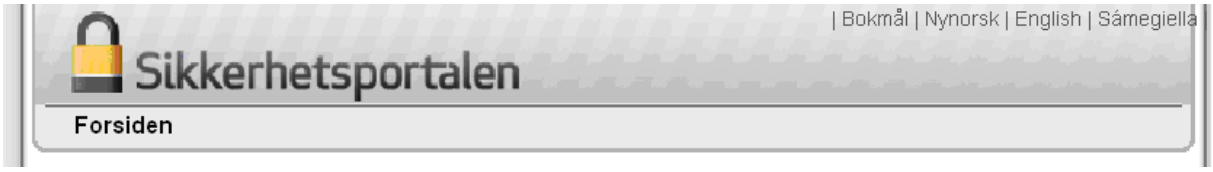
b) Hvordan kommer sluttbrukere i gang?

For å benytte tjenester fra et nettsted som krever innlogging via Sikkerhetsportalen må man først bestille en engangskode fra det aktuelle nettstedet. Personen mottar denne i posten, og bruker så koden til å bestille elektronisk ID fra en PKI-leverandør som har lov til å utstede det aktuelle sertifikatet. Alle PKI-leverandører tilbyr en registreringsautoritet som gjør at man kan skaffe sertifikater fra den enkelte leverandør. Med en elektronisk ID kan personen sikkert logge inn på nettsteder via Sikkerhetsportalen. Brukeren må ha en datamaskin, og enten installeres sertifikatet på denne eller brukeren har sertifikatet integrert i et smartkort.

4.5.3 Brukergrensesnitt

a) Er menyene intuitive?

Kravspesifikasjon for PKI i offentlig sektor [17] legger føringer på at alle brukergrensesnitt skal oppfattes som enkle og brukervennlige. Dagens brukergrensesnitt er godt og intuitivt, med gode forklaringer for hva bruker skal gjøre og hva som skjer. Sikkerhetsportalens nettsider tilbys på bokmål og nynorsk, så vel som engelsk og samisk. Se figur 4.8 for hvordan språkvalget i alle menyer er synlig i øvre del av vinduet.



Figur 4.8: Sikkerhetsportalens brukergrensesnitt har god språkstøtte.

For de som måtte ha behov for det yter Sikkerhetsportalen brukerservice via telefon og e-post. BBS har også laget veiledninger for hvordan man kommer i gang med

sertifikater fra Sikkerhetsportalen og besvarer på sine hjemmesider de vanligste spørsmålene brukere vil stille.

b) Får brukeren tydelig beskjed om hva som skjer?

I følge kravspesifikasjon for PKI i offentlig sektor [17] skal det eksistere en norsk veiledning for installasjon og bruk, og brukeren skal tydelig varsles når han er i ferd med å foreta en signering samt kunne velge å avbryte transaksjonen. Gode veiledninger for sluttbruker finnes for installasjon og bruk av sertifikater utstedt for Sikkerhetsportalen. Brukeren får tydelig beskjed om hvilke transaksjoner som utføres mot brukerstedet, uten at han må se hva som foregår bak brukerstedet.

Fordeler ved innføring av Sikkerhetsportalen

Innføring av Sikkerhetsportalen i det offentlige skal bidra til effektivisering av kommunikasjonen i offentlig sektor, og mellom offentlig sektor og vanlige borgere. Effektiviseringen skal frigjøre ressurser i administrasjon, som kan brukes til annen verdiskapning. Sikkerhetsportalen gjør det lettere for offentlige virksomheter å tilby tjenester basert på elektronisk ID og signatur. Brukerstedene får en enkel integrasjon mot Sikkerhetsportalen, og slipper å forholde seg til PKI-leverandørene bak portalen. Borgeren på sin side forholder seg kun til det aktuelle brukerstedet og ser ikke Sikkerhetsportalen.

Å ta i bruk Sikkerhetsportalen kan føre til mer effektive arbeidsprosesser, spart tid ved at man slipper postgang, raskere og enklere søk i historisk materiale, raskere kommunikasjon med brukere, samt at man slipper å manuelt legge inn elektronisk informasjon fra papir [12]. Utgifter man før hadde til papir, kopiering, porto og lignende blir også mindre, samt utgifter til egenutviklete sikkerhetsløsninger. Sikkerhetsportalen bidrar også til økt sikkerhet, siden informasjon kan overføres tryggere mellom borgere og det offentlige, og siden informasjon lagres kryptert. Elektronisk innrapportering og saksbehandling gir bedre kvalitet og større nøyaktighet enn papiroverføring, og kan gi kortere behandlingstid. I tillegg er de elektroniske tjenestene åpne døgnet rundt og dermed lett tilgjengelige for brukerne. Takket være engangspålogging, såkalt SSO, blir det også lettere å forflytte seg mellom ulike brukersted.

Sikkerhetsportalen gjør det enkelt og rimelig for brukersteder å integrere autentisering, signering og kryptering i sine tjenester, siden standardiserte moduler kan benyttes fremfor å utvikle egen funksjonalitet. Offentlig sektor kan lettere tilby sikre elektroniske tjenester, og det blir enklere for brukerne å benytte en sikkerhetsløsning som støtter tjenester fra hele den offentlige sektor og etter hvert også privat sektor.

5 FEIDE

FEIDE har vært i bruk i flere år ved en rekke utdanningsinstitusjoner. FEIDE har derfor gjort seg mange erfaringer, og har et mer etablert system enn Sikkerhetsportalen som fremdeles er i oppstartfasen og kun har et utvalg av tjenestene på plass. FEIDE er en arkitektur for identitetsforvaltning, og spesifiserer ikke autentiseringsløsning. I prinsippet kan hvilken som helst mekanisme for autentisering benyttes, i praksis benyttes kun en løsning, nemlig brukernavn og passord. I nær fremtid vil også andre løsninger tas i bruk, blant annet PKI i forbindelse med planlagt samtrafikk med Sikkerhetsportalen.

For å besvare spørsmålene i tabell 3.1 benyttes informasjon fra FEIDE og UNINETTs hjemmesider [14] og [13]. Alle spesifikasjonsdokumenter for FEIDE er åpent tilgjengelig, og disse er også i stor grad benyttet for å besvare spørsmålene i dette kapittelet. I tillegg er all kode og alle tekniske detaljer tilgjengelige fra Morias SourceForge [33] og Morias hjemmeside [34].

Dette kapittelet besvarer de samme spørsmålene for FEIDE som ble besvart for Sikkerhetsportalen i forrige kapittel. Figur 5.1 [14] viser FEIDEs logo.

Figur 5.1: FEIDEs logo.

5.1 Organisering og sikkerhetsantakelser

Denne seksjonen inneholder spørsmål som går på hvordan FEIDE er organisert og realisert. Svarene på spørsmålene er ment å gi nødvendig bakgrunnsinformasjon om FEIDE for å kunne ta fatt på en systemanalyse. Første punkt går på systemarkitektur, nærmere bestemt hvordan FEIDE er bygd opp, hvilke systemkomponenter som kommuniserer med hverandre, og hvor sikkerheten er realisert. Punkt nummer to tar for seg anvendelsesområder, samt hvilke tjenester som tilbys. Tredje punkt ser på standarder og standardisering, og fjerde punkt på autentiseringsløsninger. Punkt fem besvarer spørsmål knyttet til personvern og behandling av personopplysninger, punkt seks ser på muligheter for å dekke ulike tjenesters krav til sikkerhet. Punkt sju drøfter muligheten for at sikkerhetsantakelser og rutiner kan svikte, og punkt åtte vurderer FEIDE med tanke på mobilitet.

5.1.1 Arkitektur

a) Hvilke delsystemer eksisterer?

Institusjon
En FEIDE-institusjon er en skole, høyskole eller universitet som er tilknyttet FEIDE og som ønsker å tilby elektroniske tjenester til sine studenter og ansatte. Hver institusjon i FEIDE har sitt eget *brukeradministrative system (BAS)* som tilbyr relevant

og oppdatert informasjon om sine brukere, basert på institusjonens egne administrative datasystemer [35]. Det brukeradministrative systemet eksporterer informasjon om sine brukere til interne systemer, og til institusjonens autentiseringstjener.
Autentiseringstjeneren (AT) vet hvilke brukere som er tilknyttet institusjonen, og har informasjon om gyldige brukere. Autentiseringstjeneren oppdateres fra brukeradministrativt system, og kan aksesseres via LDAP (Lightweight Directory Access Protocol). Systemet krever at alle enheter har tillit til autentiseringstjeneren.

Klient
En klient i FEIDE-systemet er programvare som kjører på brukerens datamaskin, for eksempel webklienter og smartkortapplikasjoner. Brukeren, en person med tilknytning til en utdanningsinstitusjon, oppgir brukernavn og passord til klienten for å bevise at han er den han hevder å være. Eventuelt så kan brukeren legge frem et sertifikat som også beviser dette. Hvis informasjonen brukeren legger frem er gyldig gis brukeren tilgang til systemet. Det er en forutsetning at brukeren ikke deler sitt passord eller sertifikat med andre.

FEIDE
FEIDE er et desentralisert system hvor korrekte data vedlikeholdes hos hver enkelt FEIDE-organisasjon. Den sentrale FEIDE-tjenesten består av innloggingstjenesten *Moria*, som er en webautentiseringstjener. Moria håndterer autentisering og distribusjon av informasjon om brukere basert på autentiseringstjeneren. Moria har to ulike grensesnitt, Moria1 og Moria2. Moria2 er dagens versjon, og har vært i drift siden april 2005 [14]. Moria1 har vært i kontinuerlig drift siden juni 2003, men vil bli avsluttet.

Moria knytter en webbasert forbindelse mellom den lokale FEIDE-løsningen der brukeren hører hjemme og tjenesten som brukeren benytter seg av [14]. På denne måten trenger ikke FEIDE-tjenester en egen innloggingstjeneste siden de kan få nødvendig informasjon om brukerne gjennom Moria. Moria utfører selve innloggingen via brukerens lokale FEIDE-løsning. En bruker vil derfor kunne benytte sitt FEIDE-navn til alle webbaserte FEIDE-tjenester i hele utdanningssektoren, uten at disse institusjonene må importere brukeren i sitt eget brukeradministrative system [35]. Moria utfører autentiseringen på brukerens vegne mot autentiseringstjeneren der brukeren hører hjemme. Hvis innloggingen er vellykket henter Moria ut og overfører de data som tjenesten har bedt om og som brukeren har samtykket til at skal overføres.

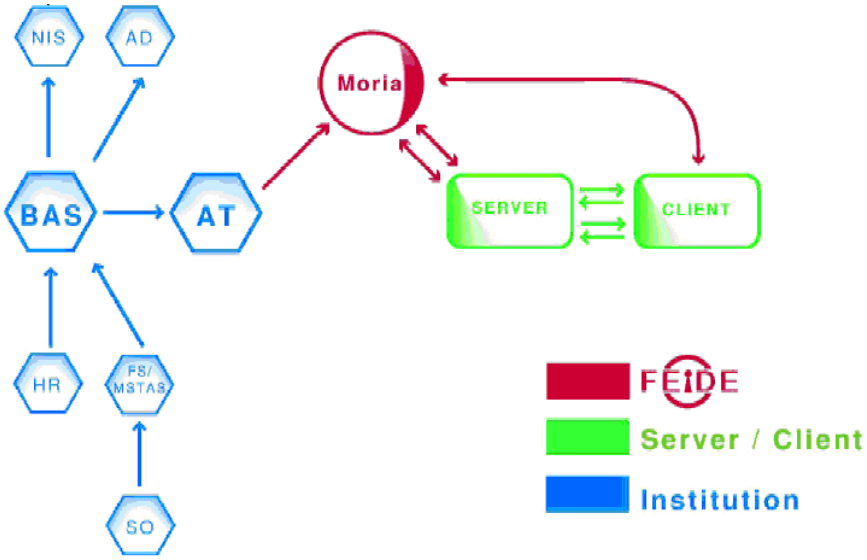
Tjener
FEIDE går ut på å innføre en identitet som kan gi brukere tilgang til aksessbeskyttede nettverksressurser. Sluttbruker er en klient som forespør en tjeneste eller en ressurs, og maskinen ressursen ligger på er en tjener. For aksessbeskyttete ressurser må bruker autentiseres og autoriseres før han får tilgang til personlige tjenester. Det må altså foretas en sjekk på at brukerens identitet er assosiert med en rolle som har tilgang til ressursen. Eksempler på nettverksressurser kan være webtjenester, nettverkspålogging, nøkkelkort for dører og lignende.

b) Hvilke av disse kommuniserer med hverandre?

Figur 5.2, modifisert fra [35], viser hovedelementene i et FEIDE-system og hvor den viktigste kommunikasjonen går. Brukeradministrativt system (BAS) innhenter informasjon fra institusjonens administrative systemer, for eksempel studiesystemer og personalsystemer. Altså foregår det kommunikasjon mellom BAS og disse systemene. På figuren er denne kommunikasjonen markert med piler mellom BAS og institusjonens datasystemer. Autentiseringstjeneren (AT) får oppdatert sin informasjon fra BAS, på figuren markert med en pil mellom BAS og AT.

Når en bruker ønsker å benytte aksessbeskyttede tjenester fra en FEIDE-institusjon må han først autentiseres, ressursen videresender derfor brukeren til FEIDEs innloggingsside. Selve autentiseringen går direkte mellom brukerens programvare og AT. Altså går det kommunikasjon mellom klienten og innloggingssystemet Moria, samt Mellom Moria og AT. Interaksjonen med det sentrale FEIDE er markert med piler mellom Moria og klienten, og mellom Moria og AT.

Etter at brukeren er ferdig autentisert presenterer han sin signerte tillatelse for nettverksressursen og får deretter autorisasjon. Ressursen utvekseler informasjon med Moria for å få tilgang til informasjon om brukerens rettigheter. Denne kommunikasjonen er indikert i figuren med piler mellom Moria og tjeneren.



Figur 5.2: Elementer i FEIDE.

c) Hvor i systemet er sikkerheten realisert?

I et system for identitetsforvaltning er det viktig at en bruker kan autentiseres på en enkel måte ved å oppgi sin identitet og en hemmelighet ingen andre kjenner. For FEIDE er dette hovedsakelig FEIDE-navn og tilhørende FEIDE-passord. Om oppgitt informasjon entydig og korrekt identifiserer en bruker i systemet, skal brukeren få tilgang til systemet og de ressurser han har autorisasjon for.

Mye av sikkerheten ligger i innloggingssystemet Moria. Hvis autentiseringen som finner sted i Moria ikke er fullstendig sikker vil heller ikke systemet som helhet være

noe sikrere. Personer uten FEIDE-identitet skal ikke få adgang til FEIDE-tjenester, og FEIDE-brukere skal ikke gis tilgang til tjenester de ikke er autoriserte for. Moria tar i mot brukernavn og passord fra klienten, og sjekker disse mot den aktuelle institusjons lokale LDAP. Slike data må ikke komme på avveie, og all kommunikasjon til og fra Moria er derfor kryptert ved SSL [14]. LDAP-tjenere og webtjenester må stole på Morias SSL sertifikat signert av VeriSign. FEIDE krever ikke kryptert kommunikasjon mellom klient og webtjeneste, men anbefaler det sterkt.

Videre er det viktig at enhver klient kun kan be om attributter den er assosiert med, eller et utvalg av disse. Ethvert forsøk på å spørre om andre attributter skal resultere i en feilmelding når klienten ber om en autentiseringssesjon. For å minske risikoen for hijacking endres billetten, Moria sesjons-ID, etter autentisering. Denne genereres slik at den er praktisk talt umulig å gjette.

Institusjonens brukeradministrative system må inneholde data av god kvalitet fra autorative kilder. Om institusjonen ikke har god sikkerhet rundt sine registrerte data er FEIDE med ett ikke sikkert lenger. FEIDE vil aldri kunne være sterkere enn sitt svakeste ledd, som sannsynligvis i de fleste tilfeller er den lokale LDAP-tjeneren. Personopplysninger må behandles og oppbevares sikkert, med gode rutiner. Og selvfølgelig kreves det at passord og private nøkler holdes hemmelig.

5.1.2 Anvendelsesområder

a) Hvor brukes systemet i dag, og i morgen?

FEIDE-innlogging benyttes av tjenester innen utdanningssektoren. Mange institusjoner innen høyere utdanning har tatt i bruk FEIDE, og i følge [36] skal de resterende brukerne innen høyere utdanning knyttes til i løpet av 2006. Totalt har rundt 125.000 brukere innen høyere utdanning fått tildelt FEIDE-identitet. NTNU, Universitetet i Bergen og Universitetet i Oslo er ferdig tilsluttet FEIDE, med henholdsvis 22.000, 20.000 og 36.000 FEIDE-navn [14]. Universitetene i Stavanger og Tromsø, samt Universitetet for miljø- og biovitenskap har også besluttet innføring, de to sistnevnte er allerede i gang. En rekke statlige høyskoler har innført FEIDE, og mange flere har tatt en beslutning om innføring eller er underveis.

Brukere av FEIDE innen høyere utdanning er studenter, ansatte og andre med tilknytning til en høyskole eller universitet. Det planlegges å innføre FEIDE også i grunnopplæringen, altså i grunnskoler og videregående skoler. FEIDE skal rulles ut i grunnopplæringen fra høsten 2006, og de første 10.000 brukerne er operative fra 30.04.2006 [36]. I grunnopplæringen vil brukerne være elever, lærere og andre med tilknytning til skolen. For å få tildelt FEIDE-navn må man ha en definert tilknytning til sin vertsorganisasjon, og denne tilknytningen skal være tilgjengelig som en del av informasjonsmodellen i FEIDE.

De offentlige grunnskolene i Norge eies og drives av kommunene, i motsetning til videregående skoler som eies og drives av fylkeskommunene [16]. Både kommuner og fylkeskommuner har mange andre oppgaver i tillegg til sitt ansvar for skolene. Dette er annerledes i universitets- og høyskolesektoren, hvor institusjonene er eid av staten og organisasjonene representerer full tilhørighet i undervisningssektoren. For grunnopplæringen vil skolesektoren være én av flere sektorer, og det er ingenting i

veien for at en kommune eller et fylke innfører lokale FEIDE-løsninger for alle sine innbyggere og alle sine ansatte.

En rekke tjenester benytter FEIDE i dag, de fleste av disse er selvbetjeningstjenester. Eksempler på noen tjenester som benytter FEIDE-innlogging er BIBSYS, Studweb, Frida, Nasjonalbiblioteket og Innsyn.

b) Hvilke sikkerhetstjenester tilbys?

FEIDE tilbyr blant annet en innloggingsside. Bruker oppgir brukernavn og passord, og etter godkjent innlogging overfører Moria data om brukerne til de aktuelle tjenestene. Moria støtter SSO både på brukersiden og på tjenestesiden [14]. På brukersiden innebærer SSO at brukere som ønsker å benytte flere FEIDE-tjenester kun trenger å logge på én gang. Når en bruker logger på en FEIDE-tjeneste lagrer Moria en billett i en informasjonskapsel i brukerens nettleser. Neste gang brukeren logger på en FEIDE-tjeneste leser Moria denne billetten, og henter ut informasjon om påloggingssesjonen. Om sesjonen fremdeles er gyldig får tjenesten tilgang til informasjon om brukeren midlertidig lagret av Moria. Er sesjonen ugyldig videresendes brukeren til FEIDEs innloggingsside. Enkelte tjenester ønsker ikke bruk av SSO, og i visse tilfeller tillates ikke SSO av sikkerhetsmessige årsaker. Om attributtene som blir etterspurt av en tjeneste i en reautentisering ikke finnes mellomlagret i Moria, krever Moria en ny pålogging for å hente ut riktig informasjon fra brukerens autentiseringstjener.

På tjenestesiden betyr SSO at en tjeneste kan logge en bruker inn i ett eller flere uavhengige delsystemer, for eksempel ved en portal med innhold fra ulike tjenester. Portaltjenesten kan da be Moria om at innloggingen til portalen også skal gjøres for de delsystemene som utgjør portalen, såkalt proxy-autentisering. Den overordnete tjenesten får en billett som den gir til den underliggende tjenesten. Med denne billetten kan den underliggende tjenesten hente ut informasjon om FEIDE-brukeren fra Moria, som har lagret en midlertidig kopi av informasjonen ved pålogging til den overordnete tjenesten. I visse tilfeller tillater Moria av sikkerhetsmessige årsaker ikke proxy-autentisering. Dette kan skje om billetten er for gammel, eller om den er ugyldig fordi Moria ikke har mellomlagret attributtene den underliggende tjenesten etterspør.

Moria har også funksjonalitet for avlogging, slik at tjenesten eller brukeren kan varsle Moria om at en innloggingssesjon er avsluttet. En eventuell SSO-billett vil da ugyldiggjøres. Men selv om man logger av Moria vil andre FEIDE-tjenester man er pålogget fremdeles kunne være aktive. Med andre ord må man logge ut av samtlige FEIDE-tjenester separat. Eventuelt kan en bruker kan velge å logge ut fra FEIDE direkte via FEIDEs utloggingsside på http://logout.feide.no.

5.1.3 Standardisering

a) Hvilke åpne standarder er systemet basert på?

FEIDE har en komponentbasert arkitektur, basert på veldefinerte, åpne standarder og grensesnitt [37]. Dette innebærer at systemkomponentene i FEIDE i stor grad er utbyttbare, altså at det kan finnes alternative løsninger for å utføre gitte funksjoner. Utbyttbarheten sikres gjennom en dokumentert arkitektur med åpne og veldefinerte grensesnitt.

Dagens FEIDE-løsning er basert på de åpne standardene HTTP, SOAP, Web Services, SSL/TLS og LDAP [38]. Tjenestene kommuniserer med Moria via SOAP (Simple Object Access Protocol) over sikkert HTTP, noe som er støttet av de fleste moderne programmeringsspråk og plattformer [14]. SOAP er rett og slett en enkel XML-protokoll for informasjonsutveksling over HTTP. Moria kommuniserer med autentiseringstjenerne via LDAP over en SSL (Secure Sockets Layer) eller TLS (Transport Layer Security) protokoll som sikrer meldingene konfidensialitet, autentisering og integritet. SSL/TLS bruker offentlig-nøkkel kryptering for å forhandle om sesjonsnøkkelen som krypterer meldinger. LDAP er en protokoll som brukes for å aksessere informasjonskataloger. Grensesnittet som brukerne ser er standard HTML (Hypertext Markup Language), et velkjent språk som brukes for å lage websider. En fremtidig FEIDE-løsning vil basere seg på standardene HTTP, SOAP, LDAP, SSL/TLS, SAML, ID-FF og ID-WSF [38]. SAML er et rammeverk for utveksling av sikkerhetsinformasjon, basert på XML. ID-FF og ID-WSF er standarder fra Liberty Alliance [22] for identitetsbaserte webtjenester.

FEIDE arbeider for tiden med å endre innloggingstjenesten for å støtte åpne standarder [14]. Samtrafikk med Sikkerhetsportalen i løpet av juni 2006 medfører blant annet innkjøp av innloggingsprogramvare fra et medlem i Liberty Alliance. Dagens innloggingsgrensesnitt Moria vil for brukerne bestå slik den er i dag selv om programvaren endres, og det vil ikke bli endring for institusjonenes lokale FEIDE-løsninger. Integrasjonen for tjenesteleverandører vil endres, men Moria2 vil bestå i alle fall til sommeren 2007. I forbindelse med innføring av PKI for sluttbrukere i FEIDE blir det endringer både for institusjoner og tjenester.

Moria er skrevet i Java og er fritt tilgjengelig som åpen kildekode. All kildekode og dokumentasjon for Moria ligger på SourceForge [33] og på Morias hjemmeside [34].

b) Er systemet i ferd med å bli en standard innen visse sektorer?

Ja, FEIDE er i ferd med å bli en standard innen utdanningssektoren. I løpet av 2006 skal de resterende brukere innen høyere utdanning knyttes til FEIDE, og samme år begynner utrullingen av FEIDE i grunnskolen [36].

5.1.4 Autentisering

a) Hvilke autentiseringsløsninger benyttes?

Per i dag er en FEIDE-identitet et unikt brukernavn og et tilhørende passord, som brukeren må oppgi for å få tilgang til aksessbeskyttede ressurser ved sin utdanningsinstitusjon. Men FEIDE-rammeverket åpner for ulike autentiseringsløsninger, og på sikt vil for eksempel et sertifikat integrert i et smartkort kunne brukes for sikker identifisering av brukere. Støtte for innlogging via Sikkerhetsportalen er under arbeid, og planlegges operativ 10.06.2006 [36]. Videre er også tonivå-innlogging i en testfase, hvor et engangspassord sendes til mobiltelefon.

FEIDE opererer med en desentralisert autentiseringsløsning, hvor innloggingsfunksjonen er felles og dataene ligger lokalt hos den enkelte organisasjon [36]. Passord eller andre personopplysninger lagres altså ikke sentralt i FEIDE, og selve autentiseringen foregår mot vertsorganisasjonenes egen ID-bank, med data som organisasjonen selv går god for.

Siden FEIDE er uavhengig av autentiseringsløsning kan man i praksis anvende en hvilken som helst form for autentisering. Hver nettverksressurs må evaluere hvilket sikkerhetsnivå som trengs for nettopp denne tjenesten [35]. Brukernavn og passord/pinkode representerer et tilstrekkelig sikkerhetsnivå for de fleste tjenester. I noen tilfeller ønsker man noe større sikkerhet, og da kan sertifikater være løsningen. For eksempel sertifikater lagret i programvare på brukerens datamaskin. For enda større sikkerhet kan man benytte smartkort, hvor brukerens sertifikat er lagret på et smartkort som er beskyttet med en pinkode. Selv om sertifikater gjerne antas å være sikrere enn passord er dette ikke nødvendigvis tilfelle, da sikkerhetsnivå avhenger av hvordan passord og nøkler genereres, distribueres og oppbevares.

b) Hvilke krav stilles til brukernavn og passord?

Attributtdokumentet for FEIDE [39] spesifiserer FEIDEs LDAP-skjema, altså hvilke attributter som kan defineres i FEIDE-institusjoners lokale LDAP-tjenere. To av disse attributtene er passord og brukernavn, som bruker oppgir når han logger inn mot den sentrale webinnloggingssiden. Attributtet 'uid', kort for 'user id', er på formen eduPersonPrincipalName og spesifiserer brukernavnet FEIDE-brukere logger inn med, det såkalte FEIDE-navnet. Dette navnet er begrenset til ASCII-tegn, mellomrom er ikke tillatt og det er anbefalt å unngå tegnsetting. En vanlig begrensning som er noe strengere innebærer at brukernavn maksimalt skal være 8 bokstaver langt, at tegnene er begrenset til a-z og 0-9, og at det må begynne med en bokstav.

Attributtet 'userPassword' identifiserer brukerens FEIDE-passord. Det er anbefalt å begrense passord til a-z, A-Z og 0-9. Bruk av æ, ø, å og andre ikke-ASCII tegn kan forårsake interoperabilitetsproblemer med systemer og nettlesere som ikke støtter internasjonale tegnsett. Det går derfor en diskusjon om å stramme inn mot bruk av æ, ø, å og andre ikke-ASCII tegn på grunn av dårlige erfaringer spesielt med passord [38]. Alle passord må også være på MD5-format. Det vil si at passordene ikke behandles i klartekst, men at den verdien man behandler er hashverdien man får etter å ha anvendt enveisfunksjonen MD5 (Message Digest Algorithm #5) på passordet. Anta at en bruker har valgt passordet 'abc123AZ'. Da er det av sikkerhetsmessige årsaker ikke denne verdien som lagres i det lokale FEIDE-systemet. Det er MD5-hashverdien av passordet som lagres, nemlig verdien 'b75194f57ecb839878af20861a33b983'.

Enkeltpersoner tildeles FEIDE-navn av sin lokale utdanningsinstitusjon som de har en definert relasjon til [36]. Før vertsorganisasjonen kan tildele FEIDE-navn må den ha en kontrakt med FEIDE, en kontrakt som regulerer organisasjonens betingelser. Kravene innebærer at det må eksistere en veldefinert og godt administrert tilknytning mellom en person og en utdanningsinstitusjon, der institusjonen kan gå god for tilknytningen og eventuelle persondata som kan formidles, og der det eksisterer en bindende avtale mellom personen og institusjonen som innbefatter et reglement som definerer plikter og rettigheter. I samarbeid med andre aktører i sektoren er det utarbeidet et forslag til standardreglement [40].

Også FEIDE-passord tildeles lokalt, og administreres i det lokale brukeradministrative systemet ved hver vertsorganisasjon [36]. Det finnes ingen standard måte å distribuere passord på, prosedyrene varierer hos institusjonene. Men i forbindelse med FEIDE-gjennomgang av det brukeradministrative systemet kvalitetssikres alle rutiner knyttet

til brukeradministrasjon. FEIDE definerer kvalitetskravene til den knytningen mellom FEIDE-navn og person som prosedyrene må oppfylle. For studenter er det vanlig å sende eller dele ut passord i et brev. Mange får også førstegangspassord tildelt ved personlig oppmøte, deretter må de selv endre passordet første gang de logger inn. Andre igjen velger passord og brukernavn selv via en selvbetjent webtjeneste. I utgangspunktet er det altså kun brukeren som kjenner sitt eget passord, unntaket er ved utsending av førstegangspassord for nye brukerkontoer.

Både brukernavn og passord oppbevares i den enkelte vertsorganisasjons brukeradministrative system. Passord skal aldri sendes eller oppbevares i klartekst, og tjenester behandler i utgangspunktet aldri passord. Dette er et særdeles viktig prinsipp i FEIDE, og det er kun innloggingsløsningen som ser passordet brukeren taster inn. For å minske risikoen ved bruk av delte datamaskiner er det mulig å reservere seg mot SSO fra innloggingssiden. Passordene oppbevares i kryptert MD5-format hos brukerens vertsorganisasjon. Krav til kryptering og oppbevaring i LDAP-tjener er dokumentert i FEIDEs attributtdokument [39].

Hvor lenge passordene er gyldige defineres lokalt, og inngår som en rutine rundt det brukeradministrative systemet [36]. FEIDE sentralt krever at autentiseringen av en person tilknyttet en vertsorganisasjon opphører når tilknytningen opphører. For eksempel at autentiseringen av en student opphører når studenten avlegger siste eksamen. Brukeren kan velge å selv skifte passord på et vilkårlig tidspunkt. Nytt passord lagres da kryptert i det brukeradministrative systemet med kopi til lokal LDAP-katalog.

Hvis en bruker har grunn til å tro at andre enn han selv kjenner sitt passord bør han umiddelbart skifte passord. Passordet bør ikke være lett å gjette, og bør helst inneholde både store og små bokstaver, og tall. Hvis brukeren ikke har anledning til å endre passord eller dersom det er driftspersonell ved den lokale vertsorganisasjonen som får kunnskap om at passordet er kompromittert bør brukerkontoen sperres inntil videre. Om passord kompromitteres uten at man skifter passord eller stenger brukerkontoen kan man komme ut for en situasjon hvor andre utgir seg for å være denne personen og får uberettiget tilgang til denne personens tjenester.

5.1.5 Personvern

a) Hvilke personopplysninger lagres, og hvor lagres de?

Data om FEIDE-brukere ligger lagret i de lokale FEIDE-løsningene ved vertsorganisasjonene. Alle data som ligger der må være korrekte, komplette og konsistente, og organisert på en standardisert måte. Høy datakvalitet er meget viktig, og for å lage en sikker og pålitelig elektronisk identitet må derfor personopplysningene identiteten bygger på være kvalitetssikret [16]. Kravene til sikkerhet og personvern er godt tatt vare på, både hos vertsorganisasjonen og hos tjenestene [14]. FEIDE sørger blant annet for at brukeren kan få innsyn i egne data og at brukeren må gi godkjennelse til overføring av data til tjenester.

FEIDEs LDAP-skjema [39] viser en omfattende oversikt over samtlige obligatoriske og valgfrie attributter for lagring av opplysninger om FEIDE-brukere og organisasjoner. Her følger en kort oversikt gjengitt i tabeller, over de obligatoriske attributtene for personer og organisasjoner. Forklaringene er hentet fra [14]. Tabellene

5.1 og 5.2 viser henholdsvis obligatoriske og frivillige attributter for personer. Tabellene 5.3 og 5.4 viser obligatoriske og frivillige attributter for organisasjoner.

Attributtnavn	**Beskrivelse**
cn (commonName)	Fullt navn
sn (surname)	Etternavn
eduPersonPrincipalName	FEIDE-navn
uid	Lokalt brukernavn
userPassword	Passord
mail	E-postadresse
norEduPersonNIN	Fødselsnummer
eduPersonAffiliation	Rolle ved organisasjonen
eduPersonOrgDN	Intern referanse til organisasjonen

Tabell 5.1: Obligatoriske attributter for personer.

Bilde (*jpegPhoto*), lokal brukeridentifikasjon (*norEduPersonLIN*), foretrukket språkform eller språk (*preferredLanguage*), fornavn (*givenName*), tittel (*title*), overordnede (*manager*), navn i foretrukket form (*displayName*), hjemmeside (*labeledURI*), fødselsdato (*norEdupersonBirthDate*), mobilnummer (*mobile*), telefonnummer ved organisasjonen (*telephoneNumber*), telefonnummer hjemme (*homePhone*), faksnummer (*facsimileTelephoneNumber*), postadresse ved organisasjonen (*postalAddress*), postadresse hjemme (*homePostalAddress*), postboks ved organisasjonen (*postOfficeBox*), postnummer ved organisasjonen (*postalCode*), geografisk tilhørighet (*l* (location)), gateadresse ved organisasjonen (*street*), organisasjon (*o* (organizationName)), intern referanse til primær organisasjonsenhet (*eduPersonPrimaryOrgUnitDN*), primærrolle ved organisasjonen (*eduPersonPrimaryAffiliation*), rolle i en angitt organisasjon/domene (*eduPersonScopedAffiliation*), URI som indikerer et sett av rettigheter til spesifikke ressurser (*eduPersonEntitlement*), digitalt sertifikat i X.509-format (*userCertificate*), digitalt sertifikat i X.509-format til bruk for e-post og andre S/MIME-applikasjoner (*userSMIMECertificate*), intern referanse for organisasjonsenheten (*eduPersonOrgUnitDN*).

Tabell 5.2: Valgfrie attributter for personer.

Attributtnavn	**Beskrivelse**
cn (common name)	Fullt navn
federationFeideSchemaVersion	Versjon av FEIDE-skjema
norEduOrgUniqueIdentifier	SO-nummer (Samordnet Opptak) for organisasjonen
mail	E-postadresse
o (organizationName)	Organisasjon
eduOrgLegalName	Navn på organisasjonens juridiske objekt
dc (domainComponent)	Domenekomponent for LDAP

Tabell 5.3: Obligatoriske attributter for organisasjoner.

Forkortelse for organisasjonen (*norEduOrgAcronym*), søkeside for personer i organisasjonen (*eduOrgWhitePagesURI*), hjemmeside for organisasjonen (*eduOrgHomePageURI*), organisasjonens sertifikatpolicy for digitale sertifikat (*eduOrgIdentityAuthNPolicy*), nummerkode for organisasjonsenhet (*norEduOrgUniqueIdentifier*), organisasjonsenhet (*ou* (organizationalUnitName)).

Tabell 5.4: Valgfrie attributter for organisasjoner.

Når en bruker er autentisert mottar klienten forespurte data fra Moria, og det er nå opp til klienten å ta vare på disse så lenge den har behov for de [14]. Hvis klienten senere trenger mer data eller ønsker dataene på nytt må brukeren autentiseres på nytt.

b) Hvilke rutiner og mekanismer er på plass?

Datatilsynet har laget en veiledning i informasjonssikkerhet for kommuner og fylker, som påpeker en rekke viktige momenter som angår sikkerhet [29]. Veiledningen stiller krav til personellsikkerhet, fysisk sikkerhet og systemteknisk sikkerhet.

I utgangspunktet er det kun brukeren selv som har tilgang til sine egne data. Av og til kan det imidlertid være nødvendig for driftspersonell å skaffe seg tilgang til en brukers private område, dennes filer eller data [40]. Dette kan være aktuelt i tilfeller der det er nødvendig for å hindre skade eller unødig belastning av IT-ressurser eller deres integritet, hvor institusjonens rykte trues eller institusjonen risikerer å pådra seg et ansvar. I andre situasjoner kan en tredjepart ønske en kopi av eller innsyn i filer eller opplysninger, for eksempel politi eller påtalemyndighet. Behandlingsansvarlig og driftspersonell skal ikke behandle personopplysninger på annen måte enn det som på forhånd er avtalt. Etter forvaltningsloven § 13 har IT-ansatte taushetsplikt for alle taushetsbelagte opplysninger de får kjennskap til gjennom utøvelse av sin stilling [40].

Det meste av data ligger i de lokale løsningene ute hos vertsorganisasjonene. Derfor er det nødvendigvis også her sikringen først og fremst skjer, lokalt for hver LDAP. Sikring mot tap av data realiseres i form av filter eller brannmur, ved hjelp av SSL for dataoverføring, og ved at FEIDE utfører bind-operasjon som om den var brukeren [38]. I tillegg er sikkerhetskopier av viktige data en god forsikring mot uforutsette forhold som diskkrasj og feilaktig sletting av data [14].

I følge personopplysningsloven skal den behandlingsansvarlige ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen [4]. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes. En brukers konto ved en institusjonen skal ha like lang varighet som tilknytningen brukeren har til institusjonen [40]. I tillegg kan brukeren få tre måneder til å rydde opp før kontoen sperres, etter nye seks måneder slettes kontoen, og etter 5 år slettes sikkerhetskopierte data. Det bør gå minst 10 år mellom siste dato den eksterne FEIDE-ID kunne brukes til å få aksess til ressurser for en person, ved hvilken som helst FEIDE-organisasjon, og til den første datoen det samme eksterne FEIDE-navnet kan brukes til å få aksess til ressurser for en annen person [35]. Slik sikres det at identitetskollisjoner aldri forekommer.

Datatilsynets veiledning i informasjonssikkerhet for kommuner og fylker [29] beskriver noen aspekter ved sletting av data. Sletting av sensitive personopplysninger er aktuelt både som følge av lovpålagte bestemmelser, ved gjenbruk av elektroniske lagringsmedier og i forbindelse med utrangering av utstyr. Ved utrangering av utstyr er det et særlig behov for å slette tidligere data, slik at sensitive personopplysninger ikke kommer på avveie. Det må foreligge tilfresstillende rutiner for sletting eller tilintetgjøring av alle lagringsmedier som brukes. Medier som inneholder sensitive personopplysninger skal også merkes slik at disse ikke kommer i gale hender.

c) Logges transaksjoner, er de i så fall sikret mot endringer?

Innlogginger og andre transaksjoner i FEIDE logges og tidsstemples [38]. Maskinen kjører NTP (Network Time Protocol) for korrekt klokke, og er koblet nært til riktig klokke som tas ned i samme rom.

d) Ivaretas personverninteresser generelt, og oppfylles personopplysningsloven?

FEIDE skal oppfylle både personopplysningsloven [4] og personopplysningsforskriften [30]. Personopplysningsloven beskytter brukere mot at personvernet krenkes gjennom behandling av personopplysninger, og dreier seg om hvordan personopplysninger skal samles inn, oppdateres, oppbevares og behandles. Rutiner som sikrer god informasjonssikkerhet skal være på plass. Se kapittel 4.1.5.d) for flere detaljer om innholdet i personopplysningsloven og personopplysningsforskriften.

I FEIDE blir brukeren informert om hvilke data en aktuell tjeneste skal få om han på Morias innloggingsside [14]. Slik er brukeren alltid informert om hvilke data som brukes og må gi sitt samtykke i hvert tilfelle, i tråd med et godt personvern.

5.1.6 Sikkerhetsbehov

a) Hva antas om grad av nødvendig sikkerhet for ulike tjenester?

Ulike tjenester stiller ulike krav til sikkerhet, derfor er det viktig at nettverksressursene tar stilling til hvilket sikkerhetsnivå hver tjeneste krever. Noen muligheter for realisering av ulike sikkerhetsnivå er beskrevet i NOU2001:10 [41]. Brukernavn og passord eller pinkode er en mye brukt løsning, særlig for tjenester med ikke altfor store krav til sikkerhet. Men brukernavn og passord kan også brukes for tjenester med et veldig sterkt sikkerhetsbehov, så lenge passordet, gjerne et engangspassord, distribueres og oppbevares på en sikker nok måte. Samtlige FEIDE-tjenester tilbyr i dag passordbasert innlogging. Et alternativ er autentisering med softsertifikater, altså digitale sertifikater med nøkler som er lagret i programvare. Nøklene kan for eksempel være lagret på brukerens datamaskin eller på en diskett, og tilgang til nøklene må kreve autentisering. Sertifikater av typen ”Person-Standard” vil ofte være en god løsning for sikker identifisering. Der det stilles svært store krav til sikkerhet vil sertifikater med nøkler lagret på smartkort med fordel kunne tas i bruk. Alle kalkulasjoner utføres da i smartkortet, og løsningen tilbyr stor grad av sikkerhet så lenge ingen andre enn eieren selv har tilgang til smartkortet. Sertifikater av typen ”Person-Høyt” og ”Virksomhet” tilbyr sikker autentisering av henholdsvis personer og virksomheter for tjenester med veldig strenge sikkerhetskrav. Mange antar at

sertifikater generelt er sikrere enn et passord, noe som ikke nødvendigvis er riktig. Et passord distribuert på riktig måte kan være minst like sikkert som et digitalt sertifikat.

5.1.7 Systemsvikt

a) Hva er konsekvensene om sikkerhetsantakelsene ikke slår til?

Det ligger en rekke sikkerhetsantakelser til grunn for FEIDE-systemet, blant annet antas det at alle etablerte sikkerhetsrutiner følges. En sikker behandling av personopplysninger er helt nødvendig for den totale sikkerheten, som settes på spill dersom personer eller systemer som håndterer sensitive opplysninger svikter sine rutiner. Resultater av svikt i rutiner kan være at uvedkommende får tilgang til utstyr hvor sensitive personopplysninger behandles, og at brukernes personverninteresser settes på spill. Tyveri av datamaskiner og sikkerhetskopier, eller sabotasje og hærverk mot vitale deler av informasjonssystemet, kan avsløre personopplysninger eller informasjon som angår sikkerheten i systemet.

Gode sikkerhetsrutiner er på plass og følges opp. Rutinene realiserer blant annet adgangskontroll, sikring av personopplysninger og informasjon som angår informasjonssikkerheten, samt tiltak mot fysiske angrep. Allikevel er det umulig å være fullstendig sikret mot uautorisert adgang. Målet er derfor at valgte sikkerhetsløsninger skal kunne oppdage forsøk på uautorisert inntrenging, samt kunne forsinke angrepet slik at respons på utløst alarm kan ha mulighet til å avverge eller begrense konsekvensene av sikkerhetsbrudd [29].

Misbruk av en annen persons identitet skal kunne forhindres så lenge man holder sitt passord skjult for andre, og så lenge passord kun behandles i kryptert form. Personer som har tilgang til samme datamaskin vil imidlertid kunne spore opplysinger som kommer fra denne maskinen.

5.1.8 Mobilitet

b) Hvor lett er det å benytte tjenester fra nye lokasjoner og med nytt utstyr?

I dag er det meget lett for FEIDE-brukere å benytte sine vanlige FEIDE-tjenester fra nye lokasjoner og med nytt utstyr. FEIDE benytter per i dag brukernavn og passord for innlogging. Hvis softsertifikater skulle benyttes ville det være nødvendig å ha nøkler og sertifikat lagret på alle maskiner FEIDE-tjenester skulle benyttes fra. For smartkortapplikasjoner kreves det at en smartkortleser medbringes, samt at programvaren for kortleseren installeres på alle maskiner man ønsker å benytte FEIDE-tjenester fra.

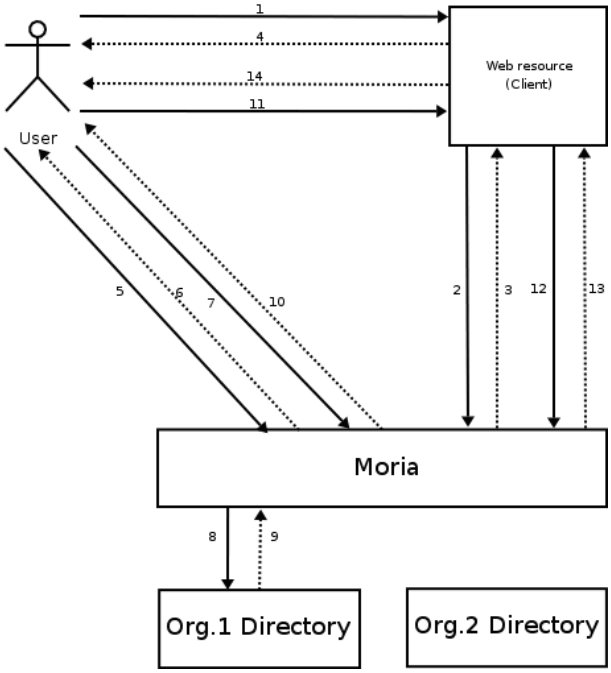
5.2 Meldingskompleksitet

Denne seksjonen inneholder spørsmål om hvordan meldingsutvekslingen foregår i FEIDE. Første punkt ser på hvor de ulike meldingene går, andre punkt ser på hvilke mekanismer som sikrer meldingene under sending.

5.2.1 Meldingenes gang

a) Hvordan går meldingene ved autentisering?

Figur 5.3 [34] viser hvordan autentisering mot Moria kan foregå ved webinnlogging. En overordnet beskrivelse av trinnene i autentiseringsprosessen følger under [35].



Figur 5.3: Autentisering ved bruk av FEIDE.

En bruker ønsker å nå en aksessbeskyttet webressurs fra en utdanningsinstitusjon (1). For at brukeren skal få tilgang til tjenesten må han ha en tilknytning til institusjonen, han må ha en FEIDE-identitet, og være assosiert med en rolle som har tilgang til tjenesten.

Siden ressursen er personlig kreves det at brukeren kan identifisere seg ved hjelp av sitt FEIDE-navn og et hemmelig passord. Webtjenesten ber om en autentiseringssesjon fra Moria (2), og med dette kallet sendes en liste over brukerattributter tjenesten ønsker. Moria svarer med å returnere en URL til innloggingssiden (3). Brukerens nettleser videresendes så til en nettside for FEIDE-innlogging. Først sendes en melding til brukerens nettleser med URL'en Moria returnerte (4). Nettleseren sender en forespørsel for innloggingssiden (5), og brukeren presenteres for et påloggingsskjema (6). Videre overføres brukernavn og passord til innloggingstjenesten ved at brukeren fyller ut et HTML skjema med brukernavn og passord til Moria (7).

Når brukeren har oppgitt brukernavn og passord foretar Moria selve autentiseringen. Moria finner riktig LDAP-tjener, og åpner en forbindelse til denne (8). LDAP-forbindelsen lagres i Moria-sesjonen for senere bruk. LDAP-tjeneren returnerer svar til Moria på om autentiseringen er vellykket (9), hvis den ikke er det får brukeren opp et nytt innloggingsskjema.

Etter at brukeren er autentisert av Moria sendes han tilbake til webtjenesten (10, 11). Han har da en billett i URL'en, som ble generert etter en suksessfull autentisering. Klienten spør etter brukerattributtene fra Moria, identifisert ved billetten (12). Om denne er gyldig for en autentisert bruker returnerer Moria de forespurte attributtene (13). Om ingen attributter er forespurt eller hvis disse er utilgjengelige, returneres en tom tabell som en bekreftelse på at brukeren er autentisert men ingen data er tilgjengelige (13). Til slutt returneres webressursen til brukerens klient, og brukeren har fått innvilget aksess til webressursen (14). Etter at tjenesten har mottatt forespurte attributter fra Moria er FEIDE-tjenesten avsluttet, og tjenesten må selv mellomlagre nødvendige data. For å få nye data om brukeren må en ny autentisering foretas.

I utgangspunktet skal innloggingsfunksjon via Moria benyttes av alle FEIDE-tjenester [14]. Det finnes imidlertid tilfeller hvor vertsorganisasjoner ønsker å la sine brukere benytte FEIDE-navn og passord til pålogging, men ikke kan bruke funksjonaliteten i Moria. I slike tifeller kan en tjeneste for eksempel logge inn mot den lokale FEIDE-katalogen, såkalt LDAP-innlogging. Denne formen for pålogging brukes kun for tjenester som er lokale for vertsorganisasjonen. Et annet alternativ er at tjenestene bruker et eget innloggingssystem som er synkronisert mot FEIDEs lokale løsning, eventuelt at tjenestene benytter direkteautentisering. Slike metoder som ikke benytter innlogging via Moria medfører økt sikkerhetsrisiko, siden tjenestene selv må håndtere brukernavn og passord. Derfor må de kun brukes når det er tatt spesielt hensyn til sikkerhet, for eksempel ved å kryptere kommunikasjonen mot LDAP-katalogen. LDAP-katalog og tjener kan ligge i samme domene, det bør være god adgangskontroll på tjeneren, tjenester bør ikke lagre eller videresende passord, og tjenester bør ikke hente ut mer data om en person enn det personen har gitt tillatelse til.

Det arbeides med nye grensesnitt mot FEIDEs innloggingstjeneste [14]. Disse vil være alternative metoder for FEIDE-innlogging for tjenester som ikke er webbaserte. To metoder har vært i testdrift siden høsten 2005, begge to skjuler detaljer rundt kommunikasjonen med Moria for tjenesten. Den første av de to er direkteautentisering via LDAP, et grensesnitt som gjør det mulig for en tjeneste å logge inn direkte med FEIDE-navn og passord mot lokal LDAP-katalog. Den andre er direkteautentisering via JAAS-modul (Java Authentication and Authorization Service), Javas teknologi for autentisering og autorisasjon. JAAS-modulen gjør at tjenester laget i Java kan tilby sine brukere direkte FEIDE-pålogging.

b) Hvordan går meldingene ved kommunikasjon med brukersted?

Når en bruker ved en utdanningsinstitusjon ønsker å kommunisere med sitt brukersted uten at det stilles krav til sikkerhet går kommunikasjonen direkte mellom bruker og brukersted. Dette kan for eksempel være tilfelle når en student ønsker å laste ned informasjon som ikke krever at han identifiserer seg. Autentiseringsprosessen og kommunikasjon med brukerstedet etter autentisering krever at meldingene overføres på en sikker måte. Slik sikkerhetsinformasjon skal ikke kunne endres på veien, man skal være sikker på hvem avsender er, og innholdet skal være uforståelig for de som måtte lykkes i å fange opp meldinger under sending. For å realisere dette brukes digitale signaturer og kryptering av innhold.

For en fremtidig FEIDE-løsning basert på PKI og digitale sertifikater vil signering og kryptering av innhold kunne realiseres på samme måte som for Sikkerhetsportalen.

Studenter med FEIDE-tilknytning kan for eksempel ha et smartkort integrert i studentkortet sitt, med en privat nøkkel som brukes til å fremstille digitale signaturer inne i kortet. Når noen ønsker å sende kryptert informasjon til studenten krypterer de informasjonen med studentens offentlige nøkkel, og ved mottak kan studenten dekryptere med sin private nøkkel. Studenten kan også selv kryptere informasjon med mottakers offentlige nøkkel. Nøkler og sertifikater trenger ikke nødvendigvis lagres i maskinvare, de kan også lagres i programvare på brukers private datamaskin.

I esignaturloven [23] stilles det en rekke krav til kvalifiserte elektroniske signaturer. En slik signatur skal være entydig knyttet til undertegneren, være laget ved hjelp av midler bare undertegneren har kontroll over, og knyttet til andre elektroniske data slik at det kan oppdages om disse er endret etter signering. Videre skal den være basert på et kvalifisert sertifikat, og fremstilt av et godkjent signaturfremstillingssystem. Siden FEIDE er uavhengig av autentiseringsløsning, spesifiseres ingen fast prosedyre for signaturfremstilling og bruk av signaturer. Men det anbefales at hvis digitale signaturer benyttes for identifisering så bør sertifikater og signaturer fremstilles, sikres og anvendes på en slik måte at de oppfyller esignaturloven.

5.2.2 Sikring av meldingene

a) Kan sensitiv informasjon leses ut av meldinger på avveie?

   Nei, i teorien skal det være vanskelig å lese informasjon ut av meldinger på avveie. Dette fordi all trafikk til og fra Moria er kryptert ved hjelp av SSL, og det anbefales også sterkt at kommunikasjonen mellom sluttbruker og webtjeneste er beskyttet ved kryptografi. Det må uansett tas et visst forbehold, siden all informasjon en bruker oppgir på sin lokale datamaskin kan spores av andre med tilgang til samme maskin.

b) Hvilke mekanismer sikrer meldingene?

   Meldingene sikres ved to tekniske mekanismer, kryptering av innhold og digital signatur. Kryptering av innhold gir konfidensialitet, det vil si at innholdet i dokumentet ikke kan bli kjent av uvedkommende [42]. Digital signatur realiserer autentisering og ikke-benekting av opphav, altså er innholdet beskyttet mot at utenforstående har forfalsket det, og den som har signert dokumentet kan ikke senere benekte dette.

   FEIDE antar at all kommunikasjon som involverer unike ID'er går gjennom krypterte nettverk [35]. Eventuelt så har kommunikasjonen tilsvarende beskyttelse, slik som en fysisk barriere mellom smartkort og smartkortleser. All kryptering og dekryptering foregår i endesystemene, slik at brukerinformasjon aldri finnes dekryptert andre steder enn hos lokalt brukeradministrativt system og lokal LDAP, samt mellomlagret hos tjenester som har mottatt informasjon fra Moria.

5.3 Robusthet mot feilsituasjoner

Denne seksjonen ser på FEIDEs robusthet. Første punkt identifiserer mulige trusler for systemets tilgjengelighet og ser på systemets dimensjonering, andre punkt ser på hva som gjøres for å sikre høy tilgjengelighet. Punkt nummer tre identifiserer mulige flaskehalser i systemet.

5.3.1 Feilsituasjoner

a) Er det mulig å gjøre systemet utilgjengelig ved diverse angrep?

Det er naturligvis mulig å gjøre FEIDE-systemet utilgjengelig ved å rette angrep mot systemet. Det mest effektive er å ta ut det settet av maskiner som kjører innloggingstjenesten, enten ved å gjøre ting med ruting, navneoppslag eller trafikklast [38].

Når det gjelder den lokale delen av FEIDE-systemet må både autentiseringstjeneren og det brukeradministrative systemet være godt beskyttet. Autentiseringstjeneren må være beskyttet mot hacking og falsifikasjon av informasjon [35], det er jo her alle personopplysninger ligger. Det brukeradministrative systemet må også være godt beskyttet, da det er dette systemet autentiseringstjeneren oppdateres fra. Her ligger personlige opplysninger og informasjon om institusjonens indre liv. Nettverksressurser må ha SSL/TLS sertifikat eller tilsvarende, signert av noen autentiseringstjeneren stoler på for å sikre at kommunikasjonen mellom nettverksressursen og autentiseringstjeneren er beskyttet både mot bugging og replay angrep. Alle nettverksressurser og autentiseringstjenere må bære tjenersertifikat godkjent av FEIDE.

Sesjonskapring går ut på å overta en sesjon ved å avlytte kommunikasjon mellom bruker og webressurs [14]. For å minske risikoen for kapring av sesjoner endres Morias sesjons-ID, den såkalte billetten, etter autentisering. Billetten genereres slik at den skal være praktisk talt umulig å gjette. Det eneste stedet man kan kapre en sesjon er i stegene hvor brukeren sendes tilbake til webressursen etter å ha verifisert brukernavn og passord mot lokal LDAP-katalog. En kaprer må altså stoppe forespørselen mellom Moria og bruker eller mellom bruker og webressurs, og bruke billetten til å presentere seg selv for webressursen og fortsette som en autentisert bruker. Ved å kryptere forbindelsen reduseres risikoen for kapring av sesjoner betydelig, og det anbefales derfor sterkt å kryptere all kommunikasjon mellom brukere og webressurser, inkludert videresendingen fra Moria tilbake til webressursen.

I sin veiledning i informasjonssikkerhet [29] kommer Datatilsynet med forslag til tiltak for å minske skadene av ødeleggende program. Det anbefales tekniske sikkerhetsbarrierer som gjør det mulig å hindre utførelse av program som automatisk overføres fra eksternt datanett, og de siste sikkerhetsoppdateringer for brannmur og operativsystem skal være på plass. Sikkerhetsbarrieren skal være motstandsdyktig mot DoS-angrep. Sikkerhetstiltak skal også omfatte sikring mot ødeleggende programmer; i form av virussjekk av innkommende filer og flyttbare lagringsmedium.

b) Hvor mange brukere, brukersteder eller transaksjoner er systemet designet for å håndtere?

FEIDE-systemet bør skalere til noen få millioner individer, og klientløsningen til noen hundre tusen brukere [35]. Tjenerløsningen bør skalere til noen tusen tjenere, og løsningen for autentiseringstjenere til noen hundre tjenere, typisk en per institusjon. Altså bør det kunne finnes noen hundre tusen FEIDE-brukere i systemet, noen tusen tjenestetilbydere og noen hundre institusjoner.

c) Hva skjer om forbindelsen brytes eller systemet av andre grunner går ned?

Hvis systemet går ned utilgjengeliggjøres tjenesten og en feilmelding dukker opp hos brukeren. Alle transaksjoner avbrytes og sesjoner ugyldiggjøres. Det vil si at når systemet er oppe igjen må brukere autentisere seg på nytt for å få tilgang til tjenestene de var pålogget for da systemet gikk ned i første omgang.

5.3.2 Tilgjengelighet

a) Hvor stor tilgjengelighet forventes systemet å ha?

FEIDE skal i utgangspunktet være tilgjengelig døgnet rundt hele året, og har ingen planlagt nedetid i forbindelse med oppdateringer og periodisk drifting. Dette lar seg gjøre fordi FEIDE kjører parallelle systemer, og oppdaterer ett av disse om gangen. Først tas det ene systemet ned, så oppdateres det og settes i drift igjen, før det andre tas ned og oppdateres.

b) Hva gjøres for å sikre høy tilgjengelighet?

FEIDE sørger gjennom sine driftsrutiner og redundans, samt gjennom innloggingstjenestens design og arkitektur, for at vertsorganisasjonene kan stole på at innloggingstjenesten har en meget høy tilgjengelighet [14]. Moria er en kritisk komponent i FEIDE, og mye er gjort for å sikre at Moria har høy tilgjengelighet. FEIDE er designet for å kunne håndtere alle forespørsler om autentisering, og all kommunikasjon skal være sikret. Videre skal innloggingstjenesten kun hente ut de data som autentiserte brukere har tillatt å gi fra seg. Alt dette gjør at vertsorganisasjonene stoler på FEIDE.

FEIDE benytter lastbalansering mellom flere servere for å sikre at innloggingstjenesten alltid skal være tilgjengelig. En hot stand-by med ett ekstra sett av servere bidrar til høy tilgjengelighet.

5.3.3 Flaskehalser

a) Finnes det deler av systemet som har stor innvirkning på den totale ytelsen?

Når det gjelder det sentrale FEIDE-systemet har det vært lite ytelsesproblemer, og det er i all hovedsak lokal LDAP som er den største flaskehalsen. Det er rundt lokal LDAP det har vært mest diskusjon om ytelse.

5.4 Implementerings- og driftskostnader

Denne seksjonen identifiserer kostnader knyttet til implementering og drift av FEIDE; sentralt, for brukersteder og for sluttbrukere.

5.4.1 Kostnader til implementering og drift

a) Hvilke kostnader har man sentralt?

Det finnes mange måter å betale for elektronisk ID og signatur på. I et dokument om forretningsmodeller for bruk av elektronisk ID og signatur [8] skisseres en rekke modeller for betaling. I løsninger der brukerne betaler kan det enten være en engangsavgift som inkluderer startpakke, abonnement og all bruk, startpakken kan ha en egn pris og i tillegg kommer et abonnement som dekker all bruk, eller i tillegg til et fast abonnement kan det komme en variabel kostnad knyttet til bruk.

Enkelte har sett at brukersteder har større betalingsvilje enn sluttbrukerne, og har derfor lagt opp til en forretningsmodell der brukerstedene betaler. En måte å realisere dette på er å la brukerstedet betale en høy inngangspris og en lav pris per bruker for all bruk. Alternativt kan man droppe inngangsprisen og la brukerstedene betale en fast pris per bruker. For brukersteder som ikke har noen fast brukergruppe eller der bruken per bruker er veldig sjelden kan transaksjonsbaserte modeller være en løsning. Brukersteder med mange små transaksjoner kan ha fordel av en omsetningsbasert modell, der brukerstedet betaler en fast andel av omsetning.

Disse modellene kan gjerne formes som trappetrinnsmodeller, slik at det blir billigere jo flere brukere et brukersted har. Volumforpliktelser bør også gi lavere priser per bruker eller per transaksjon. Gjerne benyttes kombinasjoner av modellene, slik at både sertifikatinnehaver og sertifikatmottaker betaler. Prisene kan variere i forhold til sikkerhetsnivå, og prisene kan avhenge av om sertifikatet benyttes for autentisering eller ikke-benkting. I tillegg til kostnadene knyttet til bruk av Sikkerhetsportalen er det betydelige etableringskostnader forbundet med å ta i bruk elektronisk ID og signatur, og utfordringen er å finne gode modeller som deler disse utgiftene.

Den sentrale FEIDE-tjenesten drives av UNINETT AS. Finansieringen av tjenesten blir etter all sannsynlighet i fremtiden basert på tilknytningsavgift, og for frittstående tjenesters del en bruksavgift [16]. I perioden fram til full innføring er den sentrale FEIDE-tjenesten tilført midler fra Kunnskapsdepartementet og UNINETT AS, til driften og til utvikling av enkelte programvarekomponenter.

Noen kostnadsfaktorer knyttet til den sentrale FEIDE-tjenesten er maskinvare, daglig drift og implementering av Moria [38]. Maskinvaren kommer på omtrent 70.000 kroner i året, daglig drift og vaktordning døgnet rundt kommer på omtrent ett årsverk i året, og implementering av Moria kommer på rundt tre årsverk per år.

b) Hvilke kostnader har brukerstedene?

Å ta i bruk FEIDE krever en god del utstyr ved den enkelte FEIDE-institusjon. Blant annet trengs det datasystemer og -maskiner, noe de fleste utdanningsinstitusjoner allerede har uavhengig av om de er tilknyttet FEIDE eller ikke. Det trengs et brukeradministrativt system for brukeradministrasjon, og det trengs registre med persondata av høy kvalitet. Dette kan være registre for eksempel for opptak, karakterer og lønn. Videre trengs det en sikker autentiseringstjener, og en tjeneste som skal benytte FEIDE-innlogging.

Brukersteder som skal ta i bruk FEIDE trenger en FEIDE-mellomvare for autentisering av brukere, og organisasjonen er tilkoblet en sentral innloggingstjeneste som muliggjør bruk av eksterne tjenester og som gir en mulighet til å tilby organisasjonens egne eksterne tjenester for folk utenfra [16]. De andre resultatene av FEIDE er endringer i organisasjonens ordinære drift og administrasjon. Dette er i hovedsak opprydding og generell forbedring av persondatahåndtering, noe som har stor egenverdig uavhengig av FEIDEs bruk av dataene. Brukerstedene dekker sine egne kostnader med det brukeradministrative systemet og rutiner for datavask og vedlikehold av personopplysninger [14]. Tjenestene dekker egne kostnader med tilpasning til FEIDEs innloggingstjeneste Moria.

I tillegg til etableringskostnader kommer også driftskostnader knyttet til det å være en FEIDE-institusjon. For bruk av innloggingstjenesten i det sentrale FEIDE-systemet betalte institusjoner i 2005 en krone per bruker som benyttet FEIDE-innlogging, pluss et mindre engangsbeløp [14].

c) Hvilke kostnader har sluttbrukere?

Å ta i bruk tjenester fra FEIDE gir ingen direkte kostnad til studenter og lærere. En person som skal ta i bruk FEIDE-innlogging får tildelt et brukenavn og passord fra sin utdanningsinstitusjon uten å selv måtte betale for det. For FEIDE-institusjoner som måtte ønske å benytte PKI må institusjonene sørge for sertifikater til sine brukere.

5.5 Brukervennlighet

Denne seksjonen ser på FEIDEs brukervennlighet. Første punkt ser på brukerutstyr, andre punkt på hvordan brukersteder og sluttbrukere kommer i gang med FEIDE, og tredje punkt vurderer brukergrensesnittet.

5.5.1 Krav til brukerutstyr

a) Er løsningen plattformuavhengig med hensyn til operativsystem og nettleser?

FEIDE er en ikke-kommersiell tjeneste for teknologi- og plattformuavhengig autentisering av personer i utdanningssektoren [14]. FEIDE fungerer godt uavhengig av hvilket operativsystem eller hvilken nettleser brukeren benytter. Av alle operativsystemer og nettlesere FEIDE er testet med er det ikke funnet kombinasjoner som FEIDE ikke fungerer med. Av operativsystemer er Windows XP, 2000 og 98 testet, samt diverse Linux varianter, Mac OSX og Mac OS9 [38]. Av nettlesere er Internet Explorer, Opera, Firefox, Mozilla, lynx og links testet. Det er sannsynligvis kombinasjoner av operativsystem og nettlesere det ikke er bekreftet at FEIDE fungerer med, men FEIDE har 100.000 brukere og ingen rapporterte problemer så løsningen kan nok sies å være plattformuavhengig.

b) Stilles det krav til brukerens maskinvare/brukerterminal?

Sluttbrukere av dagens passordbaserte FEIDE trenger ikke å installere ekstra maskinvare for å ta i bruk tjenester fra FEIDE, det eneste som trengs er at brukeren har et brukernavn og passord. Ved eventuell realisering av innlogging med sertifikater kan det være aktuelt å ta i bruk smartkort og tilhørende smartkortleser.

5.5.2 Å ta i bruk systemet

a) Hvordan kommer brukersteder i gang?

Før et brukersted tar i bruk FEIDE-innlogging må det ryddes opp i institusjonens datasystemer, samt at brukeradministrativt system og autentiseringstjener må settes opp. Rutiner og støttesystemer som sikrer god datakvalitet i registre der persondata forvaltes må være på plass [43]. For hver datatype velges ett register som autorativt kildesystem. Autorative personopplysninger er opplysninger som kommer fra den mest pålitelige kilden, for eksempel er folkeregisteret autorativ kilde for en persons navn og fødselsdata, mens en høyskole er autorativ kilde for en persons tilknytning til høyskolen. Sannsynligvis gjør man en engangsopprydning her, og til slutt sørger man for at det er mulig å eksportere persondata fra de autorative kildesystemene.

Videre må institusjonen innføre elle oppgradere et brukeradministrativt system (BAS) som får persondata fra de autorative kildene og som oppretter brukerkontoer. Videre må institusjonen legge ut en katalog, en autentiseringstjener (AT), som knyttes til FEIDEs sentrale innloggingstjeneste Moria. Med denne katalogen på plass kan brukere logge på FEIDE-tjenester ved hjelp av sitt FEIDE-navn. Ved behov tilbyr FEIDE hjelp og støtte til sine brukersteder via telefon eller e-post.

b) Hvordan kommer sluttbrukere i gang?

For å benytte FEIDE-innlogging må en person være tildelt en FEIDE-identitet ved sin utdanningsinstitusjon. Ved første gangs pålogging endres førstegangspassordet til et selvvalgt passord. Generelt er det veldig lett for sluttbrukere å komme i gang med FEIDE. Hvis et brukersted skulle ønske å ta i bruk sertifikater for autentisering og signering må brukere få utstedt et sertifikat før de tar i bruk FEIDE, lagret i enten programvare eller maskinvare.

5.5.3 Brukergrensesnitt

a) Er menyene intuitive?

Innloggingssiden for FEIDE er intuitiv og lett å forstå. Siden inneholder forklaringer på hvordan man logger inn og hvilken informasjon som formidles om brukeren, samt svar på noen av de vanligste spørsmål knyttet til innlogging.

I likhet med Sikkerhetsportalen har også FEIDEs innloggingssider støtte for begge de norske målformene, samt for engelsk og samisk. Se figur 5.4 for hvordan valg av språk er synlig i innloggingsvinduet.

Figur 5.4: FEIDEs innloggingsside har støtte for flere språk.

b) Får brukeren tydelig beskjed om hva som skjer?

Fra FEIDEs innloggingsside får man beskjed om hvilken informasjon som formidles. Ved å oppgi brukenavn, passord og institusjon og trykke på innloggingsknappen

samtykker man i at Moria videresender disse brukerattributtene. Man kan også velge å avbryte en tjeneste om man ikke ønsker at informasjonen skal formidles. Generelt holdes brukeren orientert om hvilke transaksjoner som utføres og hvilken informasjon som tilgjengeliggjøres.

Fordeler ved innføring av FEIDE

Innføring av FEIDE i utdanningssektoren skal gi en mer samkjørt og effektiv identitetsforvaltning for norske skoler, høyskoler og universiteter. En engangsopprydning i de enkelte institusjoners personopplysningsregistre og tildeling av FEIDE-identiteter etter en felles standard skal sikre at personinformasjon er korrekt og oppdatert, samt at enhver FEIDE-bruker kan gjenkjennes også ved hvilken som helst annen FEIDE-institusjon enn sin egen.

FEIDE-innføring gir i første omgang gevinster for lærestedene. Det er positivt for det enkelte lærestedet å sørge for en sikker knytning mellom FEIDE-navnet og personopplysningene i organisasjonens elev- student- og personalregistre [14]. Videre vil det være penger å spare på at alle tjenester benytter de samme personopplysningene, man er sikker på at det ikke finnes motstridende opplysninger i systemene og at de til enhver tid er gyldige. Når all informasjon er samlet og unødvendig redundans fjernet blir det også færre systemer og mindre informasjon som skal beskyttes mot innbrudd og annen uautorisert tilgang. Derfor bedres samtidig informasjonssikkerheten og personvernet. Ved hjelp av passord eller sertifikater sørger FEIDE for en sikker knytning mellom identitet og person, og med en slik sikker identifikasjon kan mange flere tjenester bli selvbetjente.

En tjeneste som bruker FEIDE-innlogging har samtlige elever, studenter og ansatte i hele sektoren som potensielle brukere, og kan stole på identiteten til alle FEIDE-brukere siden de andre utdanningsinstitusjonene håndterer identitetsforvaltning på samme måte som dem selv. Sluttbrukere av FEIDE kan ikke bare bruke tjenester fra sin egen institusjon, men også alle andre FEIDE-tjenester som er åpnet for de.

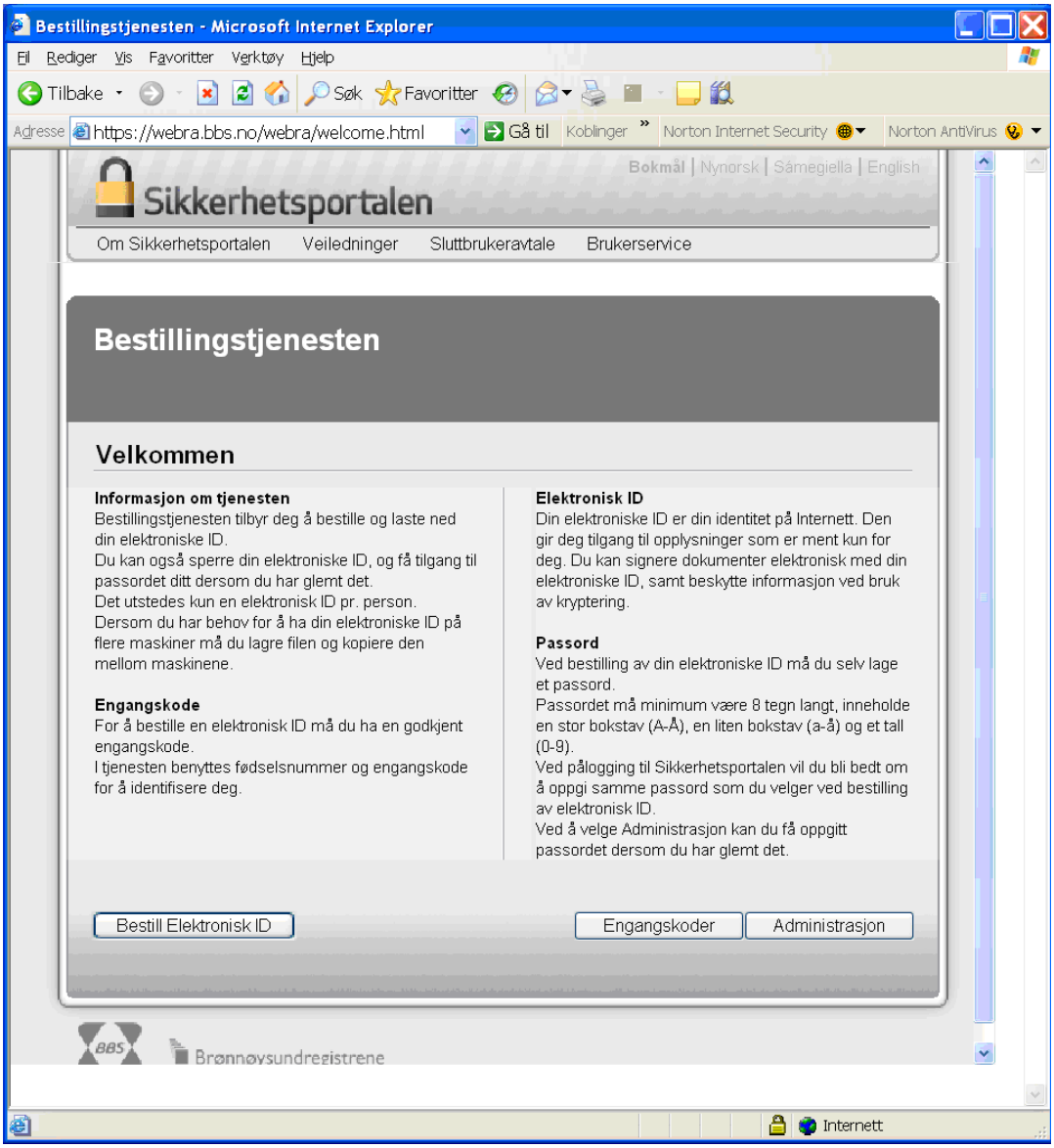
6 Eksperimentell del

For å bygge opp under det teoretiske arbeidet med denne oppgaven er det utført en eksperimentell del. I Sikkerhetsportalsystemet ligger all informasjon om brukere lagret i sertifikater, og det er sertifikatene som brukes for autentisere brukere og for å utveksle denne informasjonen. Derfor er sertifikatene som brukes i systemet særlig interessante, og de studeres nærmere i en eksperimentell del i kapittel 6.1. Det studeres hvilke sertifikater som er tilgjengelige for bruk med Sikkerhetsportalen i dag, hvordan man får tak i disse, hvordan man installerer de, og hva de kan brukes til. Eksperimentet bidrar til å forstå sertifikatenes rolle i Sikkerhetsportalsystemet, og til å fastslå hvor brukervennlig systemet er for sluttbrukere.

FEIDE har en helt annen struktur på sine elektroniske identiteter, basert på brukernavn og passord og en mengde brukerdata som ligger hos den enkelte hjemmeorganisasjon. FEIDE har en åpen testtjeneste som gjør det mulig å integrere FEIDE-innlogging i egne tjenester, og en slik integrasjon er gjennomført i forbindelse med denne oppgaven. Hvordan integrasjonen kan foregå beskrives i kapittel 6.2. Eksperimentet er ment å gi et godt innblikk i hvilke integrasjonsmuligheter som eksisterer, hvordan kommunikasjonen går i FEIDE, og hvordan FEIDEs designvalg med billetter i brukerens URL gjør at brukere autentiseres og tjenester henter ut brukerdata fra Moria på en sikker måte.

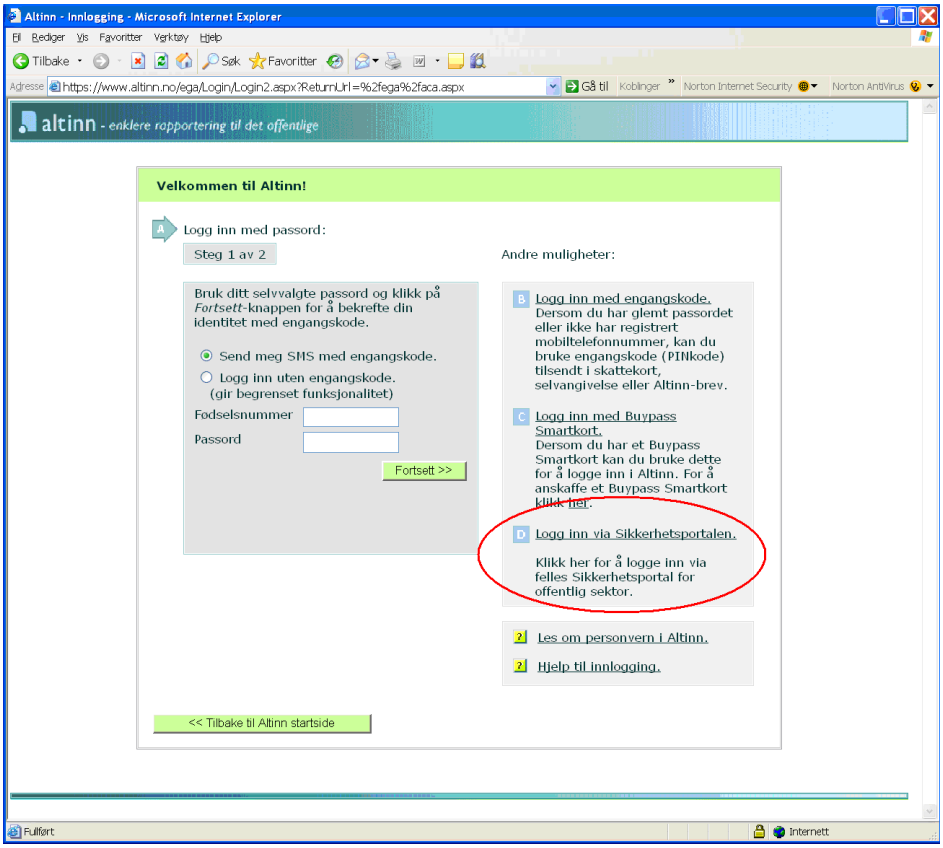
6.1 Sikkerhetsportalens sertifikater

I forbindelse med denne oppgaven ble sertifikatene ZebSign utsteder for bruk med Sikkerhetsportalen studert. Disse sertifikatene er av typen ZebSign Standard ID, og oppfyller kravene til sikkerhetsnivået ”Person-Standard” i kravspesifikasjon for PKI i offentlig sektor [17]. Før man som sluttbruker kan ta i bruk innlogging via Sikkerhetsportalen må et sertifikat, en såkalt en elektronisk ID, bestilles og lastes ned fra https://webra.bbs.no. Det første som må gjøres i den forbindelse er å bestille engangskoder fra BBS, man oppgir navn og fødselsnummer og får noen dager senere engangskodene sendt til folkeregistrert adresse. Med disse kodene kan man bestille sin elektroniske ID ved å oppgi fødselsnummer, en engangskode og et selvvalgt passord. Man må også godta en sluttbrukeravtale samt oppgi en gyldig e-postadresse. I neste omgang mottar man en e-post med lenke til nedlastingssted for sin elektroniske ID. Man identifiserer seg med fødselsnummer, og laster deretter ned en PKCS#12-fil (Public Key Cryptography Standard) som inneholder både sertifikat og privat nøkkel. Sertifikatet kan installeres flere ganger, for eksempel i ulike nettlesere og på ulike maskiner. Det kan imidlertid lastes ned bare én gang, så det er lurt å lagre en kopi av sertifikatet for senere bruk. Dersom man senere ønsker å benytte tjenester fra Sikkerhetsportalen fra en annen maskin enn man har sertifikatet installert på og man ikke har lagret sertifikatfilen, må man bestille og laste ned et nytt sertifikat. I det man laster ned det nye sertifikat vil det gamle sertifikatet ugyldiggjøres. Man kan også selv når som helst sperre sertifikatet sitt fra https://webra.bbs.no. God dokumentasjon for hvordan sertifikatene installeres er tilgjengelig for de vanligste nettleserne Internet Explorer, Firefox, Mozilla, Netscape, Opera, Konqueror og Safari. Dokumentasjonen veileder brukeren gjennom installasjonen og gir gode føringer i forhold til valg av sikkerhetsnivå. I det man installerer sertifikatet godkjenner man samtidig at operativsystemet automatisk kan klarere sertifikater utstedt av ZebSign Standard ID CA, ved å installere leverandørens rotsertifikat. Figur 6.1 viser startsiden for https://webra.bbs.no, hvor man kan bestille engangskoder og elektronisk ID, samt administrere denne ID’en.

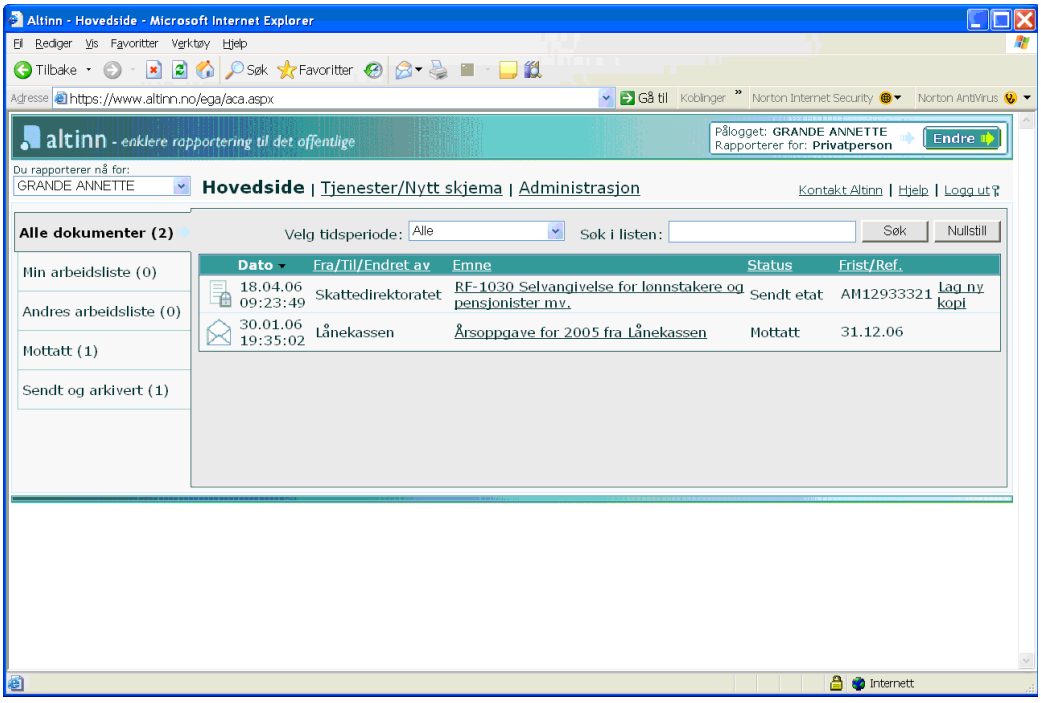


Figur 6.1: Tjeneste for bestilling av engangskoder og elektronisk ID.

Når man har installert sitt ZebSign Standard ID sertifikat i nettleseren kan man for eksempel logge inn på Altinn via Sikkerhetsportalen. Figur 6.2 viser påloggingssiden til Altinn, http://www.altinn.no, hvor man blant annet kan velge innlogging via Sikkerhetsportalen. Etter å ha valgt denne innloggingstypen må man velge riktig sertifikat samt godta at data signeres med tilhørende private nøkkel. Til slutt må man også oppgi passordet man valgte ved bestilling av sertifikatet. Hovedsiden i Altinn inneholder en oversikt over arbeidslister, og over sendte og mottatte dokumenter. På hovedsiden finnes også lenker til diverse skjemaer, samt til en administrasjonsside hvor man kan administrere sin profil. Figur 6.3 viser hvordan en hovedside i Altinn kan se ut.



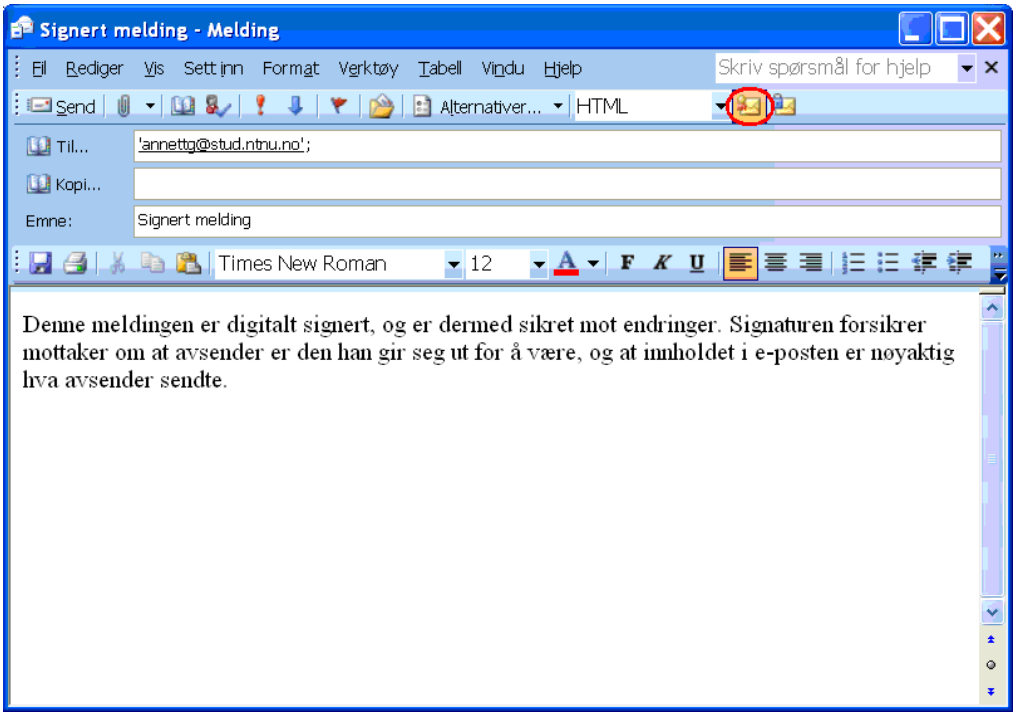
Figur 6.2: Påloggingssiden i Altinn.



Figur 6.3: Slik kan en hovedside i Altinn se ut.

I tillegg til innlogging for Altinn og andre nettbaserte tjenester kan sertifikatene ZebSign utsteder også brukes for signering av e-post. Figur 6.4 viser en e-post opprettet i Microsoft

Outlook. Legg merke til det lille ikonet på verktøylinjen som forestiller en konvolutt med en rød sløyfe, at dette symbolet er aktivert indikerer at meldingen skal signeres. Ikonet ved siden av som forestiller en konvolutt med en blå hengelås indikerer kryptering av meldinger. Det er ikke mulig å bruke de sertifikatene ZebSign i dag utsteder for Sikkerhetsportalen til kryptering. Dette er angitt av et felt i sertifikatet som heter ”bruk av nøkler”, feltet har i dagens sertifikater verdiene ”digital signatur” og ”ikke-avvisning”. Fra og med 31.12.2006 skal Sikkerhetsportalen etter planen støtte kryptering, så innen da må det også kunne utstedes krypteringssertifikater. For å kunne bruke ZebSign-sertifikatet for signering må man i sikkerhetsinnstillingene velge at digital signatur skal legges til i utgående meldinger, og man må spesifisere signeringssertifikat. Samtidig velges krypteringsformat, for eksempel S/MIME, og om sertifikatene eventuelt skal sendes med den signerte meldingen. I forsøkene utført i forbindelse med denne oppgaven ble S/MIME kryptering benyttet, og i e-posten mottaker får er det vedlagt en fil ved navn ”smime.p7s” som er en PKCS #7-signatur. PKCS #7 er en standard for kryptering og signering av meldinger. Mottakers nettleser bruker avsenders vedlagte offentlige nøkkel til å dekode og verifisere sertifikatet, om det stemmer vet mottaker at meldingen faktisk kommer fra riktig avsender.



Figur 6.4: En e-post med valg for digital signatur aktivert.

Et annen ting verdt å merke seg med ZebSign Standard ID sertifikatene for bruk med Sikkerhetsportalen er at brukerens private nøkkel er generert hos ZebSign, og ikke i brukerens nettleser som er et vanlig alternativ. I teorien kunne altså ZebSign signere på vegne av sine brukere, eller dekryptere meldinger ment for disse brukerne. Dette er selvfølgelig ikke ønskelig, og det antas at ZebSign genererer brukernes private nøkler i et beskyttet system, og at nøklene ikke lagres hos ZebSign. Grunnen til at man i dag ikke kan laste ned en sertifikatfil med sertifikat og privat nøkkel mer enn en gang er nok at ZebSign ikke lenger har denne nøkkelen den i første omgang genererte. Det at brukerne selv slipper å generere nøkler kan om ikke annet gjøre det lettere for brukere å komme i gang med sine digitale sertifikater. Videre må det antas at i fremtidige sertifikater med sikkerhetsnivå ”Person-Høyt” vil private nøkler genereres hos brukeren, for eksempel i et smartkort.

6.2 Integrasjon mot FEIDE

For å få et nærmere innblikk i hvordan utdanningsinstitusjoner kommer i gang med FEIDE ble det i forbindelse med denne rapporten foretatt en integrasjon mot FEIDE for å realisere FEIDE-innlogging for egne tjenester. Et komplett FEIDE-system består av en autentiseringstjener (AT) og et brukeradministrativt system (BAS) ute hos den enkelte utdanningsinstitusjon. Institusjonen må også ha et brukersted og en eller flere tjenester som ønsker å benytte FEIDE-innlogging. En hvilken som helst LDAP-tjener kan benyttes som autentiseringstjener, for eksempel OpenLDAP. Denne tjeneren ved utdanningsinstitusjonen inneholder korrekte og oppdaterte brukerdata på form som spesifisert i FEIDEs LDAP-skjema [39], dataene kommer fra utdanningsinstitusjonens brukeradministrative system. Et brukersted kan enklest settes opp som en Javaweb, for eksempel en Tomcat webserver, deretter legger man inn et filter som gjør det mulig å bruke innlogging via Moria.

Det finnes tre ulike måter for et brukersted å foreta en integrasjon mot feide på [45]:

1. Web Service
2. JAX-RPC (Java API for XML-based RPC)
3. Ferdigskrevet filter

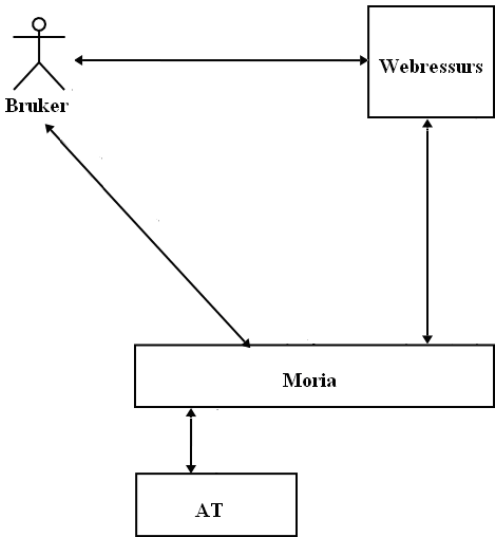
Dette er altså ulike måter å få webressursen i figur 6.5 til å kommunisere med Moria på. Den første metoden innebærer at man laster ned en WSDL-fil (Web Services Description Language) fra https://login.feide.no/moria2/v2_1/Authentication?WSDL. Denne WSDL-filen beskriver Moria-grensesnittet som en Web Service. Fordelen med metoden er at få linjer med kode kreves, kun to kall må gjøres mot Moria. Man kan også fritt velge programmeringsspråk og SOAP-implementasjon.

Metode nummer to innebærer bruk av et ferdig Java API. Brukere av Java 1.4 kan nemlig benytte seg av FEIDEs ferdigkompilerte JAX-RPC bibliotek [14]. Dette biblioteket gjør det enkelt å implementere FEIDE-løsning i egen javakode. I tillegg til HTTP-redigering av brukeren samt uthenting av autentiseringsnøkkel fra URL kreves kun to kall for å gjennomføre en autentisering. Detaljerte beskrivelser for hvordan FEIDE-autentisering kan implementeres i egne java-applikasjoner er tilgjengelige fra FEIDEs nettsider, og ferdig kompilert programvare lastes ned fra UNINETTs FTP-tjener [46]. En rekke biblioteker må ligge i applikasjonens classpath, og videre må konfigurasjonsfilen for webtjenesten inneholde tjenestens brukernavn og passord. Klassen som skal bruke FEIDE-autentisering må importere det som trengs av pakker, og et sett med properties må settes. I tillegg må det spesifiseres hvilke attributter tjenesten ønsker å få tilgang til, og Moria må vite hvor brukeren skal sendes etter autentisering.

Den tredje metoden innebærer integrasjon via et servlet filter. Det ferdigskrevne filteret plugges inn foran en eksisterende servlet uten at denne trenger endringer i koden. Det eneste som trengs er å konfigurere filteret i webapplikasjonens konfigurasjonsfil, slik at alle forespørsler sendes gjennom filteret. Dette gjøres ved å registrere filteret og sette opp en mapping for filteret. Integrasjonen benytter FEIDEs JAX-RPC bibliotek av javapakker, og integrasjonen tar liten tid. Men husk at FEIDE kun tilbyr autentisering og at funksjonalitet for autorisasjon må realiseres i tillegg, for eksempel i servleten eller i et annet filter. FEIDE har laget en demonstrasjonsservlet som bruker FEIDEs autentiseringsfilter. Dette er en meget enkel servlet som tillater en eksisterende FEIDE-bruker å logge inn, og så viser tjenesten hvilke attributter som er hentet ut via FEIDE for denne brukeren. Henvendelser til en servlet

sendes først gjennom eventuelle filtre, for eksempel autentiseringsfilteret og et tilsvarende autorisasjonsfilter. Hvis filtrene tillater det sendes forespørselen videre til servleten.

De ulike metodene for integrasjon mot FEIDE vil ikke beskrives i ytterligere detaljer her, men all nødvendige informasjon for å kunne ta i bruk Moria-innlogging i egne tjenester finnes på [14], [33] og [34].



Figur 6.5: Integrasjon mot FEIDE.

I forbindelse med denne oppgaven ble en integrasjon foretatt mot FEIDE, i form av en enkel demonstrasjonstjeneste som foretar autentisering av brukere via Moria. En webserver av typen Apache Tomcat 5.5.9 ble satt opp, på en maskin med operativsystemet Windows XP og Java-miljø JDK 1.5.0. En Java-integrasjon av feide ble så gjennomført ved å følge veiledinger fra FEIDEs nettsider [14]. I korte trekk gikk integrasjonen ut på å skrive en servlet. En rekke nedlastede jar-filer ble plassert i en bestemt katalog hos webapplikasjonen, brukernavn og passord ble satt i konfigurasjonsfilen, de nødvendige klasser ble importert, og en del egenskaper ble satt. For autentiseringstjeneren ble det spesifisert hvilke attributter tjenesten ønsker tilgang til, og hvor brukere skal sendes etter autentisering. Et eget brukeradministrativt system og en egen LDAP-tjener ble ikke satt opp i forbindelse med dette eksperimentet, fordi det ville vært en omfattende jobb og ikke tilført oppgaven noe. En gruppe testbrukere ble imidlertid lagt inn i UNINETTs LDAP-tjener.

Når en bruker aksesserer demonstrasjonstjenesten fra sin nettleser videresendes han til Morias innloggingsside, se figur 6.6. Brukeren oppgir brukernavn og passord, og velger den organisasjonen han tilhører, deretter logger han inn. På dette tidspunktet kan URL'en i brukerens nettleser for eksempel se slik ut:

> https://login.feide.no/moria2/Login?moriaID=AXCEjR7TAAABC2qhYBNDTvTm9SU5N1rcHXYN0y8pTbOZ4EsfrSs0lP-AYNJnjhsuAJxeeZjP5NpBWS-kKAc

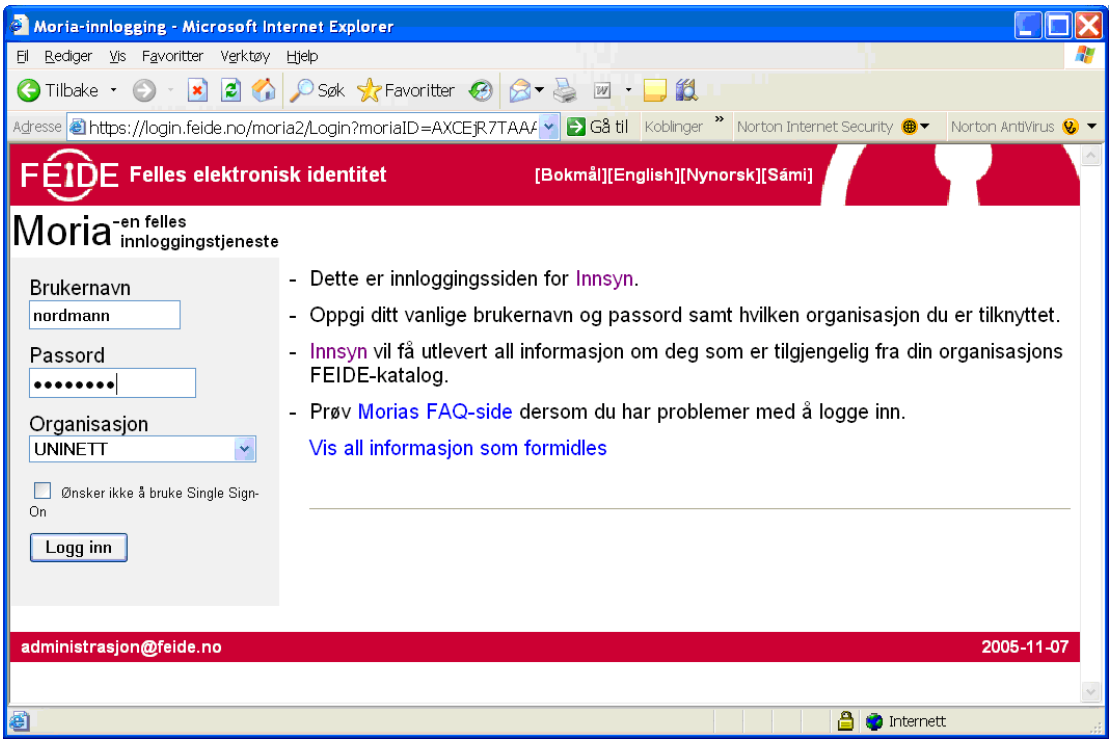
Når Moria har verifisert brukernavn og passord mot den aktuelle organisasjons LDAP-tjener får tjenesten tilgang til de attributter om brukeren den i første omgang ba om. I dette tilfellet var det en innsyntjeneste som ble realisert, og alle brukerattributter som finnes om brukeren i FEIDE skrives ut. Se figur 6.7. Legg merke til at etter autentisering endres URL'en, den kan for eksempel se slik ut:

https://login.feide.no/moria2/InformationService?moriaID=AXCEjR7TAAABC2qllhhtTXXcMNW3UQnX-oZMAigO1EJN7NYX-X96pspO7-d3bQ0x7EFzSgZzeKAY6HMupAE

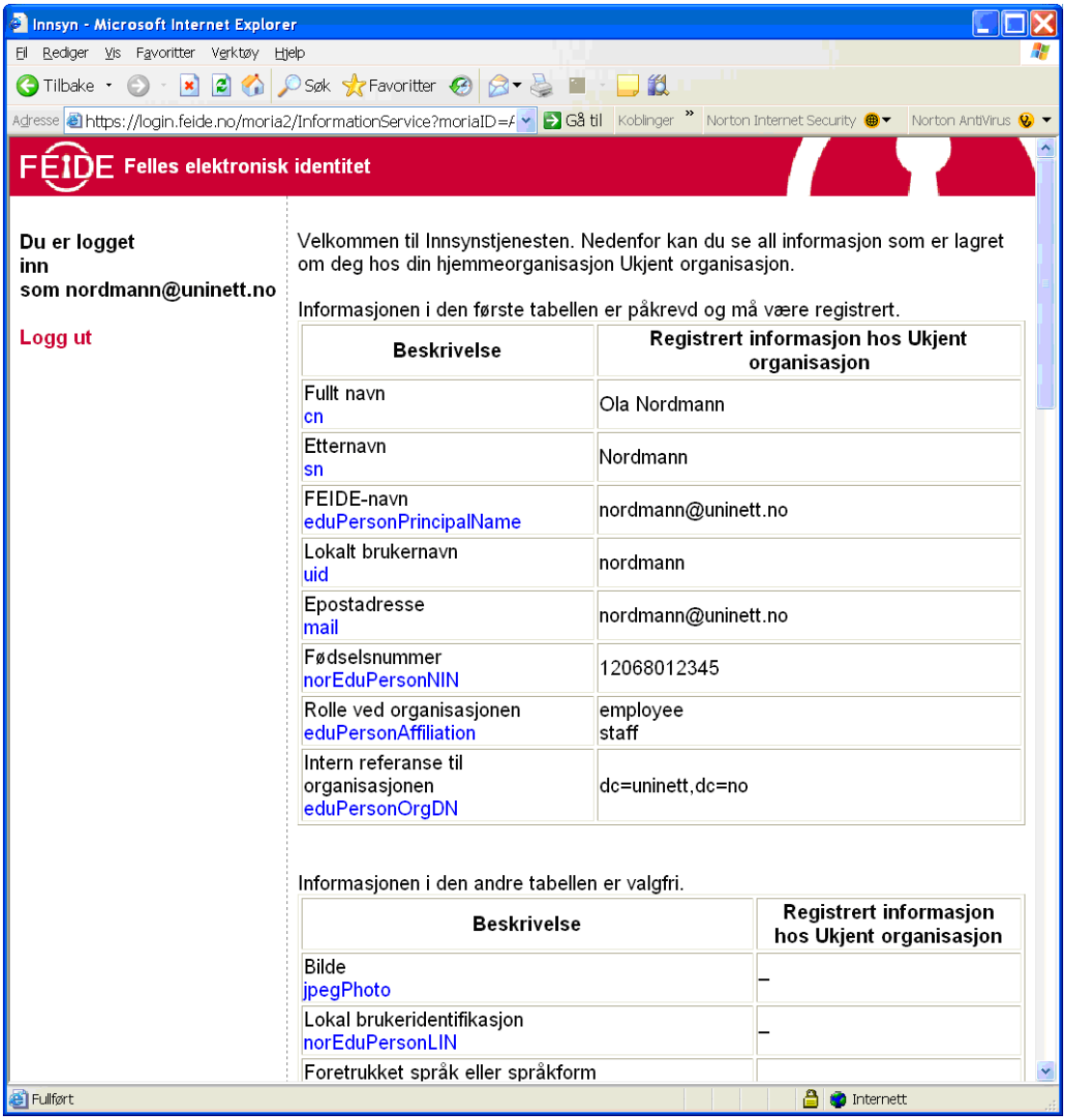
Billetten eller den såkalte sesjons-ID'en, det vil si den delen av URL'en som kommer etter "?MoriaID=", endres altså fra (1) til (2) idet brukeren autentiseres. Det er denne billetten webtjenesten benytter mot Moria for å få hentet ut attributter om brukeren. Det skal være så godt som umulig å gjette seg frem til (2) ut i fra (1), og det eneste stedet man potensielt kan gå inn og kapre en gyldig FEIDE-sesjon er etter autentisering. Derfor er det viktig at kommunikasjon mellom bruker og brukersted også er kryptert, selv om dette ikke er påkrevd.

(1) AXCEjR7TAAABC2qhYBNDTvTm9SU5N1rcHXYN0y8pTbOZ4EsfrSs0lP-AYNJnjhsuAJxeeZjP5NpBWS-kKAc

(2) AXCEjR7TAAABC2qllhhtTXXcMNW3UQnX-oZMAigO1EJN7NYX-X96pspO7-d3bQ0x7EFzSgZzeKAY6HMupAE



Figur 6.6: FEIDEs innloggingsside.



Figur 6.7: Registrerte attributter om en innlogget FEIDE-bruker.

7 Sammenligning

Dette kapittelet drøfter og sammenligner Sikkerhetsportalen og FEIDE på systemnivå, med særlig fokus på organisering, meldingskompleksitet og robusthet. Det må tas med i betraktningene at Sikkerhetsportalen er et meget ungt system i forhold til FEIDE, og at mye av Sikkerhetsportalens funksjonalitet ennå ikke er på plass. Per i dag finnes det også mye mindre informasjon om Sikkerhetsportalen enn det gjør om det mer etablerte FEIDE-systemet. Kapittel 7.1 inneholder noen tanker rundt organisering av og sikkerhetsantakelsene bak Sikkerhetsportalen og FEIDE. Kapittel 7.2 ser på systemenes meldingskompleksitet, og 7.3 på deres robusthet. Kapittel 7.4 ser på kostnadene forbundet med systemene, og 7.5 på brukervennlighet. Kapittel 7.6 oppsummerer noen av de viktigste likhetene og ulikhetene med systemene.

7.1 Organisering og sikkerhetsantakelser

En av hovedforskjellene på de to arkitekturene er at Sikkerhetsportalen er en PKI, mens FEIDE er et uavhengig rammeverk som støtter ulike autentiseringsløsninger. Sikkerhetsportalens PKI-leverandører skal oppfylle kravspesifikasjon for PKI i offentlig sektor, og det er planlagt at godkjenning fra en offentlig godkjenningsordning skal foreligge innen 1.7.2006 som sier at Sikkerhetsportalen oppfyller spesifikasjonen [12]. PKI og bruk av offentlig-nøkkel kryptering er en av flere mulige løsninger for FEIDE, men per i dag er FEIDE i all hovedsak basert på innlogging med brukernavn og passord. Det at Sikkerhetsportalen er en PKI og benytter offentlig-nøkkel sertifikater for å realisere sikkerhet innebærer at personopplysningene ligger i hver enkelt brukers sertifikat. Dermed blir det viktig å beskytte sertifikatene, og passord og koder må holdes hemmelig. Sertifikatene i seg selv skal være sikre, i og med at de oppfyller kravspesifikasjon for PKI i offentlig sektor [17]. På grunn av sertifikatbruk blir datamengden som må holdes hemmelig veldig liten, og det blir rimeligere å vedlikeholde kritiske komponenter. I FEIDE ligger derimot personopplysningene lagret i institusjonenes brukeradministrative system, og det blir særdeles viktig å beskytte disse lokale systemene og autentiseringstjenerne Moria henter informasjonen fra.

En del av prinsippene rundt de to arkitekturene er ganske like, blant annet består begge av en sentral og en lokal bit. Sikkerhetsportalen har en sentral sikkerhetsserver hos BBS og en lokal integrasjonsmodul hos det enkelte brukersted. Tilsvarene har FEIDE en sentral innloggingstjener, Moria, og en lokal autentiseringstjener hos hver hjemmeorganisasjon. Felles for de to systemene er også den desentraliserte oppbevaringen av personopplysninger. I et sentralisert autentiseringssystem ville Sikkerhetsportalen holdt opplysninger om sine brukere i sikkerhetsserveren, og FEIDE ville hatt opplysninger om sine brukere liggende i Moria. Tilfelle er at Sikkerhetsportalsystemet har personopplysninger lagret i sertifikater, og FEIDE i institusjonenes brukeradministrative system.

Mens Sikkerhetsportalen realiserer en identitetsforvaltning for offentlig sektor er FEIDE optimalisert for utdanningssektoren. Dette innebærer at systemene har forskjellige bruksmønstre og ulike krav til dimensjonering. Hele Norges befolkning er potensielle brukere av statlige og kommunale tjenester som krever Sikkerhetsportalens tjenester, og det er regjeringens målsetning at flest mulig skal ta i bruk disse tjenestene i løpet av noen få år. For FEIDE er alle i skole og utdanning potensielle brukere, i tillegg til alle andre som på annet vis er tilknyttet utdanningsinstitusjoner. Dette er mange brukere, men ikke så mange som for

Sikkerhetsportalen. På den annen side vil mange av tjenestene utdanningsinstitusjoner tilbyr være tjenester studentene benytter ofte, for eksempel pålogging for e-post, tilgang til skolens nettverk, adgang til datasaler og lignende. De fleste tjenester fra det offentlige er tjenester man bruker en sjelden gang, i alle fall gjelder dette for innlevering av selvangivelser, flyttemeldinger, søknad om barnehageplass og så videre. Sikkerhetsportalen må også være dimensjonert med hensyn til at en stor andel av befolkningsmassen bruker de samme tjenestene samtidig. I år leverte for eksempel 303.000 nordmenn inn selvangivelsen sin elektronisk siste døgn, halvparten av disse leverte mellom 19.00 og midnatt [44].

Per i dag er brukernavn og passord den vanligste form for autentisering i FEIDE-systemer. Så lenge brukerne hemmeligholder sine passord, og institusjonenes lokale datasystem er godt beskyttet, tilbyr et slikt skjema tilstrekkelig sikkerhet for de tjenester skoler og universiteter tilbyr i dag. Sikkerhetsportalen har valgt å bruke PKI og digitale sertifikater, som ofte antas å gi større sikkerhet enn brukernavn og passord. Husk imidlertid at en PKI kun håndterer autentisering, og ikke brukerautorisasjon, navngiving eller å etablere tillit til andre entiteter [1]. En PKI gjør ikke applikasjoner, operativsystemer eller plattformer sikre, og gjør heller ikke at brukere og administratorer oppfører seg mer pålitelig. Det må finnes mekanismer som forhindrer at angrep skaper problemer, blant annet brannmurer, systemer som detekterer innbrudd, backup-lagring av kritiske data og varme reservesystemer. Brukeropplæring er også nødvendig, uten at brukerne beskytter sine private nøkler er ikke systemet til å stole på. En PKI etablerer en binding mellom en brukers unike navn og nøkkelpar, ved å signere en datastruktur som inneholder både den offentlige nøkkelen og navnet. Brukerens unike navn kan brukes til å identifisere brukeren i det aktuelle miljøet, og kan for eksempel være brukerens fødselsnummer, e-postadresse eller hva som helst annet som unikt identifiserer brukeren. Nøkkelparet kan brukes til sikker digital signering og konfidensialitet, i sanntidskommunikasjon og i transaksjoner som krever langvarig integritet, autentisering eller kryptering anvendt på data. Dokumenter som lagres i Sikkerhetsportalens tiltrodde digitale arkiv over en lengre periode er eksempel på kommunikasjon som ikke foregår i sanntid.

Sikkerhetsportalen har ikke selv kontroll på sine brukeres offentlige nøkler. Hver gang den har behov for en offentlig nøkkel sender Sikkerhetsportalen en forespørsel til PKI-leverandøren som utstedte brukerens sertifikat i første omgang. Man kan derfor lure på om Sikkerhetsportalen i det hele tatt trenger sertifikater. Ta dagens ZebSign Standard ID sertifikater utstedt for bruk med Sikkerhetsportalen som et eksempel. Den offentlige nøkkelen i disse er generert av ZebSign, som også har signert forbindelsen mellom sertifikateiers identitet og nøkkelen. Når Sikkerhetsportalen uansett henvender seg til utstederen for å få tak i offentlige nøkler kunne vel PKI-leverandørene like gjerne holdt en enkel liste over nøklene, i stedet for en liste over datastrukturer signert av seg selv som inneholder disse nøklene. Men nå er det jo slik at sertifikatene også inneholder informasjon om sertifikateieren, og om PKI-leverandørene hadde en liste over offentlige nøkler i stedet for å bruke sertifikater måtte personopplysningene ligge et annet sted, for eksempel hos Sikkerhetsportalen. Slik det er i dag gis brukersteder tilgang til en bestemt informasjonsmengde fra sertifikatet, og slipper å lagre personinformasjon annet enn når en gitt bruker faktisk bruker dens tjenester. Altså er sertifikater en lur måte for sikker distribuering av personinformasjon og nøkler. Men trenger Sikkerhetsportalen å henvende seg til PKI-leverandørene for hver signatur som skal verifiseres, kunne ikke Sikkerhetsportalen hatt en egen katalog med sertifikater for sine brukere. Poenget med å gå til den enkelte PKI-leverandør er nok at på sikt skal mange PKI-leverandører være tilknyttet Sikkerhetsportalen. Sikkerhetsportalen skal ikke behøve å vite hvem sine potensielle brukere er, fordi sertifikatene som brukes med Sikkerhetsportalen i utgangspunktet kan være utstedt for helt andre formål. Dersom BankID inngår en avtale med

BBS om å levere PKI-tjenester for Sikkerhetsportalen kan brukere som har fått et BankID smartkort fra banken sin bruke sertifikatet i dette kortet for innlogging i Sikkerhetsportalen så vel som for innlogging i nettbanken. På samme måte, om Buypass inngår avtale med BBS vil smartkortene fra Norsk Tipping kunne brukes for innlogging via Sikkerhetsportalen.

7.2 Meldingskompleksitet

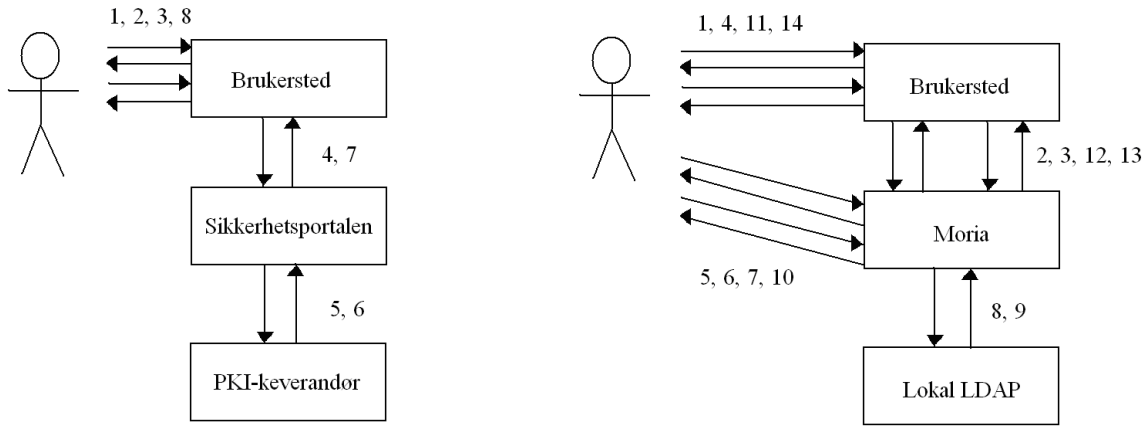
Sikkerhetsportalen og FEIDE er optimalisert for ulike formål, med ulike krav til sikkerhet og med ulike autentiseringsløsninger. Derfor vil også meldingsflyten i de to systemene være forskjellig. I Sikkerhetsportalen kommuniserer sluttbrukere kun via en kanal, nemlig mot brukerstedet. Videre er det brukerstedet som tar seg av interaksjon med Sikkerhetsportalen, og Sikkerhetsportalen bruker tjenester fra de ulike PKI-leverandørene. Unntaksvis har sluttbrukeren også interaksjon med PKI-leverandøren, for eksempel for å få utstedt en elektronisk ID i første omgang. I FEIDE derimot har sluttbrukere to kommunikasjonskanaler, en mot brukerstedet og en mot Moria. Først henvender brukeren seg direkte til tjenesten han ønsker å benytte, deretter sendes han til innloggingssiden og oppgir brukernavn og passord direkte til Moria. At FEIDE har valgt en slik modell gjør at tjenestene aldri trenger å se brukernavn og passord, den eneste personinformasjonen FEIDE-tjenester ser er de attributter de får fra tilsendt fra Moria som brukeren har samtykket til idet han logget inn. Bruk av billetter og det faktum at klienten får oversendt nødvendige attributter i forbindelse med selve autentiseringen gjør at Moria slipper å huske tilstand og informasjon for hver innloggete bruker. FEIDE får uansett en ekstra kommunikasjonskanal fra brukeren som må sikres.

All kommunikasjon til og fra Sikkerhetsportalen og Moria går via krypterte kanaler, så det er i teorien vanskelig å få noe meningsfullt ut av meldinger fanget opp under sending. Kommunikasjonen mellom brukere og brukersted i FEIDE er ikke nødvendigvis kryptert, men dette anbefales på det sterkeste. Om kommunikasjonen her ikke er sikret er det mulig å kapre etablerte sesjoner ved å lytte til brukerens URL som inneholder en gyldig sesjons-ID. Ved å sikre kommunikasjonen er muligheten for kapring av sesjoner minimal. En annen stor utfordring er å sikre lokal LDAP, samt å sørge for at denne til enhver tid er oppdatert og korrekt. I Sikkerhetsportalen er det viktig for brukere å ta godt vare på sine private nøkler og passord, så lenge disse holdes hemmelige er det vanskelig for andre å få uautorisert tilgang til personlig eller sikkerhetsrelatert informasjon. Sikkerhetsportalens brukersteder får tilgang til informasjon fra brukernes sertifikater, informasjon som kun må brukes til angitt formål.

Figur 7.1 viser de meldinger som utveksles ved autentisering i henholdsvis Sikkerhetsportalen og FEIDE. Meldingene går slik:

Sikkerhetsportalen:
(1) Bruker aksesserer beskyttet tjeneste fra brukersted
(2) Brukersted ber bruker om gyldig sertifikat
(3) Bruker viser sertifikat og krypterer melding med privat nøkkel
(4) Brukersted sender kryptert melding til Sikkerhetsportalen
(5) Sikkerhetsportalen sender kryptert melding til riktig PKI-leverandør
(6) PKI-leverandør dekrypterer meldingen med brukers offentlige nøkkel og sender melding til Sikkerhetsportalen om at brukeren er autentisert og for hvilket sikkerhetsnivå
(7) Sikkerhetsportalen sender svaret til brukersted
(8) Brukersted får tilgang til informasjon fra sertifikatet og sender melding til bruker om at han er autentisert

FEIDE:
(1) Bruker aksesserer beskyttet tjeneste fra brukersted
(2) Brukersted ber Moria om autentiseringssesjon og brukerattributter
(3) Brukersted mottar URL for innloggingsside
(4) Brukersted sender URL til bruker
(5) Bruker aksesserer URL
(6) Moria presenterer innloggingsskjema
(7) Bruker oppgir brukernavn og passord
(8) Moria ber lokal LDAP sjekke brukerens passord
(9) Moria mottar kryptert passord og sjekker at det stemmer med oppgitt passord
(10) Moria sender ny URL til bruker, med ny billett
(11) Bruker aksesserer URL
(12) Brukersted anvender brukerens billett til å hente brukerattributter fra Moria
(13) Brukersted mottar attributter den har bedt om og er klarert for å få
(14) Bruker får beskjed om at han er autentisert



Figur 7.1: Kommunikasjon ved autentisering i Sikkerhetsportalen og i FEIDE.

Det utveksles altså flere meldinger i FEIDE enn i Sikkerhetsportalen i forbindelse med en autentisering. I tillegg har man en ekstra kommunikasjonskanal i FEIDE, nemlig mellom sluttbruker og Moria.

7.3 Robusthet mot feilsituasjoner

Sikkerhetsportalen og FEIDE kan aldri være trygge for at et angrep skal sette de ut av spill, men begge systemene forsøker ved hjelp av ulike tiltak å minimere sannsynligheten for at et angrep eller andre omstendigheter skal gjøre tjenestene deres utilgjengelige. All kommunikasjon som inneholder personopplysninger eller sikkerhetsrelatert informasjon går via krypterte kanaler, og alle systemkomponenter er sikret og vanskelige å få uautorisert tilgang til. Systemene forventes å være tilgjengelige døgnet rundt året rundt, noe som i begge tilfeller sørges for gjennom arkitekturenes design og redundante systemer. For FEIDE vil de største utfordringene knyttet til ytelse ligge hos brukerstedenes lokale LDAP-kataloger. Kanskje er de største ytelsesmessige utfordringene for Sikkerhetsportalen knyttet til overbelastning på de enkelte brukerstedenes tjenester.

7.4 Implementerings- og driftskostnader

Å tilpasse brukersted og tjenester til Sikkerhetsportalen eller FEIDE koster. Brukerstedet må tilpasses interaksjon med systemene, og tjenestene systemene leverer koster i seg selv. For å komme i gang med Sikkerhetsportalen trengs en oppgradering av maskiner, programvare og nettverk ved brukerstedet. En integrasjonsmodul utplasseres ved brukerstedet og tjenesten som skal benytte sikre tjenester må være tilpasset Sikkerhetsportalen. Kostnadene brukerstedet har til forberedelser for integrasjon dekker de selv, videre betaler brukerstedet også for bruk av sikkerhetstjenester, per transaksjon eller per bruker. I tillegg til de mest åpenbare kostnadene er det utgifter knyttet til opplæring og uforutsette problemer, og en integrasjon mot Sikkerhetsportalen vil føre til en omlegging av gamle arbeidsprosesser. På sikt vil uansett kostnadene forbundet med å ta i bruk Sikkerhetsportalen veies opp av en mer effektiv håndtering av sikkerhetstjenester. For å komme i gang som brukersted for FEIDE kreves en opprydning i institusjonens datasystemer, et brukeradministrativt system med data av god kvalitet, og en autentiseringstjener. I tillegg må brukerstedet ha en tjeneste som skal benytte FEIDE-innlogging. Det enkelte brukersted betaler selv tilpasningen til Moria, og de betaler for hver aktive bruker ved brukerstedet. Både Sikkerhetsportalen og FEIDE krever altså en tilpasning og en viss omlegging av arbeidsprosesser hos brukestedene, samt noe program- og maskinvare. Det tar tid å gjennomføre endringene, men i det lange løp vil opprydningen gi en mer oversiktlig og effektiv organisasjon.

7.5 Brukervennlighet

Både Sikkerhetsportalen og FEIDE er uavhengige av operativsystem og nettleser, noe som er en stor fordel. Som sluttbruker av systemene trenger man heller ikke noen spesiell maskinvare, annet enn et smartkort med leser hvis man benytter smartkort med integrerte sertifikater. For personer som er vant med datamaskiner og Internett er verken Sikkerhetsportalen eller FEIDE vanskelige å ta i bruk som sluttbruker. For FEIDE mottar man brukernavn og passord, og så er det bare å sette i gang. For Sikkerhetsportalen må man selv bestille og laste ned en elektronisk ID, et såkalt sertifikat, dette installeres i nettleseren og er klart til bruk. Sikkerhetsportalen har gode brukerveiledninger for prosessen med å skaffe og ta i bruk sertifikater. Sikkerhetsportalen og FEIDE har begge enkle og intuitive brukergrensesnitt, hvor brukeren tydelig informeres om hvilke transaksjoner som skjer og hvilken informasjon som utveksles.

Integrasjon mot FEIDE er lett å realisere, da alt av kode, dokumentasjon og veiledning er åpent tilgjengelig på Internett. Integrasjon mot Sikkerhetsportalen skal heller ikke være vanskelig, men det meste av tekniske detaljer rundt Sikkerhetsportalen har konfidensiell status, og det er lite teknisk informasjon å få før abonnementsavtalen er signert. Åpenhet rundt systemene er viktig for samkjøring med andre systemer. I motsetning til FEIDE hvor alle tekniske detaljer og all kode er fritt tilgjengelig, er Sikkerhetsportalen i stor grad preget av hemmelighold. Sikkerhetsportalen er imidlertid ennå i en oppstartsfase, og det er bare få måneder siden systemet ble lansert 15. desember 2005. På sikt bør også Sikkerhetsportalen gjøre dokumentasjon og detaljer rundt integrasjon lettere tilgjengelig, slik at det blir enklere for offentlige og private aktører å foreta integrasjon. Detaljer som kan true systemets sikkerhet må naturligvis forbli konfidensielle.

7.6 Likheter og ulikheter

Sikkerhetsportalen har vært operativ i kun et halvt år, siden desember 2005, mens FEIDE har vært operativ siden 2003. Dette gjør at FEIDE har funksjonalitet og dokumentasjon på plass, mens Sikkerhetsportalen ennå er i oppstarten og mye av funksjonaliteten er fremdeles ikke operativ. For FEIDE er alle spesifikasjoner og all kode med dokumentasjon tilgjengelig fra deres nettsider, for Sikkerhetsportalen derimot er det så langt lite teknisk dokumentasjon som er tilgjenglig. Ellers skal Sikkerhetsportalen i første omgang brukes sammen med tjenester fra det offentlige, mens FEIDE brukes med tjenester fra utdanningssektoren.

Sikkerhetsportalen tilbyr sikker autentisering, signering og kryptering, samt en registrerings- / bestillingstjeneste, tiltrodd digitalt arkiv og kundeweb. FEIDE tilbyr en felles påloggingstjeneste, en tjeneste for uthenting av dataattributter, samt en tjeneste for avlogging. Både Sikkerhetsportalen og FEIDE støtter også SSO, som gjør at man slipper å logge på hver enkelt tjeneste man benytter innenfor et domene. Systemene bygger også på mange av de samme standardene, i alle fall dersom man tar den fremtidige FEIDE-løsningen i betraktning.

Når det gjelder organisering av systemene har begge valgt en desentralisert autentiseringsløsning, med en sentral og en distribuert bit. Sikkerhetsportalen har en lokal del i hvert brukersted, som kommuniserer med en sentral sikkerhetsserver hos BBS. I tillegg benyttes tjenester fra en rekke PKI-leverandører. FEIDE har et lokalt system hos hver hjemmeorganisasjon, og en sentral innloggingstjener som kommuniserer mot tjenester og mot de lokale systemene. Mens Sikkerhetsportalen har valgt å benytte offentlig-nøkkel sertifikater av ulike sikkerhetsnivåer for autentisering, er FEIDE i prinsippet uavhengig av autentiseringsløsning. Den løsningen FEIDE i all hovedsak benytter i dag er for så vidt basert på brukernavn og passord. I Sikkerhetsportalen er alle personopplysninger lagret i brukernes egne sertifikater, informasjon som tjenester får tilgang til via brukerstedets integrasjonsmodul etter autentisering. I FEIDE ligger personopplysninger hos den enkelte institusjons brukeradministrative system, som aksesseres via institusjonens lokale LDAP-tjener. Ved fullført autentisering får tjenester hentet ut på forhånd klarerte personopplysninger via Moria.

I begge systemene går all kommunikasjon til og fra den sentrale delen av systemet via krypterte kanaler, slik at det skal være vanskelig for uvedkommende å få noe ut av kommunikasjonen. Mens all kommunikasjon mellom sluttbruker og Sikkerhetsportalsystemet går mot brukerstedet, har FEIDE både en kanal mot webressursen og en kanal mot Moria. Den ekstra kommunikasjonskanalen i FEIDE gjør at tjenesten aldri trenger å se brukerens passord, da innloggingen foregår direkte mellom sluttbruker og Moria. FEIDEs løsning med sesjons-ID i URL gjør også at autentisering og uthenting av brukerattributter utføres på en elegant måte.

Sikkerhetsportalen og FEIDE er uavhengige av operativsystem og nettleser, og for FEIDE er det eneste som trengs en FEIDE-identitet og en datamaskin. For bruk av Sikkerhetsportalen trenger man å få utstedt et digitalt sertifikat, og man trenger en viss programvare. Tabell 7.1 oppsummerer noen viktige likheter og forskjeller ved Sikkerhetsportalen og FEIDE.

	Sikkerhetsportalen	**FEIDE**
Operativ siden	15. desember 2005.	12. mai 2003.
Anvendelsesområder	Offentlige tjenester med behov for elektronisk ID og signatur, etter hvert også private tjenester. Per i dag er Altinn det eneste brukerstedet, lanseringen av MinSide lar vente på seg.	Tjenester innen utdanningssektoren. I dag for universitets- og høyskolesektoren, snart også i grunnskoler og videregående skoler.
Sikkerhetstjenester	Autentisering, signering og kryptering. SSO, registreringstjeneste, bestillingstjeneste, tiltrodd digitalt arkiv, kundeweb.	Felles påloggingstjeneste, SSO, uthenting av dataattributter og avlogging.
Åpne standarder	ID-FF, ID-WSF, SAML, Web Services, HTTPS, SSL.	ID-FF, ID-WSF, SAML, HTTP, SSL/TLS, SOAP, LDAP, Web Services.
Systemdokumentasjon	Overordnete beskrivelser er tilgjengelige, men tekniske detaljer anses som konfidensielle.	Alle spesifikasjoner og all kode med dokumentasjon er veldig lett tilgjengelig.
Delsystemer	Sluttbruker, brukersted med integrasjonsmodul, sentral sikkerhetsserver hos BBS, PKI-leverandører.	Institusjon med BAS og AT, klient, Moria, tjeneste.
Kommunikasjon mellom sluttbruker og system	Én kanal mot brukersted.	To kanaler, mot webressurs og mot Moria.
Komponenter som realiserer sikkerhet	Sertifikater, integrasjonsmodul, sikkerhetsserver, PKI-leverandører, kryptert kommunikasjon.	Lokal LDAP, Moria, kryptert kommunikasjon, sesjons-ID.
Autentiseringsløsning	Offentlig-nøkkel sertifikater tilpasset tre ulike sikkerhetsnivå, ”Person-Standard”, ”Person-Høyt” og ”Virksomhet”.	Uavhengig av autentiseringsløsning, men brukernavn og passord som er utbredt i dag.
Personopplysninger	Ligger i brukernes sertifikater. Tjenester får etter fullført autentisering tilgang til informasjon fra sertifikatene via brukerstedets integrasjonsmodul.	Ligger hos den enkelte institusjons BAS og aksesseres via lokal LDAP (AT). Tjenester får etter fullført autentisering hentet klarert informasjon via Moria.
Brukerutrustning	Uavhengig av operativsystem og nettleser. Bruker må ha sertifikat fra godkjent PKI-leverandør.	Uavhengig av operativsystem og nettleser. Bruker må ha en FEIDE-identitet.

Tabell 7.1: Likheter og ulikheter ved Sikkerhetsportalen og FEIDE.

8 Konklusjon

Denne rapporten har sett på to systemer for storskala identitetsforvaltning, Sikkerhetsportalen og FEIDE. Relevante kriterier er utarbeidet, og en rekke egenskaper ved systemene er beskrevet, med hensyn til organisering og sikkerhetsantakelser, meldingskompleksitet, systemrobusthet, kostnadsfaktorer og brukervennlighet. I tillegg til det teoretiske arbeidet med rapporten er også en eksperimentell del gjennomført. Sikkerhetsportalens sertifikater er studert, og en integrasjon av FEIDE-innlogging i egen tjeneste er gjennomført. Sikkerhetsportalen er et relativt ungt system, og all funksjonalitet er ikke på plass i dagens løsning. Det finnes relativt lite tilgjengelig informasjon om Sikkerhetsportalen, særlig når det gjelder tekniske detaljer. For FEIDE derimot er alle spesifikasjonsdokumenter tilgjengelige, sammen med all kode og dokumentasjon.

Både Sikkerhetsportalen og FEIDE foretar autentisering av sine brukere basert på en elektronisk identitet hver av brukerne er i besittelse av. I Sikkerhetsportalen er den elektroniske identiteten et sertifikat utstedt av en PKI-leverandør Sikkerhetsportalen har en avtale med. I FEIDE er den elektroniske identiteten som oftest et brukernavn og passord utstedt av brukerens utdanningsinstitusjon. Men FEIDE er uavhengig av autentiseringsmekanisme og kan også støtte løsninger basert på sertifikater. Sikkerhetsportalen og FEIDE er begge gode systemer for identitetsforvaltning, tilpasset ulike formål. Dagens passordbaserte FEIDE-system tilbyr tilstrekkelig sikkerhet for de tjenester utdanningsinstitusjoner tilbyr i dag, men kan også ta i bruk PKI der kravene til sikkerhet måtte kreve det. Sikkerhetsportalen tilbyr en minst like sikker form for autentisering, med sertifikater på tre ulike sikkerhetsnivå.

Mange av prinsippene rundt systemene er forholdsvis like. Blant annet har begge valgt en desentralisert arkitektur, og informasjon om brukerne vedlikeholdes i henholdsvis brukersertifikater og i brukersteders lokale datasystem. Sikkerhetsportalen har en sentral sikkerhetsserver, og en lokal modul hos hvert brukersted som kommuniserer med denne. FEIDE har tilsvarende en sentral innloggingstjeneste, og et lokalt system hos hver hjemmeorganisasjon. FEIDE har en ekstra kommunikasjonskanal i forhold til Sikkerhetsportalen, som gjør at FEIDE-tjenester aldri trenger å se brukernavn og passord. FEIDEs autentiseringsløsning er billettbasert, og gir tjenester tilgang til brukerdata på en sikker måte. Sikkerhetsportalen gir sine brukersteder tilgang til brukerdata fra brukernes egne sertifikater. For begge systemene er kommunikasjon som inneholder personopplysninger og sikkerhetsrelatert informasjon sikret ved kryptering, og begge systemene ivaretar et godt personvern. Det skal med andre ord være vanskelig å få informasjon ut av meldinger fanget opp under sending. I FEIDE er kommunikasjonen mellom bruker og brukersted ikke nødvendigvis kryptert, men dette anbefales sterkt for å minimere sjansen for kapring av etablerte sesjoner. I tillegg må også lokale autentiseringstjenere beskyttes godt. Tilsvarende for Sikkerhetsportalen er det viktig at brukerne holder passord og private nøkler hemmelige.

Sikkerhetsportalen egner seg særlig godt for organisasjoner som ønsker å tilby tjenester til store grupper, da organisasjonene ikke trenger å utstede elektronisk identitet på egen hånd. Dette er det en rekke PKI-leverandører som tar seg av. FEIDE egner seg godt for organisasjoner som har behov for å oppbevare informasjon om sine brukere i egne systemer.

9 Referanser

[1]: Carlisle Adams and Steve Lloyd, *Understanding PKI, 2nd edition*, Pearson Education Inc., 2003.

[2]: William Stallings, *Network Security Essentials, 2nd edition (International)*, Pearson Education Inc., 2003.

[3]: Ragna Kronstad, *Kroppen Din Erstatter Pinkoden*, Teknisk Ukeblad nr 11, mars 2006.

[4]: Justis- og politidepartementet, *Lov om behandling av personopplysninger (personopplysningsloven)*, LOV 2000-04-14 nr 31, april 2000.

[5]: Espen Leirset, *Forbyr Bruk Av Fingeravtrykk*, Teknisk Ukeblad nr 11, mars 2006.

[6]: Finn Halvorsen, *Større Interesse For Biometri*, Teknisk Ukeblad nr 12, april 2006.

[7]: Department of Defense USA, *DoD Biometrics*, 2006.
http://www.biometrics.dod.mil (Sist sjekket: 5.6.2006)

[8]: Kristian Bergem, *Forretningsmodeller for bruk av elektronisk ID og signatur*, Moderniseringsdepartementet, desember 2004.

[9]: Transportøkonomisk institutt (TØI), *Setter vår lit til Storebror ...og alle småbrødre med? Befolkningens holdning til og kunnskap om personvern*, TØI rapport 789/2005, september 2005.

[10]: Moderniseringsdepartementet, *"eNorge 2009 – det digitale spranget"*, juni 2005.

[11]: Nærings- og handelsdepartementet, *"Regjeringens handlingsplan for Et enklere Norge 2005-2009, Forenkling og tilrettelegging for næringslivet"*, juni 2005.

[12]: Brønnøysundregistrene, *Sikkerhetsportalen – felles sikkerhetsportal for offentlig sektor*, 2006.
http://www.brreg.no/sikkerhetsportal/ (Sist sjekket: 5.6.2006)

[13]: UNINETT, *UNINETT – Forskningsnettet i Norge*, 2006.
http://www.uninett.no (Sist sjekket: 5.6.2006)

[14]: FEIDE, *FEIDE: Felles Elektronisk Identitet*, 2006.
http://www.feide.no (Sist sjekket: 5.6.2006)

[15]: Utdannings- og forskningsdepartementet, *Program for digital kompetanse 2004-2008 – programbeskrivelse*, 2004.

[16]: UNINETT, *FEIDE veivalg og veiviser, Veiledning i å innføre FEIDE-løsninger*, versjon 1.5, august 2005.

[17]: Moderniseringsdepartementet, *Kravspesifikasjon for PKI i offentlig sektor*, versjon 1.02, januar 2005.

[18]: Commfides, *Commfides*, 2005.
http://www.commfides.com (Sist sjekket: 5.6.2006)

[19]: Siemens Business Services AS, *Siemens Business Services AS*, 2006.
http://www.sbs.siemens.no (Sist sjekket: 5.6.2006)

[20]: Fornyings- og administrasjonsdepartementet, *MiSide blir ikkje lansert første kvartal*, Pressemelding 11/2006, 13. mars 2006.

[21]: Moderniseringsdepartementet, *Bruk av åpne IT-standarder og åpen kildekode i offentlig sektor*, juni 2005.

[22]: Liberty Alliance project, *Liberty Alliance Project – Digital Identity Defined*, 2006.
http://www.projectliberty.org (Sist sjekket: 5.6.2006)

[23]: Nærings- og handelsdepartementet, *Lov om elektronisk signatur (esignaturloven)*, LOV 2001-06-15 nr 81, juni 2001.

[24]: Nærings- og handelsdepartementet (NHD), *Forskrift om krav til utsteder av kvalifiserte sertifikater mv.*, FOR-2001-06-15-611, juni 2001.

[25]: SEID-prosjektet, *Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater*, versjon 1.02, februar 2005.

[26]: ZebSign, *Avtalevillkår for bruk av ZebSign Standard ID*, versjon 1.0.

[27]: ZebSign AS (Heleid datterselskap av BBS), *ZebSign AS*, 2004.
http://www.zebsign.no (Sist sjekket: 5.6.2006)

[28]: Dag Slettemeås, *Grunnlagsdokument – forbrukervinkling på Public Key Infrastructure (PKI)*, Statens Institutt for Forbruksforskning (SIFO), oktober 2004.

[29]: Datatilsynet, *Veiledning i informasjonssikkerhet for kommuner og fylker*, januar 2005

[30]: Moderniseringsdepartementet, *Forskrift om behandling av personopplysninger (personopplysningsforskriften)*, FOR 2000-12-15 nr 1265, desember 2000.

[31]: Gunnar Nordseth (Kantega), *Slik kobler du deg til MinSide og Sikkerhetsportalen*, Bank-ID konferansen 2005 i Trondheim, desember 2005.

[32]: Brønnøysundregistrene, *Hvordan ta i bruk Sikkerhetsportalen*.
http://www.brreg.no/sikkerhetsportal/kristoffersen2.pdf (Sist sjekket: 5.6.2006)

[33]: FEIDE, *SourceForge.net: Moria*, 2006.
http://sourceforge.net/projects/moria (Sist sjekket: 5.6.2006)

[34]: UNINETT FAS, *Moria Web Authentication Service*, 2001-2006.
http://moria.sourceforge.net (Sist sjekket: 5.6.2006)

[35]: FEIDE, *FEIDE System Architecture*, versjon 1.2.

[36]: FEIDE ved Ingrid Melve, *Eksisterende autentiseringsløsninger i FEIDE*, notat til Moderniseringsdepartementet, desember 2005.

[37]: UNINETT ABC, *Rammeverk for bruk av FEIDE i grunnopplæringen*, juni 2005.

[38]: Ingrid Melve, daglig leder for FEIDE.

[39]: FEIDE, *norEdu Object Class Specification 1.3*, mai 2004.

[40]: UNINETT, *Utkast til IT-reglement for Institusjonen*, desember2004.

[41]: Arbeids- og administrasjonsdepartementet, *NOU 2001:10 Uten penn og blekk, bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen*, mars 2001.

[42]: Alf Hansen (UNINETT FAS), Anund Lie og Jon Ølnes (NR), *FEIDE: Elektronisk ID for UoH-sektoren*, september 2000.

[43]: FEIDE, *Samtale om FEIDE-innføring*.

[44]: Niels Ravnaas, *Avviser skattetrøbbel*, NA24.no, mai 2006. http://pub.tv2.no/nettavisen/na24/nyheter/article624702.ece (Sist sjekket: 5.6.2006)

[45]: Lars Preben S. Arnesen (UiO), *FEIDE Moria*, PowerPoint-presentasjon, 2003.

[46]: UNINETT, UNINETTs FTP-tjener. ftp://ftp.uninett.no/uninett/feide/w3ls (Sist sjekket: 5.6.2006)