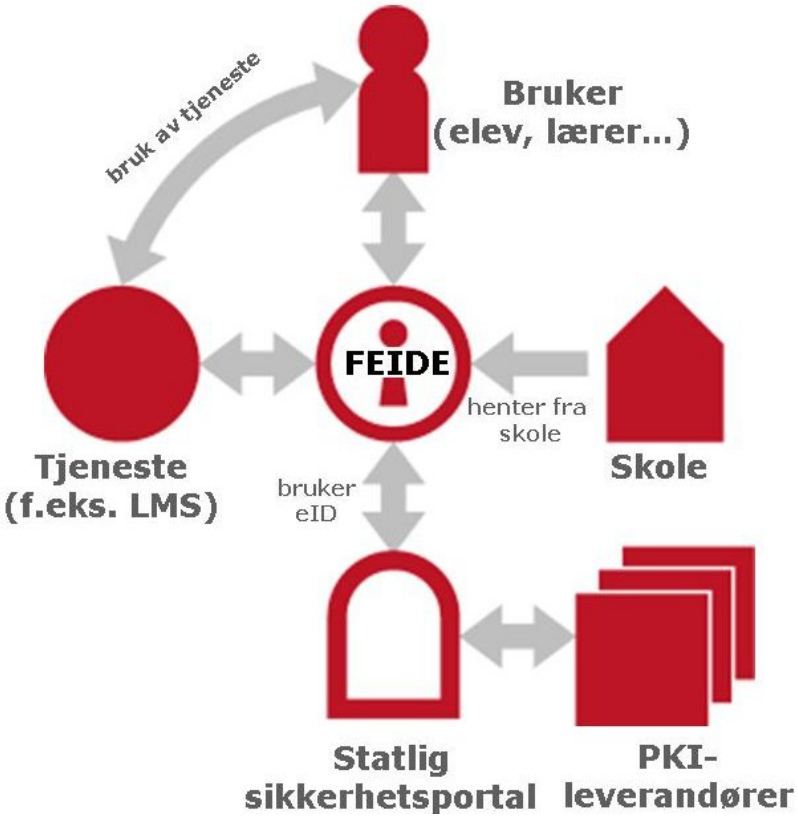
Rapport

OM BRUK AV FEIDE I GRUNNOPPLÆRINGEN



FORORD.

I Stortingsproposisjon. Nr 1 (2004-2005) heter det: ”Arbeidet for å få etablert ein identitetsforvaltning innanfor utdanningssektoren vidareførast. I dette arbeidet vil FEIDE-prosjektet, som er UNINETT si satsing på identitetsløysingar for UH-sektoren, vere sentralt. Departementet vil i 2005 ta stilling til korleis FEIDE-teknologien skal takast i bruk grunnopplæringa.”

På denne bakgrunn oppnevnte Utdannings- og forskningsdepartementet (UFD) 18. mars 2005 en arbeidsgruppe som skulle utarbeide et grunnlag for en beslutning om FEIDE i grunnopplæringen, jf vedlagte mandat for arbeidsgruppen. Arbeidsgruppen har hatt medlemmer fra Moderniseringsdepartementet, Utdanningsdirektoratet, Uninett og Utdannings- og forskningsdepartementet.

Arbeidsgruppens hovedoppgave (jf kap 5.3 Mandat for arbeidsgruppen) var å lage en anbefaling til UFD om hvordan FEIDE-teknologi skal tas i bruk i grunnopplæringen. Anbefalingen skal ligge til grunn for en politisk beslutning om eventuell innføring av FEIDE-teknologi i grunnopplæringen.

Gruppen ble særlig om å vurdere følgende punkter:

- Teknologiske og andre betingelser som må være på plass for innføring av FEIDE-teknologi i grunnopplæringen
- Innføringstakt i grunnopplæringen
- Grenseflaten mot PKI-anvendelser i offentlig sektor
- Organisatorisk løsning for FEIDE-arbeidet

INNHOLD

1. SAMMENDRAG OG ANBEFALINGER

Norske elever og studenter bruker i sin undervisningssituasjon e-post og læringsplattformer (LMS), de logger seg på nettverk og elektroniske opptakssystemer, de avlegger digital eksamen. I utdanningssektoren, som ellers i samfunnet, er det vekst i antallet digitale ressurser og tjenester som baserer seg på elektronisk identifikasjon som tilgangskontroll. Dette stiller krav om en enhetlig elektronisk identitetsforvaltning, slik at individer kan identifisere seg elektronisk og få tilgang til digitale ressurser eller tjenester.

Prosjektet *Felles elektronisk identitet* (FEIDE) er opprettet med det siktemål å utforme en enhetlig nasjonal identitetsforvaltning i utdanningssektoren. Prosjektet er forankret ved og blir ledet av UNINETT AS. FEIDE autentiserer personer tilknyttet norske utdanningsinstitusjoner via en innloggingstjeneste. FEIDE er også en standard for hvordan man skal håndtere personopplysninger om brukere i administrative systemer ved norske utdanningsinstitusjoner.

Det er en sterk internasjonal trend med felles elektronisk identitet (Federated Identity) også innen utdanning. På internasjonal basis er det aktiviteter for å samordne og koble sammen nasjonale initiativ for felles tilgangssystemer. De fleste slike aktiviteter er fremdeles konsentrert om høyere utdanning, men Storbritannia, Canada, Australia og Danmark har initiativ for identitetsløsninger i grunnopplæringen. Gjennom EU-prosjektet GEANT2 skal FEIDE kobles sammen med store deler av europeiske forskningsnett i en infrastruktur kalt eduGAIN for webinnlogging og trådløs tilgang.

FEIDE ble i en første fase utviklet for bruk i høyere utdanning. I dag deltar ca. 25 universiteter og høyskoler i FEIDE-prosjektet med til sammen vel 115 000 FEIDE-brukere.

I grunnopplæringen har FEIDE fått aktualitet, både i videregående opplæring og i grunnskolen. Både kommuner og fylkeskommuner har satt i gang prosjekter i samarbeid med UNINETT ABC med sikte på FEIDE-tilpasning. Spørsmålet om bruk av FEIDE i grunn-opplæringen omtales i flere styringsdokumenter, inkludert i programbeskrivelsen for *Program for digital kompetanse 2004 – 2008* (PfDK).

Før en endelig beslutning om hvorvidt FEIDE i grunnopplæringen skal tas, er det nødvendig å få belyst ulike sider av FEIDE. Regjeringen har besluttet at en egen kravspesifikasjon for PKI-anvendelser skal ligge til grunn for all autentisering i offentlig sektor som krever PKI. Dette reiser viktige prinsipielle og praktiske spørsmål om grenseflaten mellom FEIDE-arbeidet og utrullingen av PKI-anvendelser i offentlig sektor. Arbeidsgruppen som har utredet FEIDE i grunnopplæringen, har særlig drøftet og konkludert på disse problemstillingene.

Utfordringer som setter krav til en godt fungerende identitetsforvaltning i grunnopplæringen, omtales i kapittel 2 av denne rapporten. Kapittel 3 beskriver FEIDE og den felles infrastrukturen for eIdentitet og e-signatur i offentlig sektor (PKI), og hvordan FEIDE og PKI kan virke sammen for å imøtekomme utfordringer gitt i kapittel 2. Utfordringer knyttet til sikkerhet, økonomi og administrasjon er omtalt i kapittel 4.
Vedlagt ligger mandatet for arbeidsgruppen (vedlegg 5.1), en omtale av status på området IKT i grunnopplæringen, en beskrivelse av digitale undervisnings- og vurderingsformer (vedlegg 5.2) og en ordliste (vedlegg 5.3).

I tillegg til denne rapporten foreligger det en egen utredning om administrative og økonomiske rammebetingelser for FEIDE i grunnopplæringen, og en utredning om hvordan

FEIDE kan tas i. Begge disse delutredningene er utført på oppdrag av UNINETT ABC ved Lars Olaf Sterud, Aesop.

I rapporten peker arbeidsgruppen på at

- Grunnopplæringen har spesielle utfordringer (jf kap 2), og at en manglende nasjonal samordning kan medføre at skolene ikke oppnår de effektiviseringsgevinster de ellers kunne ha fått.
- Skolene blir også i økende grad avhengig av databaserte skolesystemer, og med det økt avhengighet av private leverandører. Det er viktig å hindre at enkeltleverandører kommer i en posisjon der de kan utvikle stengsler mot andre leverandører gjennom informasjons-monopol og tekniske integrasjoner. Det er derfor behov for standardisering (jf kap 4.1).
- Grunnopplæringen tar i økende grad i bruk personaliserte tjenester. Dette stiller krav om en identitetsforvaltning i grunnopplæringen. Løsningen må blant annet ivareta sikkerhetsbehov i forhold til sensitive opplysninger.
- Både løsninger av typen FEIDE og PKI vil være sentrale tiltak for å møte de utfordringer grunnopplæringen står overfor i tiden framover.
- Selv om FEIDE og PKI på noen områder overlapper, fremstår de i hovedsak som komplementære løsninger for digital autorisering og autentisering.

Grunnopplæringen har behov for en identitetsforvaltning som bygger på prinsippene for FEIDE og PKI. Med dette menes at en identitetsforvaltning må kunne imøtekomme følgende krav:

- Sikker identifikasjon av individer.
- Klar rolledefinering (er dette en lærer, elev/student, hvilke rettigheter har vedkommende)
- Tjenester og ressurser skal være tilgjengelige og delbare nasjonalt og internasjonalt (tilgang lokalt, til andre skoler, nasjonalt til tjenester og læringsresurser)
- Tjenester og systemer må samhandle slik at elever og lærere får forenklet hverdagen

Arbeidsgruppen anbefaler derfor at

Det besluttes innført en identitetsforvaltning for grunnopplæringen som bygger på FEIDE og PKI, og som tilfredsstiller følgende krav og forutsetninger:

- Løsningen må dekke grunnopplæringens behov. Gjennom Indigoprosjektet (jf kap 4.5) skal det vinnes erfaringer med tjenester med ulike krav til sikkerhet.
- Sentrale FEIDE-komponenter og viktige grensesnitt skal være basert på åpne spesifikasjoner.
- Utviklede spesifikasjoner av komponenter og grensesnitt skal tilrettelegge for at FEIDE-komponenter vil kunne leveres av private leverandører i et marked med reell konkurranse.
- FEIDE og PKI må virke sammen gjennom bruk av sikkerhetsportalen
- FEIDE-løsningen for grunnopplæringen må samordnes med FEIDE-løsningen i UH-sektoren
- UNINETT ABC bidrar gjennom veiledning til å sette grunnopplæringen i stand til å innføre FEIDE.

2. SKOLENS UTFORDRINGER OG BEHOV

Gjennom flere prosjekter er utfordringer ved bruk av IKT i skolen kommet tydelig fram. Samtidig er det fra politisk nivå konkretisert ambisiøse mål for bruk av IKT i skolene. Det er i spennvidden mellom den faktiske situasjonen i skolene og konkrete politiske ambisjoner at spørsmålet om FEIDE i grunnopplæringen må avklares.

Realiseringen av Stortingets og Regjeringens skolepolitiske målsettinger må forutsette at en tar utgangspunkt i skolenes situasjon. Spørsmålet blir hvordan IKT kan benyttes som en katalysator for systematisk å skape positive endringer i skolene. Avgangsprøver og eksamener er viktige endringsfaktorer. Digital eksamen er derfor en sterk katalysator for endring av den pedagogiske virksomheten. Elever som bruker PC i læringssituasjonen, bør også kunne bruke PC ved gjennomføring av eksamen.

Nedenfor har vi tatt frem noen av hovedutfordringene rundt dette.

2.1 Grunnopplæringen har spesielle utfordringer

Grunnopplæringen står overfor store utfordringer i innføringen av digitale verktøy. En sammenligning med UH-sektoren illustrerer dette (se oversikt til høyre). Det er et stort antall skoler, til dels store ulikheter skolene i mellom, og det er stor variasjon i skolenes lærer- og elevsammensetning: Dette setter i stor grad krav til samordnende tiltak, på linje med det som er gjort i UH-sektoren. Manglende nasjonal samordning kan medføre at skolene ikke oppnår de effektiviseringsgevinstene (pedagogisk og administrativt) de ellers kunne ha fått.

	UH-sektoren	Grunn-opplæring
Antall elever	**249.942**	**777.686**
Antall lærere	**15.246**	**92.743**
Antall Skoler	**70**	**4.458**

2.2 Grunnopplæringen har behov for et mer effektivt vurderingssystem

Vurdering av elever er et område som er i sterk endring, blant annet som følge av innføringen av nasjonale prøver. Det er også et behov for å skape en tettere kobling mellom vurdering og undervisning. I tillegg til pedagogiske effekter fra innføringen av nye vurderingsformer, er det også behov for en mer effektiv eksamensgjennomføring. Dagens papirbaserte løsning krever store ressurser både fra Utdanningsdirektoratet, fra skoleeier og fra den enkelte skole.

Overgang til et digitalt eksamenssystem (der elevene kan bruke PC som del av selve eksamen og der de kan levere besvarelser digitalt), vil være en viktig forutsetning for å hente ut både pedagogiske og administrative effekter som er kort beskrevet over.

2.3 Grunnopplæringen har behov for digitale læringsressurser

Bred tilgang til digitale læringsressurser vil være en avgjørende faktor for om IKT skal få en bred plass i skolen. Dette gjerlder enten de er utviklet av ulike profesjonelle utviklere og/eller læremiddelprodusenter (eks. forlag) eller blir stilt til rådighet gjennom deling mellom brukerne (lærere og elever), Med FEIDE vil elever og lærere kunne gjennomføre samordnede søk i de baser som knyttes til en felles inngang.

2.4 Grunnopplæringen har behov for felles standarder

Mange skoler har allerede foretatt omfattende IKT-investeringer, blant annet i digitale læringsplattformer. Digital eksamen, nasjonale prøver, flytting av elevmapper mellom ulike læringsplattformer (LMS) og andre felles IKT-løsninger for eksempel innen digitale læringsressurser, øker behovet for teknisk samordning av skolenes dataløsninger.

Dette forsterker behovet for åpne standarder som retningsgivende for skolenes investeringer i IKT. Bruk av åpne standarder medfører åpen kommunikasjon mellom skoler med forskjellige dataløsninger.

2.5 Felles sikkerhetsløsning i grunnopplæringen

Grunnopplæringen vil i økende grad ta i bruk personaliserte tjenester. Dette er tjenester som håndterer personlige data om brukeren, og som forutsetter at personvernet ivaretas. Utdanningsdirektoratet har på sin side behov for å beskytte sensitive dokumenter som for eksempel eksamensoppgaver.

For i det hele tatt å kunne tilby tjenester på personnivå, er man avhengig av en identitetsforvaltning i utdanningssektoren. Uansett hva man skal utføre må man kunne identifisere seg, og det kan komme utfordringer i forbindelse med at identitetsforvaltning er avhengig av komplette, oppdaterte og fullstendige brukerdata fra de forskjellige nivåene (skole, skoleeier, fylkeskommune) etc.

Sikkerheten blir aldri bedre enn det svakeste ledd. Dette medfører at det også vil være utfordringer knyttet til forvaltning av brukerdata og de menneskelige holdningene til sikkerhet.

2.6 Oppsummering

- Grunnopplæringen er kjennetegnet ved et stort antall skoler med til dels store ulikheter i både størrelse og infrastruktur. Organisering og oppfølging i form av veiledning og støtte vil derfor være sentralt dersom grunnopplæringen skal kunne ta i bruk FEIDE.

- Overgang til et digitalt eksamenssystem, vil stille krav til en god og sikker identitetsforvaltning.

- Økende bruk av digitale læringsressurser og andre digitalt baserte tjenester i grunnopplæringen øker behovet for standardiserte løsninger, ikke minst i form av åpne standarder. Dette gjelder for eksempel flytting av elevmapper mellom ulike LMS-er og andre felles IKT-løsninger (jf 2.4).

3. OM FEIDE OG PKI

3.1 Hva er elektronisk identitetsforvaltning

Mange av oss har de siste årene ervervet ulike elektroniske identiteter, av og til uten at vi har vært klar over det. Vi bruker nettbank med kontonummer og engangspassord, vi leverer selvangivelsen over nettet ved å oppgi fødselsnummer og PIN-kode fra Skatteetaten, vi leser e-post etter å ha logget oss på med brukernavn og passord. Noe som mange kan vite (ditt kontonummer, fødselsnummer) sammen med noe som bare du vet om (PIN-kode, passord), knytter den elektroniske identiteten til deg som person. Hva som identifiserer deg, er avtalt mellom deg og den tjenesten du vil bruke. Du kan f. eks. ikke benytte e-postens brukernavn og passord til å levere selvangivelsen.

Identitetsforvaltning i vid forstand handler om å identifisere individer og kontrollere deres tilgang til ulike ressurser. Elektronisk identitetsforvaltning handler således om at individer kan identifisere seg elektronisk og få tilgang til digitale ressurser eller tjenester.

I grunnopplæringen, som ellers i samfunnet, er det et økende antall digitale ressurser og tjenester som baserer seg på elektronisk identifikasjon som tilgangskontroll. Det følgende vil argumentere for at en enhetlig elektronisk identitetsforvaltning vil løse de utfordringene dette skaper for utdanningssektoren.

3.2 FEIDE – enhetlig identitetsforvaltning i UH-sektoren

FEIDE står for Felles Elektronisk IDEntitet og er en enhetlig identitetsforvaltning for utdanningssektoren. FEIDE er allerede i bruk i universitets- og høgskolesektoren (UH), og vel 115 000 personer har så langt fått en FEIDE-identitet. Den mest brukte tjenesten med FEIDE-støtte har hatt over en million innlogginger hver måned.

Den elektroniske identiteten i FEIDE bygger på kvalitetssikrete personopplysninger som navn, fødselsnummer og utdanningsinstitusjonen som personen er tilknyttet. Til denne identiteten hører et unikt brukernavn og passord.

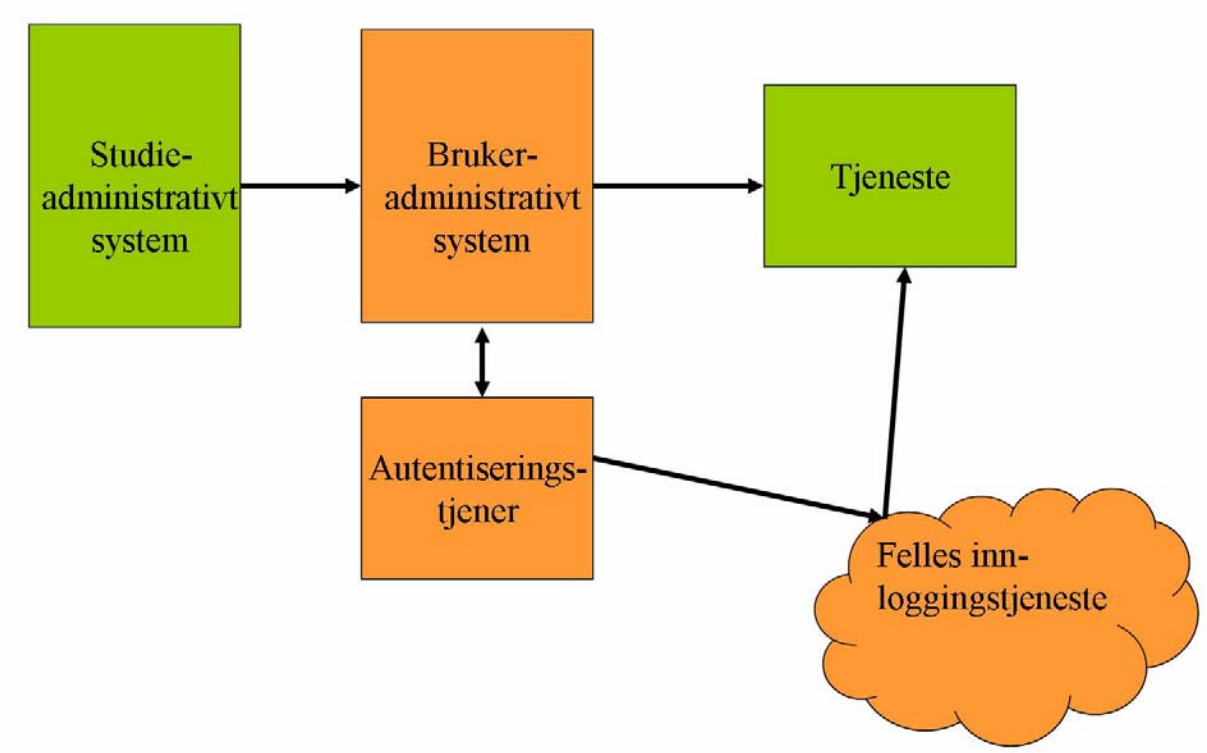
At FEIDE-identiteten er ”felles” innebærer to ting. Grunnlaget for den elektroniske identiteten bygger på de samme prinsippene uavhengig av hvilken utdanningsinstitusjon personen er tilknyttet. I tillegg skal den FEIDE-identiteten en person tildeles, kunne brukes til å få tilgang til mange ulike tjenester via en felles påloggingstjeneste for sektoren.

FEIDE-identiteten bygger på data fra UH-institusjonenes studieadministrative systemer. I FEIDE-modellen er det i tillegg innført et brukeradministrativt system (BAS). Det brukeradministrative systemet har flere viktige funksjoner: det kvalitetssikrer data fra det studieadministrative systemet, produserer unike elektroniske brukeridentiteter og passord, og eksporterer persondata til tjenester som har behov for slike.

Det brukeradministrative systemet legger dessuten ut informasjon om brukerne i en lokal autentiseringstjeneste, som kommuniserer med den nasjonale innloggingstjenesten. Den lokale autentiseringstjenesten kan, som eneste ledd i kjeden, si fra om det er oppgitt riktig brukernavn og passord ved innlogging.

I FEIDE-sammenheng er BAS et konsept, ikke et bestemt produkt. Det er allerede flere ulike kommersielle og ikke-kommersielle BASer i drift i UH-sektoren.

Figuren nedenfor viser elementene i FEIDEs kjede av informasjonsbehandlende elementer der mengden av informasjon som blir lagret om brukeren øker fra venstre mot høyre. Kvalitetssikrete data fra studieadministrativt system fører til opprettelse av unike elektroniske identiteter i det brukeradministrative systemet. Det brukeradministrative systemet legger dessuten til ny informasjon om brukeren som for eksempel brukernavn, passord og e-postadresse. Informasjon om brukeren kan deretter overføres til tjenestene etter behov, men tjenestene kan også selv lagre ytterligere informasjon om brukeren, som for eksempel hvilke ressurser brukeren har tilgang til, brukerens preferanser på nyheter, farger, etc.



Figuren viser FEIDE-modellen.

Når FEIDE skal beskrives med ord, er det tre aspekter som må vektlegges:

FEIDE forutsetter og tilrettelegger for datakvalitet.
Etablering av et brukeradministrativt system ved en institusjon medfører økt fokus på datakvaliteten i institusjonens administrative datasystemer. For mange av institusjonene som bruker FEIDE i dag, har økt datakvalitet vært et hovedargument for innføringen av FEIDE. I tillegg er mange tjenesteleverandører avhengige av korrekte opplysninger om brukerne av tjenestene. På grunn av FEIDEs høye krav til datakvalitet er tjenestene som kobles til FEIDE sikret korrekte opplysninger.

FEIDE tilbyr en sektoromgripende innloggingstjeneste.
Innloggingstjenesten støtter engangspålogging til flere tjenester (single sign-on[1]) og overføring av begrensete informasjonspakker om brukeren til tjenestene ved pålogging.

[1] Felles pålogging til mange tjenester

Den unike FEIDE-identiteten sammen med informasjonspakken om brukeren kan brukes til å gi personer i UH-sektoren tilgang til eksterne ressurser ved andre utdanningsinstitusjoner, hos kommersielle leverandører, nasjonale aktører etc. Eksempler på slike eksterne ressurser er bibliotektjenester, Samordnet Opptak (SO), studentweb og nedlasting av programvare på studentlisenser. Samtidig blir personopplysningene som identiteten bygger på kun lagret lokalt ved institusjonen som personen tilhører. Slik forenkles samarbeid mellom ulike aktører, og brukerne sikres tilgang til fellesressurser i hele sektoren.

FEIDE har bygd et tillitsnettverk for UH-sektoren.
FEIDE er en nasjonal overbyggende organisasjon som tar hånd om avtaler med institusjonene og med tjenesteleverandørene. FEIDE-avtalene garanterer at tjenestene bare får tilgang til de opplysningene som er nødvendige for at en person kan benytte tjenesten, og de pålegger institusjonene ansvaret for lokal brukeradministrasjon.

Den enkelte FEIDE-institusjon må selv identifiserer sine brukere og gå god for at disse skal få tilgang til visse tjenester. Hva slags opplysninger en tjeneste har bruk for vil variere fra tjeneste til tjeneste; noen trenger kanskje bare å vite hvilken institusjon individet tilhører, mens andre vil for eksempel ha behov for fullt navn, adresse og fødselsnummer.

3.3 PKI – Public Key Infrastructure – autentisering og elektronisk signatur basert på kryptografi. Felles løsninger for offentlig sektor.[2]

Brukere av elektroniske tjenester kan autentisere seg (dvs. forsikre om hvem de er) på flere ulike måter overfor en elektronisk tjeneste på Internett – f.eks. ved hjelp av PIN-koder, passord, engangspassord fra en ”kalkulator” eller mobiltelefon, eller en kode fra et ”skrapeark”. PKI gjør dette ved hjelp av en hemmelig kryptonøkkel, som brukeren har kontroll over, slik at ingen uvedkommende får bruke den.
PKI-tjenesten kan verifisere at brukeren er i besittelse av den rette hemmelige nøkkel ved å matche denne mot en ”offentlig” nøkkel som er allment tilgjengelig. Koblingen mellom en bruker og dennes offentlige nøkkel er bekreftet av en tiltrodd tredjepart (sertifikatutsteder).
I tillegg til autentisering, kan den samme infrastrukturen også tilby tjenester for uavviselighet (ikke-benekting), dvs. en ”ekte” elektronisk signatur, som uavviselig knytter avsenderen til innholdet i et dokument. Dokumentet blir samtidig forseglet elektronisk, slik at alle forsøk på manipulasjon etter signering vil bli oppdaget.
Endelig, kan den private og offentlige nøkkelen benyttes til å kryptere (forvrenge) innholdet i et oversendt dokument, slik at kun den rette mottaker får se innholdet, men ingen andre.

PKI legges til grunn som foretrukket sikkerhetsløsning for autentisering og signering i offentlig sektor, fordi:

- det er ønskelig at publikum skal kunne bruke én og samme sikkerhetsløsning ved all elektronisk kontakt med offentlig sektor, og at det ikke etableres ulike løsninger i ulike etater som har publikumskontakt
- PKI vurderes som sikker nok teknologi når det gjelder utstrakt gjenbruk mot mange ulike tjenester
- det er ønskelig at publikum skal kunne bruke samme sikkerhetsløsning mot offentlig sektor som mot private tjenesteytere

[2] Jf http://odin.dep.no/mod/norsk/tema/ITpolitikk/pkiorgan/bn.html

- det er ønskelig at sikkerhetsløsninger i størst mulig grad skal kunne fungere sammen, både innen den enkelte sektor og mellom sektorer, samtidig som kostnader ved disse reduseres
- det er behov for elektronisk signatur, både fra borgere, næringsliv og forvaltning, og PKI vurderes som eneste tilgjengelige teknologi som gir mulighet for å knytte avsender til meldingsinnhold på en standardisert måte.

Felles infrastruktur for bruk av eID og e-signatur i offentlig sektor
Offentlig sektor skal legge til rette for en felles infrastruktur for bruk av eID og e-signatur, utstedt i det norske markedet, slik at dette kan brukes i kommunikasjon med og i offentlig sektor. Brønnøysundregistrene vil på vegne av staten og kommunesektoren inngå og forvalte rammeavtaler med aktørene i markedet som tilbyr nødvendige tjenester og produkter. Viktige komponenter i infrastrukturen vil være:

- En sikkerhetsportal som skal understøtte elektroniske tjenester rettet mot borgere og næringslivet. Portalen skal levere autentiseringstjenester, signeringstjenester, elektronisk notar-tjenester og tjenester for felles pålogging (single sign-on). Portalen skal tilby ett, enkelt grensesnitt mot sine tjenester og derved senke terskelen for å ta i bruk eID og e-signatur i små etater. Bruk av tjenester fra en sikkerhetsportal er pålagt for alle statsetater som skal gjøre anskaffelse av nye løsninger for bruk av eID/e-signatur fra og med november 2005. Kommunal sektor anbefales å bruke portalen. Det er åpnet for overgangsordninger for de etater som allerede har alternative sikkerhetsløsninger i bruk, med den målsetting å gå over til eID/e-signatur på en slik måte at bruken av eksisterende elektroniske tjenester ikke går ned.

- Sikkerhetsportalens registreringstjeneste, som skal understøtte rask distribusjon av eID/e-signatur til borgere, med utgangspunkt i andre former for elektronisk autentisering, så som passord og sikkerhetskoder utlevert av offentlige etater til bruk mot egne tjenester. Det vil også bli etablert ordninger for distribusjon av sertifikater på høyt sikkerhetsnivå, der personlig fremmøte er nødvendig, gjennom offentlige kontorer (f.eks. NAV-sentra, biblioteker e.l.).

- En felles avtale om utstedelse av eID/e-signatur til offentlige virksomheter og for ansatte i offentlig sektor. Leverandøren som får avtalen skal tilby enkel og pålitelig distribusjon av eID/e-signatur til en akseptabel pris, og med muligheter for å etablere lokale kataloger og valideringstjenester i offentlige virksomheter. Slike eID skal benyttes i intern elektronisk kommunikasjon i forvaltningen og til kommunikasjon mot næringslivet i forbindelse med offentlige innkjøp, ev. andre former for samhandling som krever sikker autentisering av offentlig ansatte og offentlige virksomheter.

For å sikre at løsninger som inngår i denne infrastrukturen oppfyller kravene nedfelt i *Krav-spesifikasjon for elektronisk ID og signatur (PKI) i offentlig sektor*[3], vil det bli etablert en frivillig, offentlig godkjenningsordning. Tilbydere av eID/e-signatur i det norske markedet vil kunne få godkjenning for sine tjenester og løsninger i forhold til de tre ulike sikkerhetsnivåer som er vedtatt brukt i offentlig sektor: Person Høyt, Person Standard og Virksomhet. Forvalter av ordningen skal sørge for at det til enhver tid finnes en liste med godkjente

[3] Publisert av Moderniseringsdepartementet i januar 2005.

leverandører og skal følge opp godkjenninger overfor disse. For leverandører som ønsker å tilby sine tjenester gjennom sikkerhetsportalen vil godkjenningen være obligatorisk.

I den elektroniske tjenesteportalen Altinn, som samler tjenester rettet mot næringslivet, er det i dag implementert en PKI-løsning tilsvarende sikkerhetsnivå Person Høyt. Løsningen kan benyttes til pålogging i portalen og til signering av dokumenter, primært gjeldsbrev fra Statens lånekasse for utdanning. Altinn tilbyr for øvrig autentiseringstjenester med bruk av andre løsninger enn PKI (statisk og dynamisk passord, kombinert med fødselsnummer).

Den planlagte portalen MinSide skal i første omgang tilby tjenester som krever sikkerhetsnivå Person Standard, med felles pålogging. Tjenestene vil være av typen tilgang til registerinformasjon og noen transaksjonstjenester (bytte av fastlege, meldekort i Aetat, flyttemelding ol.) som kun krever autentisering på det nevnte nivå.

3.4 Utfordringer knyttet til identitetsforvaltning i grunnopplæringen

Grunnopplæringen består av mange ulike skoler av ulik størrelse. Alle skolene har behov for å lagre en mengde opplysninger om personer som er tilknyttet organisasjonen, enten det er lærere, elever, administrativt ansatte eller foresatte. Vi sier at disse opplysningene er samlet i et skoleadministrativt system (tilsvarer UH-sektorens studieadministrative system), og det er denne datakilden som gjelder for personopplysninger i skolen. Det skoleadministrative systemet kan bestå av et papirbasert arkiv, det kan være et regneark, eller det kan (som i de videregående skolene) være kommersiell programvare som er utviklet for skoleadministrasjon.

Det er altså et stort spenn i teknologiske løsninger for skoleadministrative systemer. Samtidig fins det ikke noen mal for enhetlig håndtering av personopplysninger. Resultatet er svært varierende kvalitet på de persondata som er lagret.

Når en person begynner ved en skole, enten som ansatt eller elev, må personen også opprettes i alle de elektroniske systemene som skolen bruker. Personen skal kanskje bruke en læringsplattform, lese e-post, få tilgang til digitale læringsressurser eller koble seg på et trådløst nettverk på skolen.

Slike systemer trenger informasjon om deg som person for å gi deg riktig tilgang til tjenesten. Mange tjenester har for eksempel behov for informasjon om hvilken rolle en person har ved skolen. En læringsplattform (LMS) må kunne skille mellom lærere og elever, i tillegg må den kunne vite hvilken lærer som er kontaktlærer for hvilke elever, hvilke elever som tilhører hvilket trinn og hvem som er foresatt til hvilken elev.

Dersom de ulike systemene ikke kan få kvalitetssikrete personopplysninger fra skolens administrative system, må personen opprettes manuelt i hvert enkelt system. Dette medfører stor risiko for feil og fare for data av dårlig kvalitet. Mange skoleeiere er klar over at dette er et stort problem i deres skoler.

Dårlig datakvalitet, manuell overføring av persondata til tjenester og separat opprettelse av elektroniske identiteter hos de enkelte tjenestene har to alvorlige konsekvenser for skolesektoren.

- For det første mangler mange skoler oversikt over hvilke opplysninger som er registrert hvor og hvordan de ulike systemene bruker disse opplysningene. Dette gjør

det umulig å oppfylle kravene i *Lov om behandling av personopplysninger* (Personopplysningsloven) om at enhver virksomhet som lagrer personopplysninger skal kunne dokumentere hvilke opplysninger som er lagret om den enkelte og hvordan disse opplysningene brukes.

- For det andre får elever og lærere etter hvert et uhåndterlig antall elektroniske identiteter å holde styr på. Når stadig flere digitale tjenester tas i bruk i skolene, øker antallet steder en person må logge på for å få tilgang til tjenestene. I dag må lærere og elever skrive inn ulike brukernavn og passord for hver ny tjeneste de vil benytte. Det er lett å glemme ett av mange brukernavn og passord, og IKT-ansvarlige bruker ofte mye tid på å dele ut nye.

3.5 FEIDE for grunnopplæringa

FEIDEs datakvalitetskrav, innloggingstjeneste og tillitsnettverk kan langt på vei løse de utfordringene for grunnopplæringa som er skissert tidligere. Skoleeiere som tar i bruk FEIDE, får bedre datakvalitet og kontroll over egne data, elever og lærere får færre elektroniske identiteter, og den felles innloggingstjenesten senker terskelen for utvikling av nye tjenester for skolemarkedet.

Nedenfor beskrives hvordan innføring av FEIDE kan ha positive effekter for skolen på lokalt, regionalt og nasjonalt nivå.

Lokalt på den enkelte skole
Lærere og elever som får tildelt FEIDE-identiteter kan bruke disse til å logge på alle de tjenester som har gjort avtaler med FEIDE og slipper dermed å huske mer enn ett brukernavn og passord. Identiteten kan også benyttes til en rekke lokale IKT-tjenester som for eksempel kobling av elevers og læreres PCer til et lokalnett (kablet eller trådløst), utskrift og lagring av dokumenter.

Dersom skolen benytter en læringsplattform kan man ved hjelp av FEIDE automatisk opprette brukere i LMSen på grunnlag av opplysningene i det skoleadministrative systemet. I tillegg får man automatisk en tildeling av roller (lærer, elev, foresatt) og adgang til ulike virtuelle ”rom” basert på opplysninger om for eksempel klasse, trinn, fag og liknende.

Regionalt i kommuner og fylkeskommuner
Skoleeiere som ønsker å ta FEIDE i bruk, må sette fokus på kvaliteten i sine persondata. Å få orden på personopplysninger og bruken av dem er en stor utfordring for skoleeiere i grunnopplæringa. Skoleeierne må gjennomgå denne prosessen uavhengig om de skal innføre FEIDE eller ikke, men FEIDE-innføring kan bidra til at dette gjøres på en enhetlig og kvalitetssikret måte.

Det er store fordeler ved kun å lagre personopplysninger på ett sted i organisasjonen, og at endringer i disse opplysningene kun må gjøres ett sted for automatisk oppdatering av alle systemer. Dette effektiviserer håndteringen av personopplysninger og reduserer faren for uriktige data. I tillegg blir det langt enklere å oppfylle kravene i Personopplysningsloven.

FEIDE-innføring kan dessuten være et skritt på veien mot sentralisering av IKT-driften i kommuner og fylker, da dette vil forenkle behandling av personopplysninger for skoleeier. Det er betydelige potensielle økonomiske gevinster ved slik sentralisering.

Når alle data om en person er registrert i det skoleadministrative systemet, blir det opprettet

en bruker i IKT-systemet, og vedkommende får tildelt rettigheter på grunnlag av opplysninger om hvilken rolle personen har ved skolen. FEIDE letter automatisering av slike rutiner.

Nasjonalt
På nasjonalt nivå ser vi at det finnes stadig flere ressurser, tjenester og tiltak som kan nyttiggjøre seg en enhetlig identitetsforvaltning for utdanningssektoren. Vi tenker her på for eksempel nasjonale prøver, eksamen med IKT, opptakssystemer, portaler som utdanning.no og innholdstjenester som f.eks. nasjonalt digitalt bibliotek.

Med en FEIDE-løsning kan elever og lærere identifisere seg på en sikker måte, samtidig som viktig basisinformasjon (som årskull, skoletilhørighet, lærer/elev, fagplan osv.) kan overføres til tjenestene. Tjenester som trenger sterkere identifikasjon av brukeren, som for eksempel en IKT-basert eksamen, kan oppnå dette ved engangspassord på SMS, PKI, biometrisk identifikasjon eller liknende. Disse teknologiene kan integreres med FEIDE-teknologien slik at man slipper å innføre et nytt system for identitetsforvaltning.

Skalering av FEIDE
Ved bruk av FEIDE er det tilstrekkelig å utvikle en eneste løsning for hele sektoren, der man i dag ofte må ty til skreddersøm for å tilfredsstille lokale behov. Tjenester som i dag må bygge opp egne systemer for brukeridentifikasjon, kan overlate dette til FEIDE.

FEIDE er mer velegnet for store enn for små enheter. Omkostningene ved å ta FEIDE i bruk, for eksempel utgifter til utstyr, programvare og spisskompetanse, bør deles på flest mulig brukere. I grunnopplæringen er det derfor ressursmessig fordelaktig å se på kommuner og fylkeskommuner som enheter for å innføre FEIDE for sine skoler, og ikke den enkelte skole.

Hvis grunnopplæringen som helhet tar i bruk FEIDE, får man en positiv effekt av samordning mot UH-sektoren, både fordi tjenestene er tilnærmet identiske og fordi identiteten vil ha et livsløp gjennom hele utdanningssektoren.

FEIDE-forsøksvirksomhet i grunnopplæringa
UNINETT ABC har valgt å starte et innføringsprosjekt kalt Indigo hvor FEIDE skal innføres i grunnopplæringa for de videregående skolene i to fylkeskommuner, Østfold og Hedmark. Målet er at over 20 000 elever og lærere vil ta FEIDE-identiteten i bruk mot et bredt utvalg tjenester i løpet av 2006. Indigo-prosjektet er nærmere omtalt i kapittel 4.5 i denne rapporten.

3.6 FEIDE og den offentlige satsingen på felles infrastruktur for eID og e-signatur

FEIDE er en tjeneste for forvaltning av felles elektronisk identitet for UH-sektoren. FEIDE er sammensatt av en innloggingsfunksjon, en datamodell og en tillitsstruktur som til sammen danner identitetsforvaltning for personer tilknyttet høyere utdanningsinstitusjoner. FEIDE forholder seg kun til personer som har veldefinerte forhold til utdanningsinstitusjoner.

Innloggingsfunksjonen i FEIDE er i dag basert på åpen egenutviklet programvare som støtter single sign-on og overføring av basisinformasjon om brukeren til de aktuelle tjenester. Innlogging skjer i dag bare ved bruk av brukernavn/passord, selv om FEIDE i utgangspunktet er nøytral i forhold til valg av teknologi for autentisering (PKI, passord, engangspassord, biometri). Ingen av de tjenestene innen utdanningssektoren som har implementert FEIDE-innlogging har satt krav til elektronisk signatur, noe som ville utløst behov for PKI for

sluttbrukere. Dagens bruk av PKI innen UH-sektoren er på tjenersiden for sikring av kommunikasjon.

Datamodellen for FEIDE støtter opp under den lokale brukeradministrasjonen og er knyttet til de lokale administrative funksjonene ved utdanningsinstitusjonen. Tillitsstrukturen definerer plikter og krav for brukere, institusjoner, tjenester og FEIDE sentralt.

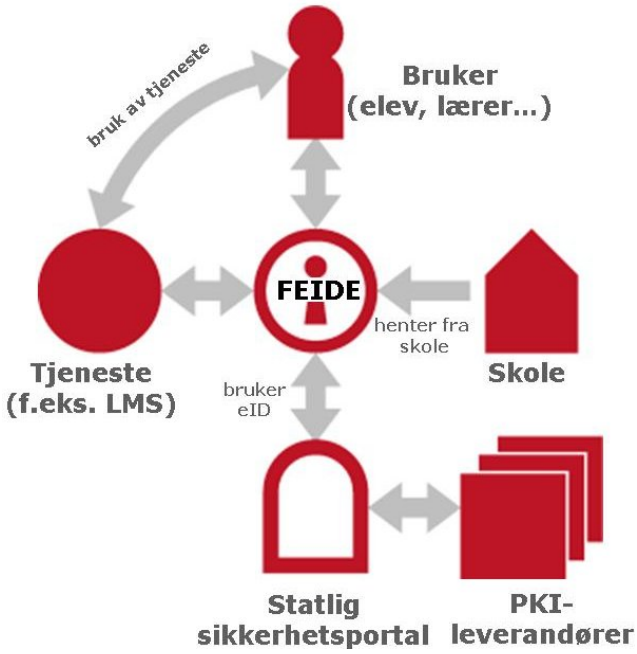
Innen UH-sektoren er det stor bruk av IT til de daglige læringsprosessene, og en stor mengde hverdagstjenester (eLæringssystemer, bibliotektjenester, portaler) gjør bruk av FEIDE til innlogging.

Kravene til sikkerhet øker, og det vil komme tjenester som har behov for signering. Til nå har de tjenestene som har sett behovet blitt stoppet av kostnadene knyttet til PKI. For populære hverdagstjenester har transaksjonskostnadene med PKI blitt vurdert som for høye.

For UH-sektoren er det viktig at FEIDE er mer enn bare innlogging, det er også muligheten for tjenester til å få basisinformasjon om brukeren, slik at behovet for kopiering av personinformasjon og føring av parallelle personregister minker.

Det mest nærliggende spørsmålet å stille er i hvilken grad ansatte i utdanningssektoren som helhet og brukere av tjenester fra sektoren (elever, foreldre) vil benytte en løsning for eID / e-signatur som er i samsvar med krav i Kravspesifikasjon for PKI i offentlig sektor, og som kan benyttes til intern elektronisk kommunikasjon i det offentlige eller til tilgang og bruk av elektroniske tjenester fra offentlig sektor. F.eks. kan det tenkes at foreldrene har fått en slik løsning i forbindelse med deres bruk av tjenester i portalene Altinn og/eller MinSide. Elevene kan ha fått løsningen i forbindelse med etablering og bruk av en bankkonto (forutsetter en alder på 15 år) eller i annen sammenheng (eks. e-handel på nettet eller tilgang til MinSide).

Dersom dette vil være tilfellet, må det vurderes om FEIDE også kan tilby sine tjenester med utgangspunkt i at brukeren har denne type identifikasjon/signatur. Dette vil kreve at FEIDE-tjenesten kan autentisere/validere signaturer basert på sertifikater utstedt i henhold til sikkerhetsnivåene Person Høyt og Person Standard og at aktuelle tjenester i utdanningssektoren er tilrettelagt for bruk av denne type sikkerhetsløsninger (gjerne via mekanismer for single sign-on).



FEIDE vil støtte PKI-innlogging for tjenester som har dette behovet så snart PKI blir tilgjengelig med en prismodell tilpasset utdanningssektoren. Slik tilgjengelighet forventes som en følge av løsningen for eID/eSignatur for offentlig sektor (sikkerhetsportalen). FEIDE har som mål å følge de krav som stilles opp i tilknytning til denne løsningen. Kostnadene for tilpasning til sikkerhetsportalen vil bli klarlagt når rammeavtalen er på plass og prisvilkår blir offentliggjort.

3.7 Oppsummering

Grunnopplæringen har et bredt digitalt tjenestespekter. Tjenestene har ulike behov for informasjon om brukerne og ulike krav til sikkerhetsnivå, her eksemplifisert ved fire sentrale tjenester:

- Digital eksamen krever høyere sikkerhetsnivå enn normalt, trolig vil Person Høyt være riktig nivå. For å sikre at riktig person leverer eksamen må fødselsnummer oppgis sammen med skoleinformasjon.
- Lånekassen trenger fødselsnummer og sikkerhet på høyt nivå, og er i ferd med å ta i bruk sikkerhetsportalens funksjonalitet. Det er i dag ikke avklart hvordan Lånekassen skal få overført informasjon fra skolene om elever og avlagte eksamener.
- eLæringssystemer trenger først og fremst skoleinformasjon med roller og klassetrinn, for eksempel om personen er lærer eller elev, hvilke klasser er læreren kontaktlærer for, hvilket trinn går eleven på. I dag er normalt sikkerhetsnivå (Person Standard) tilstrekkelig. Det vil være en fordel om de som har eID kan logge seg inn med denne.
- Leverandører av læremidler, som for eksempel forlag, har behov for å vite både om en person har tilgang (har skolen kjøpt produktet?) og hva slags informasjon personen skal få tilgang til ved pålogging. En elev på første trinn har behov for annen informasjon enn en elev på femte trinn, og lærere trenger tilgang til andre ressurser enn elever. Det vil dermed være behov for informasjon om skole, rolle og klassetrinn. Sikkerhetsnivået trenger ikke å være spesielt høyt, og lavest mulig pris er avgjørende for forlagene.

Tjenestenes ulike krav til sikkerhet og ulike behov for informasjon om brukeren medfører behov for ulike løsninger.

Kostnaden knyttet til ulike løsninger vil også ha betydning for sektoren. Tjenestene vil karakteriseres av svært ulik bruksfrekvens i tillegg til at de har ulikt sikkerhetsbehov. For noen tjenester vil lave kostnader knyttet til et lavt sikkerhetsnivå være å foretrekke.

Både sikkerhetsportalen og Feide vil kunne utvikle seg med hensyn på sikkerhetsnivåer og prisstrukturer relatert til dagens løsninger. Men løsningene inneholder grunnleggende sett komplementære egenskaper slik at arbeidsgruppen konkluderer med at disse løsningene utfyller hverandre

4. ASPEKTER VED FEIDE-INNFØRING

4.1 Økonomi og marked

For å få oppslutning om en velfungerende identitetsforvaltning i grunnopplæringen, må de økonomiske rammebetingelsene være forutsigbare for skolene og skoleeierne. Det må foreligge en langsiktig finansieringsplan basert på de reelle kostnadene for de valgte løsningene. I den vedlagte utredningen, "Rammeverk for bruk av FEIDE i grunnopplæringa", presenteres de kostnadene som må fordeles på aktørene, og fordelingen av disse blir diskutert.

En identitetsforvaltning for grunnopplæringen bør samordnes med FEIDE i UH-sektoren. Det er mye å hente på at hele utdanningssektoren følger samme arkitektur for identitets-forvaltning: Lavere utviklingskostnader, stordriftsfordeler samt et felles reservoar av kompetanse og erfaringer.

På et overordnet nivå har innføring av FEIDE åpenbar nytteverdi for utdanningssektoren:

- Skoleeiere unngår teknisk innelåsing til enkeltleverandører, og vil stå fritt til å velge nye tjenesteleverandører uten på nytt å måtte utvikle nye og kostbare rutiner for overføring av personopplysninger.
- FEIDE bidrar til fornuftig gjenbruk av persondata mellom tjenester og organisasjoner ved at data bare registreres og behandles på et sted, men kan benyttes av alle tjenestene etter behov. Dette er en effektiviseringsgevinst som utdanningssektoren bør høste.
- FEIDE-klargjorte tjenester vil kunne tas i bruk i hele utdanningssektoren med et minimum av lokale tilpasninger.

Også for tjenesteleverandører har FEIDE stor nytteverdi:

- Tjenesteleverandører får tilgang til kvalitetssikrede personopplysninger på åpne, standardiserte formater.
- De slipper å vedlikeholde autentiseringsmekanismer i egen applikasjon.
- Bruk av FEIDE som enhetlig identifikasjonsinfrastruktur for utdanningssektoren vil minske utviklingskostnadene for nye produkter og tjenester. Dette vil kunne bidra til å øke konkurransen blant tjenesteleverandørene.

FEIDEs kostnadselementer foreslås fordelt på tjenesteleverandører, institusjoner, institusjonseiere og departement med utgangspunkt i blant annet nytteverdien på hvert enkelt nivå. Viktige elementer i denne diskusjonen vil være verdien av FEIDE-innføring for de enkelte aktørene. Dagens kostnadsnøkkel for UH-sektoren er et aktuelt utgangspunkt, men trenger å tilpasses situasjonen i grunnopplæringen.

4.2 Roller og ansvar

I mange sammenhenger er det viktig å ha klare roller både for individer og for organisasjoner. For individer vil rollene man innehar kunne benyttes til for eksempel å gi rettigheter til tjenester og ressurser, men rollene kan også medføre ansvar av forskjellig slag. For organisasjoner kan klare roller avklare hvilke administrative rettigheter og ansvar organisasjonen har, og rollene kan lette arbeid med blant annet kostnadsfordeling.

FEIDE har et klart definert sett med roller for individer som kan benyttes av alle

utdanningsinstitusjoner og tjenesteleverandører. Eksempler på roller er elev, ansatt og foresatt.

Med klare rolledefinisjoner unngår man å skape forvirring rundt hva en rolle innebærer i en gitt situasjon eller en gitt tjeneste. Det fins rutiner for hvordan lista over aksepterte roller i FEIDE kan endres. Rollelista vil på den måten være konsistent og vil bli gjort tilgjengelig for alle undervisningsinstitusjoner og tjenesteleverandører.

FEIDE har også klare definerte roller for organisasjoner av forskjellig slag som kan benyttes i verdikjedene rundt tjenester i FEIDE. Gjennom bruken av roller som vertsorganisasjon, tjenesteleverandør og brukere kan grensesnitt mellom forskjellige aktører defineres på en klar og konsis måte.

4.3 Sikkerhet og personvern

En tilstrekkelig grad av sikkerhet vil være helt nødvendig for mange av tjenestene som benyttes i dag og i fremtiden. Mange av de nye tjenestene er knyttet direkte opp mot Internett med de mulighetene og truslene dette gir. Hver tjeneste som tas i bruk i utdanningssektoren må avklare sitt sikkerhetsnivå i forhold til hvilken type tjeneste det er og hvilke data som tjenesten benytter. For eksempel vil en tjeneste rundt digitale eksamener ha et annet sikkerhetsnivå enn en kalendertjeneste.

Hver organisasjon må ha sitt eget sikkerhetsregime som er avpasset i forhold til de tjenestene de benytter. Dette regimet vil blant mye annet inneholde metoder for autentisering, autorisasjon, innholdsfiltrering, kryptering av dataoverføring, rutiner og IT-reglementer osv. Innenfor et slikt regime vil FEIDE kunne sikre en omforent autentiseringsmetode for hele sektoren.

Med den arkitekturen FEIDE har kan mange forskjellige autentiseringsmekanismer benyttes. For kalendertjenesten vil en kanskje bare benytte brukernavn og et passord, mens for digitale eksamener ønsker en sterkere autentisering på grunn av et høyere sikkerhetsnivå. Dette kan være mekanismer som engangspassord, digitale sertifikater (Sikkerhetsportalen for offentlig sektor) eller lignende. Fordi FEIDE ikke er bundet til en spesiell autentiseringsmekanisme, kan enhver mekanisme legges inn i FEIDE når det er hensiktsmessig for utdanningssektoren.

Informasjon fra FEIDE må kunne benyttes av tjenestene til tilgangskontroll i en del tilfeller der dette er ønskelig. Men bruk av FEIDE sier for eksempel ingenting om hvordan en tjeneste skal forholde seg til en mindreårig bruker; dette skal og bør avklares mellom tjenesteleverandør og skoleeier (som kunde).

Den store mengden tjenester som etter hvert blir tilgjengelig for skolene, gjør at det av personvernshensyn vil bli veldig viktig å vite hvilken informasjon som ligger lagret hvor og hvordan denne benyttes. FEIDE hjelper utdanningsinstitusjonene med å oppfylle de kravene som er satt i Personopplysningsloven. Med den tilgjengelige innsynstjenesten kan alle personer se hvilke opplysninger som er lagret om seg selv. Ved pålogging til en FEIDE-klargjort tjeneste får brukeren oversikt over hvilke opplysninger tjenesten vil få oversendt og kan avslå eller akseptere denne overføringen.

FEIDE er ikke et sentralt register som samordner informasjon fra andre registre, men muliggjør overføring av informasjon fra en utdanningsinstitusjon til en tjeneste på en sikker

måte. Tjenestene får utlevert de personopplysningene som er avtalt med FEIDE og ikke noe mer. Tjenestene har heller ingen mulighet til å søke etter informasjon hos utdanningsinstitusjonene [4].

Arkitekturen er altså bygd opp slik at den minimaliserer flyten av personopplysninger og synliggjør for brukeren hvilke personopplysninger tjenester får tilgang til.

4.4 Bruk av åpne standarder

Offentlig sektor har i den senere tiden hatt et økt fokus på bruken av åpne standarder. I "eNorge 2009 – det digitale spranget" [5] står det blant annet i kapittel 3.2 at innen 2009 skal alle nye tjenester i offentlig sektor benytte åpne standarder. Også for dokumentoverføringer skal det innen 2008 benyttes forvaltningsstandarder som skal settes i 2006. Åpne standarder er også viktig for FEIDE for å sikre at komponentene i arkitekturen skal fungere sammen når mange aktører er inne i bildet både på tjeneste- og driftsiden. Uten bruk av åpne standarder ville det være vanskelig å realisere de fordelene som ligger i FEIDE i dag. Komponenter i FEIDE-arkitekturen (skoleadministrative system, brukeradministrative system og tjenester) kan byttes ut når det er hensiktsmessig uten at hele arkitekturen blir påvirket.

Alle grensesnitt som benyttes i FEIDE-sammenheng er basert på åpne standarder. Det er også åpne standarder under utarbeidelse for kommunikasjon mellom skoleadministrative system, brukeradministrative system og tjenester.

4.5 Innføringsprosjektet Indigo

Indigoprosjektet er et samarbeidsprosjekt mellom Uninett ABC og to fylkeskommuner. Prosjektet er koordinert med FEIDE-satsningen i UH-sektoren.

De to fylkeskommunene vil innføre FEIDE-identiteter for sine elever i videregående opplæring, samtidig som de ønsker å gi et løft på regionale tjenester til elevene. Elevene og ansatte vil få et godt og helhetlig tilbud både lokalt på skolen, regionalt i fylket og på nasjonale tjenester som vil bli FEIDE-klargjort gjennom prosjektet.

Tjenestetilbudet vil legge til rette for samarbeid og understøtte de pedagogiske målsettingene som fylkene har. Et ledd i den fylkesvise satsingen er å sikre tilstrekkelig nettkapasitet helt ut til sluttbruker.

Foreløpig deltar Hedmark og Østfold i Indigo, men prosjektet kan bli utvidet til også å innføre FEIDE i andre fylkeskommuner.

En viktig målsetting med prosjektet er erfaringsoverføring til andre skoleeiere. Det planlegges ulike virkemidler for erfaringsoverføring, ett av disse er å dokumentere organisatoriske, pedagogiske og tekniske erfaringer fra innføringen i de to fylkeskommunene. Via prosjektet vil det bli utarbeidet kravspesifikasjoner, modeller og planer for en nasjonal utrulling av FEIDE i grunnopplæringen.

[4] For mer informasjon, se: http://www.feide.no/vert/personvern.html
[5] Rapporten finnes her: http://odin.dep.no/mod/norsk/tema/ITpolitikk/enorge/bn.html

Det vil særlig bli lagt vekt på å dokumentere visse grensesnitt mellom FEIDE-elementene for å tilrettelegge for en mest mulig effektiv innføring for andre skoleeiere. Utarbeidelsen av spesifikasjonene vil være basert på fylkeskommunenes behov og i dialog med leverandører. Indigo-prosjektet vil også kunne verifisere deler av kostnadsmodellen som er utarbeidet.

4.6 Oppsummering

- For skoler og skoleeiere vil FEIDE bidra til en strukturert identitetsforvaltning, og som muliggjør bytte av tjenesteleverandører uten på nytt å måtte utvikle nye og kostbare rutiner for overføring av personopplysninger.
  - FEIDE vil hjelpe utdanningsinstitusjoner med å oppfylle krav satt i Personopplysningsloven.
- Tjenesteleverandører vil få tilgang til kvalitetssikrete personopplysninger, og de vil slippe vedlikehold av autentiseringsmekanismer i egen applikasjon.
  - FEIDE vil også bidra til å øke konkurransen blant tjenesteleverandørene.
- FEIDE er fleksibel med hensyn til autentiseringsmekanismer, og eIdentitet og eSignatur (PKI) kan legges inn der det er hensiktsmessig.
- Kostnadene ved FEIDE vil måtte bæres av sentrale myndigheter, tjenesteleverandørene og brukerne i fellesskap

5. VEDLEGG

5.1 Mandat for FEIDE-

1. Bakgrunn

Prosjektet Felles elektronisk identitet (FEIDE) er opprettet med det siktemål å utforme en enhetlig nasjonal identitetsforvaltning i utdanningssektoren. Prosjektet er forankret ved og blir ledet av UNINETT AS. FEIDE har i en første fase blitt utviklet og rullet ut i høyere utdanning. I dag deltar ca 25 universiteter og høyskoler i FEIDE-prosjektet med til sammen ca 150 000 FEIDE-brukere.

Spørsmålet om bruk av FEIDE i grunnopplæringen (FEIDE2GO) omtales i flere styringsdokumenter:

- I programbeskrivelsen for Program for digital kompetanse (PfDK) er følgende resultatmål satt opp: ”Alle institusjoner i UH-sektoren skal ha et nasjonalt brukernavn innen 2006, og alle i grunnopplæringen innen 2008. Implementering av FEIDE-teknologien spiller en sentral rolle her. Det skal etableres en identitetsforvaltning innenfor utdanningssektoren innen 2005.”
- I Stortingsprp. Nr 1 (2004-2005) heter det: ”Arbeidet for å få etablert ein identitetsforvaltning innanfor utdanningssektoren vidareførast. I dette arbeidet vil FEIDe-prosjektet, som er UNINETT si stasing på identitetsløysingar for UH-sektoren, vere sentralt. Departementet vil i 2005 ta stilling til korleis FEIDE-teknologien skal takast i bruk grunnopplæringa.”

Regjeringen har besluttet at en egen kravspesifikasjon for PKI-anvendelser i offentlig skal ligge til grunn for all autentisering i offentlig sektor som krever PKI. Dette reiser viktige prinsipielle og praktiske spørsmål om grenseflaten mellom FEIDE-arbeidet og utrulling av PKI-anvendelser i offentlig sektor.

2. Rammebetingelser

Arbeidsgruppen rapporterer til Utdannings- og forskningsdepartementet.

Arbeidet skal rette seg mot behovet skoleeiere ved KS og (fylkes-)kommunene vil ha for en fremtidig identitetsforvaltning., og bør derfor være normerende for aktiviteten til departementet, Utdanningsdirektoratet og UNINETT på dette området.

Arbeidsgruppen må holde seg orientert om arbeidet med utrulling av PKI-anvendelser i offentlig sektor.

3. Arbeidsoppgave

Arbeidsgruppens hovedoppgave er å lage en anbefaling til UFD om hvordan FEIDE-teknologi skal tas i bruk i grunnopplæringen. Anbefalingen skal ligge til grunn for en politisk beslutning om evt innføring av FEIDE-teknologi i grunnopplæringen.

Gruppen bes særlig om å vurdere følgende punkter:

- Teknologiske og andre (?) betingelser som må være på plass for innføring av FEIDE-teknologi i grunnopplæringen
- Innføringstakt i grunnopplæringen
- Grenseflaten mot PKI-anvendelser i offentlig sektor
- Organisatorisk løsning for FEIDE-arbeidet

4. Leveranser, frister og sammensetting

Arbeidsgruppen skal legge frem en samlet anbefaling for UFD. Arbeidet starter opp 15.3.05. Arbeidsgruppen skal presentere sin anbefaling innen 14.05.05

Følgende inviteres til å delta i arbeidet:

- 2 representanter fra UFD – v/Adm(leder) og OA
- 1 representant fra Utdanningsdirektoratet
- 1 representant for Kommunenes Sentralforbund
- 1 representant for UNINETT
- 1 representant for USIT (i egenskap av prosjektleder for FEIDE2GO)
- MOD inviteres med 1 observatør i gruppen

Utdannings- og forskningsdepartementet stiller med sekretariatsressurs.

5. Økonomi

Utdannings- og forskningsdepartementet vil finansiere sekretariat og evt konsulentutgifter. Deltakende etater og virksomheter finansierer selv sin deltakelse i arbeidet.

6 Avslutning

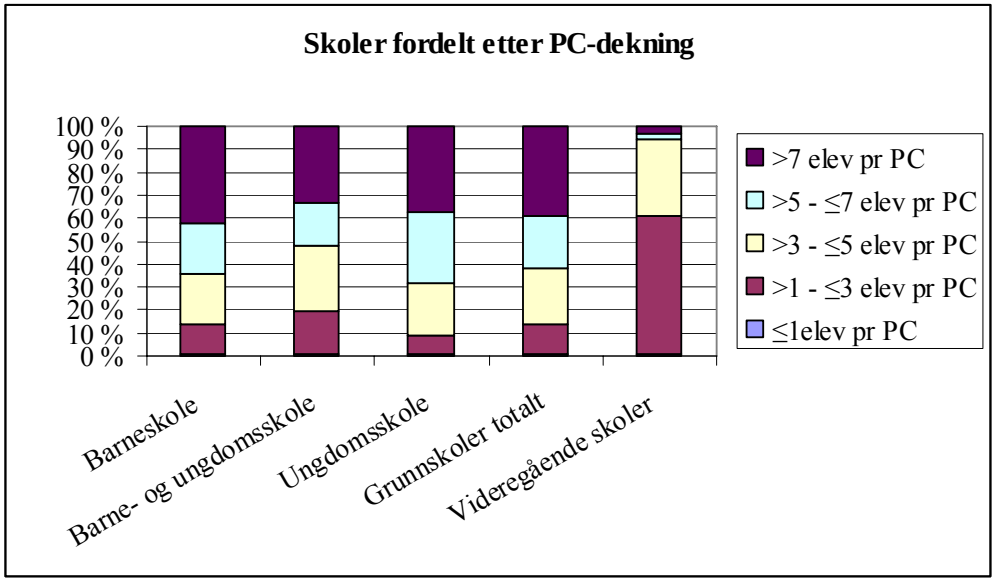
Gruppens arbeid anses avsluttet når anbefalingen er overlevert tilUFD

5.2 Status for IKT i grunnopplæringen

Det mest typiske for IKT i grunnopplæringen er de store forskjellene både når det gjelder tilgang til utstyr (datamaskiner, programvare og infrastruktur) og anvendelsen av dette. De store forskjellene finner vi ikke først og fremst mellom ulike deler av landet, eller mellom fylker, men mellom kommuner og skoler.

5.2.1 Maskintetthet og infrastruktur

På utstyrssiden er forskjellene størst på grunnskolenivå der ca 38 % av skolene har en maskintetthet på 5 elever pr. PC eller bedre. Til sammenligning er situasjonen i videregående opplæring at over 90 % av skolene har tilsvarende dekning. ca. 60 % av de videregående skolene har en dekning på 3 elever pr. PC eller bedre, mens tilsvarende for grunnskolen er 14 % (jf fig 5.1)



Figur 5-1

Et annet viktig aspekt er variasjonen i kvaliteten på maskiner og nettverksløsninger. Fra tidligere undersøkelser vet v at det i grunnskolen er mange eldre PCer og som ofte vil ha dårlig kapasitet.

Vi finner en tilsvarende situasjon mht infrastruktur. Videregående opplæring har en større del av sine datamaskiner koblet til Internet enn grunnskolen, og de videregående skolene har gjennomgående bedre båndbredde.

I tillegg til de utfordringer som er knyttet til investeringer i utstyr og infrastruktur byr driftsituasjonen spesielt på grunnskolenivå på store utfordringer både når det gjelder valg av løsninger for nær framtid og kvalitet og stabilitet på de tjenester som er i drift.

5.2.2 Lærernes kompetanse og interesse

Rapporter og undersøkelser som ITU-monitor og Telenors undersøkelse ved enkelte skoler i Oslo, viser at det også når vi ser på anvendelser i læringsarbeidet, er store forskjeller. Dette

henger selvsagt delvis sammen med det tekniske spriket vi har vist til tidligere, men er i minst like stor grad koblet til den enkelte lærers interesse for og evne og vilje til å ta teknologi i bruk i læringsarbeidet. Til tross for den relativt brede satsingen på LærerIKT, er det fremdeles et stort behov for kompetansetiltak overfor skolens pedagogiske personale. Her mener vi behovet er like stort i hele grunnopplæringen.

5.2.3 Nye læreplaner

I de nye læreplanene er bruk av digitale verktøy en av de grunnleggende ferdigheter som skal være gjennomgående i alle trinn i opplæringen. Dette tilsier at digitale medier vil få en mye mer sentral plass i læringsarbeidet i nær framtid enn det som er vanlig i dag. Det krever tilgang til medierike, digitale læringsressurser og verktøy for å bruke disse i ulike sammenhenger, og digitale vurderingsformer vil måtte få en naturlig plass i læringsforløpet.

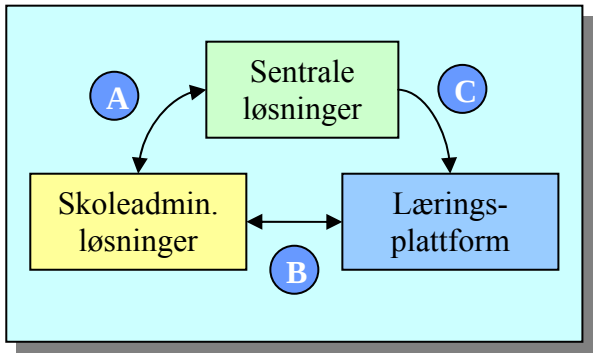
"Et sosiokulturelt perspektiv bygger på et konstruktivistisk syn på læring. Man legger vekt på at kunnskapen blir konstruert gjennom samhandling, ikke bare gjennom individuelle prosesser." (Olga Dyste 1999; Ulike perspektiv på kunnskap og læring)

I et slikt perspektiv vil det både være behov for et rikt tilfang av læringsressurser for egen bruk og samtidig muligheter for samhandling med andre, elever, lærere og ulike fagmiljøer. Slikt samarbeid kan selvsagt knyttes til et lokalt læringsmiljø, men digital teknologi gir også rike muligheter til samhandling på tvers mellom elever, klasser og skoler regionalt, nasjonalt og internasjonalt. For at slikt samarbeid skal være så åpent og transparent som mulig, er det viktig at skolene ikke blir isolert i proprietære læringsmiljøer. Ved pålogging til et eventuelt lokalt, digitalt læringsmiljø må elevene også får tilgang til samhandlingsarenaer ut over egen skole samt et vidt spekter av læringsressurser.

5.2.4 Digitalt eksamenssystem (teknisk infrastruktur)

Fase 1 av prosjektet Den digitale skole prøver ut nye digitale undervisnings - og eksamensordninger. Forsøket med digital eksamensavvikling involverer tre digitale overføringer av informasjon:

A) Informasjon om eksamensavviklingen og eksamensresultater (sensur)
Overføringen av informasjon starter i Utdanningsdirektoratet og inneholder generell informasjon om en bestemt eksamen og hvordan denne skal avvikles og sensureres. Etter at eksamen er avviklet, returneres sensurresultater.



B) Informasjon om eksamenspartier
Den enkelte skole bruker sentral eksamens-informasjon til å opprette eksamenspartier i sine skoleadministrative løsninger. Informasjon om eksamenspartier overføres skolens læringsplattform hvor det opprettes digitale eksamensrom for hvert enkelt eksamensparti. Etter at eksamen er avviklet og sensurert, returneres sensurresultatet til skoleadministrativ løsning for etterbehandling.

C) Digitale eksamensoppgaver

Digitale eksamensoppgaver overføres til det digitale eksamensrommet på hver skole. På eksamensdagen åpner eksaminandene det digitale eksamensrommet med engangs PIN-kode og leverer inn besvarelsene digitalt. Sensor logger seg på læringsplattformen, går til "sin" sensuroversikt og sensurerer eksamensbesvarelsene der.

Informasjonssikkerheten i forsøket er delvis basert på eksisterende sikringsmekanismer i skolenes løsninger og delvis basert på innføring av nye sikringsmekanismer.

Informasjonssikkerheten er også definert som et felles anliggende mellom involverte parter i forsøket. Datatilsynet er blitt presentert forsøket med digital eksamen, og hadde ingen innvendinger til hvordan informasjonssikkerheten ivaretas i forsøket.

Forsøket med digital eksamensavvikling er en pilot på et fremtidig digitalt eksamenssystem. Det gjenstår fremdeles viktige policymessige avklaringer før et nasjonalt digitalt eksamenssystem kan beskrives i detalj. En slik avklaring vil være å beskrive hvordan ivareta informasjonssikkerheten i et nasjonalt digitalt eksamenssystem.

5.2.5 Nye undervisnings- og vurderingsformer basert på de muligheter IKT gir

I tillegg til digital eksamensavvikling, prøver fase1 av Den digitale skole også ut nye undervisningsformer som baserer seg på bruk av digitale medier, for eksempel prosessorientert læring ved bruk av digitale mapper.

Forsøket viser at det er stort behov for å samordne utvekslingen av digitale mapper mellom skolens egen infrastruktur og elektroniske læringsplattformer. Behovet for samordning inkluderer også tiltak for å ivareta et ønsket sikkerhetsnivå.

Samarbeid med bruk av digitale mapper på tvers av skoler, vil sannsynligvis være en naturlig utvidelse av digital undervisning. For eksempel kan en elev velge å ta med seg sin personlige digitale mappe til en annen skole og bruke innholdet av mappen i undervisningen der. Et annet eksempel er at elever på forskjellige skoler utveksler digitale mapper i forbindelse med samarbeidsprosjekter.

Det er behov for å se samlet på sikkerheten ved en undervisning og en eksamen som i stor grad utnytter de digitale mulighetene. En må finne fram til sikringsmekanismer som ikke er begrenset til løsninger hos den enkelte skole, men som fungerer på tvers av skoler og dataløsninger.

5.2.6 Nasjonale prøver

Alle elever i 4., 7. og 10. trinn i grunnskole og grunnkurs i videregående opplæring, skal ta nasjonale prøver i lesing, skriving, matematikk og engelsk.

På nettstedet www.nasjonaleprover.no kan resultatene av nasjonale prøver gjennomført på skolene legges inn. I tillegg kan elever gjennomføre elektroniske nasjonale prøver i engelsk. Nettstedet har i underkant av 270 000 registrerte bruker, hvorav 250 000 er elever og ca 20 000 er administrativt personell. Fødselsnummer er brukt som intern identifikator for en person, men er ikke brukt som personens brukernavn for å logge seg på nettstedet.

Utdanningsdirektoratet vil være svært forsiktig med å innføre ny funksjonalitet på nettstedet for å unngå at skoleeiere, skoler og elever blir usikre på gjennomføringen av de nasjonale prøvene.

5.3 Ordliste

Ord	**Forklaring**
ABC enterprise	Et XML-skjema laget spesielt i forbindelse med utviklingen av FEIDE. Se også XML-skjema.
autentisering	Å sjekke at noen faktisk er den man utgir seg for å være. En kjent metode er brukernavn med tilhørende passord, mens nye metoder kan være digitale sertifikater eller fingeravtrykklesere.
autentiseringstjeneste	En tjeneste som utfører autentisering. F.eks. det en bruker møter når han logger seg på med brukernavn og passord.
autorisasjon	Å gi en bruker autorisasjon vil si å gi en bruker adgang til informasjon eller tjenester.
BAS	Forkortelse for brukeradministrativt system. Se dette.
basisinformasjon	Grunnleggende informasjon om f.eks. personer. Eksempelvis navn og telefonnummer.
Bruker	1) En persons identitet i et IKT-system. Til brukeren hører et brukernavn og passord, og en bruker kan få tildelt bestemte rettigheter til tjenester og filer. 2) En person som bruker et IKT-system.
brukeradministrasjon	Håndtering av brukerne i et datasystem, blant annet oppretting og sletting av brukere.
brukeradministrativt system	Forkortes BAS. Inneholder informasjon om brukerne ved en organisasjon, basert på opplysninger fra et skoleadministrativt system (SAS). Et BAS oppretter brukere, lager brukernavn og passord og lagrer andre påkrevde opplysninger. I tillegg oppgir det etter avtale nødvendige opplysninger til tjenester som har behov for informasjon om brukerne.
brukernavn	Navn som identifiserer en bruker, ofte knyttet til navnet på personen som eier brukeren.
datakvalitet	Tilstand for data/opplysninger. God datakvalitet betyr at opplysningene er korrekte, oppdaterte og samstemte. Dårlig datakvalitet kan bety at opplysninger er utdaterte, ukorrekte eller ufullstendige.
eID	1) Forkortelse for elektronisk identitet. Se dette. 2) Den elektroniske identiteten som knyttes til den offentlige Sikkerhetsportalen (MinSide - http://www.norge.no/minside/framside.asp).
elektronisk identitet	Noe som kan identifisere en person elektronisk (en elektronisk form for legitimasjon). Brukes for å bevise at en person er den han gir seg ut for å være på Internett. Kan f.eks. være brukernavn og passord, PIN-kode, sertifikat.

elektronisk signatur	Fellesbegrep om metoder/teknikker som sikrer utveksling av informasjon mellom to parter. En elektronisk signatur knytter en person sammen med en melding eller et dokument. Ut fra signaturen kan mottaker verifisere hvem som faktisk har sendt dokumentet. Den elektroniske signaturen som blir brukt i PKI kalles digital signatur.
e-signatur	Se elektronisk signatur.
eStandard-prosjektet	En del av Utdannings- og forskningsdepartementets Program for digital kompetanse. Prosjektet fokuserer på standardisering av systemer for e-læring.
FEIDE	Står for Felles Elektronisk IDEntitet. En enhetlig identitetsforvaltning for utdanningssektoren. Se også identitetsforvaltning.
identitetsforvaltning	Håndtering av hvem og hva en person er. I vid forstand: Prosessen med å identifisere personer og kontrollere deres tilgang til tjenester og informasjon.
IMS Enterprise	IMS er en internasjonal organisasjon som har utviklet en rekke spesifikasjoner innen e-læring. IMS Enterprise er et standardisert format for utveksling av informasjon mellom administrative tjenester. For mer informasjon: http://www.imsglobal.org/enterprise/
Indigo-prosjektet	UNINETT ABCs prosjekt for innføring av FEIDE i grunnopplæringa for de videregående skolene i to fylkeskommuner, Østfold og Hedmark.
informasjonspakke	I denne sammenheng: Opplysninger om en person som en tjeneste har bruk for (f.eks. navn og klassetrinn).
komponentbasert	Bestående av et visst antall atskilte (selvstendige) deler som hver for seg kan byttes ut uten at helheten påvirkes.
kryptering	En prosess der informasjon forvrenges for å hindre at uvedkommende skal kunne forstå den. For å gjøre informasjon forståelig igjen må prosessen reverseres (informasjon dekrypteres).
kryptografi	Prinsipper og teknikker for å forvrenge informasjon, brukes for å sikre kommunikasjonssystemer. Se også kryptering.
kryptonøkkel	En variabel verdi som brukes sammen med en krypteringsalgoritme for å kryptere eller dekryptere en melding. Kryptonøkkelens lengde er avgjørende for hvor vanskelig det er å knekke koden.
LDAP-katalog	En database som er strukturert på en bestemt måte (kalles elektronisk katalog). Man kommuniserer med databasen ved hjelp av en standard kalt LDAP (Lightweight Directory Access Protocol). Katalogen inneholder som regel informasjon om personer og institusjoner.

metadatamerking	Metadata beskriver innhold, f.eks. innholdet i en database. Ved å standardisere metadatamerking kan innhold beskrives på en sånn måte at det kan forstås på tvers av tjenester.
Moria	FEIDEs autentiseringstjeneste. Se også autentiseringstjeneste.
Nøkkel	Se kryptonøkkel.
Open Source	Et program kan kalle seg "Open Source" om det er lisensiert under en av lisensene godkjent av organisasjonen Open Source Initiative (OSI). For at et program skal være ”Open Source” må det tilfredsstille noen kriterier, blant annet skal programmet kunne distribueres fritt, kildekoden må følge med og det skal være lov å gjøre om på programmet som man vil. Les mer om definisjonen av Open Source her: http://www.opensource.org/docs/definition.php.
passord	Et ord eller uttrykk som må oppgis før en bruker får adgang til en tjeneste. Benyttes for å kontrollere adgang til tjenesten.
personalisert tjeneste	En tjeneste spesielt tilpasset den brukeren som til enhver tid er innlogget.
PKI	PKI står for Public Key Infrastructure, og er ikke en teknologi i seg selv i form av programvare eller maskinvare. PKI er en beskrivelse av en infrastruktur der private og offentlige nøkler benyttes for å muliggjøre sikker elektronisk kommunikasjon mellom flere aktører. Hvordan selve infrastrukturen i en PKI er sammensatt, dvs. hvilke aktører som er med i infrastrukturen, er ikke entydig bestemt, men kan variere fra sted til sted (f.eks. fra land til land), og over tid. PKI gjør det mulig å benytte digitale sertifikater for sikker autentisering, signering og kryptering.
SAS	Se skoleadministrativt system.
Shibboleth	Amerikansk prosjekt som utvikler en ”single sign-on”-løsning for akademiske institusjoner. For mer informasjon se http://shibboleth.internet2.edu/.
single sign-on	En prosess for autentisering som gjør at brukeren kun behøver å skrive inn brukernavn og passord én gang for å få tilgang til mange tjenester.
skoleadministrativt system	En samling av opplysninger om personer (lærere, elever, administrativt personale, foreldre) tilknyttet organisasjonen (skolen). Kan være på papir eller på elektronisk form.
systemkomponent	En del som et system består av.

Tiltrodd tredjepart	Det kan være behov for at mottaker skal kunne kontrollere at informasjon som mottas faktisk kommer fra den personen man kommuniserer med. Dette er spesielt viktig dersom informasjon utveksles mellom to parter som ikke kjenner hverandre. En tiltrodd tredjepart kan, uavhengig av sender og mottaker, bekrefte eller avkrefte sammenhengen mellom det som sendes og avsenderen.
Tjener	En datamaskin som har som hovedoppgave å tilby tjenester over nettet til brukere som sitter ved andre datamaskiner.
tjeneste	Alt som vi bruker våre IKT-systemer til, også det vi kan få tilgang til via Internett, er tjenester. Eksempler er e-post, tekstbehandler, viruskontroll og www.nasjonaleprover.no.
tjenestekvalitet	En tjeneste kan leveres med en gitt tjenestekvalitet. Det betyr at det stilles visse krav til tjenesten.
uavviselighet	Et krav for økt sikkerhet. Vil si at en person som elektronisk har signert et dokument eller kommunisert med noen ikke kan nekte for å ha signert dokumentet eller sendt en melding.
XML-skjema	XML er et standardisert programmeringsspråk som er godt egnet for å få til integrasjon mellom ulike tjenester. XML egner seg for utveksling av data. Detaljene for hvordan en datautveksling skal foregå er bestemt i et XML-skjema. For mer informasjon se: http://www.w3.org/XML/
åpen standard	En standard som er tilgjengelig for liten eller ingen kostnad, slik at alle kan få tilgang til den. Dermed sikrer man at data og informasjon kan utveksles uavhengig av programvareleverandør. (Se rapport fra Moderniseringsdepartementet om åpne standarder: http://odin.dep.no/filarkiv/252170/Bruk_av_apne_standarder_og_apen_kilde kode_off_sektor.pdf) EUs definisjon setter fire minimumskrav for at en standard skal betraktes som en åpen standard: • Standarden er anerkjent og vil bli vedlikeholdt av en ikke-kommersiell organisasjon, og det løpende utviklingsarbeidet foregår på basis av beslutningsprosess som er åpen for alle interesserte parter (kan være konsensusdrevet, basert på flertallsavgjørelser osv). • Standarden er publisert og dokumentasjonen er tilgjengelig, enten gratis eller til en ubetydelig avgift. Det må være tillatt for alle å kopiere, distribuere og bruke standarden gratis eller for en ubetydelig avgift. • Den intellektuelle rettighet knyttet til standarden (eks. patenter) er gjort ugjenkallelig tilgjengelig uten royalty. • Det er ingen forbehold om gjenbruk av standarden .