NOSIP 3

NOSIP 3

Datakommunikasjonsstandard for offentlig forvaltning

Statskonsult

Utgitt av Statskonsult 2000

Omslagsdesign: Anisdahl, Sand & Partnere AS
Sats: Prepress As
Trykk: Gjøvik Trykkeri As

ISBN 82-7483-086-5

Forord

Effektiv og samordnet IT-kommunikasjon i statlig forvaltning er en forutsetning for at departementene og de underliggende etatene kan løse sine oppgaver bedre og mer effektivt og derigjennom kunne tilby borgerne bedre tjenester.

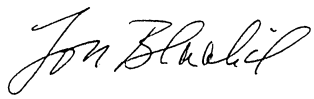
Som en forvaltningsstandard for IT-kommunikasjon er NOSIP et fundament for å lage en helhetlig og velfungerende IT-infrastruktur innen offentlig forvaltning. I denne utgaven av NOSIP er det fokusert på å utnytte de eksisterende investeringene i offentlig sektor samtidig som man tar i bruk Internett med tilhørende teknologier.

Når vi har valgt IP (InternetProtocol) som fundament for NOSIP, har vi valgt en standard som er stabil, og som er den dominerende protokollen for datakommunikasjon.

Dette gjør at forvaltningen vil bruke de samme standardene som benyttes i samfunnet for øvrig, og forvaltningen får dermed et bedre grunnlag for å tilby elektroniske tjenester til brukerne.

Arbeidet med denne utgaven av NOSIP startet høsten 1998 og har pågått kontinuerlig fram til nå. I arbeidet med å fornye NOSIP har mange departementer, etater og enkeltpersoner deltatt, både gjennom deltakelse i en referansegruppe, deltakelse på faglige diskusjonsmøter, og gjennom høringer. Seniorrådgiver Endre Grøtnes har vært prosjektleder for arbeidet.

Statskonsult, januar 2000



Jon Blaalid

Innhold

1

NOSIP – bakgrunn, formål og virkeområde

1.1. Formålet med NOSIP

NOSIP (Norsk OSI profil) er en forvaltningsstandard for datakommunikasjon. Formålet med NOSIP er å presentere et sett med krav og anbefalinger som skal gjøre det enklere å kommunisere på tvers av ulike sektorer og på tvers av forvaltningsnivåer. NOSIP skal også gjøre det enklere å kommunisere elektronisk med forvaltningens brukere samt å formidle og presentere informasjon til disse.

1.2. Bakgrunn og formell forankring

Ved kgl. res. av 6.12.1991 fikk Arbeids- og administrasjonsdepartementet hjemmel til å kunne pålegge statsforvaltningen å bruke standardprodukter i løsninger for datautveksling mellom sine edb-systemer. Departementet fulgte opp vedtaket i statsråd med sitt pålegg den 18.12.1991, og pålegget trådte i kraft 1.2.1992. Dette pålegget omtales som NOSIP-pålegget.

Statskonsult er gjennom brev fra Arbeids- og administrasjonsdepartementet av 18.12.91 tillagt ansvaret for å opprette et standardiseringssekretariat og vedlikeholde NOSIP. Sekretariatet er organisatorisk lagt til Statskonsults IT-avdeling.

NOSIP-pålegget sier at de obligatoriske kravene i NOSIP skal følges ved kjøp av datakommunikasjonsprodukter. Det foreligger vide muligheter for å velge andre løsninger dersom vurderinger innenfor den enkelte sektor skulle tilsi det. Det er opp til det enkelte departement/etat å fravike pålegget med grunnlag i visse unntaksbestemmelser. Det kan gjøres unntak fra kravene i NOSIP når:

1) Kost-/nyttevurderinger tilsier andre løsninger, 2) spesielle sikkerhetsbehov ikke tilfredsstilles, 3) kravene er til vesentlig

hinder for forvaltningsbedrifters konkurranseevne og 4) forskning og utvikling krever andre løsninger.

1.3. Virkeområde

NOSIP gjelder primært for statlig forvaltning. Kravet er at ved anskaffelser av datakommunikasjonsutstyr skal kravspesifikasjonen bygge på og referere til NOSIP.

Gjennom EØS-avtalen er hele offentlig sektor omfattet av EUs Rådsbeslutning 87/95, den såkalte "Standardiseringsbeslutningen". Ved kjøp av kommunikasjonsløsninger som overstiger 100 000 ECU, er det krav om henvisning til internasjonale standarder. Ved henvisning til NOSIP oppfylles dette kravet. Også loven om varekjøp, basert på EUs innkjøpsdirektiv, stiller krav om spesifikasjoner ved hjelp av henvisninger til standarder. Implisitt vil dette si at NOSIP gjelder for hele offentlig forvaltning.

1.4. Hvorfor en ny utgave av NOSIP?

Bruken av NOSIP er begrenset, men store deler av statsforvaltningen har valgt OSI-baserte produkter for e-post (X.400). Grunnlaget for NOSIP har de siste årene blitt svekket i og med at markedsutviklingen har skapt nye og relativt billige produkter og tjenester som er basert på Internett-teknologi. Det produseres også svært lite nye tjenester og produkter basert på ISO-kommunikasjonsstandarder. Forskjellen i pris og produkttilfang mellom OSI-baserte og Internett-baserte produkter gjør at man etter en kost-/nyttevurdering i hovedsak vil velge Internett-baserte produkter og tjenester. Fravikelse av kravene i NOSIP-pålegget blir dermed snarere regelen enn unntaket.

Trenden i samfunnet er at nesten all datakommunikasjon og e-post baserer seg på Internett-teknologi og -standarder. Skal forvaltningen kunne kommunisere med virksomheter og publikum, må de benytte de samme standardene som disse benytter, eller benytte gatewayløsninger. Det mest rasjonelle er å benytte de samme standardene. Dette er de viktigste argumentene for å endre hovedkravene i NOSIP fra OSI-baserte standarder til Internett-baserte standarder.

Den forgående utgaven av NOSIP (versjon 2) var ikke oppdatert i forhold til Internett-teknologi og tilhørende standarder. For at NOSIP skulle ha praktisk nytte, måtte den oppdateres.

1.5. Mål for utarbeidelsen av NOSIP versjon 3

Ved utarbeidelsen av forslag til NOSIP v3 har følgende mål ligget til grunn:

- Kravene/anbefalingene skal være oppdatert med hensyn på Internett-teknologi og Internett-standarder
- Kravdelen skal være mindre omfattende
- Kravene skal være markedsorientert, dvs. det skal finnes gode produkter som tilfredsstiller kravene
- Veiledningsmaterialet skal gjøre det enklere å forholde seg til kravene, og det skal tas hensyn til dagens investeringer i IT-løsninger

1.6. Utviklingen av standarder på IT-området

Utviklingen av standarder på IT-området er mangeartet. Fra utviklingen av dejure standarder i formelle internasjonale standardiseringsorganisasjoner som CEN (European committee for standardization) og ISO (International organization for standardization) til defacto standarder utviklet av et enkelt firma. Mellom disse ytterpunktene finnes det standardiseringsorganisasjoner og konsortier med ulik grad av formalisme, anerkjennelse av myndighetene, åpenhet og gjennomslagskraft.

Tradisjonelt har standardene i NOSIP vært basert på standarder utarbeidet av standardiseringsorganisasjoner som er anerkjent av norske myndigheter, som CEN og ISO. Disse organisasjonene bruker vanligvis lang tid på å komme fram til standarder, og standardene er ofte store og omfattende. Representanter fra nasjonale standardiseringsorganisasjoner sitter ofte som representanter i styrende organer i de internasjonale organisasjonene. Man representerer sitt land når man deltar på møter i de formelle standardiseringsorganisasjonene, og man har formelle avstemninger om de enkelte standardene.

Gjennomslagskraften i markedet for standarder utviklet av de formelle standardiseringsorganisasjonene er varierende. Et eksempel på en standard som markedet har mottatt med entusiasme, er GSM-standarden for mobiltelefoner. Et eksempel på det motsatte er sørgelig nok flere av OSI-standardene for datakommunikasjon.

Standardene fra ISO og CEN er på datakommunikasjonsområdet i utgangspunktet papirstandarder. Det er ikke krav om at det må finnes produkter som implementerer standardene som er vedtatt. Juridisk er standarder utarbeidet av CEN bindende for Norge. Dette gjør at standarder fra formelle standardiseringsorganisasjoner er viktige innen det offentlige.

Som et motstykke til standardiseringsprosessen i ISO og CEN kommer standardiseringsprosessene i organisasjoner som IETF (The Internet Engineering Task Force) og W3C (The World Wide Web Consortium). Her er det produsentene, brukerne og fagpersonene som er drivkraften i utviklingen av standarder. Medlemskap i organisasjonene er åpent for alle.

Innen IETF utvikles standarder på følgende måte. Standarder utvikles i små dedikerte arbeidsgrupper og baseres på virkende kode og omtrentlig enighet ("Running code and rough consensus"). Dette gjør at det tar kort tid å utvikle nye standarder, og at standarder og implementasjon av standarder foregår omtrent samtidig.

Foreslåtte standarder (proposed standard) må resultere i produkter fra flere leverandører og ha en god markedsutbredelse før de kan løftes opp som en "Draft standard". Er ikke disse kravene til stede, vil den foreslåtte standarden enten bli gjort om eller forkastet.

Ingen nasjonale myndigheter er juridisk bundet av standarder som disse organisasjonene utarbeider.

Markedet har på IT-området i stor grad valgt produkter og tjenester basert på standarder utarbeidet av standardiseringsorganisasjoner som ikke er anerkjent av de nasjonale myndighetene. Dette skaper et misforhold mellom de kravene som nasjonale myndigheter stiller til IT-produkter og tjenester, og de kravene markedet for øvrig stiller. Ved nyanskaffelser av datakommunikasjonsløsninger benytter i dag EU i all hovedsak Internett-baserte løsninger. Et eksempel på dette er IDA-prosjektet (http://158.169.51.200/ida/idahome.htm). Offisiell informasjon finnes i Official Journal som Common Position {EC} NO 8/1999 og Common Position {EC} NO 9/1999.

I denne versjonen av NOSIP er det stilt krav som bringer sammen de beste standardene fra de ulike standardiseringsorganisasjonene og sørge for at man får et samvirkende hele internt i offentlig forvaltning og eksternt mot andre aktører. Ved valg av standarder har det vært viktig at det foreligger produkter som følger standarden.

1.6.1. Referanser til standarder

NOSIP v3 refererer til standarder fra ulike kilder. I tillegg til dejure-standardene fra ISO, CEN og ITU-T som NOSIP v2 primært forholdt seg til, refererer NOSIP v3 til standarder fra andre organisasjoner, først og fremst IETF og W3C. Som rettesnor er benyttet at det kan refereres til industristandarder når disse innholdsmessig og på grunn av (forventet) utbredelse i markedet anses

som markedsledere. Refererte industristandarder skal tilfredsstille krav til åpenhet, plattformuavhengighet og stabilitet.

1.7. Relaterte dokumenter og prosjekter

Nedenfor beskrives prosjekter og standarder i forvaltningen som er relatert til NOSIP v3.

1.7.1. Forvaltningsnettsamarbeidet

Forvaltningsnettsamarbeidet er ett av flere tiltak i samarbeidet mellom kommunesektoren og staten på IT-området (KOSTIT). Målet er å fremme enkel, sikker og kostnadseffektiv elektronisk informasjonsutveksling innad i offentlig sektor og utad mot andre brukere.

Forvaltningsnettsamarbeidets innkjøpsordning støtter og forenkler innkjøpsprosessene for hver enkelt virksomhet. Ordningen består av en samling rammeavtaler, inngått sentralt, med veiledninger og ferdige forslag til skjemaer for utfylling ved anskaffelse (kjøpsavtaler).

NOSIP v3 vil være en premissgiver og et utgangspunkt for utarbeidelse av kravspesifikasjoner ved neste runde av anbudsinnbydelser i Forvaltningsnettsamarbeidet. De produktene som tilbys over Forvaltningsnettsamarbeidets rammeavtaler, skal være i overensstemmelse med de kravene som vil være gjeldende i NOSIP v3.

NOSIP skal gi råd og veiledning til de ansvarlige for innkjøp av IT-utstyr i statlig sektor. Forvaltningsnettsamarbeidets innkjøpsordning vil være en sentral kilde for innkjøp av IT-utstyr. Det er derfor naturlig at det under utarbeidelsen av NOSIP v3 er lagt vekt på det arbeidet som er gjort i Forvaltningsnettsamarbeidet. Så langt som mulig er det prøvd å utarbeide krav som er i samsvar med Forvaltningsnettsamarbeidets kravspesifikasjoner.

Forvaltningsnettsamarbeidets innkjøpsordning kan ses på som realisering av de kravene som NOSIP fastsetter. NOSIP og Forvaltningsnettsamarbeidet vil derfor være viktige premissleverandører for framtidens IT-infrastruktur i offentlig sektor, blant annet gjennom samarbeid med andre store IT-prosjekter og utviklingstiltak i det offentlige, gjennom å sette krav til kommunikasjonsprotokoller og standarder og ved å skissere en arkitektur for offentlig sektor som er basert på kravene i NOSIP.

1.7.2. Statens Generelle Kravspesifikasjon og Norsk Arkivsystem

Statens Generelle Kravspesifikasjon for elektronisk saksbehandling og ledelse (*SGK*) spesifiserer veiledende funksjonelle krav til sluttbrukerapplikasjoner på saksbehandlingsområdet. Ny versjon av SGK forelå høsten 1997. Norsk Arkivsystem (*NOARK*) versjon 4 er en kravspesifikasjon for elektroniske arkivsystemer i offentlig forvaltning. Kun arkivformater for langtidslagring av dokumenter er direkte relatert til NOSIP. Både SGK og NOARK-4 forutsetter indirekte på flere områder at krav NOSIP stiller blir fulgt, særlig gjelder dette for formater (kapittel 4) og sluttbrukertjenester (kapittel 5).

1.7.3. NORBÅS

Norsk rammeverk for bruk av åpne systemer i forvaltningen (*NORBÅS*) omhandler tekniske krav til applikasjonsomgivelser i forvaltningen. Den anses som foreldet og blir ikke vedlikeholdt.

1.8. Målgruppe for NOSIP

Følgende grupper utgjør målgruppen for NOSIP v3:

- Ledere og ansvarlige for strategi for informasjonsteknologi (IT-strategi) og IT-planlegging i departementer, offentlige etater, institusjoner og bedrifter
- Ansvarlige for innkjøp av edb-utstyr i departementer, offentlige etater, institusjoner og bedrifter
- Ansvarlige for utvikling av administrative løsninger
- Leverandører som ønsker å tilby kommunikasjonsprodukter og tjenester til offentlig forvaltning

1.9. Viktigste endringer siden forrige versjon

Dette er de viktigste endringene siden forrige versjon av NOSIP:

- OSI-protokollen er erstattet av IP med tilhørende protokollfamilie.
  - Det er ingen krav til de lavere lags protokoller som følge av bruken av IP
- SMTP/MIME erstatter X.400
  - X.400 kan fremdeles benyttes av dem som har det
- LDAP skal brukes som grensesnitt mot kataloger
- HTTP, HTML og FTP er nye standarder til bruk ved informasjonsutveksling
- Antall obligatoriske krav og omfanget er blitt redusert

Av OSI-standarder det ble stilt krav til i NOSIP v2, er det i dag først og fremst X.400 og X.500 som er i bruk i noen utstrekning. Krav til X.400- og X.500-løsninger er inkludert også i NOSIP v3, og for X.400 er krav som skal ivareta samtrafikk mellom X.400 og SMTP/MIME (Internett e-post) angitt.

1.10. Kategorier av krav

Kravkategoriene fra NOSIP v2 er beholdt i NOSIP v3. Disse er:

- Obligatorisk krav (O) == skal …/skal kunne …
- Betinget krav (B) == dersom … skal …
- Langsiktig krav (L) == på sikt skal …/skal være forberedt på …
- Interimskrav (I) == inntil L-krav er oppnådd skal …
- Opsjon (-) == kan …

Der B-krav er anvendt, er betingelsene beskrevet i teksten. Kravene utgjør i mange tilfeller et implisitt "kravhierarki". Et obligatorisk krav om støtte for gitte delfunksjoner i en tjeneste er for eksempel betinget av at tjenesten som sådan støttes. I slike tilfeller er krav om den aktuelle funksjonen angitt som obligatorisk, selv om det kan argumenteres for at det er et betinget krav – avhengig av om den overordnede tjenesten støttes. Dette vil imidlertid fremgå av teksten og ikke markeres ved bruk av B-kategorien.

Eksempel: Det stilles ikke obligatoriske krav til bruk av EDIFACT syntaks. Dersom EDIFACT syntaks velges, er det imidlertid et obligatorisk krav at EDIFACT versjon 4 støttes. At dette kravet er betinget av valget av EDIFACT i første omgang (nivået over i et kravhierarki) angis som tekst, og fører ikke til at kravet kategoriseres som betinget. Derimot er støtte for syntaksnivå UNOH (ISO 8859-4) et betinget krav, der betingelsen er behov for støtte for samiske tegn dekket av dette tegnsettet.

Kravene er oppsummert i kravtabeller etter hvert kapittel, i kapittel 5 etter hvert avsnitt. Kravtabellene er imidlertid kun ment å gi en rask oversikt, og er *ikke* å regne som selvstendige. Dette er spesielt viktig i forhold til implisitte betingelser for O-krav, som kun vil fremgå av teksten.

Eksempel: Det stilles ikke obligatoriske krav om benyttelse av OSI-tjenester i NOSIP v3. *Dersom* X.400 eller X.500 velges, er det imidlertid et obligatorisk krav at kommunikasjonsstandardene for OSI lag 4-7 støttes som angitt.

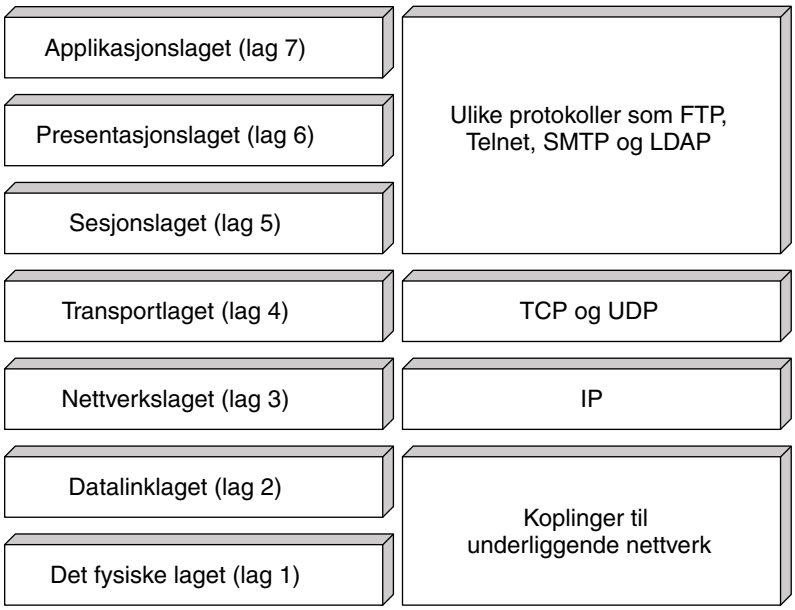
2

Grunnleggende kommunikasjon og interoperabilitet

2.1. TCP/IP

Utgangspunktet for kravene i denne utgaven av NOSIP er at all kommunikasjon skal baseres på og bygges rundt IP (Internet Protocol) [RFC 791]. Denne protokollen kan ses på som limet som binder alle de andre protokollene sammen med de underliggende nettverkene.

OSI-referansemodellen er gjerne et utgangspunkt når man skal snakke om oppbyggingen av nettverk. Den er lagdelt og består av 7 ulike lag, se figur 1. Hvert lag bestiller tjenester av laget over og under. Man snakker om et protokollhierarki, hvor man finner en protokoll på et gitt nivå i OSI-modellen.



Figur 1. OSI-modellen og forholdet til IP-protokollfamilien

Prøver man å tilpasse protokollstrukturen blant Internett-standardene til OSI-modellen, vil den se ut omtrent som vist i figur 1.

Protokollene på hvert lag i OSI-modellen utfører en mengde tjenester. Det er mulig bare å velge en liten del av disse og danne det man kaller en profil. Det kan dermed finnes mange OSI-profiler som omfatter ulike tjenester. Dette kan skape inkompatibilitet. IP-protokollen, som tilsvarer lag 3 i OSI-modellen, håndterer derimot kun et fåtall tjenester, som alle skal implementeres. Basisfunksjonene som IP-protokollen skal håndtere, er adressering og oppdeling av kommunikasjon i pakker. Ved bruk av IP har det vært forholdsvis få problemer med inkompatibilitet mellom ulike implementasjoner.

En grunn til at IP-protokollen har vært så vellykket, er at den er så enkel, og kun konsentrerer seg om å sende data mellom to maskiner i et nettverk. I RFC 791 kapittel 1.2 kan man lese følgende om IP-protokollen: *"The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system of networks. There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols."*

Sett i lys av IP-protokollen og det begrensede settet med tjenester den tilbyr, er det nødvendig å benytte denne sammen med en transportprotokoll som kan tilby flere tjenester. I de fleste tilfeller benytter man her TCP (Transmission Control Protocol) [RFC 793]. Man snakker dermed om kommunikasjon basert på TCP/IP. Denne kombinasjonen har vist seg svært robust, og danner i dag grunnlaget for det meste av kommunikasjonen som skjer på åpne nett.

Det faller dermed naturlig å sette som et grunnleggende krav for kommunikasjon mellom *enheter* (se definisjon i avsnitt 2.2) at den skal baseres på TCP/IP.

For å slippe å ha to ulike protokoller for kommunikasjon eksternt og internt anbefaler NOSIP at enhetene også benytter TCP/IP for intern kommunikasjon.

2.2. Definisjon av en enhet

NOSIP stiller krav til kommunikasjon mellom ulike virksomheter i statlig forvaltning. En virksomhet kan være distribuert, og dermed ha behov for å følge de samme kravene til datakommunikasjon internt som eksternt. For å dekke opp alle alternativer har vi valgt å betegne partene som kommuniserer som *enheter*. En enhet kan være et departement, et direktorat, en lokal del av en virksomhet, en enkelt avdeling osv. Det som betegner en enhet er følgende:

- En enhet har en spesifikk sikkerhetspolicy
- Enhetens ledelse har ansvar og myndighet for all bruk av IT i enheten
- En enhet har kun ett punkt som kommunikasjon med omverdenen skjer igjennom

NB: Ved denne definisjonen av en enhet vil f.eks. et hjemmekontor eller en bærbar maskin tatt med på reise falle inn under definisjonen.

2.3. Design og oppbygging av kommunikasjonsinfrastruktur

Enheter med behov for ekstern kommunikasjon har selv ansvar for å knytte seg opp mot et eksternt nettverk. Dette kan skje enten via en nettverksoperatør eller via en annen enhet. Enhetene har videre ansvar for å bestemme hvilke krav til funksjonalitet og sikkerhet som skal gjelde for tilknytningen så lenge valget blir gjort innenfor de rammene som gis i dette dokumentet, og innenfor de rammene som øvrig lov og regelverk setter.

Alle enheter som skal kommunisere internt, gjør dette via et lokalt nettverk (LAN). Enheter vil ha ulike LAN, avhengig av størrelse, sikkerhetspolicy og nasjonal utbredelse. Merk at noen enheter kan være spredt utover landet på en slik måte at ulike deler av enheten kommuniserer med hverandre via én eller flere nettverksoperatører. Man kan også forestille seg enheter som er så små at deres LAN kun består av et fåtall maskiner.

Det anbefales at kommunikasjonen mellom enheter baseres på den til enhver tid eksisterende Internett-infrastrukturen i Norge. Det vil framover være behov for forbedringer i denne infrastrukturen for å kunne tilfredsstille brukernes behov for ulike typer av tjenestekvalitet og sikkerhet. Det er fullt mulig å benytte andre IP-nettverk for kommunikasjon mellom enheter, men for å forenkle beskrivelsen vil kommunikasjon mellom enheter i NOSIP bli omtalt som kommunikasjon over Internett.

Kommunikasjon mellom enheter er oppbygd ved at ulike lokale nett er koplet sammen ved hjelp av rutere. I tillegg finnes det ofte en brannmur som skiller det interne nettet fra det eksterne. De delene av de sammenkoplede nettene som eksponeres for omverdenen, utgjør et hele i form av at de deler adresserom og navnerom, og at det er forbindelse mellom alle maskinene i nettet.

Deling av adresserom gjøres ved at de ulike nettene får tildelt adresser som er unike innen Internett. Hver nettverksoperatør har adresser tilgjengelige til sine kunder.

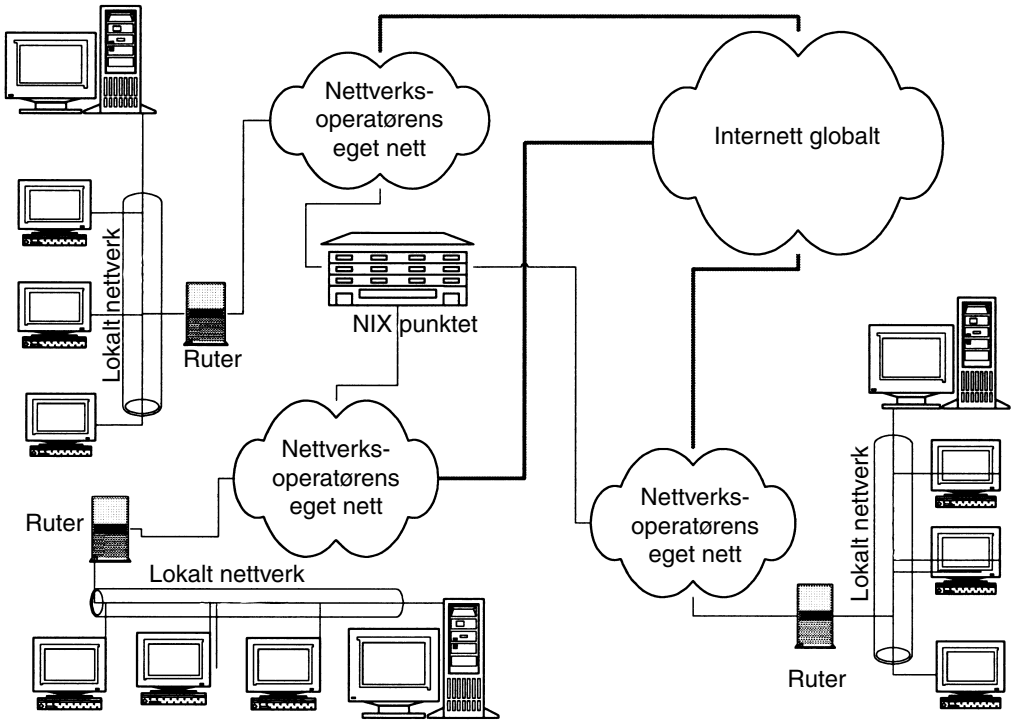
Deling av navnerom skjer ved bruk av Domain Name System (DNS) [RFC1034-1035]. DNS er en hierarkisk oppbygd navnestruktur, og i Internett har man et hierarki av navnetjenere som bl.a. kan besvare navneoppslag.

Forbindelse mellom nettene ivaretas av rutere. Nettets topologi framkommer som resultat av sammenkopling av nett. Rutere har egne metoder for utveksling av informasjon om nettverk (rutingprotokoller) som sørger for forbindelse.

NOSIP stiller krav til enhetene i forbindelse med nettverksstruktur, forbindelse, adressestruktur og navnerom.

Statskonsult har utarbeidet en veileder om tilknytning til Internett [TILK]. Kapittel 1 i dette dokumentet gir utfyllende informasjon om Internett.

Figur 2 viser et forenklet bilde av hvordan enheter kan kommunisere via Internett-infrastrukturen i Norge.



Figur 2. Konseptuell skisse av Internett-infrastrukturen i Norge

2.4. Adresse- og navnestruktur

Skal to maskiner kunne kommunisere med hverandre, må de vite navnet eller adressen til den de skal kommunisere med. I Internett må alle adresser være entydige. Alle adresser en enhet skal presentere til omverdenen, må være globalt entydige.

Siden det i den senere tid har vært et stort press på de globale adressene, har mange virksomheter valgt en løsning som går på at man har kun et fåtall globale adresser og et større antall interne adresser. Ved hjelp av adresseendringsteknologi (NAT-teknologi) oversetter man mellom de interne adressene og de eksterne adressene. Man oppnår dermed blant annet å minske presset på det globale navnerommet samt å skjule de interne IP-adressene for omverdenen. En ulempe med denne adresseoversettingen er at en del tjenester som krever ende-til-ende-forbindelse mellom maskiner, ikke virker ved bruk av denne typen teknologi. Bruk av NAT-teknologi blir dermed en avveining mellom ulike hensyn.

Merk at nettverksoperatører tildeler adresser til sine kunder. Dette medfører at i tilfeller der enheter ønsker å bytte leverandør, vil dette medføre bytte av alle globale IP-adresser hos enheten.

Enheter som har krav til store globale landsdekkende nett, kan vurdere å bygge opp sine egne interne IP-nettverk med adresser tildelt organisasjonen direkte, og således operere som sin egen nettverksoperatør. Dette er ikke en vanlig løsning.

For å kunne foreta endringer i nettet på en hensiktsmessig måte skal enhetene benytte en nettkonfigurasjonsprotokoll, som Dynamic Host Configuration Protocol (DHCP) [RFC 2131] i sine nett for alle maskiner som ikke er nødt til å ha manuelt konfigurerte adresser. Av sikkerhetshensyn kan enkelte maskiner unntas fra dette kravet.

Alle maskiner i nettet, inkludert alle rutere, skal ha et navn for hver IP-adresse på sine maskiner registrert i en DNS-tjener. Innenfor hver enhet skal det være minst to DNS-tjenere som kan besvare navneoppslag. Enheten er fri til selv å velge hvem som skal oppdatere sine navnetjenere [RFC 2181]. For adresser som ikke skal være synlig utenfor enheten, skal navn og adresser være registrert i en DNS-sone som heller ikke er synlig utenfor enheten.

Det forutsettes at enhetene velger domenenavn i henhold til den navnestrukturen som er etablert innenfor forvaltningen, og som gjelder for den enkelte enhet. Informasjon om navnestrukturer og valg av navn kan fås av blant annet Statens forvaltningstjeneste, AAD, Post- og teletilsynet, NORID, Brønnøysundregistrene, Sentralkontoret for folkeregistrering og Kommunenes Sentralforbund.

2.5. Nettverksadministrasjon

Formålet med nettverksadministrasjon er å kontrollere forbindelse, overvåke belastning samt oppgradere programvare i aktuelle nettverksprodukter. Hver enhet har ansvar for at denne oppgaven

blir utført i henhold til enhetens sikkerhetspolicy og øvrige driftsrutiner.

NOSIP stiller ikke krav til bruk av spesiell programvare til dette formål, utover at de ulike nettverksproduktene skal la seg overvåke ved hjelp av Simple Network Management Protocol (SNMP). Det er et obligatorisk krav at man har støtte for overvåkning ved hjelp av SNMP versjon 1 [RFC 1157]. Et langsiktig krav er overvåkning og kontroll ved hjelp av SNMP versjon 3 [RFC 2570–2575].

NOSIP anbefaler at man kun anskaffer nettverksprodukter hvor programvaren lar seg oppgradere via nettet. Av sikkerhetshensyn kan enkelte maskiner unntas fra dette kravet.

2.6. Definisjon av TCP og IP

Siden RFC 791 (IP) og 793 (TCP) ble skrevet, har en vunnet mye erfaring i bruken av disse standardene, og deler av dette er vesentlig for implementasjonen. Således bør TCP/IP-baserte systemer støtte følgende standarder:

For IP:

- [RFC 791] (IP)
- [RFC 792] (ICMP)
- [RFC 950] (subnetting)
- [RFC 919] (Broadcast)
- [RFC 922] (Broadcast with Subnetting)
- [RFC 1112] (IGMP)
- [RFC 1122] "Requirements for Internet Hosts (communication layer)"
- [RFC 1812] "Requirements for IPv4 routers"

For TCP:

- [RFC 793] (TCP)
- [RFC 1122] "Requirements for Internet Hosts (communication layer)"
- [RFC 2581] "TCP Congestion Control"

I tillegg er også UDP vesentlig for IP-baserte nettverk, og er definert i [RFC 768] og [RFC 1122].

DNS er definert i [RFC 1034] og [RFC1035], men er videre presisert og utvidet i [RFC 1123], [RFC 1982], [RFC 1995], [RFC 1996], [RFC 2136], [RFC 2181] og [RFC 2308].

Grunnleggende DNS inneholder ikke sikkerhetsfunksjoner, men utvidelser for å sikre DNS-informasjon foreligger i [RFC 2535–2537]. Implementasjon av dette er et langsiktig krav.

2.7. Kravtabell om interoperabilitet basert på IP

Krav	Kategori	Kommentar	Henvisning
All kommunikasjon mellom enheter skal skje ved bruk av IP [RFC 791]	O	Det anbefales at også kommunikasjon *internt* i enheter baseres på IP	Se avsnitt 2.6
Kontroll med IP-trafikken skal skje ved bruk av TCP [RFC 793]	O		Se avsnitt 2.6
Eksterne nettverk skal ha støtte for UDP [RFC 768]	O	Nødvendig for bruk av DNS og SNMP	
Alle enheter skal benytte en nettkonfigurasjonsprotokoll for konfigurasjon av noder iht. RFC 2131	B	Det gjøres unntak for sentrale tjenermaskiner med dedikert drift	Se avsnitt 2.4
Alle maskiner med IP-adresse skal være registrert i en DNS-tjener iht. RFC 1034–1035 og 2181	O		Se avsnitt 2.4
Alle DNS-tjenere skal støtte sikker DNS [RFC 2535–2537]	L	Ved behov og tilgjengelig produktstøtte	Se avsnitt 2.6
Alle nettverksnoder skal la seg overvåke ved bruk av SNMP	O		Se avsnitt 2.5
Alle nettverksnoder skal kunne oppgraderes over nett	B	Av sikkerhetshensyn kan enkelte maskiner unntas fra dette kravet	Se avsnitt 2.5

2.8. Støtte til OSI-tjenester over IP

OSI-tjenestene X.400 (e-posttjeneste) og X.500 (katalogtjeneste) benytter samme sett av kommunikasjonsstandarder for OSI lag 4-7, dvs. lagene transport, sesjon, presentasjon og basis tjenesteelementer på applikasjonslaget. Krav til kommunikasjon for disse lagene er angitt i dette kapitlet.

Kravkategori er satt under forutsetning av at X.400 eller X.500 skal benyttes.

2.8.1. Krav til transport-, sesjons-, og presentasjonslagene

TCP/IP er basis også for OSI-tjenestene. ISO transportklasse 0 skal benyttes over TCP/IP [RFC 1006], og det settes krav til at sesjonslaget kan benytte ISO transportklasse 0.

Transportlaget

Kravene er under forutsetning av at X.400 eller X.500 skal benyttes

Krav	Kategori	Kommentar	Henvisning
ISO/IEC 8073:1997/ITU-T X.224:1995 Protocol for Providing the Connection-mode Transport Service	O		
ISO/IEC 8072:1996/ITU-T X.214:1995 Transport Service Definition	O		
RFC 1006 – ISO Transport Service on top of the TCP	O		

Sesjonslaget

Kravene er under forutsetning av at X.400 eller X.500 skal benyttes

Krav	Kategori	Kommentar	Henvisning
ISO/IEC 8326:1996/ITU-T X.215:1995 Session Service Definition	O		
ISO/IEC 8327-1:1996/ITU-T X.225:1995	O		
Basic Connection Oriented Session Protocol: Protocol Specification	O		

Presentasjonslaget

Kravene er under forutsetning av at X.400 eller X.500 skal benyttes

Krav	Kategori	Kommentar	Henvisning
ISO/IEC 8822:1994/ITU-T X.216:1994 Presentation Service Definition	O		
ISO/IEC 8823-1:1994/ITU-T X.226:1994 Connection Oriented Presentation Protocol: Protocol Specification	O		
ISO/IEC 8824-1 til 4:1995 ITU-T X.680-X.683:1997 Abstract Syntax Notation One (ASN.1)	O		
ISO/IEC 8825-1:1995 /X.690:1997 ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	O	NOSIP v3 stiller kun krav til å anvende BER	

2.8.2. Basis tjenesteelementer på applikasjonslaget

På applikasjonslaget settes det krav til følgende basis tjenesteelementer:

- ACSE – Application Control Service Element
- RTSE – Reliable Transfer Service Element
- ROSE – Remote Operations Service Element

X.400 benytter ACSE, RTSE og ROSE, mens X.500 benytter ACSE og ROSE.

ACSE

Kravene er under forutsetning av at X.400 eller X.500 skal benyttes

Krav	Kategori	Kommentar	Henvisning
ISO/IEC 8649:1996/ITU-T X.217:1995 Service Definition for the Association Control Service Element	O		
ISO/IEC 8650-1:1996/ITU-T X.227:1995 Connection-oriented Protocol for the Association Control Service Element: Protocol Specification	O		

RTSE

Kravene er under forutsetning av at X.400 eller X.500 skal benyttes

Krav	Kategori	Kommentar	Henvisning
ISO/IEC 9066-1:1989/ITU-T X.218:1993 Reliable Transfer – part 1: Model and Service Definition	O	ISO og ITU har ulike navn på standarden	
ISO/IEC 9066-2:1989/ITU-T X.228:1988 Reliable Transfer – part 2: Protocol Specification	O	ISO og ITU har ulike navn på standarden	

ROSE

Kravene er under forutsetning av at X.400 eller X.500 skal benytttes

Krav	Kategori	Kommentar	Henvisning
ISO/IEC 13712-1:1995/ITU-T X.880:1994 Remote Operations: Concepts, Model and Notation	O		
ISO/IEC 13712-2:1995/ITU-T X.881:1994 Remote Operations: OSI Realizations – Remote Operation Service Element (ROSE) Service Definition	O		
ISO/IEC 13712-3:1995/ITU-T X.882:1994 Remote Operations: OSI Realizations – Remote Operations Service Element (ROSE) Protocol Specification	O		

3 Sikkerhet

3.1. Innledning

Bruk av NOSIP i konkrete anvendelser vil være betinget av at sikkerheten er tilfredsstillende ivaretatt. I tillegg til konkrete sikkerhetskrav inneholder derfor NOSIP en god del diskusjonsstoff om sikkerhet (avsnitt 3.2 til 3.9). Sikkerhetskrav er oppsummert i avsnitt 3.10.

NOSIP er ikke en erstatning for eksisterende regelverk om informasjonssikkerhet. NOSIP-pålegget gjelder heller ikke når en enhet har spesielle sikkerhetsbehov og krav som ikke dekkes av NOSIP. For forholdet til gjeldende regelverk og informasjon om informasjonssikkerhet, se avsnitt 3.4.

3.2. Trusselbilde, risiko og sårbarhet

Sikkerhetstiltak settes inn for å motvirke konkrete trusler. En trussel medfører en viss risiko, definert som sannsynligheten for at trusselen skal slå til. Sårbarheten relatert til en trussel kan defineres som risiko multiplisert med effekt, der effekten er de kostnadene (i en vid betydning av ordet) som en realisert trussel vil medføre. Sårbarheten, og dermed behovet for sikkerhetstiltak, vil variere sterkt fra tilfelle til tilfelle.

Krav til sikkerhet kan defineres relativt til tilgjengelighet, integritet og konfidensialitet av informasjon. I noen tilfeller er det også aktuelt å ta med sporbarhet – muligheten for i ettertid å framskaffe bevis (av en eller annen styrke) for hendelser. I forhold til dette kan en dele trusler i følgende kategorier, hvorav NOSIP bare stiller krav i forbindelse med de tre siste:

- ”Fysiske” hendelser som brann og oversvømmelse
- ”Tilfeldige” feil i system, programmer og liknende

- Utilsiktet feil bruk
- Tyveri og sabotasje
- Uautorisert modifisering av system eller informasjon
- Uautorisert tilgang til informasjon
- Benektelse av ansvar for utførte handlinger

Sikkerhetstiltak kan deles i tre kategorier: forebyggende, oppdagende/avskjærende og opprettende. NOSIP kan i prinsippet omfatte alle kategorier, selv om fokus primært er på forebyggende tiltak. Innen hver kategori er det igjen tre typer tiltak: fysiske, logiske og administrative. NOSIP dekker kun logisk sikring.

Det er dermed alltid et behov for sikring ut over det som defineres i NOSIP, som diskutert nedenfor.

3.3. Sikkerhetsstrategier og kvalitetssikring

En sikkerhetsstrategi vil omfatte overordnede retningslinjer for virksomhetens sikkerhet, en risikoanalyse, og basert på dette spesifikke sikkerhetstiltak for virksomhetens ressurser/informasjon. Bruk av anbefalingene i NOSIP skal forankres i sikkerhetsstrategien, og henge sammen med andre sikkerhetstiltak.

Et sikkerhetsdomene defineres som en samling ressurser underlagt en spesifikk sikkerhetsstrategi, og en definert sikkerhetsautoritet. NOSIP definerer at en enhet skal være underlagt én sikkerhetsstrategi og én myndighet. En enhet tilhører altså ett sikkerhetsdomene (et domene kan omfatte flere enheter). En typisk organisering vil være at en enhet er et toppnivå sikkerhetsdomene der overordnet sikkerhetsstrategi og overordnet ansvar legges, og at enhetene så kan ha underdomener underlagt forskjellige lokale autoriteter. Et underdomene kan tilpasse sikkerhetsstrategien, men kan ikke være i konflikt med den overordnede strategien.

En sikkerhetsstrategi skal alltid plassere ansvar. Dette gjelder ansvar for gjennomføring av de forskjellige tiltakene sikkerhetsstrategien definerer, ansvar for vedlikehold og endringer i sikkerhetsstrategien selv, og ansvar for håndtering av sikkerhetsrelevante hendelser. Altså: Enhver virksomhet skal ha en sikkerhetsorganisasjon.

Sikkerhetsrelevante hendelser kan deles inn i tilfeldige feil og bevisste angrep. Beskyttelse mot tilfeldige feil (inkludert overbelastning m.m.) består i hovedsak av kvalitetssikring av systemer, programmer og nettverk, fornuftig dimensjonering av komponenter, og tilstrekkelig redundans. Dette bidrar primært til økt tilgjengelighet og integritet.

Beskyttelse mot bevisste angrep består av egne sikkerhetstiltak (disse bidrar også til beskyttelse mot tilfeldige feil). Imidlertid

er kvalitetssikring en meget viktig faktor også her. Her kan en spesielt peke på behovet for kvalitetssikring av programmer og systemer som tilbyr tjenester i nettverk. En rekke kategorier angrep utnytter feil og mangler i protokoller og deres implementasjon. Slike angrep vil typisk kunne omgå sikkerhetstiltak. Som ett eksempel er antakelig Common Gateway Interface (CGI) scripts av dårlig kvalitet, eller satt opp med for høye aksessrettigheter, den største risikoen forbundet med tjenester tilbudt på WWW.

Kvalitetssikring omfatter også de administrative sikkerhetstiltakene og opplæring av brukerne. Uansett tekniske sikkerhetstiltak vil det alltid være en menneskelig faktor som spiller inn. Svært ofte er den største risikoen knyttet til lovlige brukere som enten gjør feil, går ut over sine rettigheter, eller utnytter sine rettigheter på en uautorisert måte. En sikkerhetsstrategi er ikke verdt stort dersom den bare er et papirdokument. Strategien må implementeres (institusjonaliseres) i virksomheten på en slik måte at hver enkelt bruker ser sin rolle – både med hensyn på hvilke trusler brukerens aktiviteter medfører for virksomheten, og hvordan brukeren kan bidra til å forhindre og oppdage relevante hendelser. Dette krever opplæring av brukerne.

3.4. Forholdet til annet regelverk om informasjonssikkerhet

For informasjon som er gradert i henhold til Sikkerhetsinstruksen [S-INST] eller Beskyttelsesinstruksen [B-INST], gjelder Datasikkerhetsdirektivet [D-DIR] med tilhørende veiledninger. For personinformasjon gjelder "Lov om personregistre" [P-VERN] med tilhørende forskrifter.[1] Sikkerhetskravene i NOSIP gjelder kun for informasjon og systemer som ikke er underlagt øvrige sikkerhetsregelverk. En god del av kravene i NOSIP vil være egnet til å understøtte beskyttelse av også denne typen informasjon og systemer, men i en del tilfeller vil det være avvik. Spesifikt gjelder dette bruk av kryptografi, der [S-INST, B-INST, D-DIR] stiller egne krav til kryptoalgoritmer, utstyr og godkjennelse.

Mer informasjon om sikkerhetskrav og generell informasjon om informasjonssikkerhet kan skaffes ved henvendelse til Datatilsynet eller Forsvarets Overkommando/sikkerhetsstaben (FO/s).

[1] Det vil i løpet av kort tid tre i kraft to nye lover på området personvern og rikets sikkerhet. Disse vil ha eksplisitte sikkerhetskrav og tilhørende sikkerhetsforskrifter.

3.5. Sertifisering av organisasjoner, produkter og tjenester

Sikkerhetsmessig evaluering og sertifisering skal gi en garanti for et visst sikkerhetsnivå, i henhold til anerkjente kriterier og standarder. Det er mulig å sikkerhetssertifisere både organisasjoners informasjonssikkerhetsarbeid og sikkerhetsegenskaper til produkter og tjenester. Dette er ulike sertifiseringsopplegg. Sertifisering av organisasjoners informasjonsikkerhetsarbeid anses som det viktigste for forvaltningen.

To norske systemer for sikkerhetsmessig evaluering og sertifisering [RITS-1] er under etablering:

- *Sertifisering av organisasjoners (enheters) informasjonssikkerhetsarbeid*
  Norsk Akkreditering akkrediterer private virksomheter til å utføre sertifisering av organisasjoneres informasjonssikkerhetsarbeid. Standarden som benyttes er BS 7799:1999 [BS 7799]. Denne prosessen kan sammenliknes med sertifisering av kvalitetssystemer etter ISO:9000 serien. En enhet kan kontakte et akkreditert sertifiseringsorgan for å få utført en sertifisering av enheten etter BS 7799:1999 del 2. Dette vil være en frivillig ordning.
- *Evaluering og sertifisering av produkter*
  Sertifiseringsmyndighet for sikkerhetsmessig sertifisering av produkter vil være FO/s. Produsenter/leverandører kan levere produkter for evaluering og sertifisering. Produktet får så en sertifisering iht. et gitt sikkerhetsnivå. Kravene/kriteriene som det evalueres og sertifiseres etter er ITSEC [ITSEC] og Common Criteria [CC] som er definert som en ISO-standard [ISO/IEC 15405 del 1–3.]

3.6. Standardisering av sikkerhet

Sikker kommunikasjon mellom et stort antall parter krever standardisering av sikkerhetsfunksjonene. Områder for standardisering er:

- meldingsformater, f.eks. for sikker e-post
- kryptoalgoritmer
- protokoller for utveksling av sikkerhetsinformasjon
- representasjon av sikkerhetsinformasjon, f.eks. offentlig-nøkkel sertifikater

NOSIP inneholder krav innenfor alle disse områdene i den utstrekning det er mulig å stille fornuftige krav basert på aksepterte standarder.

I tillegg finnes det som tidligere nevnt, standarder for sikkerhetsmessig evaluering og sertifisering.

3.7. Nettverkssikkerhet og meldingssikkerhet

Sikkerhet for kommunikasjon kan legges på flere nivåer:

- I applikasjoner for spesifikke formål – dette er utenfor NOSIP, men kan være standardisert
- I sluttbrukertjenester, f.eks. sikker elektronisk post
- I kommunikasjonsprotokoller ende til ende mellom avsender og mottaker(e), f.eks. Secure Sockets Layer (SSL) mellom en nettleser og en tjenermaskin
- På IP-nivå, enten ende til ende, eller mellom noder i nettverket, f.eks. Virtuelle Private Nett (VPN) mellom rutere i nettverk
- På linknivå, punkt til punkt mellom noder i nettet – dette anbefales ikke i NOSIP, men kan eventuelt brukes f.eks. der kommunikasjonskanalen er basert på en fast, leid linje

Nettverkssikkerhet beskytter informasjon under overføring over en forbindelse mellom maskiner (ende til ende for forbindelsen, eller på deler av forbindelsen, f.eks. VPN). Dette vil være (i stor grad) transparent for applikasjoner og tjenester. Informasjonen vil være i ubeskyttet klartekst hos avsender og mottaker(e).

Meldingssikkerhet, som må legges på tjenestenivå eller applikasjonsnivå, oppnås ved at en bygger opp en sikret melding (f.eks. signert og kryptert), som så kan overføres over vilkårlige, usikrede nettverk. Meldinger kan også mellomlagres og videresendes, mens nettverkssikkerhet ikke beskytter informasjon ved mellomlagring. Digitale signaturer er et eksempel på en tjeneste som er avhengig av meldingssikkerhet.

Hvilket nivå en ønsker å legge sikkerheten på, er avhengig av hvilke krav anvendelsene stiller. Det er også mulig å kombinere forskjellige nivåer, f.eks. nettverkssikkerhet, for å sikre beskyttelse for all informasjon, og meldingssikkerhet i tillegg der det er behov for signaturer. NOSIP stiller krav både til nettverkssikkerhet og meldingssikkerhet.

3.8. Ende til ende sikkerhet, brannvegger og VPN

Sikkerhet kan legges i hver enkelt node hos enhetene, eller i brannvegger[2] mot eksterne nettverk. Brannvegger kan også brukes mellom forskjellige deler av en enhet. I praksis er nesten alltid en brannvegg formålstjenlig ved tilkopling til eksterne nettverk. Samtidig kan aldri en brannvegg løse alle sikkerhetsproblemer. Det vil alltid være nødvendig med visse sikkerhetsfunksjoner i de enkelte nodene. Et eksempel er kontroll av innhold i meldinger, der det er meget begrenset hva som kan legges i en brannvegg.

En brannvegg kan operere på IP-nivå (filtrerende ruter), kan filtrere (dvs. selektivt stoppe eller slippe gjennom) trafikk basert på informasjon i protokoller over IP, og kan i tillegg tilby (proxy eller reelle) tjenester til eksterne og interne maskiner. Funksjonene kan være fordelt på flere noder. Merk at en brannvegg ikke kan filtrere på kryptert informasjon med mindre den dekrypteres i brannveggen. Dette kan ha betydning for nivået av filtrering en brannvegg kan tilby.

Implementering av tjenester (proxy eller reelle) ligger utenom NOSIP. Merk at det ofte vil være naturlig å legge en ekstern DNS-tjener til en brannvegg.

Her defineres et Virtuelt Privat Nett (VPN) som en lukket gruppe rutere tilknyttet et åpent nettverk (f.eks. Internett). Ruterne skal kunne foreta gjensidig autentisering, og kryptere trafikk seg imellom. VPN-ruterne kan da brukes til å kople sammen lokalnett (som regnes som sikre) mellom enheter eller mellom deler av en enhet. VPN-rutere kan utgjøre komponenter i en brannvegg.

NOSIP stiller krav til brannvegger og VPN-løsninger.

3.9. Hjemmekontor og mobilt arbeid

I stadig større grad brukes løsninger som tillater ansatte å arbeide andre steder enn i virksomhetens lokaler. Spesielt gjelder dette hjemmekontor og løsninger for mobilt arbeid.

Dersom utstyr for hjemmekontor og mobilt arbeid defineres som en del av den enheten utstyret kommuniserer med, skal utstyret underlegges enhetens sikkerhetsstrategi. I motsatt fall skal kommunikasjon mellom utstyret og enheten underlegges den samme kontrollen som annen ekstern kommunikasjon.

[2] Med brannvegg mener vi her utstyr og programvare benyttet for tilgangskontroll mellom en enhets interne IT-system og eksterne nettverk. Brannvegger kan også benyttes for å skille ulike deler av en enhets interne nettverk.

Dersom utstyret er definert som en del av enheten, trengs det normalt egne løsninger for å beskytte kommunikasjonskanaler. Det mest aktuelle er et system som autentiserer utstyret (eventuelt også brukeren), og oppretter en kryptert kommunikasjonskanal basert på dette. NOSIP stiller ikke eksplisitte krav til slike løsninger.

3.10. Sikkerhetskrav

Kravkategori er satt under forutsetning av at behovet for en sikkerhetsløsning er til stede. Har man for eksempel behov for ende til ende nettverkssikkerhet, skal man benytte SSL.

3.10.1. Kryptoalgoritmer

Det skal benyttes åpent tilgjengelige, ikke hemmelige, algoritmer av anerkjent styrke og med tilstrekkelig nøkkellengde. Anbefalte algoritmer er:

- Offentlig-nøkkel kryptoalgoritme for digital signatur og utveksling av (symmetriske) krypteringsnøkler: RSA i overensstemmelse med Public Key Cryptography Specifications (PKCS) PKCS#1versjon 2 [RFC2437]
- Hash-algoritme: SHA-1 [NIST 180-1] eller MD5 [RFC1321]
- Symmetrisk kryptoalgoritme: DES [DES], Triple-DES [ANSI X9.52] eller RC5 [RFC2040]

Anbefalt nøkkellengde vil variere etter behov og hvor langt utviklingen har kommet på området kryptoanlayse, samt kostnadene forbundet ved å lage spesialmaskinvare for å knekke kryptosystemer.

3.10.2. Meldingsformater

Meldingssikkerhet skal være basert på formatet PKCS#7 [RFC2315].

Sikring av elektronisk post skal være i henhold til Secure/MIME (S/MIME) versjon 2 [RFC2311-2312].

Langsiktig krav for sikring av elektronisk post er S/MIME versjon 3 [RFC 2630-2634].

3.10.3. Protokoller, nettverkssikkerhet

Nettverkssikkerhet ende til ende eller til proxy-tjener (f.eks. nettleser til en tjenermaskin) skal følge Secure Sockets Layer (SSL) versjon 3 [SSL].

Langsiktig krav for nettverkssikkerhet er Transport Layer Security (TLS) [RFC2246].

3.10.4. Representasjon av sikkerhetsinformasjon

Offentlig-nøkkel sertifikater skal være i henhold til X.509 versjon 3 (X.509v3) [ITU-T X.509, ITU-T X.509 A1].

Tilbakekallingslister (CRL – Certificate Revocation List) skal følge X.509 CRL versjon 2 (CRLv2) [ITU-T X.509, ITU-T X.509 A1].

Algoritme for signering av X.509v3 sertifikater og CRLv2 tilbakekallingslister skal være SHA-1 [ANSI X9.30] eller MD5 [RFC1321] hash og RSA [RFC2437]. RSA-nøkkel for signering av sertifikater skal være minimum 2048 bits.

3.10.5. Brannvegger

En brannvegg skal kunne filtrere på innkommende og utgående IP-adresser og IP-adresseområder og på nettmaske, og på annen informasjon i IP-hodet (spesielt angivelse av hvilken protokoll som går over IP).

En brannvegg skal kunne filtrere på meldinger i Internet Control Message Protocol (ICMP).

Ved behov, og forutsatt ukryptert trafikk, skal en brannvegg kunne filtrere på informasjon i protokollhoder over IP-nivå.

3.10.6. Virtuelle private nett (VPN)

Rutere i et VPN skal kunne autentisere hverandre gjensidig.

Det skal finnes et system for utveksling av symmetriske sesjonsnøkler for kryptering.

Langsiktig krav er at sikring av kommunikasjonen mellom ruterne skal være basert på IPSec versjon 2 [RFC2401–2402, 2406].

3.10.7. Kravtabell

NB: Kravkategorien her er gitt under forutsetning om at enheten har behov for funksjonaliteten i sikkerhetstjenesten. Kravet er ikke at sikkerhetstjenesten skal implementeres.

Oppsummering av sikkerhetskrav:

Krav	Kategori	Kommentar	Henvisning
Kryptoalgoritmer			
RSA i overensstemmelse med PKCS#1 v2,	O	Offentlig-nøkkel kryptoalgoritme	
SHA-1 *eller* MD5	O	Hash-algoritme	
DES, Triple-DES *eller* RC5	O	Symmetrisk kryptoalgoritme	
Meldingsformater			
PKCS#7	O	Meldingssikkerhet	
S/MIME v2	O	Sikring av elektronisk post m.m.	
S/MIME v3	L	Sikring av elektronisk post m.m.	
Nettverkssikkerhet			
SSL v3	O		
TLS	L		
Representasjon av sikkerhetsinformasjon			
X.509 v3	O	Offentlig-nøkkel sertifikater	
X.509 CRL v2	O	Tilbakekallingslister	
SHA-1 *eller* MD5 hash, og RSA, minimum nøkkellengde 2048 bits	O	Signeringsalgoritme	
Brannvegger			
Filtrering på innkommende og utgående IP-adresser og IP-adresseområder, på nettmaske og på annen informasjon i IP-hodet	O		
Filtrering på ICMP-meldinger	O		
Filtrering på informasjon i protokollhoder over IP-nivå	B	Ved ukryptert trafikk	
Virtuelle private nett			
Gjensidig autentisering av rutere	O		
System for utveksling av symmetriske sesjonsnøkler for kryptering	O		
IPSec v2	L	Ved kommunikasjon mellom rutere	

4 Formater

Kapitlet inneholder krav til formater ved datakommunikasjon. Både formater for tegnsett og tegnkoding, dokumentformater og formater for innholdstyper (MIME) er behandlet. Kun formater som er felles for mer enn én tjeneste, dekkes av avsnittene under. Det henvises til kapittel 5 for detaljer om tjenestespesifikke formater, samt avsnitt 3.10 for formater relatert til sikkerhet. Krav til formater er oppsummert i avsnitt 4.4.

Dokumentformater kan deles inn i produksjonsformater, arkivformater (for langtidslagring) og utvekslingsformater (over en kommunikasjonstjeneste, f.eks. elektronisk post). NOSIP omhandler kun krav til *utvekslingsformater*.

Produksjonsformater er ofte proprietære, produktavhengige, og vanskelig å sette krav til.

For krav til arkivformater henvises det til NOARK-4. Kravene der er ISO 8859-1 (tegnformat), SGML (tekstformat), TIFF (rastergrafikkformat) og PDF (trykkformat).

Dokumentformater kan generelt kategoriseres som

- tegnformater (bokstaver og tall)
- tekstformater (med struktur/layout)
- grafikkformater (raster og vektor)
- videoformater
- lydformater
- multimediaformater (tekst, grafikk, video og lyd)

Dette kapitlet omhandler *ikke* krav til formater for de fire siste kategoriene, under fellesbetegnelsen media, da dette ikke er ønsket å ta med i denne versjonen av NOSIP.

4.1. Tegnsett og tegnkoding

Et *tegnsett* definerer en samling tegn uavhengig av hvordan disse tegnene representeres. En *tegnkoding* er et sett av regler som beskriver hvordan tegnene i et gitt tegnsett skal representeres. Skillet er viktig, men ofte oversett i spesifikasjoner og produkter, hvilket er en av grunnene til problemene som ofte oppstår innenfor området.

Regler for bruk av tegnsett er viktig for at overføring av tekstlig informasjon skal bli forstått på samme måte av partene som kommuniserer.

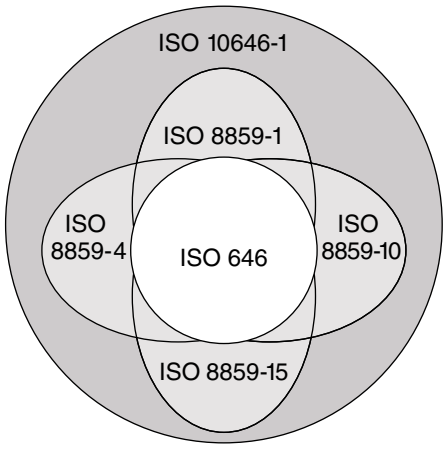
To mulige strategier for bruk:

- Tegnsett og tegnkoding er implisitt avtalt (f.eks. alle bruker kun ISO 8859-1)
- Tegnsett og tegnkoding identifiseres eksplisitt (eller avtalt innenfor mindre grupper). Flere tegnsett kan dermed støttes, men vanligvis bare et begrenset utvalg

NOSIP setter krav til både tegnsett og tegnkoding, og forsøker å presentere en funksjonell løsning som ivaretar behovene fra de forskjellige anvendelsesområdene.

4.1.1. Krav

NOSIP skiller mellom *utsendelse* og *mottak* av informasjon/dokumenter, og kravene baseres på prinsippet om å være konservativ med hva man sender ut, men liberal med hva man mottar fra andre. Figuren under illustrerer de viktigste tegnsettene i bruk i Norge i dag, og hvordan de forholder seg til hverandre.



Figur 3. Forholdet mellom ulike tegnsett

Ved utsendelse setter NOSIP følgende krav til tegnsett og tegnkoder. I alle normale tilfeller skal ISO 8859-1 [LATIN1] benyttes. Dette tegnsettet dekker alle norske tegn. Imidlertid er det ikke tilstrekkelig for å ivareta kravene fra nasjonale minoriteter. Ved behov for nordsamiske tegn skal ISO 8859-4 [LATIN4] brukes. Trengs i tillegg sørsamiske tegn, er kravet ISO 8859-10 [LATIN6]. Ved behov for det nye Euro-symbolet skal ISO 8859-15 [LATIN9] benyttes. Hvert tegn i alle tegnsettene over representeres i 8 biters kodeverdier.

Ved ytterligere behov for tegn som ikke dekkes av tegnsettene over, skal Universal Character Set (UCS) [ISO/IEC 10646-1] benyttes. UCS er en internasjonal standard som dekker de fleste tenkelige tegn i verden, og er utviklet i samarbeid med industristandardgrupperingen UNICODE. Imidlertid kan ingen applikasjon forventes å støtte hele UCS. Hvert tegn i UCS representeres i 32 biters kodeverdier.

Ved tegnkoding med et fast antall oktetter per tegn skal UCS-2 for UNICODE (16 biters kodeverdier) benyttes. Ofte tar dette for mye plass, og tegnene vil derfor kodes med et variabelt antall biter pr. tegn i stedet. For dette formålet skal transformasjonsteknikker som UTF-8 [RFC 2279] brukes.

Det foregår et kontinuerlig arbeid med å utvide ISO 10646/UNICODE med flere tegnsett. RFC 2279 gir en oversikt over noen av utvidelsene, og er et eksempel på en strategi for å forholde seg til nye revisjoner av ISO 10646.

Det bør bemerkes at bruken av ISO 8859-15 forventes gjort overflødig av UNICODE når det sistnevnte tegnsettet blir enerådende.

Ved mottak stiller NOSIP krav om at alle 8 biters tegnsettene over, samt UNICODE, skal håndteres. I tillegg skal 7 biters tegnsettet ISO 646 [US-ASCII] og ITU-T T.61 [ISO/IEC 6937] ved X.500 anvendelser fremdeles aksepteres for bakoverkompatibilitet.

4.1.2. Utfordringer

En utfordring ved kravene over gjelder sertifikater hvor bruk av ISO 8859-1 ofte ikke vil være tilstrekkelig for gjenfinning og sortering av korrekt skrevet navn. Dette vil forbli en uløst situasjon til et større tegnsett som ISO 10646/UNICODE blir enerådende.

Videre er flere ikke-standardiserte løsninger for 8 biters tegnsett og tegnkoding i bruk, hvor tegnsettet faller sammen med ISO 8859-1, men der tegnkodingen ikke er den samme. Dette gjelder bl.a. for vanlige kontorplattformer. Spesielt kodingen av det nye Euro-symbolet er det viktig å være oppmerksom på i denne forbindelse, da dette fort vil skape problemer ved kommunikasjon.

4.2. Dokumentformater

Ved utveksling av dokumenter med redigerbar eller strukturert tekst og grafikk (tekstformat) er det, i generell brukssammenheng, et betinget krav (B) å kunne utveksle dokumenter i henhold til Standardized General Markup Language (SGML) [ISO 8879]. NOSIP stiller ikke noen krav utover å støtte SGML referansesyntaks (reference concrete syntax).

SGML er strengt tatt ikke et dokumentformat, men en syntaks (dokumentbeskrivelse) for å definere en spesiell applikasjon. En forenklet variant av SGML er eXtensible Markup Language [XML]. Dette nye beskrivelsesspråket forventes å få stor utbredelse innen flere anvendelsesområder, og NOSIP stiller derfor også et langsiktig krav (L) om at XML skal benyttes ved utveksling av strukturerte dokumenter.

Avsnitt 5.3.2 inneholder en nærmere diskusjon om SGML og XML i forbindelse med anvendelser i WWW-sammenheng.

NOSIP stiller ingen krav ved utveksling av dokumenter bestående av kun tegn (tegnformater), da slike vanligvis vil inngå som en del av andre typer dokumentformater, f.eks. tekstformater. Det faller derfor ikke naturlig med separate krav til dette, annet enn at kravene til tegnsett og tegnkoding følges.

4.3. Innholdstyper (MIME)

Multipurpose Internet Mail Extensions (MIME) definerer et strukturert format for spesifikasjon av innholdstyper ved dokumentutveksling. Som det fremgår av navnet, ble MIME opprinnelig laget for utveksling av ulike typer tekstlige og ikke-tekstlige vedlegg ved Internett e-post meldingsformidling (SMTP). Nå benyttes MIME innholdstyper også f.eks. ved utveksling av dokumenter over HTTP.

MIME spesifiserer et utall innholdstyper for dokumentformater, som omfatter alt fra tegn- og tekstformater til grafikk og multimedia. Internet Assigned Numbers Authority (IANA) er ansvarlig for å godkjenne nye og vedlikeholde en oversikt over eksisterende MIME innholdstyper for e-post (http://www.isi.edu/in-notes/iana/assignments/media-types/media-types).

NOSIP setter krav om at formater for innholdstyper skal følge Multipurpose Internet Mail Extensions (MIME) [RFC 2045-2049].

4.4. Formatkrav

Oppsummering av krav til formater som er felles for flere tjenester:

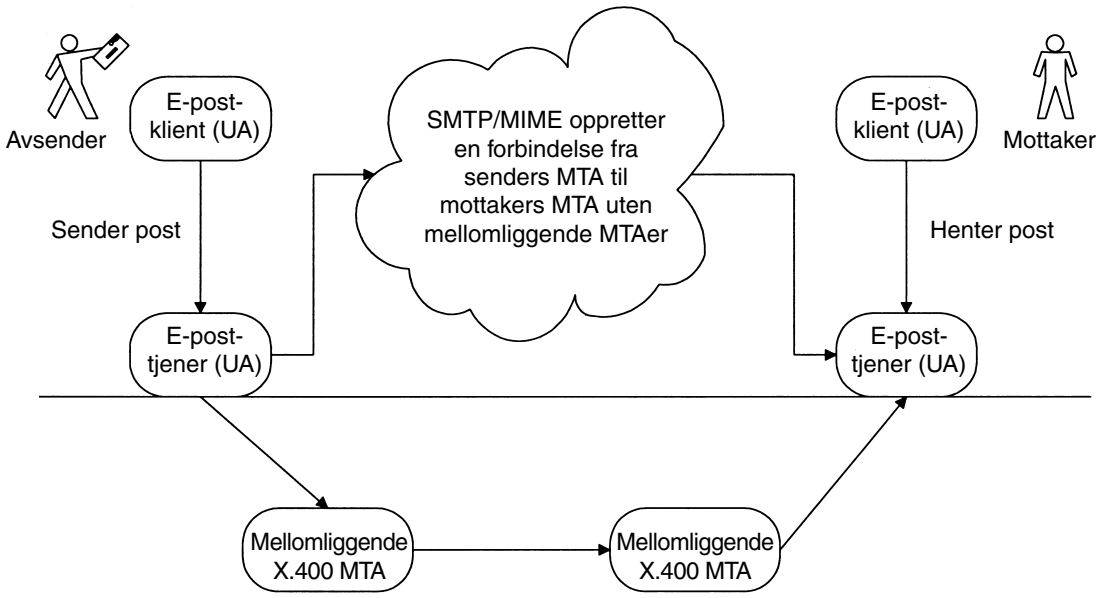
Krav	Kategori	Kommentar	Henvisning
Tegnsett og tegnkoding			
ITU-T T.61	I	Kun for mottak ved X.500-anvendelser	
ISO/IEC 646:1991	I	Kun for mottak	
ISO/IEC 8859-1:1998	O		
ISO/IEC 8859-4:1998	B	Ved behov for (nord) samiske tegn	
ISO/IEC 8859-10:1998	B	Ved behov for (sør) samiske tegn	
ISO/IEC 8859-15:1999	B	Ved behov for Euro-symbolet	
ISO/IEC 10646-1:1993 BMP / UNICODE 2.0	L	Ved behov for ytterligere tegn	
ISO/IEC 10646-1:1993 UCS-2	L	Fast tegnkoding BMP/UNICODE 2.0	
RFC 2279 – UTF-8, a transformation format of ISO 10646	L	Variabel tegnkoding for ISO/IEC 10646-1	
Dokumentformater			
ISO 8879:1986 inkludert amendment 1:1988	B	Ved behov for utveksling av strukturerte dokumenter	
XML 1.0 W3C Recommendation	L		
Innholdstyper			
RFC 2045 – Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies	O		
RFC 2046 – Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	O		
RFC 2047 – Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text	O		
RFC 2048 – Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures	O		
RFC 2049 – Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples	O		

Krav til formater som er spesifikke for enkelttjenester eller sikkerhet, er beskrevet i de respektive kapitlene.

5 Anvendelser

5.1. Elektronisk meldingsformidling (e-post)

To ulike entiteter er involvert i tjenesten elektronisk post (e-post) når meldinger utveksles mellom en avsender og en (eventuelt flere) mottaker(e). Én eller flere tjenere (Message Transfer Agent – MTA) sørger for nødvendig funksjonalitet for å flytte meldinger mellom avsender og mottaker(e). En klient (Message User Agent – UA) på avsendersiden er ansvarlig for formatering av meldingen og overføring *til* nærmeste tjener (MTA), og en klient (UA) på mottakersiden er ansvarlig for å hente meldingen *fra* nærmeste tjener (MTA).



Figur 4. E-post-forsendelse i hhv SMTP/MIME og X.400

To systemer for e-post er utbredt i dag. De er basert på henholdsvis Internett e-post (SMTP/MIME) og X.400. Internett e-post er den foretrukne e-posttjenesten i NOSIP v3.

Systemene har lik funksjonalitet på mange områder, men atskiller seg også på noen viktige felt:

- SMTP manglet i utgangspunktet kvitteringsmekanismer. Dette er kommet som et tillegg i [RFC 1891] "Leveringskvitteringer" og [RFC 2298] "Lest-kvitteringer". Ikke alle SMTP-systemer støtter disse. X.400 tilbyr både leveringskvitteringer og lestkvitteringer. Hva slags kvitteringer som kan genereres og sendes tilbake til avsender av en melding, vil avhenge av mottakers system. For kommunikasjon med Internett e-postbrukere, f.eks. til mottakere utenfor forvaltningen, hjelper det dermed lite for sendere å benytte X.400 for å sikre kvittering når mottaker leser en melding.
- Sending av X.400-basert e-post tar ofte lengre tid enn sending av SMTP-basert e-post. Dette skyldes forskjeller i e-postsystemenes arkitektur.
- Det er færre X.400-produkter enn SMTP-produkter på det norske marked.
- Prisstrukturen er ulik. En forskjell er at du betaler per X.400-melding som blir sendt, mens du vanligvis kun betaler for selve Internett-tilknytningen når du sender SMTP-meldinger. Abonnementsprisene på de to tjenestene varierer veldig, ut ifra ønsket kapasitet og tilgjengelighet. For en prissammenligning er det viktig at en ikke bare ser på anskaffelsespris, men også på bruk av systemet (drift og vedlikehold inkludert).

Ved en sammenligning mellom SMTP og X.400 kan det være andre faktorer enn de funksjonelle og prismessige som er utslagsgivende. Det kan for eksempel tenkes at applikasjoner som skal anvende e-postsystemet, begrenser valgmuligheten.

Samtrafikk mellom Internett e-post og X.400 er ikke mulig uten en portner som konverterer meldinger som utveksles mellom de to systemene. Implementasjoner basert på de to systemene vil eksistere side om side i lang tid framover. Det er derfor viktig å definere og etablere en portnertjeneste for å konvertere e-post som utveksles mellom brukere av de to e-postsystemene. Avsnitt 5.2.2.6 spesifiserer nærmere krav til en slik portnertjeneste. Disse kravene gjelder både en eventuell sentral portnertjeneste og lokale portnertjenester som brukere måtte ønske å etablere. NOSIP gir enheter som baserer seg på X.400 e-post, ansvar for å sørge for tilgang til portner for samtrafikk med Internett e-postbrukere.

5.2. Krav til elektronisk meldingsformidling (e-post)

Hovedkravet i NOSIP er at e-post skal baseres på Internett e-post (SMTP/MIME). Andre valg skal grunngis i henhold til NOSIP-pålegget.
Brukere av andre e-postsystemer, spesielt X.400-brukere, har ansvar for å sørge for portner for samtrafikk med Internett e-postbrukere, se avsnitt 5.2.2.6.

5.2.1. Internett e-post

Kravene til Internett e-post er delt inn i krav for tjener-til-tjener-kommunikasjon, klient-til-tjener-kommunikasjon, krav til meldingsformater og krav til sikker elektronisk post.

5.2.1.1. Tjener til tjener meldingsformidling (MTA til MTA)

Simple Mail Transfer Protocol (SMTP) [RFC 821] spesifiserer grunnleggende funksjonalitet for effektiv og pålitelig meldingsformidling, og skal benyttes mellom to tjenere. Enkelte presiseringer av standarden (f.eks. krav om 4-sifrede årstall) finnes i "Requirements for Internet Hosts – Applications" [RFC 1123]. Extended SMTP (ESMTP) [RFC 1869] definerer et rammeverk for utvidelse av SMTP med ny funksjonalitet, men selve utvidelsen er angitt i separate spesifikasjoner. Leveringskvittering [RFC 1891] er en slik utvidelse, som skal støttes for MTA-MTA-kommunikasjon ved Internett e-post.

Krav	Kategori	Kommentar	Henvisning
RFC 821 – Simple Mail Transfer Protocol	O		
RFC 1123 – Host Requirements	O	Relevante deler	
RFC 1869 – SMTP Service Extensions	O		
RFC 1891 – SMTP Service Extension for Delivery Status Notifications	O		

5.2.1.2. Klient til tjener meldingsformidling (UA til MTA)

Meldingsformidling mellom klient og tjener involverer to ulike situasjoner. Henting/aksessering av meldinger fra tjener til klient,

og sending av meldinger fra klient til tjener. Situasjonene stiller ulike krav.

Post Office Protocol v3 (POP3) [RFC 1939] og Internet Message Access Protocol v4 (IMAP4) [RFC 2060] er de to mest benyttede aksessmetodene i dag. POP3 er mest utbredt, mens IMAP4 har mer avansert funksjonalitet. Hovedforskjellen ligger i mye bedre støtte for ulike former for meldingsaksessering ("online" og "disconnected") i IMAP4, i forhold til POP3, som kun er beregnet for tradisjonell ("offline") aksessering.

NOSIP stiller krav om at begge aksessmetodene skal støttes på tjenersiden, mens IMAP4 er den foretrukne på klientsiden.

Ved sending av meldinger fra klient til tjener er kravene de samme som for MTA-MTA-kommunikasjon, med følgende tillegg:

Det har vist seg at en trenger økede krav til verifisering av bruker ved sending av e-post enn SMTP tilbyr. Et langsiktig krav er støtte for autentisert sending, for eksempel ved hjelp av "Message Submission Protocol" [RFC 2476] med "SMTP Authentication" [RFC 2554].

Meldingstjenere som tillater sending av e-post fra hvemsomhelst til hvemsomhelst, utnyttes i stor grad til å sende "spam" (UCE). Begrensninger basert på at avsender må være på lokalt nett eller andre adhoc-mekanismer, har vist seg å medføre operative problemer. Derfor er dette settet protokoller kommet.

Krav	Kategori	Kommentar	Henvisning
Aksess			
RFC 2060 – Internet Message Access Protocol, version 4rev1	O	Både på tjener- og klientsiden	
RFC 1939 – Post Office Protocol, version 3	O	Kun på tjenersiden	
Sending			
RFC 821 – Simple Mail Transfer Protocol	O		Se avsnitt 5.2.1.1
RFC 1869 – SMTP Service Extensions	O		Se avsnitt 5.2.1.1
RFC 1891 – SMTP Service Extension for Delivery Status Notifications	O		Se avsnitt 5.2.1.1
RFC 2476 – Message Submission RFC 2554 – SMTP Authentication	L		Se avsnitt 5.2.1.2

5.2.1.3. Format

Meldingsformat for Internett e-post skal være basert på Internet Text Message format (MAIL) [RFC 822] og Multipurpose Internet Mail Extensions (MIME) [RFC 2045–2049]. MAIL spesifiserer hovedsakelig formatet på meldingshodet ("konvolutten"), og forutsetter rent tekstlig meldingsinnhold. MIME utvider spesifikasjonen av meldingshodet til også å inkludere ikke-tekstlige vedlegg som meldingsinnhold. MIME er nærmere beskrevet i avsnitt 4.3.

Ved bruk av mekanismer for leveringskvittering er det et obligatorisk krav at meldingsformatet er i henhold til RFC 1894.

Ved bruk av mekanismer for lestkvittering er det et obligatorisk krav at meldingsformatet er i henhold til RFC 2298.

Krav	Kategori	Kommentar	Henvisning
RFC 822 – Standard for the Format of ARPA Internet Text Messages	O		
RFC 2045-2049 – MIME part One-five	O		Se avsnitt 4.4
RFC 1894 – An Extensible Message Format for Delivery Status Notifications	O		
RFC 2298 – Message Disposition	O	Ved behov	

5.2.1.4. Sikker elektronisk post

Internett e-post gir i utgangspunktet ingen ende-til-ende sikkerhet. Krav til sikker elektronisk post i NOSIP dekker meldingssikkerhet. Secure/MIME (S/MIME) [RFC 2311-2312] spesifiserer MIME innkapsling av digitalt signerte og krypterte meldinger. Den sikrede meldingen er basert på PKCS#7 formatet [RFC 2315].

Langsiktig krav for sikring av elektronisk post er S/MIME versjon 3 [RFC 2630-2634].

Meldingssikkerhet er nærmere beskrevet i avsnitt 3.7.

Krav	Kategori	Kommentar	Henvisning
RFC 2311–2312 – S/MIME version 2, Message Specification & Certificate Handling	B	Ved behov for meldingssikkerhet	Se avsnitt 3.10.2
RFC 2315 – PKCS #7: Cryptographic Message Syntax version 1.5	B	Ved behov for meldingssikkerhet	Se avsnitt 3.10.2
RFC 2630–2634 – S/MIME version 3	L		Se avsnitt 3.10.2

5.2.2. X.400 e-post

Kravene til X.400 er basert på 1992-standardene. Kravene er delt inn i generelle MHS-krav, krav for MTA-MTA-kommunikasjon og UA-MTA-kommunikasjon Alle kravene i dette kapitlet er under forutsetning av at X.400 e-postsystem benyttes.

Krav til profiler og funksjonelle grupper er angitt i avsnitt 5.2.2.3. De omhandler områdene Common Messaging og IPM (InterPersonal Messaging). Krav til EDI Messaging (EDIMG) og Voice Messaging (VM) er ikke berørt i NOSIP v3.

Generelle MHS-krav

Kravene er under forutsetning av at X.400 skal benyttes

Krav	Kategori	Kommentar	Henvisning
ISO/IEC 10021-1:1990/ITU-T X.400:1996 Message Handling System and Service Overview	O	ISO og ITU har ulike navn på standarden.	
ISO/IEC 10021-2:1996/ITU-T X.402:1995 Overall Architecture	O		
ISO/IEC 10021-3:1990/ITU-T X.407:1988 Abstract Service Definition Conventions	O	ISO og ITU har ulike navn på standarden.	
MHS Implementors' Guide versjon 13 (Juli 1995)	B	Omfatter klargjøringer og feilrettinger.	
Lavere lags OSI-kommunikasjon	O	Omfatter kommunikasjon på transport-, sesjons- og presentasjonslaget.	Se avsnitt 2.8.1

5.2.2.1. Tjener til tjener meldingsformidling (MTA til MTA)

MHS 1992-versjonen er et obligatorisk krav (O) for X.400-basert meldingsformidling.

Kravene er under forutsetning av at X.400 skal benyttes

Krav	Kategori	Kommentar	Henvisning
Basis tjenesteelementer: ACSE og RTSE	O		Se avsnitt 2.8.2
ISO/IEC 10021-4:1997/ITU-T X.411:1995 Message Transfer System: Abstract Service Definition and Procedures	O	Profiler er angitt i avsnitt 5.1.2.3.	
ISO/IEC 10021-6:1996/ITU-T X.419:1995 MHS: Protocol Specifications	O	X.400 1992 (P1) med RTSE er et obligatorisk krav (O). Profiler er angitt i avsnitt 5.1.2.3.	
RFC 1328 – X.400 1988 to 1984 downgrading RFC 1496 – MIME X.400 1988 to 1984 downgrading	B	Definerer nedgradering fra X.400/88 til X.400/84. Krav for MTA-er som kommuniserer med MTA-1984	
RTSE-modi (X.410 (1984)-mode)			
mts-transfer	O	P1-88, RTSE normal-mode	
mts-transfer-protocol-1984	–	P1-84, RTSE X.410 (1984)-mode. Opsjon for kommunikasjon med MTA-1984.	

5.2.2.2. Klient til tjener meldingsformidling (UA til MTA)

Standarder som skal følges i forbindelse med lagring av meldinger i Message Store (MS) og aksess av disse fra en klient (UA):

Kravene er under forutsetning av at X.400 skal benyttes

Krav	Kategori	Kommentar	Henvisning
Basis tjenesteelementer: ACSE, RTSE og ROSE	O		Se avsnitt 2.8
ISO/IEC 10021-5:1996/ITU-T X.413:1995 Message Store: Abstract Service Definition	O		
ISO/IEC 10021-7:1996/ITU-T X.420:1992 Interpersonal Messaging System	O	Krav for bruk av MHS til person-til-person meldingsformidling (IPM).	

5.2.2.3. Krav til profiler og funksjonelle grupper

Standard profiler for MHS/IPM er delt i to grupper: Common Messaging (CM) og Interpersonal Messaging (IPM).

CM-profilen definerer krav som er relevante for alle MHS-systemer uavhengig av den type innhold som skal behandles. IPM definerer krav til person-til-person meldingsformidling.

Profiler

Kravene er under forutsetning av at X.400 skal benyttes

Krav	Kategori	Kommentar	Henvisning
ISP 10611-1 til 5:1997 Common Messaging	O	AMH 1n	
ISP 12062-1:1998 ISP 12062-2 til 5:1997 Interpersonal Messaging	B	AMH 2n Kravet gjelder ved bruk av MHS til IPM.	

Funksjonelle grupper

I tillegg til Basic Requirements som er angitt i profilene, skal de funksjonelle gruppene i CM og IPM angitt i tabellene nedenfor støttes. Øvrige funksjonelle grupper er opsjoner.

Kravene er under forutsetning av at X.400 skal benyttes

Krav	Kategori	Kommentar	Henvisning
Distribution List (DL)	O		
Security (SEC)	B	Hvis SEC støttes, skal minimum klasse S0C* støttes.	
Use of Directory (DIR)	O	Skal støtte bruk av Directory Name ved Submission og tilgang til katalogtjeneste fra MTA. Katalogtjenesten må minimum kunne returnere O/R-adresser.	
84 Interworking (84IW)	B	Kreves for MTA-er som skal kommunisere med MHS-84 systemer.	

* Sikkerhetsklasse S0C omfatter mekanismer for innholds- (meldings-) sikkerhet. S0C dekker: Innholdsintegritet, leveringsbevis, ende-til-ende avsenderautentisering og innholdskonfidensialitet (kryptering).

I tillegg til Basic Requirements kreves støtte for følgende funksjonelle grupper for IPM.

Kravene er under forutsetning av at X.400 skal benyttes

Krav	Kategori	Kommentar	Henvisning
IPM Distribution List (DL)	O	Ingen krav i tillegg til CM DL.	
IPM Manual Forwarding (FWD)	O		
IPM Security (SEC)	B	Hvis SEC støttes, skal minimum klasse S0C støttes.	
IPM Use of Directory (DIR)	O	Skal støtte bruk av Directory Name ved Submission og tilgang til katalogtjeneste fra MTA. Katalogtjenesten må minimum kunne returnere O/R-adresser.	
IPM 84 Interworking (84IW)	I	Nødvendig for å sikre vellykket sending av innhold til MHS-84 systemer.	

5.2.2.4. Format

Meldingsdelen skal være kodet som GeneralText. Følgende vedleggstyper skal håndteres (Basic Body Parts og Extended Body Parts).

Kravene er under forutsetning av at X.400 skal benyttes

Krav	Kategori	Kommentar	Henvisning
IA5-text	O		
Message	O	For videresendte meldinger (Forwarding).	
General Text	O	Skal kunne benytte tegnsettene ISO/IEC 8859-x. Se avsnitt 4.1.1 vedr. krav til når de ulike tegnsettene skal anvendes.	
BilaterallyDefined (BP14)	O	For portnertjeneste og utveksling av meldinger med MTA-1984.	
ExternallyDefined (BP15)	O	For portnertjeneste og utveksling av meldinger med MTA-1988.	
File Transfer Body Part (FTBP)	O	For portnertjeneste og utveksling av meldinger med MTA-1992.	
PKCS #7	L	Skal benyttes av portnertjeneste for konvertering til/fra S/MIME (application/pkcs7-mime).	Se avsnitt 5.2.2.6

5.2.2.5. Sikker elektronisk post

Krav til sikker e-post dekkes gjennom krav til meldingssikkerhet (ende-til-ende sikkerhet). NOSIP setter ingen krav til sikkerhet mellom MTA-er utover det at det skal være mulig å benytte de sikkerhetsmekanismer som er definert i X.400-standarden.

Kravene er under forutsetning av at X.400 skal benyttes

Krav	Kategori	Kommentar	Henvisning
Funksjonell gruppe SEC, klasse S0C	B	Ved behov for meldingssikkerhet	Se avsnitt 5.2.2.3
Extended Body Part PKCS #7	L	Det forventes at denne vil ta over for S0C.	Se avsnitt 5.2.2.4

5.2.2.6. X.400/SMTP portner

Dersom en enhet benytter X.400 som e-postsystem og har behov for å kommunisere med brukere av SMTP, er det et obligatorisk krav (O) at enheten etablerer avtale om portnertjenester eller etablerer en slik tjeneste selv. X.400-siden er ansvarlig for at e-post som skal utveksles med SMTP/MIME-brukere, konverteres til/fra SMTP/MIME. Brukere av SMTP/MIME skal ikke "se" X.400-verdenen.

Krav til portnertjeneste er definert av et sett RFCer (MIXER – Mime Internet X.400 Enhanced Relay). Disse finnes i flere versjoner. Den nyeste versjonen er beskrevet i RFCene:

- MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME [RFC2156]
- Mapping between X.400 and RFC-822/MIME Message Bodies [RFC2157]
- Rules for Downgrading Messages from X.400/88 to X.400/84 When MIME Content-Types are Present in the Messages (HARPOON) [RFC1496]

[RFC2156] og [RFC2157] definerer konvertering mellom SMTP/MIME og X.400 (92/88/84). [RFC2156] beskriver bl.a. hvordan SMTP-"extensions", som "Delivery status notification" (DSN), kan benyttes. [RFC1496] definerer nedgradering av MIME-baserte meldinger ved sending fra X.400(88) til X.400(84).

Den nyeste versjonen av MIXER er et obligatorisk krav (O). Det er videre et krav at portnertjenesten skal benytte DSN mot de SMTP/MIME-tjenere som støtter dette.

MIXER beskriver hvordan konvertering av adresser skal gjøres. MCGAM (MIXER Conformant Global Address Mapping), som er en del av [RFC2156], definerer dette. I tillegg beskriver [RFC2156] tre metoder for å distribuere MCGAMs. Det er distribusjon vha.:

- Tekst-tabeller: Formatet er definert i [RFC 2156]
- DNS: Dette er beskrevet i Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM) [RFC 2163]
- X.500: Dette er beskrevet i "Use of an X.500/LDAP directory to support MIXER address mapping [RFC 2164]"

I NOSIP v3 er det ikke et obligatorisk krav å bruke X.500.

Kravene er under forutsetning av at X.400 skal benyttes

Krav	Kategori	Kommentar	Henvisning
RFC 2156 – MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME	O		
Bruk av Delivery Status Notification	O	Skal benyttes ved kommunikasjon med SMTP/ MIME-tjenere som støtter dette.	
RFC 2157 – Mapping between X.400 and RFC-822/MIME Message Bodies	O		
RFC 2164 – Use of an X.500/LDAP directory to support MIXER address mapping	O		
RFC 1496 – Rules for Downgrading Messages from X.400/88 to X.400/84 When MIME Content-Types are Present in the Messages (HARPOON)	O		
RFC 2158 – X.400 Image Body Parts	B	Hvis konvertering av denne Body Part tilbys av portnertjenesten.	
RFC 2159 – MIME Body Part for FAX	B	Hvis konvertering av denne Body Part tilbys av portnertjenesten.	
RFC 2160 – Carrying Postscript in X.400 og MIME	B	Hvis konvertering av denne Body Part tilbys av portnertjenesten.	
Konvertering av sikre meldinger: X.400: PKCS #7 MIME: application/PKCS#7-mime	L	Langsiktig krav ved sending av sikker e-post.	

Portnertjenesten skal ved konvertering av sikre meldinger gjøre følgende:

- Ved mottak av X.400 Body Part *PKCS #7* legge til MIME *content-type: application/pkcs7-mime*
- Ved mottak av en MIME body part med *content-type: application/pkcs7-mime* fjerne denne content-type og sende resten av MIME body part som X.400 Body Part *PKCS #7*

Content-type: application/pkcs7-mime er nærmere beskrevet i S/MIME Version 2 Message Specification [RFC 2311].

Konvertering er primært tenkt brukt ved utveksling av krypterte EDI-meldinger mellom en X.400-bruker og en Internett-bruker.

5.2.3. Distribusjon

Distribusjon av meldinger til et stort antall mottakere kan skje ved

- en-til-mange e-post over X.400 eller SMTP via distribusjonslister. Dette er i realiteten en sekvens av en-til-en e-post fra samme avsender til en adresse som representerer flere mottakere
- oppslagstavler, systemer for interesse- og nyhetsgrupper der artikler (innlegg/oppslag/meldinger) ligger tilgjengelig i en database for gruppens interessenter (medlemmer/mottakere), men ikke distribueres til den enkelte

En viktig fordel med oppslagstavler er at meldingene lagres på ett eller et fåtall steder, der leserne må henvende seg, i motsetning til distribusjonslister der meldingene oppbevares hos den enkelte mottaker. Ulempen er vanligvis at nyhetsgruppens medlemmer, som i prinsippet ikke er registrert eller kjent for "gruppen", ikke får automatisk beskjed om nye meldinger, men må aktivt "titte innom" for å se om det har kommet noe nytt siden sist.

5.2.3.1. Distribusjonslister

Meldingsformidling via distribusjonslister, særlig når det er et stort antall mottakere, krever en betydelig administrativ innsats fra den som har ansvar for listen. Ulike systemer som forenkler listeadministrasjonen og effektiviserer distribusjonen fra en liste, foreligger. Listserv Distribute Protocol [RFC1429] foreligger som Proposed Standard. RFC 1429 foreskriver en protokoll for spredning av meldinger via distribuerte lokale enheter som foretar lokal videreformidling, men den sier ingenting om listeadministrasjon for øvrig.

Både Listserv og andre systemer som Majordomo og Listproc omfatter opplegg for automatisk inn- og utmelding av lister (ved bruk av kommandoer som formidles til systemet via e-post), for meldingsovervåking (redaksjon og kontroll med videre spredning av enkeltmeldinger) og vanligvis opplegg for distribusjon av periodisk sammendrag av nye innlegg. En del konvensjoner gjør seg gjeldende på dette området, for eksempel RFC 2369, som beskriver en måte å merke listemeldinger med hvordan en kan melde seg av, men standardiseringsarbeidet er ikke kommet i gang.

Det er et betinget krav (B) at enheter som ønsker å ta i bruk opplegg for administrasjon av distribusjonslister, kontakter Statskonsult for veiledning og anbefalinger i tilknytning til valg av løsning.

Krav	Kategori	Kommentar	Henvisning
Kontakt Statskonsult før valg av opplegg for administrasjon	B	Standard foreligger ikke, men proprietære løsninger fins	5.2.3.1

5.2.3.2. Nyhetsgrupper

Det dominerende opplegget for nyhetsgrupper på Internett bygger på USENET meldingsformat [RFC1036] og NNTP, Network News Transfer Protocol [RFC977]. USENET, også kalt News, er et verdensomfattende fullstendig distribuert system for utveksling av informasjon, meninger og nyheter mellom newsbrukere (klienter) via news-tjenere (news-feeds). NNTP definerer protokollen for utveksling mellom klient og tjener og mellom tjenere. Hvilke regler den enkelte tjener følger for administrasjon og oppbevaring av meldinger og nyhetsgrupper, eller hvordan den skal reagere på forespørsler om overføring av meldinger til andre tjenere eller klienter, er ikke en del av NNTP.

News var i utgangspunktet et system for åpen spredning av meldinger. Hvem som helst kunne normalt be om å få overført meldinger fra en nyhetsgruppe, og det normale var at news-leseren ikke behøvde være registrert hos tjeneren eller kjent for en eventuell gruppeadministrator. Tanken om "lukkede nyhetsgrupper" var fremmed for RFC 977. I ulike sammenhenger er det et åpenbart behov for strengere kontroll med meldingsdistribusjon. Lukkede grupper kan for sentralisert news-tjener ordnes ved at tjeneren som oppbevarer meldingene, ikke slipper fremmede inn (passordbeskyttelse på tjener som helhet, eller på den enkelte nyhetsgruppe). Distribuerte nyhetsgrupper kan lukkes ved bruk av passordbeskyttelse på gruppen, og kryptert og autentisert ut-

veksling mellom de aktuelle tjenere. Det fins ikke en standard for NNTP-sikkerhet i dag, men det fins proprietære systemer med innebygde sikkerhetsløsninger basert på f.eks. SSL.

Ved bruk av system for utveksling i nyhetsgrupper er det et obligatorisk krav (O) at Network News Transfer Protocol [RFC977] benyttes både ved meldingsformidling mellom klient og news-tjener, og mellom to news-tjenere der det er aktuelt. Muligheten for å etablere sikre nyhetsgrupper (lukkede grupper og beskyttede news-tjenere) er et betinget krav.

Krav	Kategori	Kommentar	Henvisning
RFC 977, Network News Transfer Protocol	O	Hvis det er behov for tjenesten	5.2.3.2
Sikre nyhetsgrupper	B	Standard foreligger ikke, men proprietære løsninger fins	

5.3. Informasjonstjenester

Offentlige informasjonstjenester retter seg delvis internt mot andre deler av det offentlige, delvis eksternt mot publikum. Profilkrav for aktører i offentlig intern og ekstern informasjonsvirksomhet kan formuleres enten ut fra et ønske om å påvirke fremtidige utstyrsvalg i målgruppen og de mulighetene aktørene dermed får for å motta informasjon som presenteres ut fra gitte standarder, eller ut fra et ønske om å nå et størst mulig (eller ønskelig) publikum på et definert eller eksisterende standardnivå. NOSIP-kravene til utstyr for informasjonsaktører er satt opp ut fra sistnevnte ambisjon. NOSIP stiller ikke krav til informasjonsinnhold eller informasjonsmålsetting. Men dersom en statlig enhet følger NOSIP-kravene til utstyr og formater, vil det kunne bidra til at innholdet når frem til større deler av målgruppen og øke muligheten for å oppfylle målsettingen med et informasjonstiltak.

5.3.1. World Wide Web

World Wide Web (WWW eller bare Web) er den viktigste tjenesten for publisering og informasjonsutveksling på Internett. WWW er under kraftig og dynamisk utvikling, anvendelsområdet utvides stadig og nye utvekslings- og presentasjonsmuligheter lanseres løpende. Ulike aktører forsøker å ta kontroll over dette nye mediet ved å definere sine egne løsninger og forsøke å presse dem igjennom som de facto standarder. Parallelt med dette fore-

går et internasjonalt standardiseringsarbeid, delvis i IETF (bl.a. for HTTP, utvekslingsprotokollen, se nedenfor) og delvis W3C (bl.a. for XML, CSS og HTML, dokumentbeskrivelse og presentasjon, se nedenfor).

Karakterisering av en målgruppe for allmenne elektroniske informasjonstjenester vil, i tillegg til en beskrivelse av gruppens informasjonsbehov, inneholde en nærmere presisering av utstyrsmessige forutsetninger i gruppen. De utstyrsmessige forutsetningene lar seg vanskelig endre på kort sikt. I stor grad vil utstyrsnivået, særlig på hjemmesektoren, i de nærmeste år være bestemt gjennom de løsningene som var rådende i 1997–98. Dette vil ha betydning når informasjonsvirkemidler skal velges. Spesielt når det gjelder en tjeneste som World Wide Web, må det skilles mellom krav til eksternt rettede informasjonsleverandører, som eventuelt kan pålegges ulike krav i forhold til ulike målgrupper og som for deler av informasjonsarbeidet må ta hensyn til publikums utstyrsnivå, og krav til interne informasjonsbrukere, som eventuelt kan ha andre løsninger enn de man kan vente å finne hos publikum.

5.3.2. SGML, XML og HTML

Standard General Markup Language [SGML] er gjeldende ISO-standard for dokumentbeskrivelse. SGML brukes til å definere dokumenttyper ved en Document Type Definition (DTD) og gir grunnlag for en medieuavhengig dokumentproduksjon. HyperText Markup Language [HTML], som benyttes for å beskrive dokumenter som utveksles over WWW, er en slik DTD-definert dokumenttype. Nettlesere basert på SGML skal i prinsippet kunne tolke og presentere et vilkårlig SGML-dokument dersom dets DTD er kjent, altså også et HTML-dokument. Men for tiden vil nettlesere for WWW vanligvis tolke HTML-dokumenter direkte, uten å gå via en DTD og uten å benytte generell SGML.

SGML er et krevende beskrivelsesspråk som inneholder elementer som er lite i bruk og vanskelig å implementere. Et nytt beskrivelsesspråk, eXtensible Markup Language ([XML] 1.0, W3C Recommendation (februar 1998)), antas å ville erstatte SGML i WWW-sammenheng og bli det nye grunnlaget både for definisjonen av HTML og for nettlesere som tolker XML for andre dokumenttyper. XML definerer et subsett av SGML som antas å få større utbredelse enn full SGML. Men SGML vil fortsatt være i bruk i enkelte sammenhenger.

I tilknytning til XML-standardiseringen har W3C også fremmet et sett med standarder for dokumentstiler (Cascading Style Sheets, CSS-1 og påbygningen CSS-2 (W3C Recommendations januar 1999 og mai 1998) og videreføringen eXtensible Style

Language, XSL (W3C Working Draft December 1998)) og for håndtering av dynamikk i Web-presentasjoner (Document Object Model, DOM (W3C Recommendation October 1998)). XSL har som uttrykt målsetting å tilby formattering minst på nivå med CSS 1 og 2.

De fleste nettlesere som brukes i dag, er basert på HTML versjon 3.2, men HTML versjon 4.0 er implementert i de nyeste produktene fra markedslederne innenfor dette området, og versjon 4.0 ventes å overta etter hvert. Inntil videre vil nettlesere for XML være lite utbredt. Derimot må en vente at XML vil bli tatt i bruk for å beskrivelse nye dokumenttyper (en rekke XML-definerte DTD-er foreligger allerede), og at dokumenter som skal utveksles over WWW i stigende grad vil baseres på slike DTD-er.

Både de viktigste nettleserprodusentene og W3C har lagt vekt på bakoverkompatibilitet ved videreutviklingen av HTML. Det betyr at nettlesere for HTML 4.0 også vil kunne tolke HTML 3.2, og at XML-baserte nettlesere vil kunne presentere de fleste dokumenter beskrevet i HTML.

5.3.2.1. Skript

Den vanligste teknologien for tjenerside programskript baserer seg på Common Gateway Interface versjon 1.1 [CGI/1.1]. CGI/1.1 er hittil ikke nedfelt i en RFC, men en Internet Draft som dokumenterer gjeldende konvensjoner foreligger. Denne spesifiserer bl.a. hvordan CGI-parametre kodes og formidles fra klient til tjener, og grensesnittet for tjenerens kall av det aktuelle programskriptet. En CGI/1.2 er under utforming, men det er uklart når denne vil foreligge.

For nettleserside programvare (klientskript, applet) anbefaler WSP bruk av ECMA Standard 262 (juni 1998) [ECMA262], som definerer språket ECMAScript. ECMAScript baserer seg i hovedsak på de rådende klientskript-språkene (JavaScript og JScript) og oppfattes for alle praktiske formål som en standard for JavaScript.

5.3.3. Generelle krav til WWW

Fordi utviklingen innenfor WWW går så raskt, spesifiserer NOSIP et begrenset sett med minimumskrav til Web-basert informasjonstjeneste. Kravene er splittet i generelle krav og spesifikke krav til informasjonsleverandør (nett-tjener, se avsnitt 5.3.4) og informasjonsmottaker (nettleser, se avsnitt 5.3.5).

Det er et obligatorisk krav (O) at HTTP/1.1 [RFC2616] utvekslingsprotokoll benyttes mellom WWW klient og tjener.

Dersom tjenerside programskript tilbys, er det et betinget interimskrav (B og I) at Common Gateway Interface versjon 1.1 [CGI/1.1] følges.

For Web-basert informasjonstjeneste som krever sikker oppkobling og overføring, er det et betinget krav (B) at Secure Socket Layer SSL v3.0 [SSL] benyttes. Det er et langsiktig krav (L) at Transport Layer Security [TLS] brukes.

Krav	Kategori	Kommentar	Henvisning
RFC 2616, Hypertext Transfer Protocol HTTP/1.1	O		5.3.3
CGI/1.1, Common Gateway Interface	B, I	Hvis tjenerside programskript tilbys	5.3.2.1 og 5.3.3
SSL v3.0, Secure Sockets Layer, version 3	B	Obligatorisk når sikkerhet kreves	3.10.3
TLS, Transport Layer Security	L		3.10.3

5.3.4. Krav til informasjonsleverandører

En tilpasning til installert base for nettlesere tilsier en pragmatisk formulering av krav til statlige informasjonsleverandører knyttet til utsagn av typen "Statlige informasjonsleverandører skal bruke formater, overføringsprotokoller, hyperlenker m.m. som støttes av nest siste versjon av de tre mest utbredte nettleserne på det norske marked." Utviklingen går likevel så fort at "nest siste versjon" raskt blir lite presist.

I nærmeste framtid vil utstyr hos informasjonsbrukerne best støttes dersom offentlige informasjonsleverandører følger disse NOSIP-krav:

- Det er et obligatorisk krav (O) at dokumenter følger [HTML 3.2] og benytter [MIME]
- Det er et langsiktig krav (L) at dokumenter følger [HTML 4.0]
- Det er et langsiktig krav (L) at dokumenter følger XML 1.0 [XML]
- Det er et interimskrav (I) at Cascading Style Sheets CSS 1 [CSS1] og CSS 2 [CSS2] følges
- Det er et langsiktig krav (L) at [XSL], [DOM] og ECMAScript [ECMA262] følges

Krav	Kategori	Kommentar	Henvisning
HyperText Markup Language, HTML 3.2	O		5.3.2
HyperText Markup Language, HTML 4.0	L		5.3.2
eXtensible Markup Language, XML 1.0	L		5.3.2
Cascading Style Sheets, CSS 1 og CSS 2	I		5.3.2
eXtensible Style Language, XSL	L		5.3.2
Document Object Model, DOM	L		5.3.2
ECMA Standard 262, ECMAScript	L		5.3.2.1

5.3.5. Krav til informasjonsmottakere (nettlesere)

Det er et obligatorisk krav (O) at nettlesere kan presentere dokumenter som følger [HTML 4.0] og [MIME].

Det er et betinget krav (B) at nettlesere som brukes i SGML dokumentutveksling, følger kravene til [SGML] som angitt i avsnitt 4.2.

Det er et langsiktig krav (L) at nettlesere kan presentere dokumenter beskrevet ved [XML] versjon 1.0 og CSS 1 [CSS1] og CSS 2 [CSS2].

Det er et langsiktig krav (L) at [XSL], [DOM] og ECMAscript [ECMA262] følges.

Krav	Kategori	Kommentar	Henvisning
HyperText Markup Language, HTML 4.0	O		5.3.2
Standard General Markup Language, SGML	B	Obligatorisk når funksjonaliteten kreves	4.2
eXtensible Markup Language, XML 1.0	L		5.3.2
Cascading Style Sheets, CSS 1 og CSS 2	L		5.3.2
eXtensible Style Language, XSL	L		5.3.2
Document Object Model, DOM	L		5.3.2
ECMA Standard 262, ECMAscript	L		5.3.2.1

5.3.6. Lenker

Uniform Resource Locators [URL] er hovedgrunnlaget for å adressere ressurser på WWW. Hovedelementene i en URL er *protokoll* (f.eks. HTTP, LDAP, FTP), *tjener* (f.eks. odin.dep.no), *katalog* og *filnavn* (f.eks. aad/publ/publ.html).

Gjeldende standard for adressering ved hjelp av URL er gitt i Uniform Resource Identifiers [RFC2396].

Det er et obligatorisk krav (O) at adressering følger Uniform Resource Locators (URL, RFC 2396).

Det er et obligatorisk krav (O) at URL-protokollene HTTP og FTP kan behandles. HTTP URL er definert i RFC 2616; FTP URL er definert i RFC 1738.

I forbindelse med katalogsystemer er det et betinget krav (B) at URL-protokoll LDAP versjon 3 [LDAPv3] (se avsnitt 5.3) følges.

Krav	Kategori	Kommentar	Henvisning
RFC 1738, 1808, Uniform Resource Locators, URL	O		5.3.6
HTTP, FTP	O		5.3.6
RFC 2251–2256, Lightweight Directory Access Protocol, LDAPv3	B	Obligatorisk ved bruk av kataloger	5.4.2
RFC 2396, Uniform Resource Identifiers, URI	O		5.3.6

5.4. Kataloger

Katalogstøtte er et fundamentalt krav for kommunikasjonstjenester, både for mennesker og datamaskiner. Mennesker bruker kataloger for å finne eksempelvis telefonnummer og boligadresser (hvite sider), eller søke etter tjenesteleverandører (gule sider). Datasystemer benytter kataloger for å finne nettverksadresser og ruteinformasjon, distribuere e-post og hente fram maskinadresser m.m. på basis av mer brukervennlig navngiving. Spesielt i forbindelse med den økende bruk av elektronisk post på tvers av organisasjonsmessige skillelinjer, er samordnede katalogsystemer en nødvendighet.

Kataloger blir også stadig viktigere for å finne fram til tjenester og informasjon i nettverk. I store nettverk vil det nesten være umulig å finne de ønskede tjenestene, personene eller informasjonen uten bruk av kataloger.

I den senere tid er det kommet flere konkurrerende forslag til katalogstandarder, i tillegg til de som allerede finnes. Et felles

trekk med alle disse katalogene er at de benytter LDAP som aksessprotokoll.

Med den nye usikkerheten som er kommet inn i hvilken standard som blir den foretrukne når det gjelder å implementere katalogtjenester, vil ikke denne versjonen av NOSIP stille obligatoriske krav til hvordan en katalog skal implementeres. NOSIP stiller derimot obligatoriske krav til hvordan en katalog skal kunne aksesseres. Det vil si at alle som skal tilby katalogtjenester, må tilby et LDAP grensesnitt mot katalogen.

NOSIP spesifiserer hvordan katalogtjenester kan implementeres basert på X.500-standarden. Dette er kun anbefalinger. Kravene om bruk av LDAP er derimot obligatoriske krav. I de neste kapitlene beskrives X.500 standarden og generelle katalogbegreper samt sammenhengen mellom LDAP og X.500.

5.4.1. Katalogstandarden X.500

Katalogstandarden X.500 [X.500] [ISO/IEC 9594] (The Directory) ble først definert i 1988. Definisjonen inneholder følgende hovedkomponenter:

- DIB: Directory Information Base, samlingen av informasjon i katalogsystemet
- DIT: Directory Information Tree, samlingen av informasjon i katalogsystemet, organisert som et tre
- DUA: Directory User Agent, en applikasjonsprosess (klient) som gir brukere av kataloginformasjonen adgang til katalogtjenesten
- DSA: Directory System Agent, en applikasjonsprosess (tjener) som holder en del av katalogen og gir katalogtjenester til en DUA, enten alene eller sammen med andre DSA-er
- DAP: Directory Access Protocol, den kommunikasjonsprotokollen som benyttes mellom en DUA og en DSA
- DSP: Directory System Protocol, den kommunikasjonsprotokollen som benyttes mellom samarbeidende DSA-er

I X.500-standarden skilles det mellom sentraliserte og distribuerte katalogtjenester. En sentralisert katalog er basert på en DSA som ikke har kjennskap til andre DSA-er. En distribuert katalog har mer enn én DSA, som hver inneholder en del av DIB. Dersom en skal søke på tvers av enkeltorganisasjoners kataloger, må en ha en form for koordinering mellom dem. Det er viktig å sikre unike navn til brukeridentifikasjon (bl.a. for meldingsformidling) og for X.509-sertifikater (se kapittel 3 om X.509 og Sikkerhet).

5.4.2. LDAP, X.500 og TCP/IP

Lightweight Directory Access Protocol (LDAP) ble lansert i 1993 som et tekstbasert alternativ for X.500-katalogaksess over TCP/IP. LDAP forenkler kommunikasjonen mellom en DUA og en DSA og åpner for en enklere løsning for tilpasning av applikasjonsklienter som trenger aksess til X.500-kataloger. LDAP versjon 2 [LDAPv2] er beskrevet i [RFC1777] og en LDAPv2 API i [RFC1823]. LDAP versjon 3 [LDAPv3] er definert i [RFC2251–2256]. LDAPv2 fungererer best som en ren leseprotokoll, mens LDAPv3 også inneholder funksjoner for katalogoppdatering og henvisning (referering). LDAPv2 gir problemer i forbindelse med tegnsett, siden det tegnsettet som X.500-standarden foreskriver [ITU-T T.61], ikke representeter æøåÆÅØ på samme måte som de vanligste LDAP-implementasjonene [ISO/IEC 8859-1]. LDAPv3 løser problemet ved å gå over til [UNICODE] med overføringskoding etter [UTF-8]. LDAPv3 inneholder dessuten sikkerhetselementer, den støtter sterk autentisering og tilbyr dette sammen med krypterte forbindelser gjennom bruk av [TLS].

LDAPv3 er i ferd med å bli bindeleddet mellom ulike kataloger (både X.500-kataloger, industristandardløsninger og proprietære) og implementasjoner av LDAPv2 og LDAPv3 er tilgjengelige og i bruk i ulike katalogsammenhenger. LDAP er tatt i bruk i en rekke applikasjoner og produkter fra sentrale internettleverandører (nettlesere, ulike hvite og gule sider og adressekataloger). Oversetter (portner) fra LDAP til ordinær X.500 DAP foreligger og er i bruk. Katalogsystemer med direkte LDAP-aksess, både X.500-baserte systemer og proprietære katalogsystemer, er også vanlig. I noen kretser oppfattes LDAP som en brukervennlig enkel løsning som styrker og bidrar til spredning og utnyttelse av X.500-systemer. Andre ser LDAP som en potensiell trussel mot X.500, de ser for seg at systemer basert på andre teknologier enn X.500, men med LDAP som aksessprotokoll, vil trenge X.500 til side. Det er viktig i denne sammenhengen å påpeke at slike rene LDAP-kataloger i dag ikke gir samme koordineringsmulighet mellom kataloger og mulighet for distribuert oppdatering som X.500.

5.4.3. Krav til aksess av kataloger

Følgende krav gjelder for enheter som ønsker å tilby katalogtjenester til andre:

- Det er et obligatorisk krav (O) at applikasjoner som bruker katalogsystemer eller tilbyr katalogtjeneste, støtter LDAPv2.
- Det er et langsiktig krav at applikasjoner som bruker katalogsystemer eller tilbyr katalogtjeneste, støtter LDAPv3.

- Det er et interimkrav at et katalogsystem (DSA) tilbyr støtte for LDAPv2.
- Det er et langsiktig krav at et katalogsystem (DSA) tilbyr støtte for LDAPv3.

Krav	Kategori	Kommentar	Henvisning
LDAP v2	O	Systemer som tilbyr eller bruker katalogtjenester, skal støtte LDAP v2	
LDAP v3	L	Systemer som tilbyr eller bruker katalogtjenester, skal støtte LDAP v3	

5.5. Terminalstøtte

Skjermorientert programvare kan ha behov for ulike funksjoner som navigerer i skjermbildet, og som styrer utlegget av skjermen på en alfanumerisk terminal. Utbredelsen av delte applikasjoner, klient-tjener-løsninger, har redusert behovet for tjenester som krever slik terminalstøtte. I dag er utbredelsen av alfanumeriske terminaler i stor grad erstattet av applikasjoner som tilbyr:

- oppkobling mot fjern maskin via nettverk
- støtte for ulike terminaltyper

NOSIP stiller følgende krav i forbindelse med oppkobling mot fjern maskin:

Oppkobling skal skje i henhold til enhetens sikkerhetspolicy. Dette kan innebære bruk av telnet [RFC 854–855] eller bruk av krypterte tunneler som Secure Shell [SSH].

Krav til terminalstøtte er betinget av applikasjonen på vertsmaskinen. NOSIP stiller ikke eksplisitte krav til terminalstøtte, men forutsetter at det er mulig å anskaffe programvare som støtter de aktuelle terminaltypene som kreves for å bruke applikasjonen, samt benytte en kommunikasjonsform som er i tråd med sikkerhetspolicy.

Krav	Kategori	Kommentar	Henvisning
Oppkobling i henhold til sikkerhetspolicy	O		5.5 og kapittel 3

5.6. Filoverføring

(File Transfer Protocol, [RFC959] oktober 1985) og FTAM (File Transfer, Access, and Management, [ISO/IEC 8571]). FTAM har, som navnet sier, et videre siktemål enn FTP, men er i liten grad i bruk utover anvendelser for enklere rutinemessig overføring av hele filer. FTAM gir mulighet for å gjenta fra sjekkpunkter når brudd oppstår ved overføring av større filer, noe som benyttes i enkelte sammenhenger; denne muligheten finnes også i FTP-protokollen, men er ikke implementert overalt. FTAM er ikke på noen måte i bruk som "distribuert filsystem", slik den til en viss grad faktisk tilbyr.

FTP inneholder ikke sikkerhetselementer utover bruk av passord ved opprettelse av forbindelser. Passordene oversendes i klartekst. Det foreligger en IETF Proposed Standard for sikkerhet ved bruk av FTP, FTP Security Extension [RFC2228], fra oktober 1997, men denne er ikke i alminnelig bruk.

Det er et obligatorisk krav (O) i NOSIP at FTP støttes for filoverføring.

På grunn av FTPs dårlige støtte for sikkerhet anbefales det at en når en bruker FTP, sørger for at:

- Data som skal beskyttes mot innsyn overføres i kryptert form
- Passord som benyttes for slik overføring ikke benyttes til noe annet formål (for eksempel fjerninnlogging)
- Rutiner som logger bruk av FTP-tjenesten og forhindrer misbruk etableres

Dersom hensyn til f.eks. bakoverkompatibilitet gjør det nødvendig, er det et betinget krav (B) at FTAM ISO 8571 1-5 og FTAM standardprofiler ISO/IEC ISP 10607 1-6 [ISO/IEC 10607] følges. I forbindelse med ISP 10607-3, -4 og -5 er det et betinget krav (B) at FTAM dokumenttype FTAM 1–4 og NIST NBS 6–12, samt AOW INTAP-1, støttes. Ved bruk av NOSIP katalogsystem er det et betinget krav (B) at internasjonal standard profil ISO/IEC ISP 11190 (FDI3) benyttes.

Krav	Kategori	Kommentar	Henvisning
RFC 959 File Transfer Protocol	O		5.6
ISO 8571 1–5 (File Transfer, Access, and Management)	B	Ved FTAM	5.6
ISO/IEC ISP 10607 1–6 (FTAM standardprofiler)	B	Ved FTAM	5.6
FTAM 1–4, NIST NBS 6–12, AOW INTAP-1 (FTAM dokumenttyper)	B	Ved FTAM	5.6
ISO/IEC ISP 11190 (FDI3)	B	Obligatorisk for FTAM i forbindelse med NOSIP katalogsystem	5.6

5.7. Elektronisk datautveksling (EDI)

Utbredelsen og utviklingen av Internett-standarder har gjort nye løsninger attraktive også for strukturering, transport og sikring av EDI-utvekslinger. Dels er adhocløsninger basert på Internett-tjenester tatt i bruk, dels arbeides det med standardisering av Internett-teknologi for EDI. Slikt arbeid gjøres blant annet innenfor IETFs arbeidsgruppe EDI over the Internet (ediint) (http://www.ietf.org/html.charters/ediint-charter.html) og i XML/EDI Group (http://www.geocities.com/WallStreet/Floor/5815/). Kravene nedenfor har tatt hensyn til retningen på arbeidet i IETF/ediint.

Det er ønskelig at det i størst mulig grad benyttes samme eller kompatible syntaksversjoner, tegnsett og sikkerhetsløsninger på tvers av f.eks. ulike bæretjenester. NOSIP stiller derfor krav på disse områdene. Kravene nedenfor når det gjelder tegnsett, tegnkoding, formater for krypterte/signerte meldinger og sertifikatformat, er basert på krav i sikkerhets- og formatkapitlene (kapittel 3 og kapittel 4).

Endelige valg for en gitt EDI-løsning må gjøres ut fra en helhetsvurdering i det enkelte tilfellet, der det tas hensyn til foretatte investeringer så vel som forventet utvikling i teknologi, og på det aktuelle anvendelsesområdet. Bruk av utvekslingsavtaler mellom kommunikasjonspartnere er en etablert praksis i EDI, der blant annet slike valg reguleres. Anbefalt bakgrunnsmateriale for vurdering av løsninger er serien "Norsk veiledning i elektronisk handel og administrasjon basert på EDIFACT syntaks 4.0" [EDIPRO] fra Norsk EDIPRO. Første hefte i denne serien forelå som utkast i november 1998, og serien vil foreligge i sin helhet i første kvartal 2000. Serien erstatter tidligere utgaver av "Norsk veiledning i bruk av EDIFACT", som tidligere versjoner av NOSIP har henvist til.

5.7.1. Bæretjenester

På grunn av de store variasjonene i behov og foretatte investeringer, og den raske utviklingen på området, tar NOSIP v3 ikke stilling til valg mellom ulike bæretjenester for EDI. Ved bruk av Internett e-post eller X.400 som kommunikasjonstjeneste skal imidlertid relevante krav i 5.2.1 og 5.2.2 følges. Se også sikkerhetsrelaterte krav i 5.7.3.

Ved bruk av MIME (i PKCS#7-format over X.400, SMTP, HTTP eller andre bæretjenester) skal MIME innholdstype angis i henhold til MIME Encapsulation of EDI objects [RFC1767] (eks: Content-type:application/edifact for EDIFACT meldinger/utvekslinger).

5.7.2. Syntaks

Tradisjonell EDIFACT syntaks forventes å spille en rolle i overskuelig framtid, spesielt når det gjelder etablerte meldingsdefinisjoner, kataloger og kodeverk. NOSIP tar hensyn til dette ved å sette krav til versjoner og bruk av tegnsett (syntaksnivåer) for EDIFACT syntaks. Det antas at andre formater vil bli tatt i bruk i tiden framover, og NOSIP skal ikke være til hinder for dette. Arbeidet med f.eks. XML/EDI er imidlertid ikke kommet langt nok til at det i NOSIP kan stilles krav til XML-baserte løsninger.

Ved bruk av EDIFACT meldingssyntaks er støtte for batch syntaksregler versjon 4 [ISO 9735-1, ISO 9735-2] samt meldingstypen CONTRL [ISO 9735-4] og assosierte data [ISO 9735-8] obligatoriske krav. Det er videre et obligatorisk krav at meldinger kan mottas og genereres i henhold til EDIFACT syntaks versjon 1, 2 og 3 (bakoverkompatibilitet).

Støtte for EDIFACT syntaksnivå UNOC [ISO/IEC 8859-1] er et obligatorisk krav. Ved behov for utveksling av samiske tegn er støtte for EDIFACT syntaksnivå UNOH [ISO/IEC 8859-4] betinget interimskrav. For å oppnå full støtte for samiske tegn (og generelt språk som ikke dekkes av ISO 8859-1) antas det imidlertid at EDIFACT syntaksnivå UNOY [ISO/IEC 10646-1] må tas i bruk, og dette er derfor et langsiktig krav.

Det gjøres oppmerksom på at koder for valg av tegnkoding ved bruk av EDIFACT syntaksnivå UNOY i dag mangler for EDIFACT versjon 4. Implementasjoner bør her rette seg etter generelle krav i 4.1 og praksis på området. I mangel av andre spesifikasjoner anbefaler NOSIP følgende praksis:

Ved bruk av syntaksnivå UNOY foretrekkes tegnkoding UTF-8. Dersom nærmere spesifikasjon av tegnkoding mangler, skal mottaker av en EDIFACT-utveksling med angitt syntaksnivå UNOY anta UTF-8-koding. Ved mottak av syntaksnivå UNOY må

mottaker kontrollere at utvekslingen faktisk bare inneholder tegn i den delmengden som applikasjonen er i stand til å behandle. Er dette ikke tilfelle, må utvekslingen feilmeldes som syntaktisk ugyldig.

5.7.3. Sikkerhet

I mange tilfeller vil det være behov for sikkerhetstiltak ved elektronisk datautveksling. NOSIP stiller betinget krav om sikring på bæretjenestenivå i henhold til standard mekanismer og formater for meldingssikkerhet basert på offentlig nøkkelkryptografi som definert i kapittel 3.

EDIFACT versjon 4 angir egne mekanismer for ivaretakelse av sikkerhetsrelaterte behov for EDIFACT. I enkelte tilfeller kan det være behov for sikkerhetstiltak på dette nivået fremfor på bæretjenestenivå. Disse delene av EDIFACT versjon 4 har imidlertid i skrivende stund ikke status som internasjonal standard, og NOSIP stiller ikke spesielle krav til sikkerhet på EDIFACT-nivå.

Ved behov for digitale signaturer og/eller kryptering for meldingssikkerhet på bæretjenestenivå er det et betinget krav at meldingsinnholdet er i MIME-format og formatteres i henhold til PKCS#7, se 3.10.2.

5.7.4. Kravtabell EDI

Kravene gis under forutsetning av at EDIFACT meldigsyntaks er valgt

Krav	Kategori	Kommentar	Henvisning
EDIFACT syntaks			
ISO 9735:1998 (v. 4) del 1, 2, 4 og 8	O	Primærvalg	
ISO 9735, v. 1, 2 og 3	O	Skal kunne behandles	
UNOC, ISO 8859-1	O		4.1.1
UNOH, ISO 8859-4	B, I	Noen samiske tegn	4.1.1
UNOY, ISO 10646-1	L	Alle relevante tegn	4.1.1
RFC 1767	B	Ved bruk av MIME	4.3
PKCS#7	B	For meldingssikkerhet på bæretjenestenivå	3.10.2

5.8. Diverse

5.8.1. Kalender- og planleggingssystemer

En IETF-arbeidsgruppe har levert en Internet-Draft for definering av protokoll og informasjonsenheter knyttet til distribuert møtekalender og planlegging. Det foreligger også Standards Track dokument for Internet Calendaring and Scheduling Core Object Specification [RFC2445] og for iCalendar Transport-Independent Interoperability Protocol (iTIP) [RFC 2446] og iCalendar Message-based Interoperability Protocol (iMIP) [RFC 2447].

Det er et betinget krav at enheter som ønsker å ta i bruk opplegg for kalender- og planleggingssystemer, kontakter Statskonsult for veiledning og anbefalinger i tilknytning til valg av løsning.

5.8.2. Konferansesystemer, datastøttet samarbeid

Bruk av systemer for sanntidskonferanser har fått en økende oppmerksomhet de siste årene. Sanntidskonferanser har et stort potensiale for å effektivisere kommunikasjonen både innad i forvaltningen og ut mot publikum. Innenfor dette feltet finnes det mange ulike systemer med forskjellige anvendelsesområder og ambisjonsnivå. Løsningene spenner fra enkle tekstbaserte løsninger, slik som IRC [RFC1459], til integrerte multimedialøsninger med støtte for video- og datakonferanser.

5.8.2.1. Tekstbaserte konferansesystemer

Enkle tekstbaserte konferansesystemer kan være et effektivt kommunikasjonsmedium i enkelte sammenhenger hvor det ikke kreves høy grad av interaktivitet i kommunikasjonen. For denne type kommunikasjon anbefaler NOSIP IRC [RFC1459].

Merk at IRC ikke inneholder mekanismer for sikker identifikasjon av samtalepartnere eller sikring av trafikk mot innsyn; sikkerhet må derfor sikres på implementasjonsavhengige måter dersom det overhodet stilles sikkerhetskrav når IRC benyttes.

5.8.2.2. Multimedia konferansesystemer

Multimedia konferansesystemer lar deltakere i en konferanse kommunisere over ulike kanaler som benytter ulike medier. Eksempler på ulike kommunikasjonskanaler er i denne sammenhengen video, applikasjonsdeling og lyd. Standardiseringsarbeidet på dette området har til dels foregått i telekommunikasjonsmiljøet (ITU standardene [ITU-T T.120] og [ITU-T H.323])

og til dels i Internett-miljøet (SIP, [RFC2543]). Dette har medført at det har vokst opp ulike standarder med den samme grunnleggende funksjonalitet og stort sett de samme tjenestene. Vi vil i resten av dette avsnittet gi en kort oversikt over de tre mest aktuelle standardene i denne sammenhengen.

H.323

H.323 er den internasjonale teleunionens (ITUs) standard for audiovisuell kommunikasjon over IP-baserte nettverk. H.323-standarden er en del av en serie av kommunikasjonsstandarder som muliggjør videokonferanser over ulike typer nettverk. Denne serien, kalt H.32X, inneholder bl.a. H.320 og H.324, som adresserer videokonferanser over henholdsvis ISDN og PSTN nettverk. Målsettingen med bruk av H.323 er at produkter og anvendelser fra ulike leverandører kan kommunisere med hverandre, og flere av de store leverandørene har annonsert at de vil gi støtte for denne protokollen i sine produkter.

H.323 tilbyr primært funksjonalitet for multipunkt videokonferanser. I tillegg til de audiovisuelle kanalene for video og lyd har H.323 anvist en plass til T.120-serien for datakommunikasjon innenfor standarden.

T.120

T.120 inneholder en serie av kommunikasjons- og applikasjonsprotokoller og tjenester som støtter sanntids multipunkts datakommunikasjon. Denne funksjonaliteten er viktige byggeklosser i en mengde anvendelser som for eksempel applikasjonsdeling og andre typer flerbrukerprogrammer

SIP (Session Initiation Protocol)

I flere år har programvare for videokonferanser over Internett eksistert. Så lenge båndbredde og kvalitet er tilstrekkelig til stede, gjør økonomi dette langt å foretrekke framfor telefonbaserte videokonferanseløsninger. Det finnes imidlertid ikke noen protokoll for å "ringe", dvs. få tak i samtale-/konferansepartnere som ikke vet at du vil snakke med dem. SIP [RFC 2543] er laget for å fylle dette gapet.

Et av målene for SIP-protokollen har vært en enkel protokoll det er lett å implementere, og som gir raskere oppkoblingstid enn konkurrenten H.323. SIP er laget så lik HTTP-protokollen for WWW som mulig, men den spør om kontakt med multimedieapplikasjoner, ikke filer på en disk. Flere avsnitt i spesifikasjonen henviser bare til hvordan problemet er løst i HTTP/1.1.

Et viktig problem ved videokonferanser er forhandlinger om hvilke medier og hvilke formater for komprimering av lyd og bil-

de som skal benyttes. I IETFs arbeid er det satt av plass i SIP-standarden til meldinger om partenes preferanser, men selve formatet på medie- og formatspesifikasjonene er definert i en egen standard kalt SDP (Session Description Protocol, [RFC2327]). Denne er eldre enn SIP, og laget for å kunne brukes sammen med Session Announcement Protocol (SAP, ikke ferdig) for å annonsere eksistensen av multimediesesjoner det er mulig å ta imot (omtrent som TV-kanaler).

NOSIP har i dette avsnittet presentert tre serier av standarder som tilrettelegger for sanntids multipunkts multimediakonferanser. To av seriene, T.120 og H.323, er utviklet av ITU. H.323 og T.120 er åpne standarder som støttes opp om og leveres av mange tunge aktører innenfor telekommunikasjonsindustrien. Disse aktørene har antakelig den tilstrekkelige tyngden i markedet som skal til for at T120 og H.323 skal bli etablerte og utbredte standarder. Likevel vil SIP-standarden, som også er en åpen standard fra IETF, medføre en stor usikkerhetsfaktor som gjør at det er for tidlig å velge den ene fremfor den andre.

Det er et betinget krav at enheter som ønsker å ta i bruk opplegg for konferansesystemer eller datastøttet samarbeid gjennom dokumentutveksling, kontakter Statskonsult for veiledning og anbefalinger i tilknytning til valg av løsning.

5.8.3. Gruppe-editering

Til nå brukes WWW vesentlig for publisering, dvs. for distribusjon av informasjon. Nettlesere er i hovedsak *lesere*. [RFC 2518] definerer protokoll og informasjonsenheter knyttet til distribuert samarbeid om redigering og versjonskontroll for Web-dokumenter (WWW Distributed Authoring and Versioning, WebDAV). Denne er utarbeidet i samarbeid med W3C. Arbeidet innebærer delvis utvidelser av HTTP/1.1 som bl.a. åpner for oppdatering av dokumenter, versjonskontroll og dokumentsøkemuligheter.

Det er et betinget krav at enheter som ønsker å ta i bruk opplegg for distribuert dokumentredigering, kontakter Statskonsult for veiledning og anbefalinger i tilknytning til valg av løsning.

Krav	Kategori	Kommentar	Henvisning
Kalendersystem	B	Standardisering pågår, Statskonsult kontaktes før valg av system	5.8.1
Konferansesystem	B	Standardisering pågår, Statskonsult kontaktes før valg av system	5.8.2
Gruppeeditering	B	Standardisering pågår, Statskonsult kontaktes før valg av system	5.8.3
Gruppeeditering	L	WEBDAV [RFC 2518]	5.8.3

VEDLEGG A:

Forkortelser

ACL	Access Control List
ACSE	Association Control Service Element
AMH	X.400 profil
ANSI	American National Standards Institute
AOW	Asia and Oceania Workshop on open systems (ISO profiler)
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
BER	Basic Encoding Rules (for ASN.1)
BMP	Basic Multilingual Plane (ISO 10646-1)
BS	British Standard
CEN	European Committee for Standardization
CGI	Common Gateway Interface
CM	Common Messaging (X.400)
CRL	Certificate Revocation List (X.509)
CSS	Cascading Style Sheets (W3C)
DAP	Directory Access Protocol (X.500)
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIB	Directory Information Base (X.500)
DIS	Draft International Standard (ISO)
DISP	Directory Information Shadow Protocol (X.500)
DIT	Directory Information Tree (X.500)
DN	Distinguished Name (X.500)
DNS	Domain Name System
DOM	Document Object Model (W3C)
DOP	Directory Operational binding Protocol (X.500)
DSA	Directory System Agent (X.500)
DSN	Delivery Service Notification

DSP	Directory System Protocol (X.500)
DTD	Document Type Definition (SGML)
DUA	Directory User Agent (X.500)
ECMA	European Computer Manufacturers Association
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
ESMTP	Extended Simple Mail Transfer Protocol
ETSI	European Telecommunications Standards Institute
EWOS	European Workshop on Open Systems (ISO profiler)
FO/S	Forsvarets Overkommando/Sikkerhetsstaben
FTAM	File Transfer And Management (ISO)
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Committee
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPM	Inter-Personal Messaging (X.400)
IPSec	IP Security
IS	International Standard (ISO)
ISO	International organization for standardization
ISP	International Standard Profile (ISO etc.)
ISP	Internet Service Provider
ISSS	Information Society Standardization System (CEN/ISSS)
ITU	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MCGAM	MIXER Conformant Global Address Mapping
MD5	Message Digest 5 (hash-algoritme)
MHS	Message Handling System (ISO)
MIME	Multipurpose Internet Mail Extensions
MIXER	MIME Internet X.400 Enhanced Relay
MS	Message Store (X.400)
MTA	Message Transfer Agent (X.400)
NAT	Network Address Translator
NIST	National Institute of Standards and Technology (USA)
NIX	Norwegian Internet eXchange
NNTP	Network News Transfer Protocol
NOARK	Norsk Arkivstandard

NOSIP Norsk OSI Profil
NORBÅS Norsk Rammeverk for Bruk av Åpne Systemer i forvaltningen
NTP Network Time Protocol
OSI Open Systems Interconnection
PDF Portable Data Format
PICS Protocol Implementation Conformance Statement (ISO)
PKCS Public Key Cryptography Specifications
POP Post Office Protocol
RC2, RC4, RC5 Symmetriske kryptoalgoritmer
RFC Request For Comments
ROSE Remote Operations Service Element (ISO)
RSA Rivest Shamir Adleman (off. nøkkel kryptoalgoritme)
RTSE Reliable Transfer Service Element (ISO)
SGML Standard Generalised Markup Language
SGK Statens Generelle Kravspesifikasjon
SHA-1 Secure Hash Algorithm number 1
SIP Session Initiation Protocol
S/MIME Secure/MIME
SMTP Simple Mail Transfer Protocol
SNMP Simple Network Management Protocol
SSH Secure Shell
SSL Secure Sockets Layer
TBF Tre Bokstavers Forkortelse
TCP Transmission Control Protocol
TIFF Tag Image File Format
TLS Transport Layer Security
TTP Tiltrodd Tredje-Part
UA Session Initiation Protocol
UCS Universal Character Set
UDP User Datagram Protocol
UNICODE Kosortium for tegnsett
UNOC, UNOH, UNOY EDIFACT syntaksnivåer
URL Uniform Resource Locator
UTF UCS Transformation Format
VPN Virtuelt Privat Nettverk
VT Virtual Terminal (ISO)
W3C World Wide Web Consortium
WWW World Wide Web
XML eXtensible Markup Language
XSL eXstensible Style Language (W3C)

VEDLEGG B:

Referanser

[ANSI X9.30] Public Key Cryptography for the Financial Services Industry – Part 2: The Secure Hash Algorithm (SHA-1), ANSI X9.30.2, 1997

[ANSI X9.52] Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52, 1998

[B-INST] Instruks for behandling av informasjon som trenger beskyttelse av andre grunner enn de som er nevnt i Sikkerhetsinstruksen (Beskyttelsesinstruksen), Statens Fellesblankett X-0076, juni 1990

[BS 7799] British Standard 7799: 1998 "A code of practice for information security management"

[CC] Common Criteria version 2.0/ISO FDIS 15408

[CEN-LDAP] LDAP V3: Level of Support of an LDAP, draft 5, CEN/ISSS Directory Workshop, mai 1998

[CGI/1.1] Se http://hoohoo.ncsa.uiuc.edu/cgi/, korrekt URL pr. 17.2.1999

[CSS1] Cascading Style Sheets version 1 (CSS-1), W3C Recommendation, desember 1996, revidert januar 1999

[CSS2] Cascading Style Sheets version 2 (CSS-2), W3C Recommendation, mai 1998

[D-DIR] Direktiv for sikring av datasystemer gradert etter Sikkerhetsinstruksen eller Beskyttelsesinstruksen (Datasikkerhetsdirektivet), Statens Fellesblankett X-0078 B, oktober 1997

[DES] Data Encryption Standard definert i X9.32 eller i (FIPS) 46-1

[DOM]	Document Object Model (DOM), W3C Recommendation oktober 1998
[ECMA262]	ECMAScript Language Specification, Standard ECMA-262, 2nd edition, juni 1998
[EDIPRO]	Norsk veiledning i elektronisk handel og administrasjon basert på EDIFACT syntaks 4.0, Norsk EDIPRO, del 1 desember 1998
[FTAM]	Se [ISO/IEC 8571]
[HTML 2.0]	Se [RFC1866]
[HTML 3.2]	HyperText Markup Language, version 3.2, W3C Recommendation, januar 1997
[HTML 4.0]	HyperText Markup Language, version 4.0, W3C Recommendation, april 1998
[ITSEC]	Information Technology Security Evaluation Criteria ver 1.2 – Juni 1991
[LATIN1]	Se [ISO/IEC 8859-1]
[LATIN4]	Se [ISO/IEC 8859-4]
[LATIN6]	Se [ISO/IEC 8859-10]
[LATIN9]	Se [ISO/IEC 8859-15]
[LDAPv2]	Se [RFC1777] og [RFC1823].
[LDAPv3]	Lightweight Directory Access Protocol, se [RFC2251] – [RFC2256]
[MIME]	Multipurpose Internet Mail Extensions, se [RFC2045] – [RFC2049]
[NIST 180-1]	Secure Hash Standard, NIST FIPS PUB 180-1, mai 1994
[P-VERN]	Lov om personregistre m.m. av 9. juni 1978 nr. 48, med forskrifter
[RITS-1]	Sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner, Rådet for IT-sikkerhet, 13/11 1997
[RITS-2]	Digitale signaturer gir tillit til elektronisk kommunikasjon: Forslag til tiltak for aksept og utbredelse, Rapport med forberedende utredning fra arbeidsgruppe oppnevnt av Nærings- og Handelsdepartementet, avgitt til Rådet for IT-sikkerhet, 30/11 1998
[S-INST]	Instruks for behandling av dokumenter som av sikkerhetsmessige grunner må beskyttes (Sikkerhetsinstruksen), Statens Fellesblankett X-0076, juni 1990
[SSH]	Secure Shell protocol version 2, februar 1999, http://www.ssh.fi/sshprotocols2/

[SSL] Secure Sockets Layer version 3, november 1996, http://www.netscape.com/eng/ssl3/index.html
[TILK] Tilknytning til Internett, Statskonsult veileder, UTGITT AV STATSKONSULT 2000
[UNICODE] The Unicode Standard. Version 2.0. The Unicode Consortium, 1996
[URL] Se [RFC1738] og [RFC1808]
[US-ASCII] Se [ISO/IEC 646]
[UTF-8] Se [RFC2279]
[X.400] Se [ISO/IEC 10021]
[X.500] Se [ISO/IEC 9594]
[XML] eXtensible Markup Language (XML) version 1.0, W3C Recommendation, februar 1998
[XSL] eXtensible Style Language (XSL), W3C Working Draft, april 19989

IETF-referanser:

[RFC 768] User Datagram Protocol
[RFC 791] Internet Protocol, september 1981
[RFC 792] Internet Control Message Protocol
[RFC 793] Transmission Control Protocol, september 1981
[RFC 821] Simple Mail Transfer Protocol, august 1982
[RFC 822] Standard for the Format of ARPA Internet Text Messages, august 1982
[RFC 854] Telnet Protocol Specification, mai 1983
[RFC 855] Telnet Option Specifications, mai 1983
[RFC 919] Broadcasting Internet Datagrams
[RFC 922] Broadcasting Internet datagrams in the presence of subnets
[RFC 950] Internet Standard Subnetting Procedure
[RFC 959] File Transfer Protocol, oktober 1985
[RFC 977] Network News Transfer Protocol, februar 1996
[RFC1006] ISO Transport Service on top of the TCP, mai 1987
[RFC1034] Domain Names – Concept and Facilities, november 1987
[RFC1035] Domain Names – Implementation and Specification, november 1987
[RFC1036] Standard for Interchange of USENET Messages, desember 1987
[RFC1112] Host Extensions for IP Multicasting
[RFC1122] Requirements for Internet Hosts – Communication Layers
[RFC1123] Requirements for Internet Hosts – Application and Support, oktober 1989

[RFC1277] Encoding Network Addresses, november 1991
[RFC1278] A String Encoding of Presentation Address, november 1991
[RFC1321] The MD5 Message-Digest Algorithm, april 1992.
[RFC1328] X.400 1988 to 1984 downgrading, mai 1992
[RFC1411] Telnet Authentication: Kerberos V4, januar 1993
[RFC1412] Telnet Authentication: SPX, januar 1993
[RFC1429] Listserv Distribute Protocol, februar 1993
[RFC1459] Internet Relay Chat Protocol, mai 1993
[RFC1496] Rules for Downgrading Messages from X.400/88 to X.400/84 when MIME content-types are present in the messages, august 1993
[RFC1519] Classless Inter-Domain Routing (CIDR)
[RFC1738] Uniform Resource Locators, desember 1994
[RFC1767] MIME Encapsulation of EDI Objects, mars 1995
[RFC1777] X.500 Lightweight Directory Access Protocol, mars 1995
[RFC1801] X.400-MHS use X.500 to support X.400-MHS Routing, juni 1995
[RFC1808] Relative Uniform Resource Locators, juni 1995
[RFC1812] Requirements for IP Version 4 Routers
[RFC1823] The LDAP Application Program Interface, august 1995
[RFC1866] Hypertext Markup Language – 2.0, november 1995
[RFC1869] SMTP Service Extensions, november 1995
[RFC1891] SMTP Delivery Status Notifications, januar 1996
[RFC1894] An Extensible Message Format for Delivery Status Notifications, januar 1996
[RFC1902] Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), januar 1996
[RFC1903] Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), januar 1996
[RFC1904] Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), januar 1996
[RFC1905] Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), januar 1996
[RFC1906] Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), januar 1996

[RFC1907] Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), januar 1996
[RFC1939] Post Office Protocol, Version 3, mai 1996
[RFC1982] Serial Number Arithmetic, august 1996
[RFC1995] Incremental Zone Transfer in DNS, august 1996
[RFC1996] A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY), august 1996
[RFC2040] The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms, oktober 1996
[RFC2045] Multipurpose Internet Mail Extensions, november 1996
[RFC2046] MIME Media Types, november 1996
[RFC2047] MIME Msg Header Ext for Non-ASCII, november 1996
[RFC2048] MIME Registration Procedures, november 1996
[RFC2049] MIME Conformance Criteria, november 1996
[RFC2060] Internet Message Access Protocol v4rev1, desember 1996
[RFC2068] Hypertext Transfer Protocol – HTTP/1.1, januar 1997
[RFC2131] Dynamic Host Configuration Protocol, mars 1997
[RFC2136] Dynamic Updates in the Domain Name System (DNS UPDATE), april 1997
[RFC2156] Mime Internet X.400 Enhanced Relay, januar 1998
[RFC2156] MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME, januar 1998
[RFC2157] Mapping between X.400 and RFC-822/MIME, januar 1998
[RFC2157] Mapping between X.400 and RFC-822/MIME Message Bodies, januar 1998
[RFC2158] X.400 Image Body Parts, januar 1998
[RFC2159] A MIME Body Part for FAX, januar 1998
[RFC2160] Carrying PostScript in X.400 and MIME, januar 1998
[RFC2163] Using DNS to Distribute MCGAM, januar 1998
[RFC2163] Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM), januar 1998
[RFC2164] X.500/LDAP Directory/MIXER Address Map, januar 1998
[RFC2164] Use of an X.500/LDAP Directory to support MIXER address mapping, januar 1998

[RFC2181] Clarifications to the DNS Specification, juli 1997
[RFC2228] FTP Security Extensions, oktober 1997
[RFC2246] The TLS Protocol Version 1.0, januar 1999
[RFC2249] Mail Monitoring MIB, januar 1998
[RFC2251] Lightweight Directory Access Protocol (v3), desember 1997
[RFC2252] LDAPv3: Attribute Syntax Definitions, desember 1997
[RFC2253] LDAPv3: UTF-8 String Rep, desember 1997
[RFC2255] LDAP URL Format, desember 1997
[RFC2256] Summary of the X.500(96) with LDAPv3, desember 1997
[RFC2279] UTF-8, a Transformation Format of ISO 10646, januar 1998
[RFC2291] Requirements for a Distributed Authoring and Versioning Protocol for the World Wide Web, februar 1998
[RFC2293] Tables and Subtrees in X.500, mars 1998
[RFC2294] O/R Address hierarchy in X.500, mars 1998
[RFC2298] An Extensible Message Format for Message Disposition Notifications, mars 1998
[RFC2308] Negative Caching of DNS Queries (DNS NCACHE)
[RFC2311] S/MIME Version 2 Message Specification, mars 1998
[RFC2312] S/MIME Version 2 Certificate Handling, mars 1998
[RFC2315] PKCS#7: Cryptographic Message Syntax Version 1.5, mars 1998
[RFC2327] Session Description Protocol, april 1998
[RFC2355] TN3270 Enhancements, juni 1998
[RFC2369] The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields, juli 1998
[RFC2396] Uniform Resource Identifiers (URI): Generic Syntax, august 1998
[RFC2401] Security Architecture for IP, november 1998
[RFC2402] IP Authentication Header, november 1998
[RFC2406] IP Encapsulating Security Payload, november 1998
[RFC2437] PKCS#1: RSA Cryptography Specifications Version 2.0, oktober 1998
[RFC2445] Internet Calendaring and Scheduling Core Object Specification, oktober 1998

[RFC2446] iCalendar Transport-Independent Interoperability Protocol (iTIP), oktober 1998
[RFC2447] iCalendar Message-based Interoperability Protocol (iMIP), oktober 1998
[RFC2476] Message Submission, desember 1998
[RFC2535] Domain Name System Security Extensions, mars 1999
[RFC2536] DSA KEYs and SIGs in the Domain Name System (DNS), mars 1999
[RFC2537] RSA/MD5 KEYs and SIGs in the Domain Name System (DNS), mars 1999
[RFC2543] SIP: Session Initiation Protocol, mars 1999
[RFC2554] SMTP Service Extension for Authentication, mars 1999
[RFC2581] TCP Congestion Control
[RFC2616] Hypertext Transfer Protocol – HTTP/1.1, juni 1999
[RFC2630] Cryptographic Message Syntax, juni 1999
[RFC2631] Diffie-Hellman Key Agreement Method, juni 1999
[RFC2632] S/MIME Version 3 Certificate Handling, juni 1999
[RFC2633] S/MIME Version 3 Message Spesification, juni 1999
[RFC2634] Enhanced Security Services for S/MIME, juni 1999

ISO/IEC/ITU-referanser:

[ISO 8879] Information technology – Text and office systems – Standard Generalized Markup Language (SGML), ISO 8879:1986, inkludert Amendment 1:1998
[ISO 9735-1] Electronic data interchange for administration, commerce and transport (EDIFACT) – Application level syntax rules (Syntax version number: 4) – Part 1: Syntax rules common to all parts, together with syntax service directories for each of the parts, ISO 9735-1:1998
[ISO 9735-2] Electronic data interchange for administration, commerce and transport (EDIFACT) – Application level syntax rules (Syntax version number: 4) – Part 2: Syntax rules specific to batch EDI, ISO 9735-2:1998

[ISO 9735-4] Electronic data interchange for administration, commerce and transport (EDIFACT) – Application level syntax rules (Syntax version number: 4) – Part 4: Syntax and service report message for batch EDI (message type – CONTRL), ISO 9735-4:1998

[ISO 9735-8] Electronic data interchange for administration, commerce and transport (EDIFACT) – Application level syntax rules (Syntax version number: 4) – Part 8: Associated data in EDI, ISO 9735-8:1998

[ISO/IEC 646] Information technology – ISO 7-bit coded character set for information interchange, ISO/IEC 646:1991

[ISO/IEC 6937] Information technology – Coded graphic character set for text communication – Latin alphabet, ISO/IEC 6937:1994

[ISO/IEC 8072] Information technology – Open Systems Interconnection – Transport Service Definition, ISO/IEC 8072:1996 | ITU-T X.214:1995

[ISO/IEC 8073] Information technology – Open Systems Interconnection – Protocol for Providing the Connection-mode Transport Service, ISO/IEC 8073:1997 | ITU-T X.224:1995

[ISO/IEC 8326] Information technology – Open Systems Interconnection – Session Service Definition, ISO/IEC 8326:1996 | ITU-T X.215:1995

[ISO/IEC 8327-1] Information technology – Open Systems Interconnection – Basic Connection Oriented Session Protocol: Protocol Specification, ISO/IEC 8327-1:1996 | ITU-T X.225:1995

[ISO/IEC 8571] Information processing systems – Open Systems Interconnection – File Transfer, Access and Management
Omfatter følgende ISO/IEC internasjonale standarder:
Part 1: General introduction, ISO 8571-1:1988
Part 2: Virtual Filestore Definition, ISO 8571-2:1988

Part 3: File Service Definition, ISO 8571-3:1988
Part 4: File Protocol Specification, ISO 8571-4:1988
Part 5: Protocol Implementation Conformance Statement Proforma, ISO/IEC 8571-5:1990

[ISO/IEC 8649] Information technology – Open Systems Interconnection – Service Definition for the Association Control Service Element, ISO/IEC 8649:1996 | ITU-T X.217:1995

[ISO/IEC 8650-1] Information technology – Open Systems Interconnection – Connection-oriented Protocol for the Association Control Service Element: Protocol Specification, ISO/IEC 8650-1:1996 | ITU-T X.227:1995

[ISO/IEC 8822] Information technology – Open Systems Interconnection – Presentation Service Definition, ISO/IEC 8822:1994 | ITU-T X.216:1994

[ISO/IEC 8823-1] Information technology – Open Systems Interconnection – Connection Oriented Presentation Protocol: Protocol Specification, ISO/IEC 8823-1:1994 | ITU-T X.226:1994

[ISO/IEC 8824] Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)
Omfatter følgende ISO/IEC-internasjonale standarder:
Abstract Syntax Notation One (ASN.1): Specification of basic notation, ISO/IEC 8824-1:1995 | ITU-T X.680:1997
Abstract Syntax Notation One (ASN.1): Information object specification, ISO/IEC 8824-2:1995 | ITU-T X.681:1997
Abstract Syntax Notation One (ASN.1): Constraint specification, ISO/IEC 8824-3:1995 | ITU-T X.682:1997
Abstract Syntax Notation One (ASN.l): Parameterization of ASN.1 specifications, ISO/IEC 8824-4:1995 | ITU-T X.683:1997

[ISO/IEC 8825-1] Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules

(CER) and Distinguished Encoding Rules (DER), ISO/IEC 8825-1:1995 | ITU-T X.690:1997

[ISO/IEC 8859-1] Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1, ISO/IEC 8859-1:1998

[ISO/IEC 8859-10] Information technology – 8-bit single-byte coded graphic character sets – Part 10: Latin alphabet No. 6, ISO/IEC 8859-10:1998

[ISO/IEC 8859-15] Information technology – 8-bit single-byte coded graphic character sets – Part 15: Latin alphabet No. 9, ISO/IEC 8859-15:1999

[ISO/IEC 8859-4] Information technology – 8-bit single-byte coded graphic character sets – Part 4: Latin alphabet No. 4, ISO/IEC 8859-4:1998

[ISO/IEC 9066] Information processing systems – Text communication – Reliable Transfer
Omfatter følgende ISO/IEC-standarder og/eller ITU-T-rekommendasjoner:
Part 1: Model and Service Definition, ISO/IEC 9066-1:1989 | ITU-T X.218:1993
Part 2: Protocol Specification, ISO/IEC 9066-2:1989 | ITU-T X.228:1988

[ISO/IEC 9594] Information processing systems – Open Systems Interconnection – The Directory
Omfatter følgende ISO/IEC-standarder og/eller ITU-T rekommendasjoner:
Overview of Concepts, Models, and Services, ISO/IEC 9594-1:1995 | ITU-T X.500:1995
Models, ISO/IEC 9594-2:1995 | ITU-T X.501:1995
Abstract Service Definition, ISO/IEC 9594-3:1995 | ITU-T X.511:1995
Procedures for Distributed Operation, ISO/IEC 9594-4:1995 | ITU-T X.518:1995
Protocol specifications, ISO/IEC 9594-5:1995 | ITU-T X.519:1995
Selected attribute types, ISO/IEC 9594-6:1995 | ITU-T X.520:1995
Selected object classes, ISO/IEC 9594-7:1995 | ITU-T X.521:1995

Authentication framework, ISO/IEC 9594-8:1995 | ITU-T X.509:1995
Replication, ISO/IEC 9594-9:1995 | ITU-T X.525:1995
Use of Systems Management for Administration of the Directory, ISO/IEC DIS 9594-10
Directory Access Protocol – Protocol Implementation Conformance Statement (PICS), ISO/IEC 14608-1:1997 | ITU-T X.581:1997
Directory System Protocol – Protocol Implementation Conformance Statement (PICS), ISO/IEC 14608-2:1997 | ITU-T X.582:1997

[ISO/IEC 10021] Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS)
Omfatter følgende ISO/IEC-standarder og/eller ITU-T-rekommendasjoner:
Message Handling System and Service Overview, ISO/IEC 10021-1:1990 | ITU-T X.400:1996
Overall Architecture, ISO/IEC 10021-2:1996 | ITU-T X.402:1995
Abstract Service Definition Conventions, ISO/IEC 10021-3:1990 | ITU-T X.407:1988
Message Transfer System: Abstract Service Definition and Procedures, ISO/IEC 10021-4:1997 | ITU-T X.411:1995
Message Store: Abstract Service Definition, ISO/IEC 10021-5:1996 | ITU-T X.413:1995
Protocol Specifications, ISO/IEC 10021-6:1996 | ITU-T X.419:1995
Interpersonal Messaging System, ISO/IEC 10021-7:1996 | ITU-T X.420:1992

[ISO/IEC 10607] Information technology – International Standardized Profiles AFTnn – File Transfer, Access and Management
Omfatter følgende ISO/IEC-internasjonale standarder:
Part 1: Specification of ACSE, Presentation, and Session Protocols for the use by FTAM, ISO/IEC ISP 10607-1:1995

Part 2: Definition of Document Types, Constraint Sets and Syntaxes, ISO/IEC ISP 10607-2:1995
Part 3: AFT 11 – Simple File Transfer Service (unstructured), ISO/IEC ISP 10607-3:1995
Part 4: AFT 12 – Positional File Transfer Service (flat), ISO/IEC ISP 10607-4:1995
Part 5: AFT 22 – Positional File Acces Service (flat), ISO/IEC ISP 10607-5:1995
Part 6: AFT 3 – File Management Service, ISO/IEC ISP 10607-6:1995

[ISO/IEC 10611] Information technology – International Standardized Profiles AMH1n – Common Messaging
Omfatter følgende ISO/IEC internasjonale standarder:
Part 1: MHS Service Support, ISO/IEC ISP 10611-1:1997
Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS, ISO/IEC ISP 10611-2:1997
Part 3: AMH11 – Message Transfer (P1), ISO/IEC ISP 10611-3:1997
Part 4: AMH12 and AMH14 – MTS Access (P3) and MTS 94 Access (P3), ISO/IEC ISP 10611-4:1997
Part 5: AMH13 – MS Access (P7), ISO/IEC ISP 10611-5:1997

[ISO/IEC 10615] Information Technology – International Standardized Profile ADInn – The Directory
Omfatter følgende ISO/IEC-internasjonale standarder:
Part 2: ADI12 – DSA Support of Directory Access, ISO/IEC ISP 10615-2
Part 3: ADI21 – DSA Performer Role, ISO/IEC ISP 10615-3:1996
Part 4: ADI22 – DSA Initiator Role, ISO/IEC ISP 10615-4:1996
Part 5: ADI31 – DUA Support of Distributed Operations, ISO/IEC ISP 10615-5:1998

Part 6: ADI32 – DSA Support of Distributed Operations, ISO/IEC ISP 10615-6:1998

[ISO/IEC 10616] Information Technology – International Standardized Profile
FDI 11 – Directory data definitions – Common Directory Use (Normal), ISO/IEC ISP 10616:1995

[ISO/IEC 10646-1] Information Technology – Universal Multiple-Octet Character Set (UCS) – Part 1: Architecture and Basic Multilingual Plane, ISO/IEC 10646-1:1993

[ISO/IEC 11189] Information technology – International Standardized Profile FDI 2 – Directory Systems – MHS use of the directory, ISO/IEC ISP 11189:1997

[ISO/IEC 11190] Information Technology – International Standardized Profile FDI 3 – Directory data definitions – FTAM Use of the Directory, ISO/IEC ISP 11190:1995

[ISO/IEC 12062] Information technology – International Standardized Profiles AMH2n – Message Handling Systems – Interpersonal Messaging
Omfatter følgende ISO/IEC-internasjonale standarder:
Part 1: IPM MHS Service Support, ISO/IEC ISP 12062-1:1998
Part 2: AMH21 – IPM Content, ISO/IEC ISP 12062-2:1997
Part 3: AMH22 – IPM Requirements for Message Transfer (P1), ISO/IEC ISP 12062-3:1997
Part 4: AMH23 and AMH25 – IPM Requirements for MTS Access (P3) and MTS 94 Access (P3), ISO/IEC ISP 12062-4:1997
Part 5: AMH24 – IPM Requirements for Enhanced MS Access (P7), ISO/IEC ISP 12062-5:1997

[ISO/IEC 12072] Information Technology – International Standardized Profile FDI 5 – Directory data definitions – VT Use of the Directory, ISO/IEC ISP 12072:1998

[ISO/IEC 12073]	Information Technology – International Standardized Profile FDI 6 – Directory data definitions – EDI Use of the Directory, ISO/IEC DISP 12073
[ISO/IEC 13712]	Information Technology – Remote Operations Omfatter følgende ISO/IEC-standarder og/eller ITU-T rekommendasjoner: Remote Operations: Concepts, Model and Notation, ISO/IEC 13712-1:1995 | ITU-T X.880:1994 Remote Operations: OSI Realizations – Remote Operation Service Element (ROSE) Service Definition, ISO/IEC 13712-2:1995 | ITU-T X.881:1994 Remote Operations: OSI Realizations – Remote Operations Service Element (ROSE) Protocol Specification, ISO/IEC 13712-3:1995 | ITU-T X.882:1994
[ISO/IEC 15408 del 1–3]	The Common Criteria for Information Technology Security Evaluation
[ITU-T F.500]	International Public Directory Services, ITU-T F.500:1992
[ITU-T H.323]	Packet-based multimedia communication systems, ITU-T H.323:1998
[ITU-T T.120]	Data protocols for multimedia conferencing, ITU-T T.120:1996
[ITU-T T.61]	Se [ISO/IEC 6937]
[ITU-T X.509 A1]	OSI – The Directory – Part 8: Authentication Framework – Amendment 1: Certificate Extensions, ITU-T X.509 Amendment 1:1995 | ISO/IEC 9594-8 Amd 1:1995
[ITU-T X.509]	OSI – The Directory – Part 8: Authentication Framework, Revision 1, ITU-T X.509:1995 | ISO/IEC 9594-8:1995; se [ISO/IEC 9594]
[MHS-IMPL]	MHS Implementors' Guide, version 13, ITU-T, juli 1995