Samtlige statsetater.

Deres referanse	Vår referanse	Dato
	200405162- KDB	07.06.2005

Felles sikkerhetsportal for elektronisk kommunikasjon med offentlig sektor.

Formålet med dette brev er å gi statlige virksomheter en orientering og første brukerveiledning om sentrale beslutninger når det gjelder bruk av sikkerhetsløsninger for elektronisk identifisering og elektronisk signering av dokumenter, og skjema i forbindelse med tilgjengeliggjøring av offentlige elektroniske tjenester på nett.

I hovedtrekk har regjeringen vedtatt følgende:

1. Den vedtatte, felles kravspesifikasjonen for elektronisk ID og elektronisk signatur (PKI, se referanse s. 2) skal ligge til grunn for alle statlige anskaffelser av slike løsninger i markedet.
2. Brønnøysundregistrene skal i 2005, på vegne av staten og kommunene, inngå en rammeavtale om en felles sikkerhetsportal til bruk i offentlige elektroniske tjenester til *borgere og næringsliv*.
3. Denne rammeavtalen om sikkerhetsportalen er obligatorisk å bruke for alle statlige virksomheter og den anbefales for kommunene.
4. Brønnøysundregistrene skal i 2006 inngå felles rammeavtaler om eID til *intern bruk* for statlige virksomheter og deres ansatte.
5. Det skal opprettes en offentlig godkjenningsordning for leverandører av eID og e-signaturer. Ordningen skal vurdere om leverandørene oppfyller krav i felles offentlig kravspesifikasjon for elektronisk ID og elektronisk signatur.

Bakgrunn
Elektronisk forvaltning er et sentralt satsingsområde innen modernisering av offentlig sektor. Moderniseringsdepartementet har i det siste året fremmet en rekke sentrale tiltak innenfor rammen av den nasjonale IT-planen, eNorge 2005, som skal legge til rette for gjennomføring av elektronisk forvaltning. Fokuset har ligget på utvikling og tilgjengeliggjøring av elektroniske tjenester til befolkningen og til næringslivet. Moderniseringsdepartementet samarbeider med Nærings- og handelsdepartementet om tilrettelegging av en felles

Postadresse	Kontoradresse	Telefon	Avdeling for IT-politikk	Saksbehandler
Postboks 8004 Dep	Akersg. 59	22 24 90 90	Telefaks	Katarina de Brisis
N-0030 OSLO		Org no.	22 24 27 11	22 24 67 30
		972 417 785		

grenseflate for elektronisk kommunikasjon med brukerne av forvaltningens tjenester.

Sentrale tiltak i dette arbeidet er utvikling av *borgerportalen MinSide*, videreutvikling av *næringslivsportalen Altinn*, og utvikling og tilgjengeliggjøring av en felles løsning for elektronisk signatur og elektronisk ID gjennom en s.k. *sikkerhetsportal* som skal kunne benyttes av alle offentlige virksomheter som tilbyr elektroniske tjenester på nett.

Særlig om arbeidet med elektronisk signatur og elektronisk ID.
I et første vedtak 17.6.2004 besluttet Regjeringen at offentlig sektor skal samle og tydeliggjøre sine krav til bruk av elektronisk signatur og elektronisk ID (PKI[1]), gjennom en felles kravspesifikasjon. Kravspesifikasjonen skulle så danne underlaget for etablering av felles rammeavtaler for offentlig sektor, som skulle dekke ulike behov for bruk av PKI i elektronisk kommunikasjon med og i forvaltningen. Det skulle vurderes om rammeavtalen(e) skulle gjøres obligatoriske for statlig sektor.

Felles kravspesifikasjon for PKI i offentlig sektor – se adressen http://www.odin.dep.no/mod/norsk/dok/andre_dok/rapporter/050001-990049/dok-bn.html - forelå i november 2004. Spesifikasjonen ble godkjent av Moderniseringsministeren på vegne av staten, og av kommunenes organ KS med anbefaling om bruk i kommunene. Kravspesifikasjonen utgjør derved en forvaltningsstandard for elektronisk signatur og elektronisk ID. Versjon 1.02 av januar 2005 er siste oppdatering.

Regjeringen vedtok videre den 8.11.04 at det i tildelingsbrev til statlige virksomheter for 2005 skulle legges følgende føringer for bruk av budsjettmidler til IT-utvikling:

- Virksomheten bes om å tilrettelegge for utvikling av elektroniske tjenester rettet mot innbyggerne og næringslivet. Tjenester rettet mot innbyggerne bør også gjøres tilgjengelig i konseptet MinSide, mens tjenester mot næringslivet bør også gjøres tilgjengelig i Altinn.

Nærings- og handelsdepartementet skal i juni 2005 legge frem en ny handlingsplan for elektroniske tjenester til næringslivet. Samtidig skal Moderniseringsdepartementet legge frem en ny nasjonal IT-politisk handlingsplan – eNorge 2009. I disse dokumenter vil det bli gitt nærmere presisering av hvordan dette vedtaket skal realiseres i praksis.

- Elektroniske tjenester som forutsetter elektronisk signatur, skal baseres på felles godkjente kravspesifikasjoner. Det anbefales at virksomheten på dette området bruker et felles avtaleverk.

Vedtaket forutsetter altså at Kravspesifikasjon for e-signatur og eID i offentlig sektor legges til grunn for alle statlige etaters anskaffelser av slike løsninger. Med Kravspesifikasjonen som utgangspunkt la Moderniseringsdepartementet i februar 2005 frem en strategi for hvordan e-signatur og eID basert på PKI kan tas i bruk i elektronisk kommunikasjon med og i offentlig sektor på en mest mulig kostnadseffektiv måte, og slik at brukere av offentlig sektor skal få en enkel og samtidig trygg løsning. Strategidokumentet er tilgjengelig på adressen http://www.odin.dep.no/mod/norsk/aktuelt/nyheter/050001-990115/dok-bn.html. Hovedelementer i strategien omfatter:

[1] PKI står for Public Key Infrastructure og er en teknologi, basert på krypteringsnøkler, som kan benyttes til å sikre elektroniske dokumenters autentisitet, integritet, konfidensialitet og uavviselighet i kommunikasjon over Internett.

- En felles rammeavtale om en sikkerhetsportal for offentlige elektroniske tjenester til *borgere og næringsliv*, som skal inngåes innen 1.7.05,
- Offentlige godkjenningsordning(er) for leverandører av eID og e-signatur iht den offentlige kravspesifikasjonen som skal være på plass primo 2006,
- Rammeavtaler om elektronisk ID og signatur til *intern* bruk for virksomheter og ansatte i offentlig sektor som skal inngåes i løpet av 2006.

Formålet med en sikkerhetsportal er å gjøre det enkelt for offentlige etater som ønsker å tilby elektroniske tjenester som krever bruk av eID/e-signatur til sine brukere. Portalen skal kunne integrere e-signatur og eID-løsninger fra flere leverandører, og den skal kunne tilby mulighet for felles pålogging til flere tjenester[2], enten de er tilgjengelig gjennom en tjenesteportal (som MinSide eller Altinn), eller direkte fra ulike etaters og kommuners egne nettsider.

Portalen skal gjøre det mulig å sjekke en brukers elektroniske signatur eller –identitet uten at den enkelte etat/kommune skal måtte etablere avtaler med flere eID-tilbydere i markedet og ta kostnader ved teknisk integrasjon av deres løsninger i egen tjeneste.
Rammeavtalen skal inngås med én primærleverandør og det vil stilles krav om at minst 3 ulike, godkjente underleverandører av eID/e-signatur, skal kunne nås gjennom sikkerhetsportalen. Eksempel på mulige underleverandører er enkelte banker og Buypass AS (eid av Norsk Tipping og Posten). Underleverandørene skal være godkjent mhp om de oppfyller krav i den offentlige Kravspesifikasjonen for e-signatur og eID.

Regjeringen godkjente denne strategien 28.2.2005. Regjeringen besluttet at felles rammeavtale om en sikkerhetsportal skal inngåes og forvaltes av Brønnøysundregistrene, på vegne av staten og kommunene. Brønnøysundregistrene vil i den forbindelse etablere en forvaltningsorganisasjon i løpet av 2005.
Den nye forvaltningsenheten skal:

- Påse at det leveres kosteffektive PKI-baserte tjenester for autentisering og signering
- Bidra med løpende kostnytteanalyser for brukerstedenes utnyttelse av sikkerhetsportalens tjenester
- Overvåke hvordan rammeavtaleverket fungerer
- Ta nødvendige initiativ til å justere og videreutvikle avtalene slik at de fungerer i henhold til forutsetningene
- Overvåke at tjenester leveres med avtalt pris og til avtalt kvalitet
- Påvirke utviklingen av sikkerhetsportalens tjenestespekter
- Bidra til at tjenestene blir godt kjent og tatt i bruk.

Regjeringen besluttet videre at rammeavtalen om tjenester fra en sikkerhetsportal skal være pålagt å bruke for alle statsetater som skal gjøre anskaffelse av nye løsninger for bruk av eID/e-signatur fra og med november 2005. Vedtaket oppfordret samtidig kommunal sektor til å følge statens eksempel. Vedtaket åpnet for overgangsordninger for de etater som allerede har alternative sikkerhetsløsninger i bruk, med den målsetting å gå over til eID/e-signatur på en slik måte at bruken av eksisterende elektroniske tjenester ikke går ned.

Særlig om Kravspesifikasjon for eID og e-signatur i offentlig sektor. De tre nivåene m.v.

[2] S.k. single sign-on, som gjør det mulig for en bruker å flytte seg fra tjeneste til tjeneste på nettet uten å måtte logge seg på på nytt hver gang

Kravspesifikasjonen definerer tre standardiserte typer elektronisk ID / e-signatur som skal benyttes i offentlig sektor: Person Høyt, Person Standard og Virksomhet. De generelle kravene til disse ulike sikkerhetsnivåene på eID /e-signatur omtales i spesifikasjonens kap. 11 – Vedlegg 1. Ved tilrettelegging av elektroniske tjenester må derfor virksomheten foreta en vurdering av behovet for identifisering av brukere og signering av skjema og velge hvilket sikkerhetsnivå tjenesten skal legges på – ingen[3], Person Høyt, Person Standard eller Virksomhet. I vedlegget til dette brev gis det nærmere presisering av kravene til sikkerhetsnivå Person Standard.

Kravspesifikasjonen som forvaltningsstandard skal forvaltes og vedlikeholdes av departementet selv, med hjemmel i Forskrift om elektronisk kommunikasjon med og i forvaltningen nr 0988 av 25.6.2004, §27. Departementet utreder f.t. nødvendige rettslige forutsetninger samt prosedyrer som skal sikre at standarden til enhver tid samsvarer med behovene i offentlig sektor og er oppdatert på teknologi. Vi arbeider sammen med Nærings- og handelsdepartementet med å etablere en godkjenningsordning for leverandører av e-signaturer og eID. Ordningen skal administreres av et eksisterende offentlig organ. Vi legger til grunn at den kan være operativ i starten av 2006.

Særlig om sikkerhetsportalen og forholdet til Altinn og MinSide.
Sikkerhetsportalen skal ikke være en løsning for total sikring av elektronisk kommunikasjon med forvaltningen. Portalen skal først og fremst løse problemet med mange ulike påloggingsmekanismer som brukerne må forholde seg til. For etatene skal den gi en forenkling og kostnadsbesparelse i å utvikle og tilby elektroniske tjenester til brukere i næringslivet og til publikum, der tjenestene krever enten sikker autentisering[4] og / eller signering av elektroniske skjema eller meldinger.

Følgende tjenester skal tilbys gjennom portalen:
- Elektronisk ID iht til de 3 standardiserte nivåer, både for web-baserte tjenester og for tjenester der systemer utveksler data automatisk
- Elektronisk ID som i dag benyttes av Altinn og under Rikstrygdeverkets rammeavtale om eID/e-signatur for brukere av norsk helsenett
- Elektronisk signatur
- Tiltrodd digitalt arkiv for signerte dokumenter
- Kryptering
- Registrering for utstedelse av elektronisk ID iht til de 3 standardiserte nivåer.

I tillegg skal portalen tilby felles påloggingstjeneste, med automatisk overføring av opplysninger om en pålogget bruker fra en tjeneste til en annen.
Portalen skal være operativ ved utgangen av 2005, med et første utvalg tjenester. Flere tjenester vil bli gjort tilgjengelig i løpet av 2006. For nærmere informasjon om tilbudet i sikkerhetsportalen bør virksomheten ta kontakt med Brønnøysundregistrene.

Moderniseringsministeren har besluttet at tilgangen til tjenester i borgerportalen MinSide skal skje gjennom bruk av eID av typen Person Standard. En pålogging til MinSide skal kunne gi samtidig tilgang til alle tjenester som tilbys i de ulike etatene, uten ny pålogging. Dette skal løses gjennom bruk av sikkerhetsportalens tjenester. Virksomheter som tilbyr

[3] Dvs. det behøves ikke identifisering eller signering i tjenesten.
[4] Autentisering innebærer at man verifiserer en påstått identitet, dvs. om den som man kommuniserer med er den rette personen. Autentisering kobles ofte med autorisasjon, dvs. en kontroll av at denne personen har rett/myndighet til å foreta visse handlinger i et system, f.eks. se på persondata.

registerinformasjon eller transaksjonstjenester gjennom MinSide, vil derfor være de første brukerne av sikkerhetsportalen.

Næringslivsportalen Altinn vil ta i bruk sikkerhetsportalen for å tilby felles pålogging og felles løsning for autentisering av brukere, samt på sikt signering mv. Felles autentisering og felles pålogging gjennom bruk av sikkerhetsportalen vil bli tilgjengelig i Altinn versjon 3.2, som settes i produksjon ved utgangen av 2005. Enkelte av tjenester som vil tilbys gjennom MinSide vil også være tilgjengelig i Altinn.

Hva kan rammeavtalen bety for virksomheten?
Dersom virksomheten planlegger, eller er i ferd med å utvikle, en elektronisk tjeneste for borgere og tjenesten krever autentisering, må virksomheten henvende seg til Brønnøysundregistrene og foreta kjøp på rammeavtalen for sikkerhetsportalen. Dette for å unngå at mange offentlige virksomheter etablerer parallelle sikkerhetsløsninger mot de samme brukergrupper, noe som både skaper problemer for brukerne, og gir lite effektivt ressursbruk i offentlig sektor.
Dette kan forenkles ytterligere dersom etaten velger å tilby tjenesten sin gjennom portalen MinSide, der det vil være et etablert opplegg for slike avrop og kobling av tjenesten til sikkerhetsportalen. Dersom virksomheten skal tilby tjenester til næringslivet skal den vurdere tilkobling til portalen Altinn, og gjennom dette få tilgang til sikkerhetsportalens tjenester.
Dersom virksomheten allerede tilbyr en elektronisk tjeneste til publikum eller til næringslivet, og tjenesten krever autentisering av brukere, skal virksomheten foreta en kost-nytte vurdering av omleggingen av den eksisterende autentiseringsløsningen til bruk av sikkerhetsportalen. I en slik kost-nytte vurdering skal det inngå en kartlegging av hvor mange brukere av virksomhetens tjenester som allerede besitter en eID med den typen som sikkerhetsmessig og funksjonelt passer til etatens tjeneste (Person Høyt, Person Standard eller Virksomhet). Dersom andelen av brukere med slik eID overstiger 50% bør etaten vurdere å legge om løsningen til sikkerhetsportalens tjenester innen en periode på 6-8 måneder.

Kjøp av tjenester fra sikkerhetsportalen innebærer at virksomheten får utgifter knyttet til selve tilkoblingen til portalen (disse forutsettes ikke å utgjøre vesentlige beløp) og til bruken av de ulike tjenestene den tilbyr, jfr. oversikten ovenfor. Tjenestene vil mest sannsynlig bli priset individuelt, avhengig av type tjeneste, forventet volum og bruk.
Brønnøysundregistrene arbeider nå med mulige ordninger for kjøp av portalens tjenester, som skal gjøre det mulig å gi en viss økonomisk støtte til de første pilotbrukere av portalen, delvis i 2005 og i 2006. Det grunnleggende prinsippet for bruken av portalen er likevel at virksomheter som benytter sikkerhetsportalen, selv skal stå for betaling av portalens tjenester.

Informasjon.
Ved spørsmål til innholdet i dette brev ber vi at det tas kontakt med Moderniseringsdepartementet ved Avdeling for IT-politikk, tlf. 22 24 03 01, e-post: postmottak@mod.dep.no (med henvendelsen "sikkerhetsportalen" i tittelfeltet) eller med Brønnøysundregistrene, ved Bente Ulvund, tlf. 75 00 60 33, e-post bente.ulvund@brreg.no .

Med hilsen

Karin Moe Røisland (e.f.)
departementsråd

Hugo Parr
Ekspedisjonssjef

Kopi: Brønnøysundregistrene
KS

Vedlegg.

Vedlegg brev til offentlige virksomheter om felles offentlig sikkerhetsportal

Kravspesifikasjon for PKI i offentlig sektor, definerer tre sikkerhetsnivå, Person Høyt, Person Standard og Virksomhet. Person Høyt og Virksomhet støtter seg til eSignatur loven, forskriftsverk og internasjonale standarder når det gjelder registrering og identifisering av brukere for utlevering av sertifikater. For Person Standard er ikke prosessen for å utstede sertifikater like klart definert. Moderniseringsdepartementet har derfor fått forespørsler vedrørende hvordan brukere kan identifiseres og sertifikater utleveres på nivå Person Standard.

Kravspesifikasjon for PKI i offentlig sektor blir forvaltet av Moderniseringsdepartementet og skal justeres iht. de krav offentlig sektor har til en hver tid. I tillegg vil det bli etablert en offentlig godkjenningsordning for leverandører av Person Standard, der det vil bli skapt en praksis i forhold til tolkning av kravspesifikasjonen. Moderniseringsdepartementet vil her gjøre de første presiseringer av nivå Person Standard.

I kravspesifikasjonen for PKI i offentlig sektor står følgende:

> "*Utlevering skal skje ved utsendelse pr post til registrert adresse eller elektronisk utstedelse basert på eksisterende autentiseringsmekanisme, som gir minst like god trygghet for korrekt mottager som post til registrert adresse*."

Moderniseringsdepartementet ønsker at brukere skal kunne få utstedt Person Standard sertifikater på en enkel måte ved å gjenbruke koder som brukere allerede har fått tilsendt, som for eksempel kodene i forbindelse med innlevering av selvangivelse.

I prinsippet skal utsendelser av engangskoder til registrert adresse skje på en så sikker måte som mulig. Det er krav til at engangskoder ikke skal kunne leses gjennom konvolutten, men det er ingen krav om at engangskode og informasjon om mottager må sendes på separate ark.

Har en mottager mottatt en autentiseringsmekanisme, som for eksempel passord og brukernavn, basert på en engangskode utsendt som beskrevet over, ønskes det at denne skal kunne benyttes til å identifisere brukere ved utstedelse av Person Standard.

Moderniseringsdepartementet ønsker å tilrettelegge for enkel utstedelse av Person Standard basert på eksisterende autentiseringsløsninger fra offentlig sektor, som for eksempel Skatteetatens PIN-koder og Aetats passord og brukernavn. Departementet mottar gjerne tips om andre offentlige autentiseringsløsninger som kan være egnet for dette formål.