Rettslige krav til informasjonssikkerhet i offentlig forvaltning

Advokat dr. juris Rolf Riisnæs
Wikborg, Rein & Co
rri@wr.no
DRI1010
12. mars 2009

WIKBORG REIN

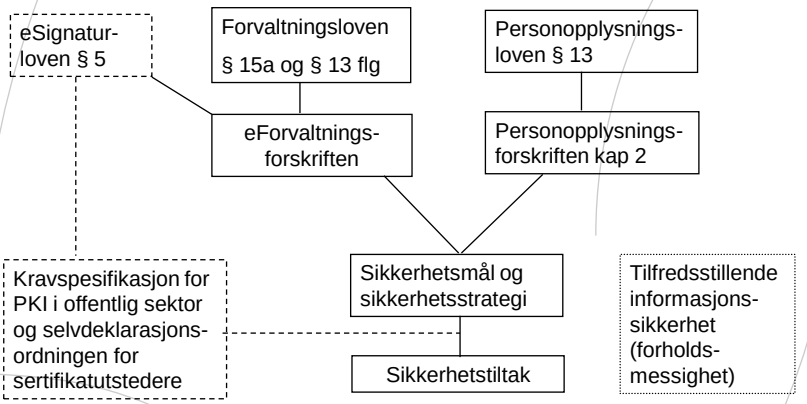
Informasjonssikkerhet

- Hvem, hva og hvorfor
- Det velkjente og det nye
- Informasjonssamfunnets utfordringer
- Totalperspektiv på informasjonssikkerhet
- Beskyttelsesperspektiv og samhandlingsperspektiv
  - Beskyttelsesperspektiv: Hvordan kan jeg sikre at det ikke "skjer noe galt" med det som er mitt og det jeg har ansvaret for?
  - Samhandlingsperspektiv: Hvordan kan jeg legge til rette for effektiv, sikker og pålitelig samhandling ved hjelp av elektronisk kommunikasjon?

Rettslig forankring

- Personopplysningsloven (pol)
  - Informasjonssikkerhet § 13
  - Personopplysningsforskriften (pof)
    - Kapittel 2 Informasjonssikkerhet
- Forvaltningsloven (fvl)
  - Taushetsplikt § 13 flg, oppbevaring av taushetsbelagt informasjon § 13c
  - Forskriftshjemmel § 15a
  - eForvaltningsforskriften (efvf)
- Sikkerhetsloven (Rikets sikkerhet)
  - Forskrifter om informasjonssikkerhet
  - Forholdet til Beskyttelsesinstruksen (skjermingsverdig informasjon i sivil sektor)
- Sektorspesifikk regulering (for eksempel helseregisterloven, IKT-forskriften mv)

Rettslig forankring



Noen begreper

- Konfidensialitet
- Tilgjengelighet
- Integritet
- Autentisering
- Uavviselighet

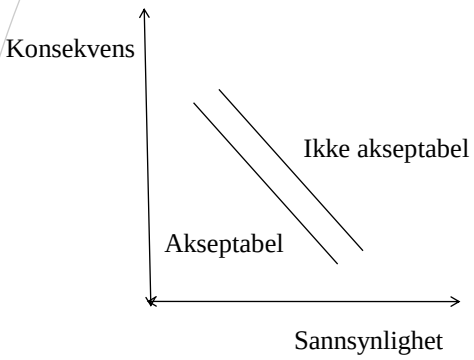
Personopplysningsloven

- Formål: Å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger
- Informasjonssikkerhet § 13
- Intern kontroll § 14
- Databehandleravtale § 15

Personopplysningsloven § 13

- Den behandlingsansvarlige og databehandleren skal
  - gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger
  - dokumentere informasjonssystemet og sikkerhetstiltakene
  - Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren, samt for Datatilsynet og Personvernnemnda
  - Den behandlingsansvarlige skal påse at databehandlere og andre oppfyller kravene
- Risikovurdering, akseptabel risiko, forholdsmessighet (pof §§ 2-1 og 2-4)
- Forskriftshjemmel – kravene er presisert i personopplysningsforskriften (pof) kap 2 (bare elektronisk behandling)

Risikovurdering



Kategorisering av risiko (eksempel)

Konsekvens/effekt	Frekvens	Kostnad for å forebygge
Katastrofe	Lite sannsynlig	Veldig høy
Kritisk skade	Veldig lav	Høy
Betydelig skade	Forekommer	Rimelig
Marginal skade	Må påregnes jevnlig	Lav
Ignorerbar	Vanlig	Høy
(Vurdere ift ulike opplysningstyper og behandling: effekt av konfidensialitetsbrudd og sannsynlighet for at det vil skje, effekt av at opplysninger ikke er tilgjengelig på aktuelt tidspunkt og hvor ofte det kan komme til å skje mv.)		

Strategi, ansvar og oppfølging

- Ledelsesforankring (pof § 2-3)
- Sikkerhetsmål (hva) og sikkerhetsstrategi (hvordan)
- Intern kontroll (pol § 14 og pof kap 3) (oppfølging og avvikshåndtering)
- Fortløpende innsamling av ordnet erfaringsmateriale:
  - sikkerhetsrevisjon (§ 2-5)
  - dokumentert avviksbehandling (§ 2-6),
  - registrering av autorisert bruk (§ 2-8) og
  - forsøk på uautorisert bruk (§ 2-14)
- Endringer, fornyet risikovurdering

Nærmere om kravene

- Konfidensialitet (pof § 2-9 til 2-11)
- Tilgjengelighet (pof § 2-12)
- Integritet (pof § 2-13)

- Det skal iverksettes tiltak når K/T/I er *nødvendig*
- Kravene må vurderes
  - for hver "type behandling" (registrering/innsamling, vurdering, lagring, utlevering)
  - for ulike typer opplysninger (sensitive, taushetspliktige, andre)
  - for ulike bruksområder
- ➢ Personvernperspektivet

Tiltak

- Fysiske (sikring av bygninger og utstyr, kryptering)
- Organisatoriske (rolle og oppgavedeling)
- Økonomiske (stimuli eller "straff")
- Pedagogiske (opplæring for å stimulere til ønsket utvikling, miljø for overholdelse)
- Normative virkemidler (regler, for eksempel instrukser)
- Iverksatte tiltak skal dokumenteres (pof § 2-14)

eForvaltningsforskriften

- Forskrift om elektronisk kommunikasjon med og i offentlig forvaltning
- Hovedprinsippene i forskriften
  - Bestemmelser om forsvarlig elektronisk samhandling
  - Krav til etablering av en sikkerhetsstrategi for forvaltningsorganene
  - Bestemmelser om elektronisk signatur, kryptering og sertifikater
  - Koordinering av forvaltningens bruk av sikkerhetstjenester

Forskriftens formål

- Forskriften skal legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen (efvf § 1).
  - Fremme forutsigbarhet og fleksibilitet.
  - Legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger.
- Legge til rette for at publikum på en enkel måte kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige.
  - Klare handlingsregler og behovstilpassede sikkerhetskrav.
  - Unngå at noen lider rettstap som følge av at nye datamaskinbaserte rutiner ikke blir forstått eller at teknologien svikter.
  - Utfordring: Unngå at noen stenges ute eller blir "annenrangs" kunder av forvaltningens tjenester fordi de ikke har tilgang til eller behersker de elektroniske tjenestene.

eForvaltning tilgjengelig for alle

- Forvaltningsorganet bør legge til rette for at elektronisk kommunikasjon med forvaltningsorganet er brukervennlig og tilgjengelig for alle (efvf. §3(5))

Samspillet mellom regler og tekniske løsninger

- Valgfrihet – frihet til å velge å delta, men også til å la være
- Forventninger om pålitelighet og forebyggende tiltak
- Forutberegnelighet – redusere usikkerhet
- Beskyttelse mot rettstap som følge av mangelfull forståelse eller oppfølging av tekniske løsninger
- Tilgang til opplysninger og dokumenter over tid

Hjemmel for eForvaltningsforskriften

Forvaltningsloven § 15a. *(elektronisk kommunikasjon)*

Kongen kan gi forskrift om elektronisk kommunikasjon mellom forvaltningen og publikum og elektronisk saksbehandling og kommunikasjon i forvaltningen, herunder nærmere regler om

a) hvilken elektronisk adresse eller informasjonstjeneste som skal benyttes,

b) signering, autentisering, sikring av integritet og konfidensialitet,

c) kvittering for mottak av elektroniske meldinger,

d) krav til de produkter, tjenester og standarder som kan benyttes,

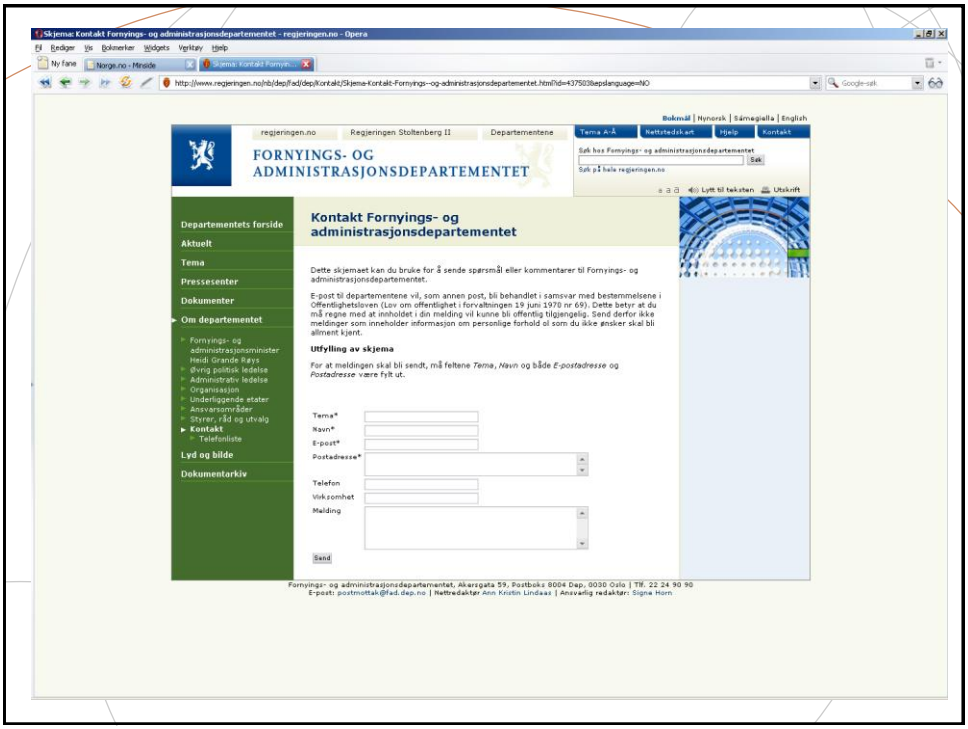
e) forvaltningens rett til å sperre for brukere som misbruker data ment for signering, autentisering, sikring av integritet eller konfidensialitet, og om hva som skal regnes som misbruk.

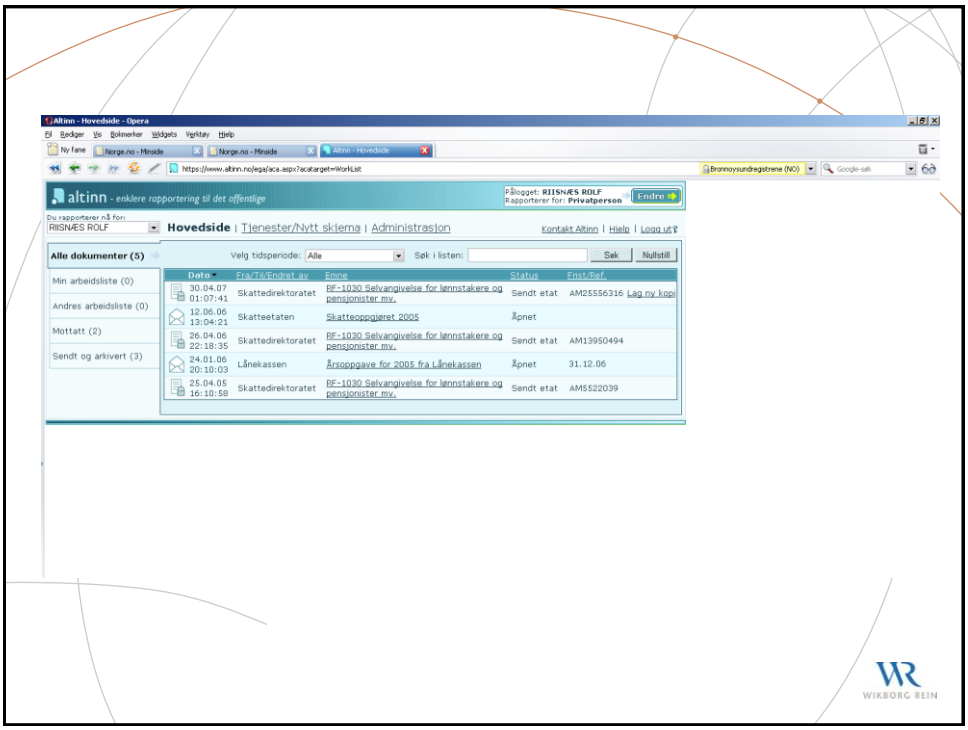
WIKBORG REIN

Valg av form og fremgangsmåte

- Forvaltningsorganet kan selv velge hvordan den elektroniske kommunikasjonen skal foregå:
  - Elektroniske skjemaer – Web-baserte løsninger
  - E-post
- E-forvaltningsforskriften
  - Først og fremst web-baserte løsninger
  - Utelukker ikke andre løsninger, se efvf §3(1) (b) og (c)
  - Henvendelser i elektronisk form skal ikke rettes direkte til saksbehandler med mindre forvaltningsorganet har lagt til rette for det
- Har forvaltningsorganet etablert en generell e-postadresse, kan den benyttes for henvendelser til forvaltningsorganet så lenge det ikke er formkrav knyttet til henvendelsen eller organet har etablert en egen tjeneste for formålet.

WIKBORG REIN


Skjema: Kontakt Fornyings- og administrasjonsdepartementet - regjeringen.no - Opera
regjeringen.no
Regjeringen Stoltenberg II
Departementene
FORNYINGS- OG ADMINISTRASJONSDEPARTEMENTET
Departementets forside
Aktuelt
Tema
Pressesenter
Dokumenter
Om departementet
Kontakt
Dokumentarkiv
Kontakt Fornyings- og administrasjonsdepartementet
Utfylling av skjema
Tema*
Navn*
E-post*
Postadresse*
Telefon
Virksomhet
Melding
Send


Altinn - Hovedside - Opera
altinn - enklere rapportering til det offentlige
Hovedside | Tjenester/Nytt skjema | Administrasjon
Alle dokumenter (5)
Min arbeidsliste (0)
Andre arbeidsliste (0)
Mottatt (2)
Sendt og arkivert (3)
WIKBORG REIN

Strategi for informasjonssikkerhet i virksomheten

- Forvaltningsorgan som benytter *elektronisk kommunikasjon* skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (§ 13).
- Sikkerhetsstrategien danner grunnlaget for fastlegging av krav etter kapittel 2.
- Helhetlig, planlagt, systematisk og dokumentert strategi, utarbeidet i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet.
- Sikkerhetsstrategien skal også omfatte sikkerhetskrav i annet regelverk.
- Forskriften utpeker enkelte temaer knyttet til PKI og elektronisk signatur som skal adresseres i den grad det er relevant.

WIKBORG REIN

Sikkerhetsstrategi (efvf § 13, forts.)

- (3) I den utstrekning det er relevant skal sikkerhetsstrategien også adressere, og om nødvendig stille krav til, bl.a.:
- a) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata,1 passord/PIN-koder og dekrypteringsnøkkel knyttet til personlige sertifikat eller sertifikat for ansatt i forvaltningen, jf. § 15, § 17 og § 20;
- b) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel knyttet til virksomhetssertifikat, jf. § 14 og § 21;
- c) prosedyrer for å etablere og opprettholde et sikkert brukermiljø der det benyttes elektroniske signaturer, kryptering eller andre sikkerhetstjenester, jf. § 18;
- d) prosedyrer for varsling og tilbaketrekking av sertifikat og passord/PIN-koder ved mistanke om tap eller misbruk, jf. § 23;

WIKBORG REIN

Sikkerhetsstrategi (efvf § 13, forts.)

- (3) I den utstrekning det er relevant skal sikkerhetsstrategien også adressere, og om nødvendig stille krav til, bl.a.:
- …
- e) prosedyrer for kontroll av sertifikater og tilbaketrekkingslister ved mottak av melding utstyrt med elektronisk signatur, herunder krav til hvor oppdatert informasjon om sertifikaters status bør være for de ulike formål sertifikatene benyttes for, jf. § 25;
- f) prosedyrer for å nekte bruk av sertifikat mv. ved misbruk av elektronisk kommunikasjon med forvaltningen, jf. § 12;
- g) prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, jf. § 5 og § 24, se også personopplysningsloven § 13 og personopplysningsforskriften kap. 2;
- h) prosedyrer for sikkerhetskopiering, oppbevaring og deponering av dekrypteringsnøkkel for opplysninger som angår forvaltningsorganet, jf. § 22.

WIKBORG REIN

Vurderingen av behovet for sikker kommunikasjon - momenter i vurderingen

- Behovene for sikring er ulike og ofte sammensatte:
- Er det formkrav som skal oppfylles, for eksempel underskriftskrav?
- Kan det ha skadevirkninger hvis andre enn tilsiktet mottaker får tilgang til informasjonen?
- Er det en fare for at innholdet kan endres på vei fra avsender til mottaker?
- Er det behov for at avsender identifiserer seg eller at forvaltningsorganet kan være sikker på hvem vedkommende er?
- Er det viktig at løsningen/tjenesten er tilgjengelig hele tiden?

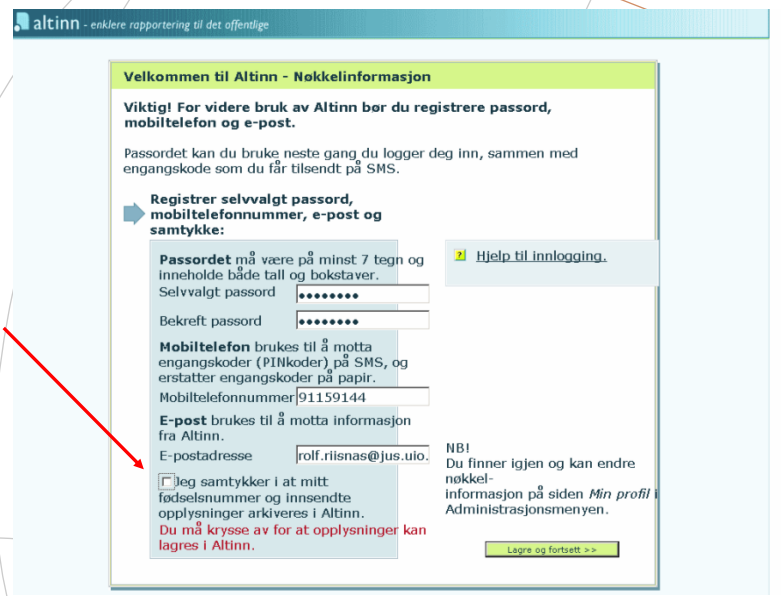
WIKBORG REIN

Fleksibilitet og behovstilpassede sikkerhetsløsninger

- Krav til bruk av sikkerhetsløsninger skal være forankret i sikkerhetsstrategien til forvaltningsorganet (efvf. § 4)
- Forvaltningsorganet skal gjøre tilgjengelig eller gi anvisning på tjenester og produkter som oppfyller kravene.
- Krav om bruk av sikkerhetsløsninger kan følge av regelverket eller av at opplysningenes eller transaksjonens art gjør det nødvendig. Dette skal fremgå av sikkerhetsstrategien.

Innhenting av opplysninger

- Forebygge uberettiget innsyn i personopplysninger og andre taushetsbelagte opplysninger (efvf § 5)
- Informere om sikkerhetstiltak og restrisiko
- Informasjon om hvordan personopplysninger blir behandlet
- Samtykke til behandling av opplysninger
- Autentisering av den som samtykker



WIKBORG REIN

Kommunikasjon med brukerne

- Forvaltningsorganet skal sende bekreftelse på at henvendelse er mottatt (efvf. § 6)
- Varsle og veilede om eventuelle feil og mangler ved adresse, fremgangsmåte eller innhold (efvf. § 7)
- Underretning om enkeltvedtak (efvf. § 8)
  - Sikre parten mot rettstap som følge av at frister løper ut uten at vedkommende har hatt foranledning til å skaffe seg kunnskap om innholdet
  - Krav om uttrykkelig samtykke
  - Varsel om at vedtak er fattet og hvordan parten kan gjøre seg kjent med vedtaket
  - Kontroll med avhenting, reserveløsninger

WIKBORG REIN

Brukernes tilgang til opplysninger

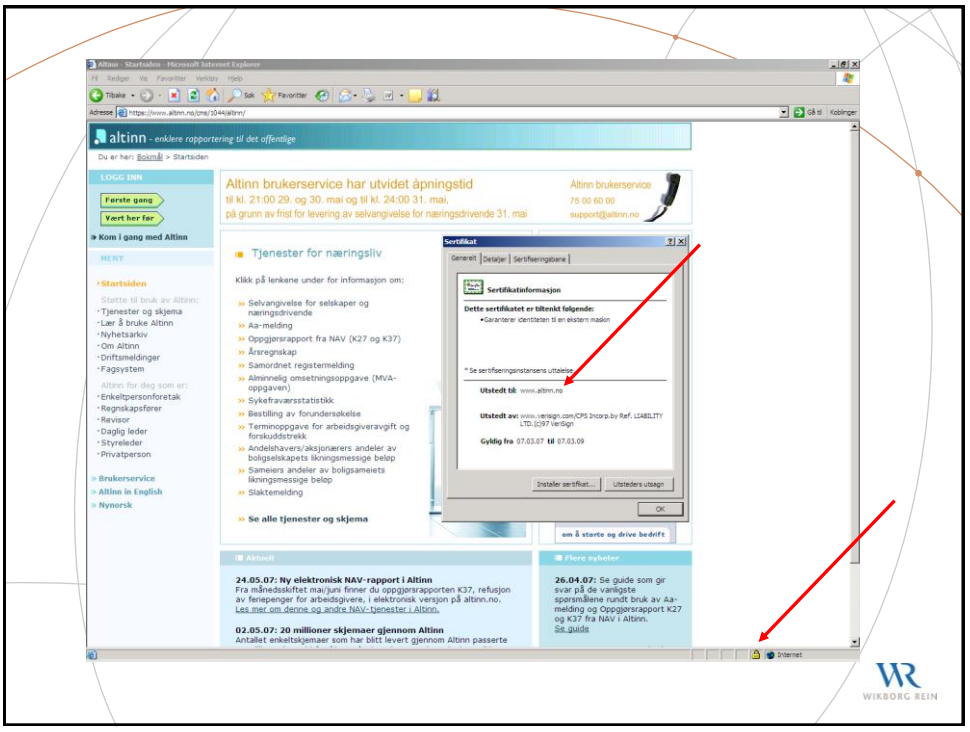
- Innsynsrett og forholdet til taushetsplikten (efvf. § 10)
  - Krav om bekreftelse av identitet og sikring av opplysninger under overføring når innsyn gis i elektroniske dokumenter
- Utlevering av signert materiale mv (§ 10 nr. 4 og 5)
  - Forvaltningen som brukernes private arkiv
  - Sikre parten tilstrekkelig dokumentasjon ift tredjepart mv

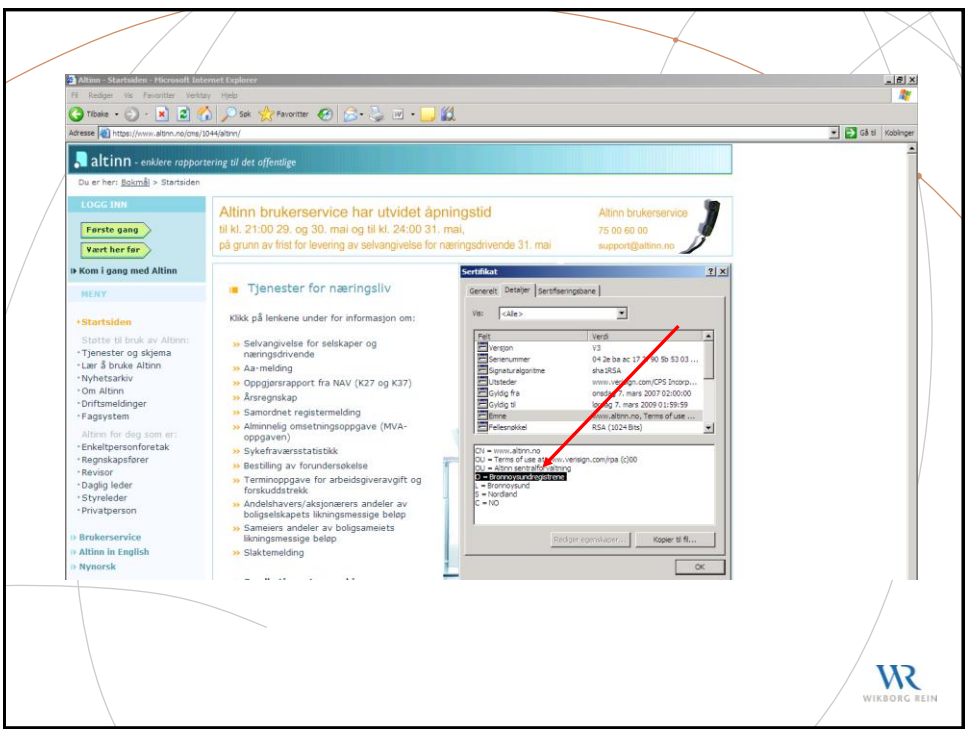
WIKBORG REIN

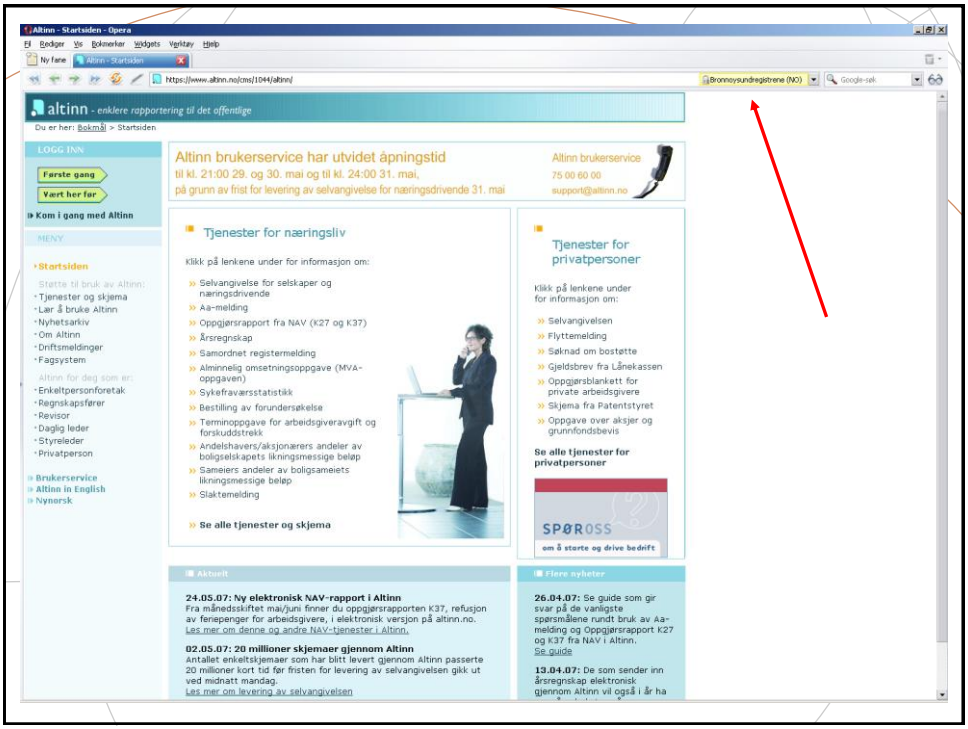
Virksomhetssertifikater

- Hvordan kan brukeren være sikker på at det er forvaltningsorganet som mottar eller avgir opplysninger?
- Om begrepene ”sertifikat” og ”eID”
- Sertifikat for forvaltningsorgan (virksomhetssertifikat § 14)
  - parten trenger bekreftelse fra forvaltningsorganet ikke fra saksbehandler
  - tillit til forvaltningsorganets rutiner
- Noen eksempler på sertifikatbruk.

WIKBORG REIN


altinn - enklere rapportering til det offentlige
Altinn brukerservice har utvidet åpningstid
til kl. 21:00 29. og 30. mai og til kl. 24:00 31. mai,
på grunn av frist for levering av selvangivelse for næringsdrivende 31. mai
Tjenester for næringsliv
Klikk på lenkene under for informasjon om:
Sertifikat
Sertifikatinformasjon
Dette sertifikatet er tiltenkt følgende:
Utstedt til: www.altinn.no
Utstedt av: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
Gyldig fra 07.03.07 til 07.03.09
Installer sertifikat...
Utsteders uttalelse
OK
24.05.07: Ny elektronisk NAV-rapport i Altinn
02.05.07: 20 millioner skjemaer gjennom Altinn
26.04.07: Se guide som gir svar på de vanligste spørsmålene rundt bruk av Aa-melding og Oppgjørsrapport K27 og K37 fra NAV i Altinn.
WIKBORG REIN


altinn - enklere rapportering til det offentlige
Altinn brukerservice har utvidet åpningstid
til kl. 21:00 29. og 30. mai og til kl. 24:00 31. mai,
på grunn av frist for levering av selvangivelse for næringsdrivende 31. mai
Tjenester for næringsliv
Klikk på lenkene under for informasjon om:
Sertifikat
Generelt
Detaljer
Sertifiseringsbane
Vis:
<Alle>
Felt
Verdi
Versjon
Serienummer
Signaturalgoritme
Utsteder
Gyldig fra
Gyldig til
Emne
Fellesnøkkel
RSA (1024 Bits)
OK
WIKBORG REIN



Informasjon og veiledning til brukerne

- Forvaltningsorganet skal sikre at brukerne får tilstrekkelig informasjon om bruk av sertifikattjenester ift forvaltningen (§ 15 jfr §19)
- Prosedyrer og forsiktighetsregler for bruk (§§ 20-23)
- Forvaltningsorganets adgang til å nekte bruk av elektronisk kommunikasjon (§ 12)

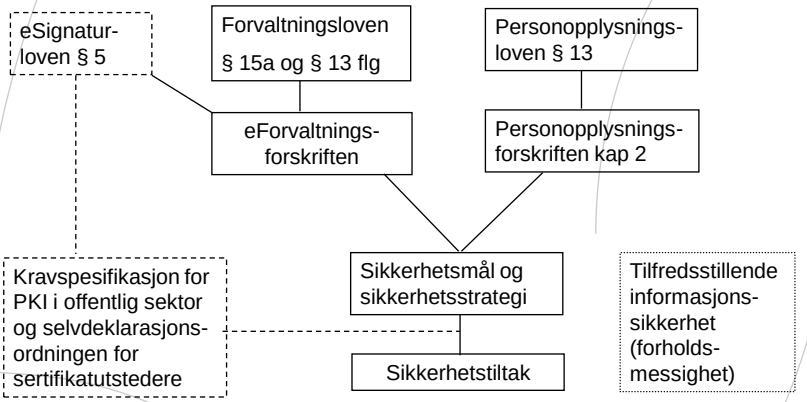
Krav til forvaltningens håndtering av elektronisk signatur og materiale som er kryptert

- Mottak av kryptert materiale (§ 24)
- Ved bruk av elektronisk signatur er det krav om at forvaltningsorganet som mottar signaturen skal
  - Kontrollere at signaturen og sertifikatet er gyldig (§ 25)
  - Ta vare på resultatet av signaturkontrollen
  - Ta vare på dokumentet som er elektronisk signert i et arkivverdig format (§ 26)

Koordinering

- Koordinerende organ for forvaltningens bruk av sikkerhetstjenester (§ 27)
  - Utarbeide krav til sikkerhetstjenester og -produkter som anbefales brukt
  - Vurdere om tilgjengelige tjenester og produkter tilfredsstiller de kravene som er stilt
  - Kan kreve at det skal benyttes tjenester og produkter som det er inngått rammeavtale om eller som på annen måte er anerkjent av koordineringsorganet.
  - Kan kreve at det bare skal benyttes tjenester som er omfattet av selvdeklareringsordningen etter esignaturloven § 16a

Rettslig forankring



Rammeverk for e-signatur

- Kravspesifikasjon for PKI i offentlig sektor
  - En obligatorisk standard ved bruk av PKI i alle statlige etater
  - Sterkt anbefalt for kommunene
- Selvdeklarasjonsordningen
  - Tilbydere av PKI iht kravspesifikasjonen (sertifikatutstedere) kan registrere seg hos Post- og teletilsynet (selvdeklarering)
  - Forvaltningsorganene skal kreve at tilbydere de benytter er selvdeklarert (se liste på http://www.npt.no)
- Portal for sikkerhetsløsning - sikkerhetsnav
  - Tidligere Sikkerhetsportalen
  - Viktig for å sikre samtrafikk og utbredt anvendelse av e-signatur
  - Forslag til strategi for bruk av eID og e-signatur i offentlig sektor, Fornyings- og administrasjonsdepartementet (2007)

Les mer

- *Veileder til eForvaltningsforskriften*, Fornyings- og administrasjonsdepartementets nettsider (veiledninger og brosjyrer)
- *Elektronisk forvaltning i Norden*, Dag Wiese Schartum (red.), Fagbokforlaget, Oslo 2007, ISBN 978-82-450-0554-7
- *Informasjonssikkerhet – Rettslige krav til sikker bruk av IKT*, Arild Jansen og Dag Wiese Schartum (red.), Fagbokforlaget, Oslo 2005, ISBN 82-450-0274-7
- Rolf Riisnæs, *Digitale sertifikater og sertifikattjenester – roller, oppgaver og ansvar,* Fagbokforlaget, Oslo 2007, ISBN 978-82-450-0589-9