



NSM

eForum: drøfting av Seid leveranse 2

16. februar 2006

John Bothner

Teknisk Avdeling

john.bothner@nsm.stat.no

www.nsm.stat.no

Agenda

- Kort om NSM
- Om Seid leveranse 2
 - 2 varianter tilleggsinfo (utenom sertifikat)
 - Via OSCP ("integrert")
 - XML / WS ("frittstående")
 - Sikkerhet
- Mulige relevant problemstillinger for næringsliv

Kort om NSM

- Direktorat underlagt FD og JD
- Sikkerhetsloven
- 130 ansatte
- Brukere: forsvaret, departementer, andre etater, private virksomheter
- Noen oppgaver
 - Sikkerhetsklarering personell
 - Godkjenne graderte IT systemer
 - Overvåke/beskytte "det norske internett" mot virus, hackerangrep, med mer.
 - VDI / Norcert
 - Og private bedrifter
 - Vurdere kommersiell kryptoutstyr
 - Utvikle egen kryptoutstyr (høy gradert)
 - Sertit (Common Criteria)

Kort om NSM (2)

John Bothner:

- Leder "Seksjon for hyllevarebasert krypto og forretningsteknologi"
 - Fokus: beskytte gradert informasjon
 - Inkluderer PKI
 - Stiller krav til hvordan krypto og PKI er implementert
 - Utgir veiledninger med våre krav (www.nsm.stat.no)

- Før NSM: deltok i SEID

”Disclaimer”

- Merk at NSM ikke selv har deltatt aktivt i SEID
- I dette arbeidsmøtet har NSM bidratt som ordstyrer og bidragsyter i å få i gang diskusjon, det betyr ikke at alle utfordringene/innspillene i denne presentasjon er NSM sin offisielle politikk.
- NSM ser som positivt om næringslivet generelt tar i bruk PKI for å bedre den generelle sikkerhetstilstanden
- NSM har spesifikke krav til PKI for de organisasjoner som etter lov må følge NSMs pålegg (ta kontakt for mer info).

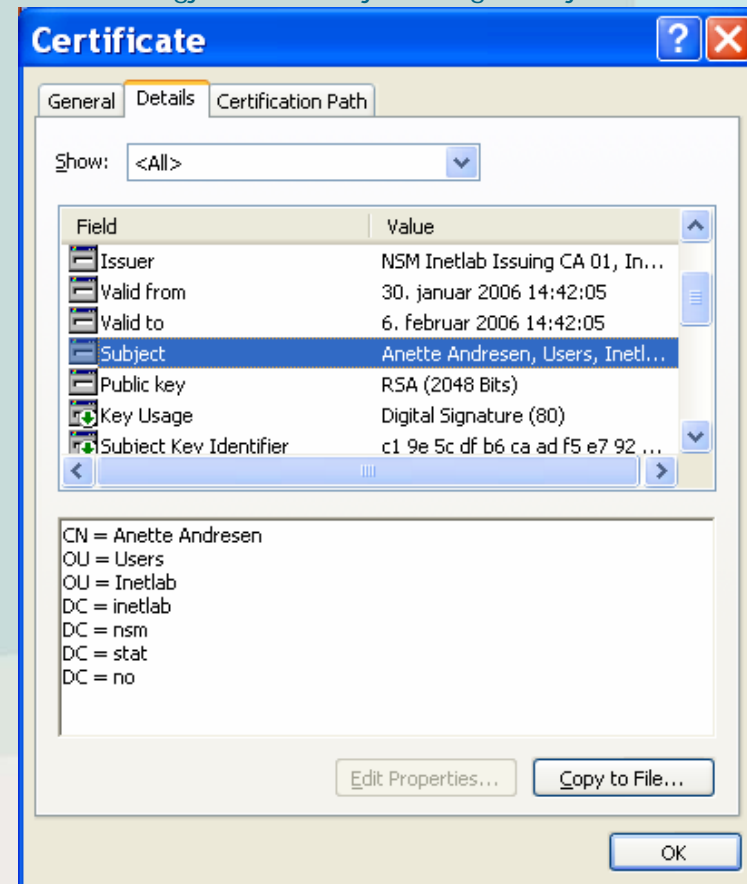
Om Seid leveranse 2

Hva er et sertifikat?

- Et ”elektronisk identitetsbevis” (sertifikat) for sluttbruken knyttes til den offentlige delen av nøklene
- Relevant bruk:
 - Pålogging datasystemer
 - Signatur på elektroniske dokumenter
 - Nøkkelutveksling
- PKI er infrastruktur + bruk av denne infrastrukturen



Elektronisk legitimasjonsbevis (PKI sertifikater) har deler man kjenner igjen fra tradisjonell legitimasjonsbevis:



Informasjon i og utenfor sertifikater

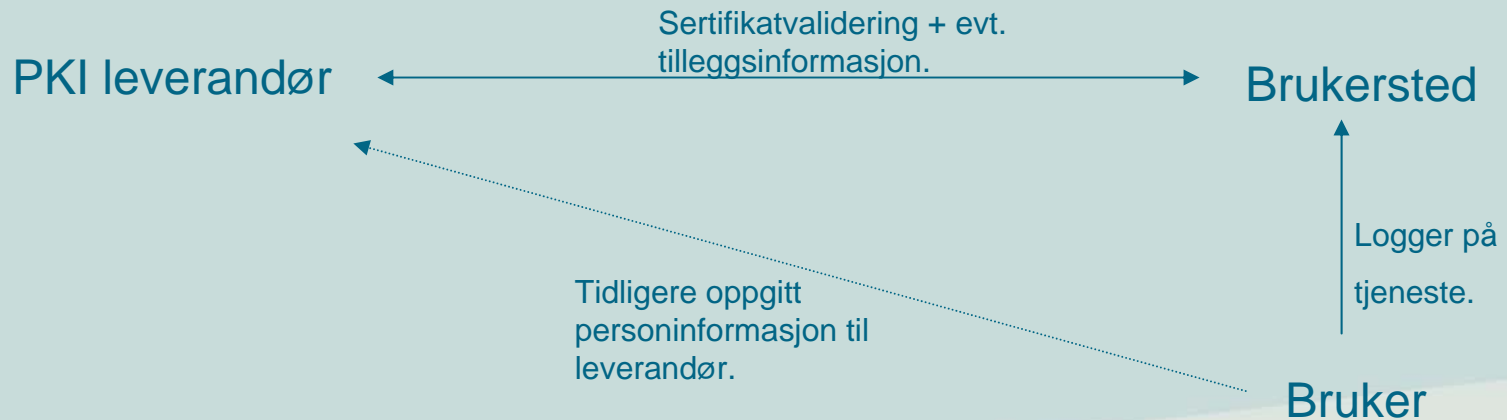
- Eksempel på informasjon om bruker *i sertifikatet*:
 - Fullstendig navn på person
 - Unid (unikt nummer koordinert i Seid)
 - Utsteder av sertifikat
 - Tidsperiode gyldighet

- Eksempel på informasjon PKI leverandør har/kan ha *i tillegg*:
 - Personnummer
 - Epost adresse
 - Telefonnumre
 - Fysisk adresse
 - Under/over 18 år?
 - Annet?

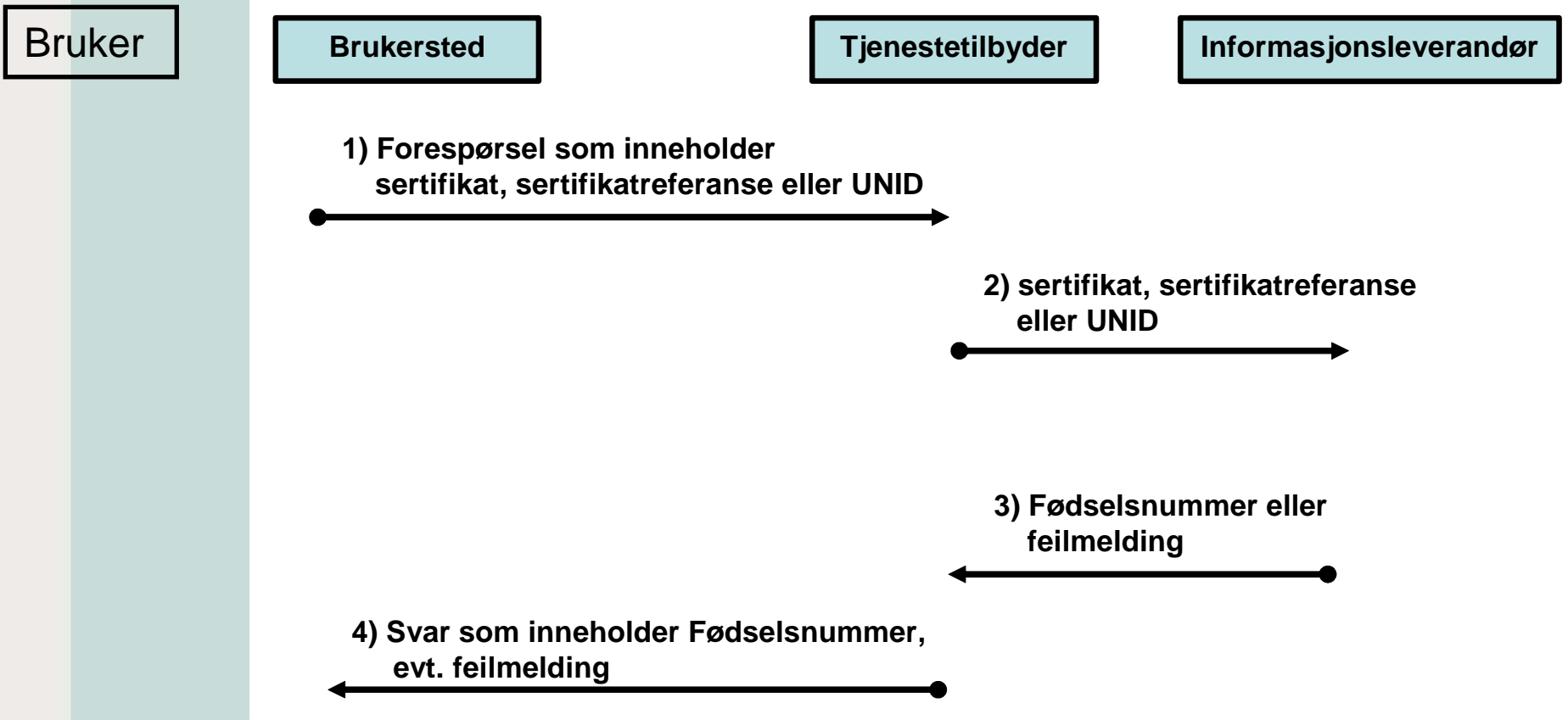
- Seid leveranse 2 har fokus på siste kategori

Tilleggstjenester ut over å bekrefte sertifikatets gyldighet

- PKI leverandør forplikter seg overfor brukersted til å bekrefte gyldighet av sertifikat
- Annen informasjon om bruker oppfattes som tilleggstjenester / ekstrainformasjon



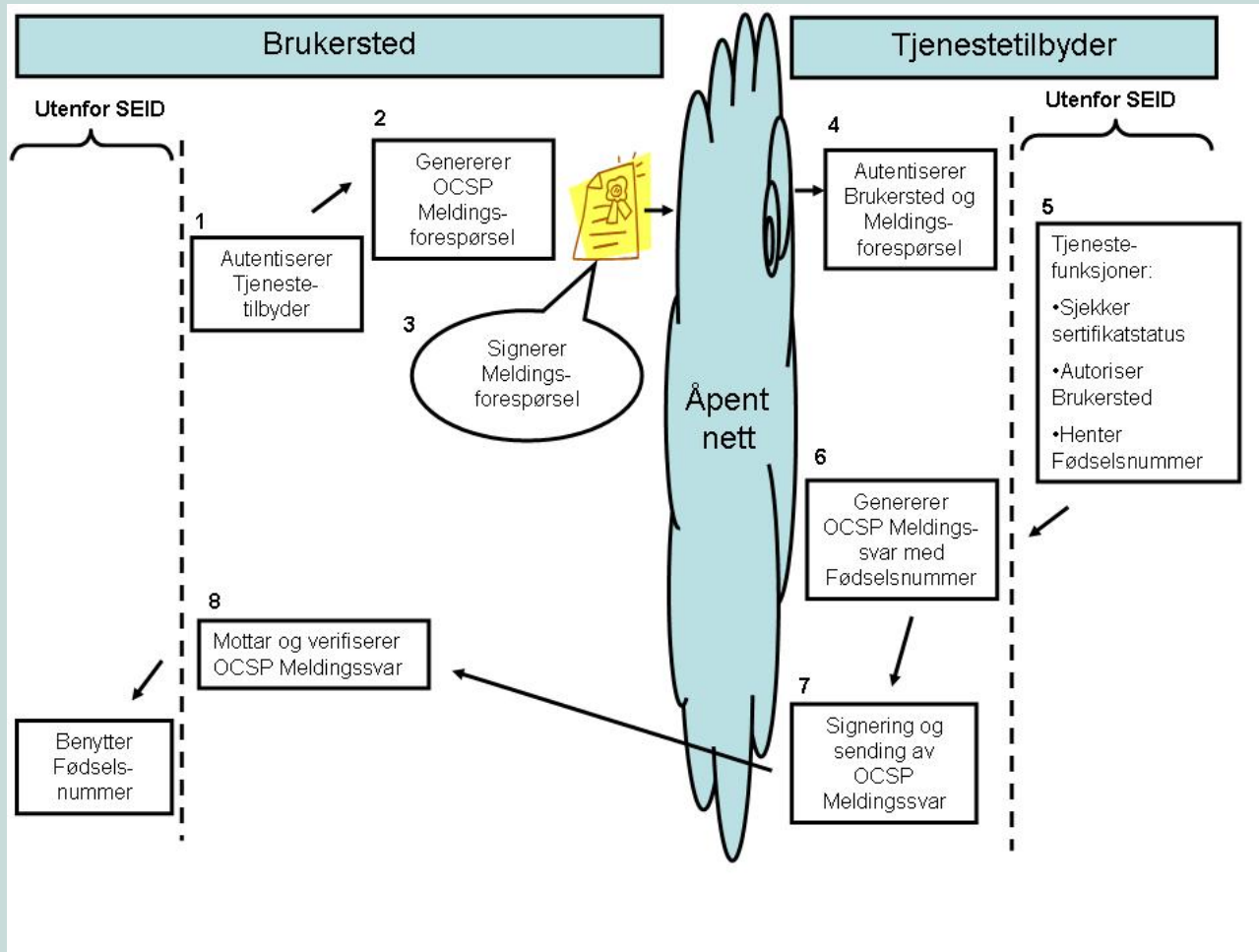
Eksempel, personnummer



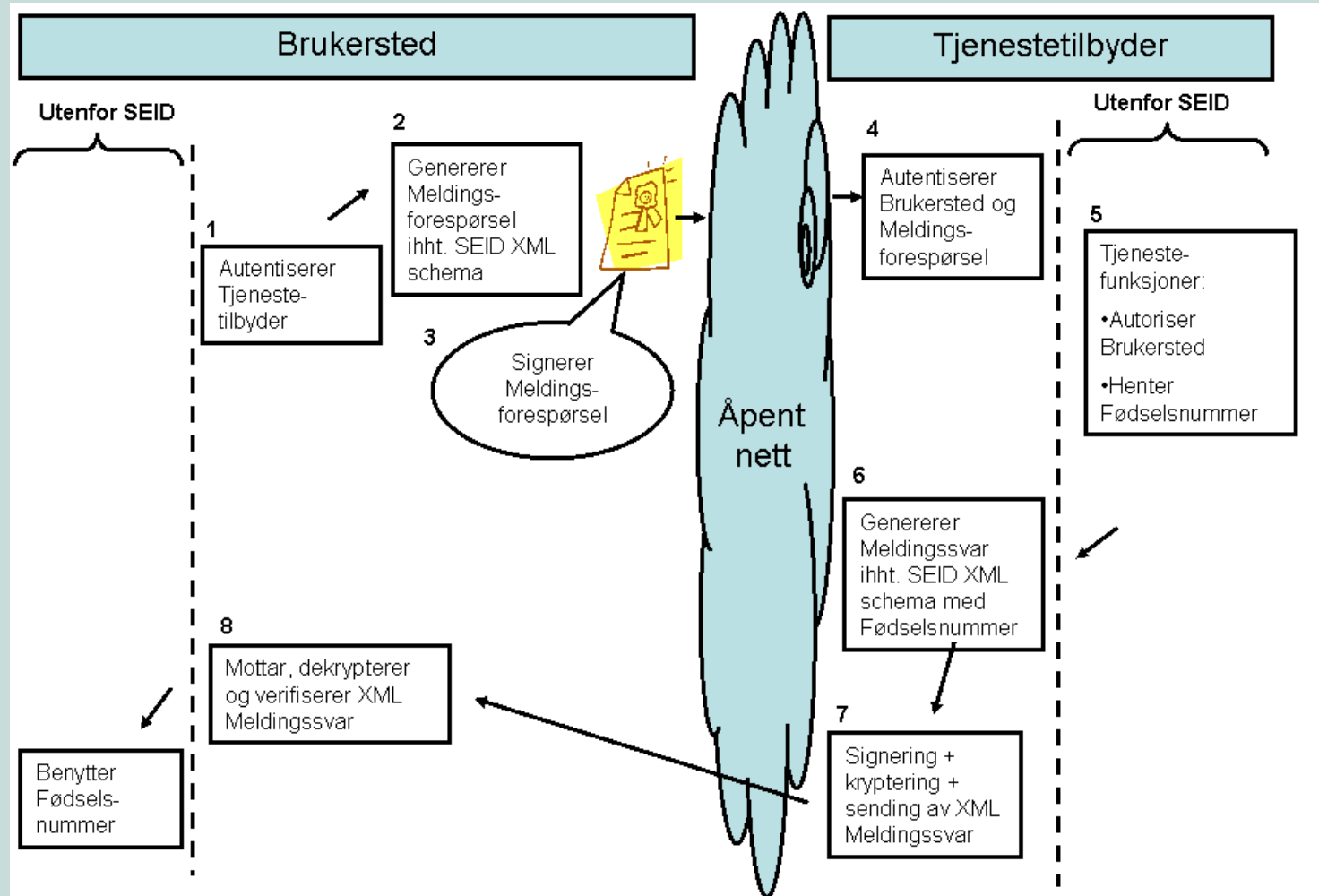
2 varianter i Seid for tilleggsinformasjon

- Integrert i handlingen sertifikatvalidering
 - Benytter protokollene OCSP eller SCVP
- Uavhengig av sertifikatvalidering
 - Benytter "SEID-XML" for overføring
 - Lignende løsning i Danmark
- 2 løsninger gjenspeiler at det er/var 2 leverandører med sine løsninger

Integrert oppslagstjeneste



Frittstående oppslagstjeneste



Sikkerhetskrav ved overføring

- I dokumentet:
 - Krav om autentisering og autorisasjon av brukersted
 - Krav om autentisering av leverandør
 - Krav om konfidensialitet av selve meldingene
 - Ikke krav om kryptering

- Kommentar:
 - Uheldig at det ikke kreves en angitt styrke i autentiseringen
 - Bør sette krav om signatur og minimum kryptografisk styrke (sterk nok RSA og SHA)
 - Uheldig at det ikke kreves kryptering av "følsom" informasjon (frivillig)

Om behov for næringslivet

Avbryt gjerne, vi skal jo gjerne ha en diskusjon.

Næringslivets behov

- Ser i hovedsak på næringslivet i betydning brukersted
- Antar bruk:
 - eHandel B2C
 - B2B neppe relevant ifm fødselsnummer ? Annet?
- Kostnader: integrasjon + kost PKI leverandør
- Inntekter: flere og bedre kunder?
- Sikkerhet: oppleves som trygt av alle parter?

Generelt

- Ansvarlig dokumentforvalter: Post og Teletilsynet
- Mer brukerstedsfokus i Seid?
- Ikke bare teknisk? Annet?

Fødselsnummer

- Ønsker/skal næringslivet ha fødselsnummer?
- Eksempler bruk
 - Helse
 - Finanstjenester
 - E-handel?
 - Neppe konsesjon på fødselsnummer
 - Tillatelse fra bruker?
 - Fødselsnummer nødvendig?
 - Bruke Unid for de som ikke har konsesjon på fødselsnummer og ikke vil være sertifikatbrugersted?

Andre opplysninger

- Andre opplysninger om bruker SEID bør standardisere nærmere?
 - Fysisk adresse
 - Tlf nr
 - Email adresse
- Tilleggstjeneste fra sertifikat utsteder

Frittstående og integrert

- Kan det være brukersteder som ikke vil benytte sertifikater men er interessert i tilleggstjenestene? Ref tidligere foil.
- Brukersteder vil klare å tilegne seg integrasjonskompetanse likt mhp de 2 alternativene?
 - XML mer kjent enn OCSP blant integratorer?
 - Er det relevant?
- Er XML formatet i "frittstående" ok for næringslivet? Tillegg?

Sikkerheten

- Er sikkerheten bra nok?
- NSM krever tilstrekkelig sterk kryptografisk styrke for systemer NSM har ansvar for:
 - Typisk SHA2, RSA2048, med mer
 - SHA1: har påviste svakheter
 - eForum: Vurdere å ”utfordre” leverandører på dette (kreve en plan)

Takk for meg!

Kontaktinformasjon:

John Bothner

john.bothner@nsm.stat.no

Telefon: 6786 4321 / 9921 5827