

# Offentlig eID og esignatur - veien videre

eKommune 2007

Tromsø 5 juni

Eivind Jahren, avdelingsdirektør

Fornyings- og administrasjonsdepartementet

# Hvorfor ny strategi for eID og e-signatur?

- ”Strategi for PKI-utbredelse i offentlig sektor” utløp i 2006
- Erfaringer fra arbeidet med felles offentlig sikkerhetsportal tilsa:
  - Bredere utgangspunkt når det gjelder teknologi
  - Finansieringsmodell som gir forutsigbarhet og bærekraft
  - Bedre forankring i offentlig sektors behov
  - Vurdering av det offentliges rolle
- For tiden gjelder for PKI-løsinger
- ”Kravspesifikasjon for PKI i offentlig sektor” (for PKI-løsinger)
- [http://www.regjeringen.no/upload/kilde/mod/rap/2004/0002/ddd/pdfv/234033-kravspek\\_pki\\_v102.pdf](http://www.regjeringen.no/upload/kilde/mod/rap/2004/0002/ddd/pdfv/234033-kravspek_pki_v102.pdf)
- Selvdeklarasjonsordning for eID-leverandører – hos Post- og teletilsynet ([www.npt.no](http://www.npt.no))

# Arbeidsgruppe for ny strategi

- Arbeidsgruppe ledet av FAD, med deltagelse fra:
  - Arbeids- og velferdsforvaltning-NAV
  - Skattedirektoratet
  - Sosial- og helsedirektoratet
  - Brønnøysundregistrene
  - KS
  - FAD
- Egen undergruppe for utvikling av rammeverk, ledet av FAD, med deltagelse fra Brønnøysundregistrene, Skattedirektoratet, NAV, Sosial- og helsedirektoratet og Kristiansand kommune.

# Arbeidsgruppens mandat

- Gi forslag til et rammeverk for sikkerhet i elektronisk kommunikasjon med og i forvaltningen hva angår autentisering og signering (sikring av uavviselighet)
- Foreslå strategi for forsyning av publikum med eID/e-signatur, og drøfte privat og offentlig sektors roller.
- Foreslå strategiske valg for felles offentlige løsninger for validering av eID og e-signatur, herunder mulig reetablering av en felles offentlig sikkerhetsportal.
- Foreslå strategiske valg for offentlig styring, spesielt for staten, herunder eierskap, forvaltning og garantiansvar.
- Foreslå strategiske valg av forretningsmodeller for bruk av fellesløsninger som virker som insentiver til spredning og bruk av eID/e-signatur.

# Ny strategi - utgangspunkter

- Strategiarbeidet har tatt utgangspunkt i en bred forståelse av eID som elektronisk identitet, som kan benyttes til autentisering og realiseres med ulike teknologier, herunder PIN-koder, sms-passord, PKI med mer.
- Elektronisk signatur forstås som løsninger som knytter et innhold til en identitet på en uavviselig måte. Løsningene kan realiseres gjennom PKI eller bruk av eID i kombinasjon med andre teknologier.

# Prosesen for strategiarbeidet

- Oppstart august 2006
- Dialog med flere leverandører av eID, portaler og integrasjons-løsninger mv.
- Samkjøring mot Justisdepartementets utredningsarbeid om nasjonalt ID-kort
- Drøfting av forslag i Faggruppen for eID og e-signatur under KoeF og i KS sitt IKT Fagråd.
- Bred offentlig høring, herunder kommunene og markedsaktører

# Anbefalinger fra arbeidsgruppen - rammeverk

- Rammeverk - Et sett med felles retningslinjer og krav som danner grunnlag for egne prosesser og vurderinger.
- Rammeverk for autentisering og uavviselighet:
  - **4 risikonivåer** knyttet til autentisering og behov for uavviselighet i elektroniske tjenester / kommunikasjon
  - **4 sikkerhetsnivåer** med krav til eID og e-signatur
- Risikonivåene motsvarer sikkerhetsnivåene

# Det foreslås 4 risikonivåer

- Nivå 1 er det lavest/ingen risiko for negative konsekvenser ved sikkerhetsbrudd i forbindelse med autentisering eller signering.
- Nivå 4 medfører store konsekvenser.
- Kriterier for vurdering av risikonivåer:
  - Konsekvenser for liv eller helse
  - Økonomisk tap/ merarbeid/ økte kostnader
  - Tap av renommé (anseelse, tillit og integritet)
  - Hindring i straffeforfølgelse
  - Uaktsomt bidrag til lovbrudd
  - Bryderi/ulempe

# Det foreslås 4 sikkerhetsnivåer

- Det er definert 4 sikkerhetsnivåer, der nivå 1 tilsvarer åpen informasjon, mens nivå 4 tilsvarer informasjon som kan være personsensitiv, forretningshemmeligheter og lignende.
- Sikkerhetsnivåer – kriterier for valg:
  - Krav til autentiseringsfaktorer og deres sikkerhetsegenskaper
  - Krav til prosedyre for utlevering av eID til bruker
  - Sikring av autentiseringsfaktorer ved lagring
  - Krav til uavviselighet (dvs. tilleggskrav som sikrer den og gir derved mulighet for elektronisk signatur)
  - Krav til offentlig godkjenning

# Anbefalinger fra arbeidsgruppen om valg av sikkerhetsnivå

## **Sikkerhetsnivå 4**

Felles tilgang til mange tjenester som krever høy sikkerhet, også tilgang til slike tjenester i virksomhetene. Vil etter hvert overta for løsninger på nivå 3.

## **Sikkerhetsnivå 3**

Felles tilgang til mange tjenester, også virksomhetenes egne tjenester som krever middels høy sikkerhet.

## **Sikkerhetsnivå 2**

De fleste eksisterende tjenester i virksomhetene. Skal over tid flytte slike tjenester over på sikkerhetsnivå 3.

## **Sikkerhetsnivå 1**

Åpen informasjon, direkte eller via portal.

# Forslag om forsyning av innbyggere med felles eID på sikkerhetsnivå 3

- Forslag om en felles ordning for utstedelse av eID på sikkerhetsnivå 3 – ”felles PIN-kode”. Gratis for brukere.
- Ordningen foreslås administrert av Skattedirektoratet.
- Det skal utvikles nærmere tekniske kravspesifikasjoner for denne type eID.
- Offentlige e-tjenester skal legge til rette for bruk av felles eID med en gang ordningen for distribusjon av eID er operativ.

# Forslag til forsyning av innbyggere med felles eID på sikkerhetsnivå 4

- Justisdepartementets arbeidsgruppe foreslår etablert en frivillig ordning for nasjonalt ID-kort med eID fra en offentlig utsteder. Brukeren skal betale kortgebyr.
- Nasjonalt ID-kort med eID er arbeidsgruppens forslag for distribusjon av eID på sikkerhetsnivå 4.
- Offentlig utstedt eID ("Person Høyt") kan i tillegg distribueres på andre kort, f.eks. helstrygdkortet til NAV.
- Plan B – rammeavtale med eID-utsteder i markedet.

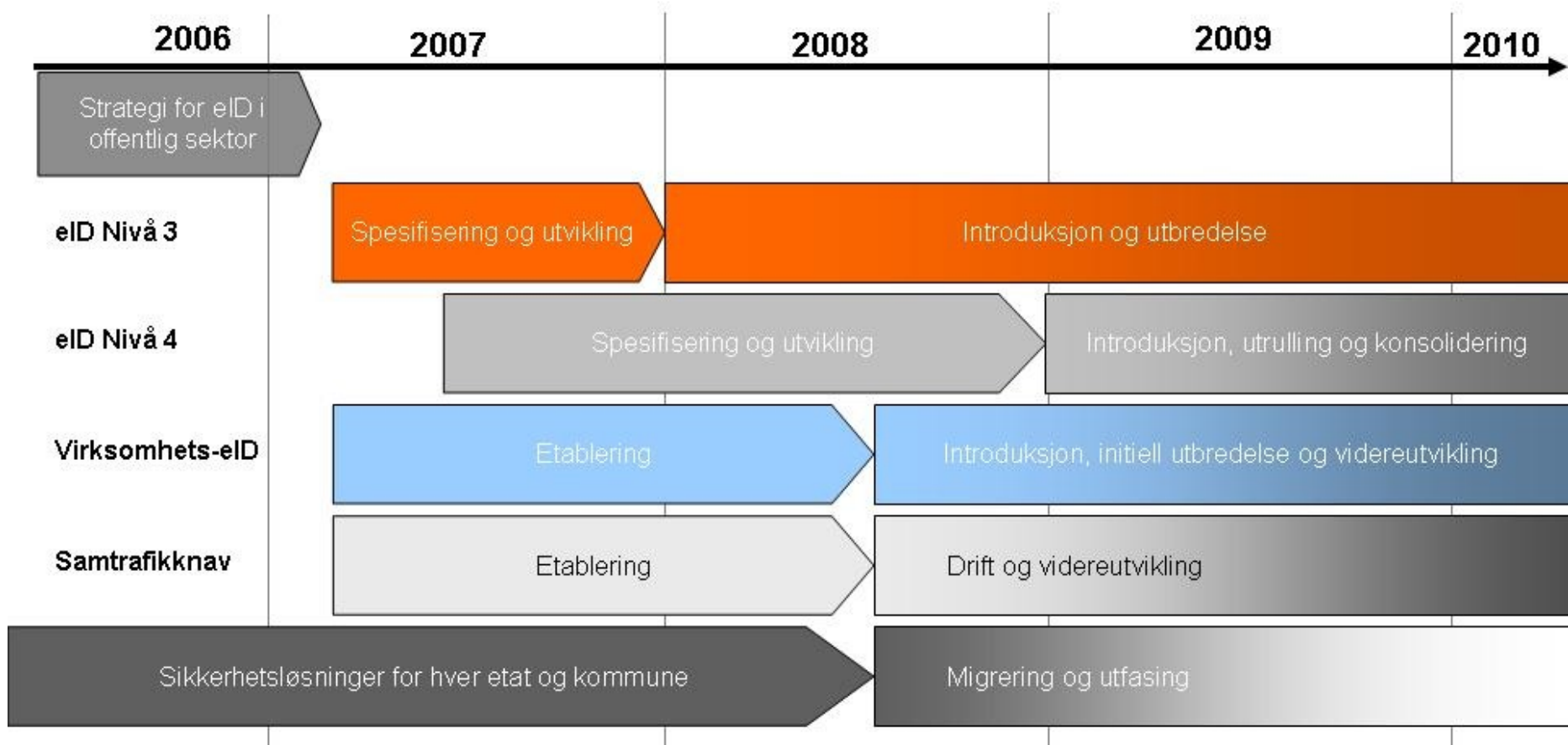
# Forslag om forsyning av virksomheter med felles eID

- Forslag om at Brønnøysundregistrene etablerer et tilbud for utstedelse av slike eID til alle organisasjoner som er registrert i Enhetsregisteret.
  - Offentlige virksomheter som vil skaffe seg en virksomhets-eID (**virksomhets sertifikater**) skal skaffe seg den fra Brønnøysundregistrene.
  - Ordningen er frivillig for ikke-offentlige virksomheter.
- Virksomhets-eID (virksomhetssertifikater) skal prises på en ikke-diskriminerende måte.

# Ny form for sikkerhetsportal

- Forslag om et offentlig **samtrafikknave** for eID og e-signatur med fire grunntjenester / funksjoner.
- Aktuelle tjenester:
  - Autentisering med felles eID
  - Signering med felles eID av webskjema, og i en lokal løsning (et fagsystem)
  - Digitalt arkiv (innsynsarkiv)
  - Felles pålogging.
- Flere tjenester på sikt, avhengig av behov
- Samtrafikknavet foreslås forvaltet av Brønnøysundregistrene.

# Strategiforslagets tids horisont



# Status

- FADs forslag om offentlig eID og esignatur har vært på bred høring. Høringsuttalelsene er i disse dager i ferd med å bli oppsummert.
- Det synes å være betydelig støtte for strategiforslaget, men også noen viktige innvendinger.
- Et hovedspørsmål er i hvilken grad det offentlige skal bruke tilbud i markedet.
- Parallelt har JD hatt sitt forslag om nasjonalt ID-kort på egen høring. Her er høringsfristen i disse dager.
- Ny strategi for offentlig eID og esignatur vil måtte ses i lys av uttalelser til begge forslagene.
- Teoretisk tidligste tidspunkt for beslutning om ny strategi vil være september/oktober dette året.