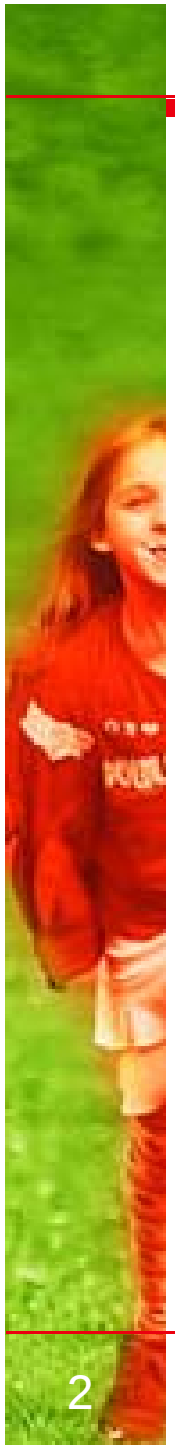
FORNYINGS- OG
ADMINISTRASJONSDEPARTEMENTET

Strategi for eID og e-signatur i offentlig sektor



Hvorfor ny strategi for eID og e-signatur?

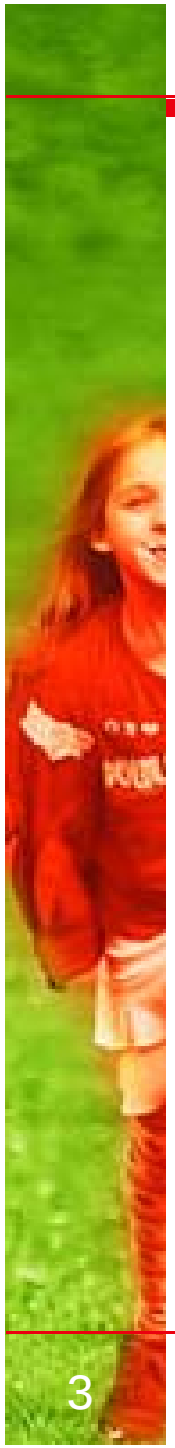
- Kravspesifikasjon for PKI i offentlig sektor – gjeldende forvaltningsstandard

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 valget elektronisk signatur)

- ”Strategi for PKI-utbredelse i offentlig sektor” utløp i 2006

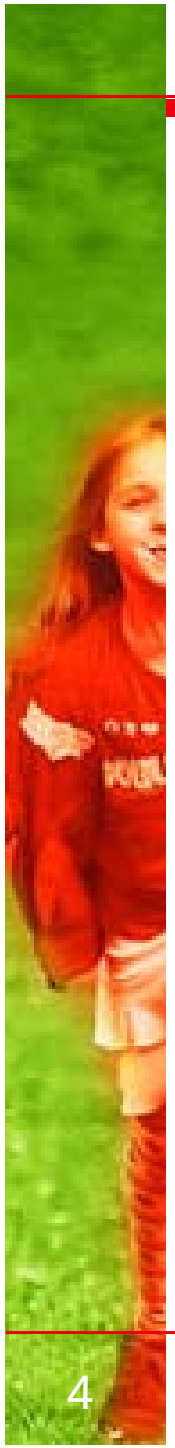
- Erfaringer fra arbeidet med felles offentlig sikkerhetsportal tilsa følgende:
  - Bedre forankring i offentlig sektors behov
  - Større grad av offentlig styring
  - Bredere utgangspunkt når det gjelder teknologi
  - Finansieringsmodeller som gir forutsigbarhet



Ny strategi - forutsetninger

- Strategiarbeidet tok 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 osv.

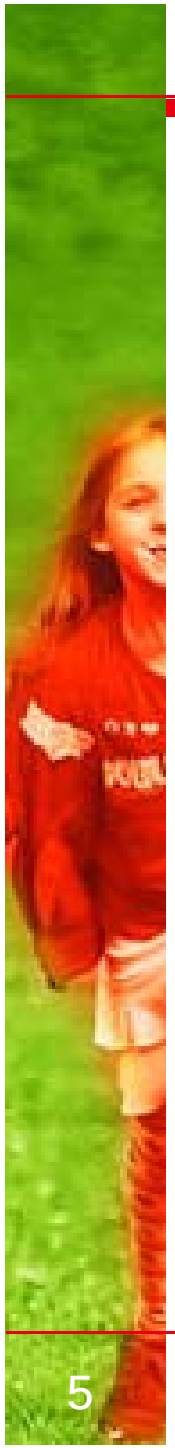
- Elektronisk signatur forstås her som løsninger som knytter et innhold til en identitet på en uavviselig måte. Løsningene kan realiseres gjennom PKI eller bruk av eID i kombinasjon med andre teknologier.



Mandatet for strategiarbeidet

- etablering av et rammeverk for sikkerhet[1] i elektronisk kommunikasjon med og i forvaltningen
- strategier for forsyning av publikum med eID/e-signatur - privat sektors og offentlig sektors rolle
- strategiske valg for felles offentlige løsninger for validering av eID og e-signatur, herunder mulig reetablering av en felles offentlig sikkerhetsportal
- strategiske valg for offentlig styring og spesielt for statens rolle, herunder eierskap, forvaltning og garantiansvar
- strategiske valg av forretningsmodeller for bruk av fellesløsninger som virker som insentiver for aktuelle aktører til spredning og bruk av eID/e-sign

[1]i forbindelse med autentisering og signering (sikring av uavviselighet)



Prosessen for strategiarbeidet

- 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.

Prosessen for strategiarbeidet

- Oppstart august 2006
- Dialog med flere leverandører av eID, portaler og integrator-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 – februar 2007 til april 2007

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

- Risikonivåer – kriterier for valg:
  - 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
- Nivå 1 er det lavest/ingen risiko for negative konsekvenser ved sikkerhetsbrudd i forbindelse med autentisering og/eller signering.
- Nivå 4 medfører store konsekvenser.

Det foreslås 4 sikkerhetsnivåer

- 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
- Det er definert 4 sikkerhetsnivåer, der nivå 1 tilsvarer åpen informasjon, mens nivå 4 tilsvarer informasjon som kan være personsensitiv, forretningshemmeligheter og lignende.

Anbefalinger fra arbeidsgruppen – valg av felles 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.

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.

Forsyning av innbyggere med felles eID på sikkerhetsnivå 4

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

Forsyning av virksomheter med felles eID

- Forslag om at Brønnøysundregistrene etablerer et tilbud for utstedelse av slike eID[1] til alle organisasjoner som er registrert i Enhetsregisteret.
- Offentlige virksomheter som vil skaffe seg en virksomhets-eID (**virksomhetssertifkater**) skal skaffe seg den fra Brønnøysundregistrene.
- Ordningen er frivillig for ikke-offentlige virksomheter.
- Virksomhets-eID (virksomhetssertifikater) skal prises på en ikke-diskriminerende måte.

[1] *Virksomhetssertifikater iht. Kravspesifikasjon for PKI i offentlig sektor.*

Ny form for sikkerhetsportal

- Forslag om et offentlig **samtrafikknav** for eID og e-signatur med fire grunntjenester / funksjoner.
- Samtrafikknavet foreslås forvaltet av Brønnøysundregistrene.
- Grunnleggende 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

Forretningsmodell

- Offentlig finansiert ordning for distribusjon av ”felles PIN-kode”.
- Gebyrfinansiert ordning for nasjonalt ID-kort med eID (kan også brukes mot private tjenester).
- Brukeren skal ikke betale for bruken av eID mot offentlige tjenester.
- Bruken av eID skal ikke prises mot offentlige virksomheter.
- Bruken av samtrafikknav foreslås finansiert sentralt for statlige virksomheter.
- Kostnadsbasert årlig avgift for bruken av samtrafikknavet i kommunene.

Strategiens tidshorisont