

KS Ikt-forum sikkerhetsgruppa



v/Veronica Jarnskjold Buer

Presenterer.....



EN ANBEFALING – ikke fasit

- Gruppa har bestått av:

- **Magnus Alsaker (sekretær)**
- Kolbjørn Johansen
- Håkon Foss
- Håvard Haugsvær
- Lisbet Nederberg
- Veronica Jarnskjold Buer
- Karine Engebretsen
- Ulf Harry Evensen
- Margrethe Noraas
- Roger Hansen
- Sigurd Lunde
- Tore Moss
- Arild Fredriksen
- Roy Kenneth Grundetjern
- Tommy Otnes
- Asbjørn Renberg
- Arnfinn Auestad



Mandat: Spesifikt ansvarsområde for faggruppen for sikkerhet

1. Kobling mot MinSide og bruk av PIN-kode løsningen

- Lage "kokebok" for hvordan kommuner kan nyttegjøre seg av PIN-kode løsningen og koble seg opp mot MinSide

2. Vurdere krav til sikkerhet for ulike tjenester (skjemaer)

- For hvilke tjenester er det tilstrekkelig med PIN-kode løsningen i MinSide, hvilke tjenester krever et høyere sikkerhetsnivå (for eksempel digital signering og PKI).

3. Felles sikkerhetsstrategi for "tjenester på nett", noen stikkord for dette er:

- Kommunikasjon fra "tjenestene på nett" mot kommunenes fagsystemer
- Kommunikasjon fra kommunens fagsystemer til "tjenester på nett" (for eksempel preutfylling av informasjon, tilgang til tidligere søknader og lignende)
- Teknologiske utfordringer som for eksempel brannmurer/soneinndelinger etc. (jf. Datatilsynet sine anbefalinger)



Forutsetning:

- Vi forutsetter at kommuner som ønsker kommunale tjenester på nett – elektroniske søknader – allerede tilfredsstillende de sikkerhetskrav som Datatilsynet setter i *Veileder for kommuner og fylker*



Informasjonsplikten

- Informasjonsplikt når det samles inn opplysninger fra den registrerte – personopplysningsloven § 19:
Når det samles inn personopplysninger fra den registrerte selv, skal den behandlingsansvarlige av eget tiltak først informere den registrerte om
 - a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant
 - b) formålet med behandlingen
 - c) opplysningene vil bli utlevert, eventuelt hvem som er mottaker
 - d) det er frivillig å gi fra seg opplysningene
 - e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, f.eks. informasjon om retten til å kreve innsyn og retten til å kreve retting



Oppfatning:

- MinSide er pr. i dag en løsning som ikke er tilrettelagt for å håndtere sensitiv informasjon
- MinID: Autentiseringsløsning som brukes på MinSide. Nivå 3, kan brukes til ordinære personopplysninger (var/er en nødløsning)



Ingen overraskelse:

- Utfallet av kontroll som Datatilsynet gjennomførte ingen overraskelse
- Sikkerhetsgruppa har hatt 2 møter med Datatilsynet vedrørende innholdet i gruppas anbefalinger
- Og gruppa er udelt positive til hva kontrollen har medført hos skjemaleverandøren – nemlig opprydding. Anbefale kontroll hos de øvrige skjemaleverandører.



Datafangst:

- Ikke skjemaer/søknader med sensitive personopplysninger
- Transport – 100% sikkerhet (putt i hva du vil)
- Meldingskryptering om du benytter deg av tredje part (innbygger ↔ ASP ↔ kommunen)
- Kanalkryptering ved skjemaløsning i eget hus
– kommunikasjon mellom to parter (innbygger ↔ kommunen)



Forts. datafangst

- Autentisering bare ved preutfylling og ved skjemaløsning i "eget hus" (ikke tredje part)
- Personnummer brukes kun ved saklig behov (holder ikke med: "..fordi jeg skal fakturere kunden etterpå..")
- SSL-sertifikat på kommunens hjemmeside



Innsyn

- Aldri innsyn uten autentisering
- Autentisering – MinID holder bare ved tilgang til ordinære personopplysninger
- Ikke innsyn til sikret sone før nivå 4-løsning og 100 % vanntette registeroppslag
- Kommunene bør vurdere autentisering ved nivå 4 => departementene MÅ på banen.
- Preutfylling = innsyn = kommunal sak



ASP-løsning:

- Skjemaleverandøren kun en databehandler som opptrer på vegne av kommunen
- Databehandleravtale, kommunen fremdeles ansvarlig for sikkerhet
- Større "frihet" for kommunen ved skjemaløsning i eget hus