

KS



Sikkerhet for tjenester på nett

Kommunens ansvar for informasjonssikkerhet

Kommunens ansvar

- De fleste kommuner benytter seg av skjemaløsninger fra ASP-leverandører
 - Kommunen er den behandlingsansvarlige
 - Skjemaleverandøren opptrer som en databehandler på vegne av kommunen
- Gjennom sin rolle som behandlingsansvarlig skal kommunen påse tilfredsstillende håndtering av kommunens data
- Risikovurderinger er sentralt med å vurdere krav til sikkerhet
- Utarbeidet anbefalinger fra sikkerhetsgruppa i "Tjenester på nett"-prosjektet



Autentisering av borger

- Autentisering er å verifisere påstått identitet
- Vurder aktuelle autentiseringsmekanismer
 - Borger blir autentisert på sikkerhetsnivå 3 gjennom Minid eller tilsvarende
 - Borger blir autentisert på sikkerhetsnivå 4 gjennom en PKI-løsning eller tilsvarende



Minid og Minside

- Minside er felles innbyggerportal for offentlige tjenesteleverandører
- Minside bruker Minid som autentiseringsløsning
- Borgeren kan bevege seg sikkert mellom offentlige tjenesteleverandører uten å måtte gjenta pålogging
- Minid kan også benyttes som autentiseringsløsning på kommunenes egne portaler
- Minid er definert til å være på sikkerhetsnivå 3 i FAD sin definisjon av nivå for krav til autentisering
- Består av faktorene:
 - Fødselsnummer (brukernavn)
 - Selvvalgt passord
 - Engangs PIN-kode



Minid

- Styrker ved Minid
 - Nasjonal løsning
 - Utbredt til borgerne
- Svakheter ved Minid
 - Masseutsendelse kan medføre tilgang for uvedkommende
 - PIN-koder og fødselsnummer distribueres sammen
 - Sikkerhetsnivå 3 begrenser hvilke tjenester som kan publiseres
 - Er beregnet for autentisering – har ikke funksjonalitet for elektronisk signering



PKI

- PKI står for Public Key Infrastructure
- PKI er en beskrivelse av en infrastruktur der privat og offentlige nøkler benyttes for å muliggjøre sikker elektronisk kommunikasjon
- Omfatter infrastruktur og tjenester for sikring av informasjonsutveksling og tilgang til systemer
 - Elektronisk signering
 - Autentisering av kommunikasjonsparter eller brukere av systemer
 - Sikring av integritet og konfidensialitet ved overføring/utveksling av informasjon (kryptering)
 - Ikke-benektning
 - Innholdet knyttes bindende til avsender, som regel i forbindelse med personlig elektronisk signatur



PKI

- Styrker med PKI:
 - Autentisering på sikkerhetsnivå 4
 - Kan benyttes for tilgang til sensitiv informasjon
 - Kan gi støtte for elektronisk signering
- Svakheter med PKI:
 - Krever fysisk gjenstand (for eksempel smartkort) dersom det skal være en sterk PKI-løsning



Elektronisk signatur på tre nivåer

- Elektroniske signaturer
 - Alle metoder som knytter en aktør til en handling eller spesifikk informasjon
 - Aktør må være autentisert
 - Handling bør være eksplisitt og valgt av aktøren
 - Sporbarhet gjennom logger
- Avanserte elektroniske signaturer
 - Sikker knytning mellom signatur og informasjon slik at endringer kan oppdages. Bare signerer har tilgang til signeringsmetode
 - Eneste teknologi i dag er digital signatur med PKI-basert eID
 - Løsninger med kvalifiserte sertifikater (for eksempel Buypass og BankID)
- Kvalifiserte elektroniske signaturer
 - Avansert signatur med tilleggskrav til utsteder av eID og til signeringsutstyr
 - Gir garantert rettsvirkning som håndskrevet signatur etter eSignaturloven
 - Kvalifisert signatur finnes ikke i det norske markedet i dag



Datafangst og innsyn

- To separate problemstillinger
 - Utfylling og innsending av skjema til kommunen, der skjema og/eller vedlegg kan inneholde sensitiv personinformasjon
 - Innsyn i egen sak hos kommunen, der saksinnholdet kan inneholde sensitiv personinformasjon



Datafangst

- Vær oppmerksom på følgende der personopplysninger kan oppgis i skjema eller som vedlegg i skjema:
 - Kommunen er behandlingsansvarlig
 - Dersom ASP-leverandør på skjema – husk databehandleravtale
 - Søker identifiseres med fødselsnummer (brukernavn)
 - Krever kryptering av enten informasjonen eller transportkanalen
 - Dersom det er mulig å registrere eller legge ved sensitive opplysninger anbefales det autentiseringsløsninger som PKI eller med tilsvarende sikkerhetsnivå 4



Vurdering av det enkelte skjema

- Hvilke opplysninger spørres det etter i skjemaet?
- Hvilket fagsystem skal opplysningene til?
- Hvordan skal opplysningene saksbehandles?
- Hvilke tjenester utløses av skjemasøknaden?



Skjema som ikke inneholder sensitiv informasjon

- Rekvisisjon av kartforretning
- Søknad kulturskole
- Melding om tiltak
- Gravemelding
- Svar offentlig høring
- Tilskudd til kulturformål
- Bestilling av avfallsbeholder
- Skjenkebevilling



Skjema som kan inneholde sensitive opplysninger

- Søknad om barnehageplass
- Søknad SFO
- Lærerstilling/ledig stilling



Skjema hvor det etterspørres sensitive opplysninger

- Ledsagerbevis
- Søknad pleie- og omsorgstjenester
- Parkeringstillatelse med legeattest
- Søknad om sosialstøtte



Tekniske løsninger

- Generelle sikkerhetsprinsipper skal ivareta krav til
 - Konfidensialitet
 - Sikre at informasjonen bare er tilgjengelig for de som skal ha tilgang
 - Tilgjengelighet
 - Sikre at informasjonen er tilgjengelig innenfor de krav som er satt
 - Integritet
 - Sikre at informasjonen er korrekt og fullstendig
 - Sikre at informasjonen ikke er endret av uvedkommende
 - Sporbarhet
 - Ha nødvendige metoder og mekanismer som skal knytte alle endringer av informasjon til den som har utført endringene



Bruk av fødselsnummer

- Fødselsnummer skal bare brukes
 - Ved saklig behov
 - Når det ikke finnes andre mulige løsninger for å oppnå tilfredsstillende identifikasjon
- Overføring av fødselsnummer skal alltid krypteres
- Fødselsnummer skal generelt ikke brukes til autentisering
- Å innhente fødselsnummer fordi fagsystemet av datatekniske årsaker bruker dette som nøkkelfelt, anses ikke som en saklig grunn



Transaksjonslagring og mellomlagring hos leverandør

- Skjemaleverandør kan lagre skjemadata i maks 72 timer
- Skjema og evt. vedlegg må slettes når kommunen bekrefter å ha mottatt dette
- Skjemaleverandør har ikke grunnlag for å mellomlagre, for eksempel delvis utfylte skjema, POL §11 og 15
- Preutfylling av visse typer data må skje gjennom at skjemaløsning henter data fra kommunens register
 - Preutfylling krever særskilt samtykke fra innbyggeren



Teknisk lagring hos skjemaleverandør

- Det skal være logiske skiller på data tilhørende ulike databehandlingsansvarlige
 - Egne databaser for hver databehandlingsansvarlige
- Sensitiv informasjon skal krypteres ved lagring hos skjemaleverandøren
- Sensitiv informasjon skal lagres i en sikker sone hos skjemaleverandøren



Sikker datakommunikasjon

- Kryptert transportkanal
 - Etablere sikker overføringslinje mellom skjemaleverandør og kommunen som brukes for å overføre data
 - Data vil være ubeskyttet når de kommer ut av den krypterte transportkanalen
- Meldingskryptering
 - Kryptering av selve informasjonen innebærer at informasjonen som sendes over blir kryptert ved for eksempel virksomhetssertifikater i en PKI-løsning
 - Informasjonen vil ligge kryptert til kommunen velger å dekryptere dataene
- Ved kommunikasjon mellom systemer må kommunen sørge for sikker autentisering av systemene ved overføring, slik at ingen uautoriserte systemer får mulighet til datatransport mellom skjemaleverandør og kommunen



Mottak av data i kommunen

- Det bør etableres dedikert server som er konfigurert til å ta imot skjemadata fra skjemaleverandør
 - Godkjent IP-adresse
 - Dedikert DMZ
- Det må aldri lagres usikret i DMZ
 - Data skal være kryptert så lenge de er i DMZ
 - Dekryptering foretas på innsiden av DMZ/intern sone
 - For sensitiv informasjon som skal til sikker sone skjer dekrypteringen i sikker sone, jfr. Kommuneveilederen fra Datatilsynet, kap. 18.3.2
- Alle innkomne data og vedlegg må skannes for ondsinnet kode
- Kommunen bør initiere datatrafikken inn til kommunens nettverk
 - Kommunen kan hente data fra skjemaleverandør (ftp/WS)
 - Kommunen kan kun tillate trafikk inn til dedikert server i DMZ. Kommunen henter data herfra til aktuelle systemer



Forvaltning av kommunens opplysninger

- Det bør opprettes en oversikt over alle behandlinger av helse- og personopplysninger i virksomheten
 - Viktig styringsdokument for informasjonssikkerhet
 - Praktisk redskap i det gjennomførende arbeidet
 - Viktig bidrag til den generelle internkontrollen
- Det bør opprettes rutiner for ”skjema på nett” som sørger for tilfredsstillende informasjonssikkerhet
- Kommunen skal ha dokumentasjon over de systemene som brukes til å behandle data i tilknytning til skjema på nett



Informasjonsplikt til borger

- Ved innhenting av opplysninger fra borger har kommunen plikt til å informere innbyggeren om den datafangsten som skjer, POL §19
- Borger bør aktivt kunne godkjenne personvernerklæringen før datafangst kan avsluttes
- Beskrive hvordan innsamling av data foregår, hvordan og hvor lenge informasjonen eventuelt lagres



Bruk av samtykke

- Samtykke til behandling av personopplysninger
 - Ved innhenting av personopplysninger må kommunen som hovedregel innhente samtykke før databehandlingen tar til
- Krav til samtykket
 - Et samtykke skal være en frivillig, uttrykkelig og informert erklæring fra den opplysningene gjelder, om hun eller han godtar behandling av opplysninger om seg selv
- Informert samtykke
 - Den som skal registreres må få tilstrekkelig informasjon til å forstå hva samtykket gjelder og hvilke konsekvenser det kan få.
- Frivillig samtykke
 - Ikke avgitt under tvang, verken fra den behandlingsansvarlige eller fra andre
- Uttrykkelig samtykke
 - Borgeren må foreta seg noe aktivt for å samtykke



Utfordringer i dag

- Minside håndterer kun ikke-sensitiv informasjon
- Mangler nasjonal ID til innbyggerne
 - I dag støtter flere kommuner både løsninger fra Minid, BankID og Buypass, dette er både fordyrende og ressurskrevende
- Mangler nasjonal infrastruktur for elektronisk signering
 - Offentlig samtrafikknave er på vei

