

”Tjenester på nett”

Anbefalinger fra sikkerhetsgruppa

Innholdsfortegnelse

Innholdsfortegnelse.....	3
Sentrale begreper.....	6
1. Bakgrunn.....	9
1.1. Målgruppe for dokumentet.....	9
1.2. Om skjemaløsninger og skjermdialoger.....	9
2. Bruk av Minid og oppkobling til Minside.....	10
2.1. Om bruk av Minid.....	10
3. Anbefalinger til autentisering av borger.....	11
3.1. Aktuelle autentiseringsmekanismer.....	11
3.1.1. Kort om Minid.....	11
3.1.2. Kort om PKI.....	12
3.2. Problemstillinger rundt datafangst og autentisering.....	12
3.2.1. Datafangst, skjemautfylling.....	12
3.2.2. Innsyn i egen sak hos kommunen.....	14
3.3. Krav til autentisering av borger.....	14
3.3.1. Mulige trusler ved datafangst.....	14
3.3.2. Mulige trusler ved innsyn.....	16
3.3.3. Konsekvenser dersom sensitive opplysninger skal håndteres.....	16
3.3.4. Hva omfatter datafangsten.....	17
3.3.5. Anbefalinger til autentisering av innbyggeren.....	17
3.4. Skjema som har krav til utfylling fra flere enn en part.....	20
3.5. Krav til elektronisk signatur fra borger.....	21
3.6. Risikovurdering av skjemaløsningene.....	22
4. Beskrivelse og anbefaling av tekniske løsninger.....	23
4.1. Generelle sikkerhetsprinsipper.....	23
4.2. Generelt om transportmetoder.....	24
4.2.1. FTP/SFTP.....	24
4.2.2. HTTP/HTTPS.....	24
4.2.3. E-post.....	24
4.2.4. Webservices.....	25
4.2.5. ebXML.....	25
4.2.6. VPN.....	26
4.3. Sikring av datafangst fra borger.....	27

4.3.1. Sikring av datakommunikasjonen.....	27
4.3.2. Ikke sikret datakommunikasjonen.....	29
4.3.3. Typer vedlegg som kan sendes ved.....	29
4.3.4. Teknisk sikring av datafangstløsningen.....	29
4.4. Autentisering og bruk av fødselsnummer.....	30
4.4.1. Bruk av fødselsnummer i dag.....	30
4.5. Datahåndtering når skjemaløsning ligger hos en databehandler.....	31
4.5.1. Transaksjonslagring og mellomlagring hos skjemaleverandør.....	32
4.5.2. Datahåndtering med og uten autentisering av borger.....	33
4.5.3. Kvittering på innsendt skjema.....	34
4.6. Datahåndtering når skjemaløsning ligger hos behandlingsansvarlig.....	35
4.6.1. Transaksjonslagring og mellomlagring hos kommunen.....	35
4.6.2. Med autentisering av borger.....	35
4.6.3. Uten autentisering av borger.....	36
4.7. Sikring av datakommunikasjon.....	36
4.7.1. Sikker datakommunikasjon.....	36
4.7.2. Dataintegritet.....	37
4.7.3. Kvitteringsmekanismer.....	37
4.7.4. Anbefalte transportmetoder.....	37
4.7.5. Autentisering av systemene.....	37
4.8. Datahåndtering hos kommunen.....	38
4.8.1. Mottak av data i kommunen.....	39
4.8.2. Eksempel på teknisk løsning	40
4.9. Tilgang og innsyn i data hos kommunen.....	40
4.10. Tilbakemelding fra kommune til borger.....	42
5. Arbeid med informasjonssikkerhet.....	44
5.1. Kommunens ansvar.....	44
5.1.1. Oversikt over behandlinger av helse- og personopplysninger.....	44
5.2. Rutine for ”skjema på nett”	45
5.3. Kommunen må dokumentere tilfredsstillende informasjonssikkerhet.....	45
5.4. Bruk av databehandler og databehandleravtale.....	45
5.5. Informasjonsplikt til borgeren.....	47
5.5.1. Informasjonsplikt når det innhentes opplysninger fra borger.....	47
5.5.2. Samtykke fra borger.....	48
Referanseliste.....	51
Vedlegg A – Figurforklaring.....	52

<u>Vedlegg B – Mal for vurdering av krav til autentisering.....</u>	<u>53</u>
<u>Vedlegg C – Eksempel på risikovurdering av skjemaløsning.....</u>	<u>56</u>
<u>Eksempel på kartlagte risikoer og trusselvurderinger.....</u>	<u>57</u>

Sentrale begreper

- Minside
- Minside er en felles borgerportal på Internett for de offentlige kontorene i Norge. Formålet med siden er at befolkningen skal ha en Internettside å henvende seg til om de ønsker kontakt med det offentlige og kunne søke om ting som skattekort og melde om flytting. Minside benytter Minid som autentiseringsløsning. Se www.norge.no/minside/ for mer informasjon.
- Minid
- Minid er en "single sign on/off" autentiseringsmekanisme for offentlig nettsteder som benyttes blant annet av Minside. Minid muliggjør at innbyggerne kan logge seg på ett nettsted med Minid og sikkert bevege seg mellom offentlig nettsteder (tjenesteleverandører) uten å måtte gjenta pålogging. Minid kan også benyttes som autentiseringsløsning på egne portaler. Dvs. en kommune eller en etat kan bruke Minid som autentiseringsløsning for sitt eget nettsted. Den eneste forutsetning er at alle relevante tjenester også tilbys i Minside
- Autentisering
- Autentisering er å verifisere påstått identitet.
- PKI
- PKI (Public Key Infrastructure) er en teknologi for utstedelse, administrasjon og bruk av digitalt sertifikat over datanett. Anvendelsesområder for PKI er autentisering (legitimering av en person, organisasjon eller gjenstands identitet), autorisasjon (tildeling av rettigheter til IT-systemer), digital signatur (av dokumenter eller programvare), og verifisering av dataintegritet (non-repudiation).
- Elektronisk ID
- Elektronisk ID er en generell betegnelse for noe som kan identifisere en bestemt person og som kan sendes elektronisk. Elektronisk ID kan være et sett med sertifikater og tilhørende private nøkler for hhv. signering, autentisering og kryptering.
- Elektronisk signatur
- Elektronisk signatur er et begrep som bl.a. er definert i eSignaturloven § 3 nr. 1. Elektronisk signatur er i esignaturloven definert på følgende måte: "*data i elektronisk form som er knyttet til andre elektroniske data og som brukes som autentiseringsmetode*".
- avansert elektronisk signatur
- En elektronisk signatur som
 - o er entydig knyttet til undertegneren,
 - o kan identifisere undertegneren,
 - o er laget ved hjelp av midler som bare undertegneren har kontroll over, og
 - o er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering

- kvalifisert elektronisk signatur - En avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem,
- Elektronisk sertifikat - Et elektronisk sertifikat er enkelt sagt legitimasjon i elektronisk form. Et elektronisk sertifikat benyttes særlig over åpne nett (som Internett) for å bevise at man er den man gir seg ut for å være. Elektroniske sertifikater benyttes også for å kontrollere at en elektronisk signatur er en gyldig og ekte signatur, og ikke en forfalsket elektronisk signatur.
- Sikkerhetsnivå 3 - FAD sin definisjon av nivå for krav til autentisering. Minid er definert til å være på nivå 3. Andre løsninger kan være:
- o Passordkalkulatorer beskyttet med PIN-kode, der første PIN-kode er sendt i separat forsendelse
 - o Engangspassord på mobiltelefon, der mobiltelefonen er registrert med en egen registreringskode distribuert til folkeregistrert adresse.
 - o Person Standard iht. Kravspesifikasjon for PKI i offentlig sektor
 - o Engangspassordlister benyttet sammen med fast passord og brukernavn. Valg av fast passord skal skje på bakgrunn av en engangskode sendt til folkeregistrert adresse (eventuelt første kode på engangspassordlisten)
- Sikkerhetsnivå 4 - FAD sin definisjon av nivå for krav til autentisering. I henhold til gjeldende regelverk må løsningene være selvdeklart i Post- og teletilsynet i forhold til om de oppfyller krav i Kravspesifikasjon for PKI i offentlig sektor når det gjelder Person Høyt og Virksomhet.
- Demilitarisert sone (DMZ) - en sone hvor brukere utenfor virksomheten kan gis tilgang, men som er skilt fra virksomhetens øvrige informasjonssystem ved hjelp av en sikkerhetsbarriere.
- Behandlingsansvarlig - Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes
- Databehandler - Den som behandler personopplysninger på vegne av den behandlingsansvarlige.
- Databehandler er en ekstern person eller virksomhet utenfor den databehandlingsansvarliges virksomhet. Det vil si at den databehandlingsansvarliges egne medarbeidere ikke er dennes databehandlere
- Fødselsnummer - Fødselsnummer er definert slik Forskrift om folkeregistrering (<http://www.lovdato.no/cgi-wift/ldles?doc=/sf/sf/sf-20071109-1268.html>):
§ 2-2. *Fødselsnummer*
Fødselsnummeret skal ha elleve siffer. De seks første siffer består av vedkommendes fødselsdato i rekkefølge to siffer for

dag, to for måned, to for år. De fem siste siffer, personnummeret, består av tre individualsiffer og to kontrollsiffer.

Sensitive
personopplysninger

- Jfr. Personopplysningsloven § 2 (se <http://www.lovdata.no/all/hl-20000414-031.html#28>):

Personopplysningsloven § 2. Definisjoner

I denne loven forstås med:

- 1) personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson,
- 2) behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter,
- 3) personregister: registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen,
- 4) behandlingsansvarlig: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes,
- 5) databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige,
- 6) registrert: den som en personopplysning kan knyttes til,
- 7) samtykke: en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv,
- 8) sensitive personopplysninger: opplysninger om
 - a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
 - b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
 - c) helseforhold,
 - d) seksuelle forhold,
 - e) medlemskap i fagforeninger.

1. Bakgrunn

Dette dokumentet er en oppsummering av det arbeidet og anbefalingene som faggruppen for sikkerhet har jobbet med i prosjektet ”Tjenester på nett”.

Arbeidsgruppen har bestått av:

Navn	Kommune	E-post
Karine Engebretsen	Halden	karine.engebretsen@halden.kommune.no ;
Eivind Olsen	Asker	Eivind.olsen@asker.kommune.no ;
Kolbjørn Johansen	Asker	Kolbjorn.johansen@asker.kommune.no ;
Lisbet Nederberg	Skedsmo	lisbet.nederberg@skedsmo.kommune.no ;
Håkon Foss	Lier	hakon.foss@lier.kommune.no ;
Ulf Harry Evensen	Smålenesveven	ulf@smaalensveven.no ;
Håvard Haugsgjerd	Drammen	Havard.haugsgjerd@d-ikt.no ;
Veronica Jarnskjold Buer	Aurskog-Høland	vjb@ahk.no ;
Pål Gjerde	Skedsmo	palg@skedsmo.kommune.no ;
Magnus Alsaker	<i>Sekretær</i>	Magnus.alsaker@kith.no

1.1. Målgruppe for dokumentet

Målgruppen for dokumentet er it-personell, leverandører og andre som arbeider med å tilrettelegge for elektroniske skjema tilgjengelige for borgeren via Internett. Språkdrakten i dokumentet er teknisk og det vil være en fordel med god it-kompetanse for å forstå innholdet.

1.2. Om skjemaløsninger og skjermdialoger

For informasjon om skjemaløsninger/skjermdialogene, integrering av løsninger mot fag-/arkivsystem etc. så henvises det til dokument fra gruppen ”Skjemaer og integrerte tjenester på nett” i prosjektet Tjenester på nett.

2. Bruk av Minid og oppkobling til Minside

Denne oversikten skal veilede kommuner om hva de må gjøre for å ta i bruk Minid til autentisering mot skjema/tjenester som er tilgjengelige via Internett. Minid kan brukes til å beskytte tilgangen til skjema og tilhørende tjenester som innbyggeren kan benytte seg av. Bruk av Minid krever at kommunen har koblet seg opp mot Minside.

I hovedsak ser en for seg tre forskjellige alternativer som avhenger av hvilke løsninger og leverandører som kommunen har valgt.

1. **Skjemaløsningen ligger hos leverandør (som ASP-tjeneste).** Når skjemaløsningen leveres som ASP-løsning slik at løsningen ligger hos leverandør, så må leverandøren ta i bruk Minid for å kunne autentisere innbyggeren. Kommuner som har slike løsninger må derfor henvende seg til skjemaleverandøren for å få denne til å ta i bruk Minid. Skjemaleverandøren kan velge å gjøre denne jobben selv eller benytte seg av ferdigutviklede Minid-integrasjonsmoduler som leveres av andre leverandører.
2. **Skjemaløsningen ligger lokalt hos kommunen og leverandør har integrert seg mot Minid.** Når skjemaløsningen ligger hos kommunen (i tilknytning til kommunens portalløsning) må kommunen kontakte skjemaleverandøren for å høre om leverandøren støtter bruk av Minid. Dersom skjemaleverandøren har integrert seg mot Minid kan kommunen bruke dette for å autentisere innbyggere for adgang til skjematjenestene.
3. **Skjemaløsningen ligger lokalt hos kommunen, men leverandør av skjemaløsningen har ikke integrert seg mot Minid.** Dersom skjemaleverandøren ikke har integrert seg mot Minid (og heller ikke har noen planer for dette) må kommunen selv sørge for å ta i bruk Minid. Kommunen kan da kontakte leverandører som har utviklet integrasjonsmoduler mot Minid og anskaffe seg en slik modul. Kommunen må så selv implementere integrasjonsmodulen mot Minid slik at den fungerer som autentisering av innbyggere for skjematjenestene.

2.1. Om bruk av Minid

Minid vil kunne fungere som en autentiseringsmekanisme for skjematjenestene som kommunen velger å legge ut på Internett via sin kommuneportal. Minid vil altså fungere som beskyttelse for skjematjenestene som kommunen velger å legge ut på Internett. Å ta i bruk Minid som autentiseringsmekanisme for skjematjenestene vil sannsynligvis ikke føre til at det må gjøres endringer/tilpasninger videre innover i kommunens IT-systemer.

Kommunene må i sine fagsystemer legge til rette for mottak av informasjon fra skjemaløsningen (og eventuelt også sørge for at informasjon kan sendes ut til skjemaløsningen), men dette er forhold som ikke kan knyttes til Minid (som er en autentiseringsmekanisme).

Det henvises forøvrig til aktuelle dokumenter hos Norge.no (<http://www.norge.no/minside/>) som beskriver hvordan Minside og Minid kan benyttes av kommuner.

3. Anbefalinger til autentisering av borger

Autentisering av innbyggeren er en viktig del av informasjonssikkerheten for ”skjema på nett”. Dette kapitlet vil beskrive problemstillinger og komme med anbefalinger til autentiseringskrav både ved datafangst og innsyn.

3.1. Aktuelle autentiseringsmekanismer

Det er flere autentiseringsmekanismer som kan brukes for å verifisere at innbyggeren er den han utgir seg for å være. I dette dokumentet er det to ulike mekanismer som vurderes:

1. Borgeren blir autentisert på sikkerhetsnivå 3 vha. Minid eller tilsvarende
2. Borgeren blir autentisert på sikkerhetsnivå 4 vha. en PKI-løsning eller tilsvarende

Autentiseringsløsninger med bare selvvalgte brukernavn/passord og lignende er ikke omhandlet i dette dokumentet da de generelt sett ansees å gi for lav sikkerhet til at faggruppen for sikkerhet ønsker anbefale dem for utbredelse til noen anvendelser rundt skjemaløsninger på nett.

3.1.1. Kort om Minid

Minid er en autentiseringsmekanisme utviklet for offentlig nettsteder. Minid muliggjør at innbyggerne kan logge seg på ett nettsted med Minid og sikkert bevege seg mellom offentlig nettsteder (tjenesteleverandører) uten å måtte gjenta pålogging.

Minid kan også benyttes som autentiseringsløsning på egen portal. Dvs. en kommune eller en etat kan bruke Minid som autentiseringsløsning for sitt eget nettsted. Den eneste forutsetning er at alle relevante tjenester også tilbys i Minside.

Minid består i dag av følgende faktorer:

- Fødselsnummer (brukernavn)
- Selvvalgt passord
- Engangs PIN-kode (enten engangskode fra tilsendt skattekort eller engangskode tilsendt vis SMS)

Styrker ved Minid:

- En nasjonal løsning som er utbredt til alle borgere som får tilsendt skattekort
- En felles løsning som for eksempel alle kommuner kan ta i bruk for autentisering

Svakheter ved Minid:

- Masseutsendelse av engangskoder i form av PIN-koder på skattekortet kan føre til at uvedkommende får tilgang til engangskoder
- PIN-koder distribueres sammen med fødselsnummeret (som fungerer som brukernavn ved bruk av Minid)

- Er kun på sikkerhetsnivå 3 og kan kun brukes for tilgang til ikke-sensitiv informasjon
- Er kun en autentiseringsløsning, har ikke funksjoner for eksempel for elektronisk signering

3.1.2.Kort om PKI

PKI står for Public Key Infrastructure og omfatter infrastruktur og tjenester for sikring av informasjonsutveksling og tilgang til systemer:

- elektronisk signering av dokumenter
- autentisering (sikker identifisering) 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 er ikke en teknologi i seg selv i form av programvare eller maskinvare. PKI er en beskrivelse av en infrastruktur der private og offentlige nøkler benyttes for å muliggjøre sikker elektronisk kommunikasjon mellom flere aktører. Hvordan selve infrastrukturen i en PKI er sammensatt, dvs. hvilke aktører som er med i infrastrukturen, er ikke entydig bestemt, men kan variere fra sted til sted (f.eks. fra land til land), og over tid.

Styrker ved PKI:

- Kan gi autentisering på sikkerhetsnivå 4 og kan brukes for tilgang til sensitiv informasjon
- En PKI-løsning kan også gi støtte for elektronisk signering

Svakheter ved PKI:

- Er pr. i dag en lite utbredt løsning hos borgere (men får større utbredelse blant via BankID og BuyPass)
- Krever en fysisk gjenstand (for eksempel smartkort) dersom det skal være en sterk PKI-løsning

3.2.Problemstillinger rundt datafangst og autentisering

Dette dreier seg om to delvis separate problemstillinger:

- 1) Utfylling og innsending av skjema til kommune ved hjelp av skjemaløsning hos ASP, og der skjema (eller vedlegg) kan inneholde sensitiv personinformasjon.
- 2) Innsyn i egen sak hos kommunen, der saksdokumentene kan inneholde sensitiv personinformasjon. Innsyn skjer gjennom Minside eller kommunal portal.

Disse to diskuteres hver for seg nedenfor.

3.2.1.Datafangst, skjemautfylling

Dagens portalløsninger for utfylling av skjema har tilgang i klartekst til all informasjon som legges inn tilknyttet et skjema. (Løsninger som tilbyr ende-til-ende kryptering fra brukeren til kommunen, er mulig, men finnes ikke tilgjengelig i dag.)

Sensitiv informasjon kan være knyttet til:

- Informasjon som fylles ut i et søknadsskjema (for eksempel sosialstøtte).
- Det at en person i det hele tatt fyller ut et skjema (igjen for eksempel sosialstøtte).
- Vedlegg til en søknad – dette kan være hvilken som helst søknad (for eksempel er søknad om barnehageplass normalt ikke sensitiv, men dersom barnets helsetilstand brukes som grunn til prioritert plass, kan et vedlegg som dokumenterer dette, gjerne ha sensitive personopplysninger).

Dersom personopplysninger (også sensitive opplysninger av en eller annen grad) skal kunne gis inn i skjema eller som vedlegg til skjema, er det en del ting å merke seg:

- Kommunen er behandlingsansvarlig for opplysningene.
- Siden ASP har tilgang til opplysningene, må det inngås en databehandleravtale med kommunen før sensitive personopplysninger kan legges inn via skjemaløsningen.
- Søkeren må *identifiseres* med fødselsnummer – enten ved at personen oppgir dette selv eller ved at det skaffes på annen måte (for eksempel basert på en eID som personen bruker). Merk at fødselsnummer er et *brukernavn* for personen, ikke et passord som kan brukes for å autorisere tilgang.
- Normalt gjør en i dag ikke *autentisering* av personen som del av søknadsprosessen. En antar at den som er identifisert i søknaden, er korrekt person. Dersom noe er feil her (noen har sendt inn søknad i en annens navn), vil det bli avdekket i saksbehandlingen eller når vedtak skal meddeles. Dette bygger på at risikoen for «falsk søknad» er liten.
- Dersom en søknad inneholder sensitive personopplysninger krever dette kryptering av enten informasjonen eller transportkanalen. I tillegg kan det hende at kommunen ønsker en sterkere verifisering, gjerne på et tidlig tidspunkt, av at søkeren er den han/hun gir seg ut for å være. Dette kan gjøres gjennom at autentisering (det vil si elektronisk signatur i en utvidet betydning av det begrepet) kreves, eller ved at saksbehandlingsprosedyrene inneholder rutiner for å verifisere en søknad manuelt som del av prosessen.
- Dersom en skal kreve autentisering, må en ha en autentiseringsmetode. Administrasjon av egne brukernavn og passord er neppe regningssvarende, og statiske passord vil gjerne bli regnet som for svak mekanisme for sensitive personopplysninger. Bruk av engangspassord (dagens Minid) eller en PKI-basert eID er mulig dersom dette er integrert hos ASP-en. Disse autentiseringsmetodene vil også gi fødselsnummer for personen.

Det store spørsmålet knyttet til bruk av ASP og håndtering av sensitive personopplysninger er hvor stor grad av separasjon som vil kreves hos ASP for løsningen for *denne* kommunen, i forhold til løsninger for andre kunder hos ASP-en. Det er et viktig prinsipp at sensitive personopplysninger bare skal kunne være tilgjengelig for de som er autorisert for det, og at det skal være separasjon både i forhold til andre systemer i egen organisasjon (dvs. i kommunen) og spesielt i forhold til andre organisasjoner.

Dette kan komme i konflikt med en effektiv implementering av en skjemaløsning, der samme skjema brukes for en hel rekke kommuner, og identifikasjon av kommunen er det som skiller når en søknad skal rutes videre. I en del tilfeller har det vært ønske om fysisk separate løsninger for forskjellige organisasjoner, men det er klart lite hensiktsmessig med en fysisk installasjon av skjemaportal for hver kommune.

Spørsmålet er da i hvor stor grad ASP-en kan sørge for logisk skille mellom informasjon tilhørende forskjellige kommuner? Dette er et element som må beskrives i databehandleravtalen mellom kommunen og ASP og som bør være risikovurdert.

Det neste, store spørsmålet er hvordan kommunen mottar søknadene fra ASP. Igjen skal sensitive personopplysninger holdes separat fra annen informasjon og være tilgjengelig bare for dem som

er autorisert for det. Det er mulig at en kommune bør sørge for at alle sensitive søknader og alle søknader med vedlegg (siden vedleggene potensielt kan holde sensitiv informasjon) bør sorteres ut og rutes separat til egne systemer og personer som er klarert for dette, heller enn at alle søknader mottas på samme sted. Dette må også håndteres korrekt hos ASP.

Autentisering av ASP og kommunens systemer og beskyttelse av trafikken mellom dem anses ikke for å være noen stor utfordring.

3.2.2. Innsyn i egen sak hos kommunen

Tilgang her antas skjer gjennom kommuneportal eller Minside. Det antas også at dagens versjon av Minside redirigerer brukeren direkte til den linken informasjon skal hentes fra, slik at det ikke passerer sensitiv informasjon gjennom Minside. Dette bør også gjelde for eventuelle andre portalløsninger som formidler tilgang til saksinformasjon, slik at de redirigere heller enn å videreformidle informasjonen (så lenge løsninger for ende-til-ende kryptering ikke er i bruk). I dette tilfellet bør det ikke være nødvendig med noen spesiell avtale med portalen.

I dette tilfellet trengs helt klart en autentiseringsløsning. Minid (engangspassord) holder for de fleste typer personopplysninger, mens ”person-høy” PKI-basert eID vil som hovedregel være påkrevd for tilgang til sensitiv informasjon.

Igen er det viktig at sensitive personopplysninger holdes separat og bare med tilgang for autoriserte personer. Dette er helt klart en utfordring når det gjelder tilgang gjennom en innsynsløsning hos kommunen.

3.3. Krav til autentisering av borger

Ser man isolert bare på autentiseringen av innbyggeren er det i hovedsak to risikoområder:

1. At innbyggeren oppgir falske opplysninger ved innsending (datafangst) av en søknad
2. At en borger får innsyn i informasjon tilhørende en annen borger

Disse to risikoområdene er beskrevet nedenfor.

3.3.1. Mulige trusler ved datafangst

Trusler	Konsekvenser	Tiltak
Borger utgir seg for å være en annen person	<ul style="list-style-type: none"> • Kommunen knytter skjema til feil borger • Feil borger blir registrert som ”søker” hos kommunen og kan for eksempel få tilbakemelding fra kommunen • Unødig ekstraarbeid for kommunen 	<ul style="list-style-type: none"> • Sikre korrekte opplysninger om borger ved datafangst (autentisering)
Borger oppgir falske opplysninger i skjema	<ul style="list-style-type: none"> • Kommunen behandler skjema på feil grunnlag → kommunen kan fatte vedtak/beslutning med basis i uriktige opplysninger • Borger kan urettmessig få tilgang 	<ul style="list-style-type: none"> • Kvalitetssikre opplysninger i behandlingsprosessen med tanke på å avdekke uriktige

	til tjenester eller lignende pga. uriktige opplysninger (lovbrudd?)	opplysninger (for eksempel fysisk oppmøte)
Borger oppgir feil e-postadresse for tilsendning av referansenummer	<ul style="list-style-type: none"> • Feil borger får tilsendt referansenummer og kan få tilgang til informasjon om en annen borger 	<ul style="list-style-type: none"> • Dobbeltsjekk registrering av e-postadresse • Ikke tillate utsending av referansenummer på e-post for skjema som kan inneholde sensitive opplysninger

Borger oppgir falske avsenderopplysninger ("ID-tyveri")

Det kan tenkes situasjoner der en borger har interesse eller motivasjon av å sende i en søknad eller et skjema i en annen innbyggers navn, selv om det ikke vises til konkrete eksempler på dette i dette dokumentet. Sannsynligheten for at dette skjer er nok lav pr. i dag og dette oppleves ikke som et problem i kommunene i dag.

Samtidig er ID-tyveri er generelt økende problem og det må nok erfaringsmessig regnes med at også misbruk for elektronisk kommuneskjema vil forekomme når slike skjemaer gjøres elektronisk tilgjengelige for innsending i økende grad. På denne bakgrunn kan det være fornuftig for den enkelte kommune å kreve autentisering av borgeren ved innsending av skjema. Dette vil redusere risikoen for misbruk både for kommunen og for den enkelte borger.

Borger oppgir falske opplysninger i skjema

Det kan tenkes at en borger oppgir falske eller uriktige opplysninger i en søknad eller et skjema for å få tilgang til en viss type tjeneste, støtte eller lignende fra kommunen. Uten autentisering av innbyggeren har en i utgangspunktet liten reell mulighet til å kunne sjekke hvem som var den faktiske innsenderen av en søknad eller et skjema. Dersom en borger blir mistenkt for å ha oppgitt falske eller uriktige opplysninger, kan dermed innbyggeren nekte for at det var han som sendte inn de aktuelle opplysningene.

Dersom innbyggeren var autentisert med for eksempel Minid er det langt vanskeligere for innbyggeren å nekte for eller motbevise at det ikke var han som sendte inn opplysningene i et skjema eller en søknad. Å kreve autentisering ved innsending av opplysninger vil sannsynligvis også føre til at det er færre som "tar sjansen" på å sende inn falske/uriktige opplysninger med viten og vilje.

For søknader/skjema som krever store behandlingsressurser fra kommunen og/eller hvor innbyggeren kan ha motiv/motivasjon til å sende inn uriktige opplysninger, så ønsker kanskje en kommune å være mest mulig trygg på at opplysningene er korrekte. I slike tilfeller kan autentisering av innbyggeren også ved innsending være en metode for kommunen å sikre at det er rimelig stor grad av sikkerhet for at opplysningene er korrekte.

Vurderinger av den enkelte kommune

Det er opptil den enkelte kommune å avgjøre hvorvidt den ønsker å kreve autentisering eller ikke ved innsending av skjema eller søknader. Det er i hovedsak kommunen som har risikoen ved mottak av søknader og skjema fra innbyggeren, så den enkelte kommune må vurdere hvor trygg den ønsker å være på at den mottar korrekte opplysninger fra riktig borger.

3.3.2. Mulige trusler ved innsyn

Trusler	Konsekvenser	Tiltak
Uautorisert tilgang til informasjon	<ul style="list-style-type: none"> • (Sensitive) opplysninger blir gjort tilgjengelige for feil borger • Tap av renommé/tillit hos innbyggere til kommunen • Negativ medieomtale etc. 	<ul style="list-style-type: none"> • Kryptering • Sikre god nok autentisering av borger ved innsyn

Uautorisert tilgang til informasjon

At opplysninger om en borger skal komme på avveie og bli tilgjengeliggjort for uvedkommende er den store trusselen når en snakker om innsynsløsninger for innbyggerne. Den enkelte kommune må derfor ha gode løsninger på dette området før den enkelte borger kan gis innsyn i egne opplysninger.

Vurderinger av den enkelte kommune

Mens truslene ved datafangst/innsending i hovedsak rammer kommunen, så rammer truslene ved innsyn også den enkelte borger blant annet fordi at egne opplysninger kan komme på avveie. Hensynet til den enkelte borger bør veie tyngst her slik at ingen kommuner må legge til rette for innsynsløsninger før hensynet til innbyggerne er godt nok ivaretatt.

I praksis betyr det at kommunene må ha autentiseringsløsninger på nivå med Minid eller bedre før innbyggerne kan gis innsyn til egne opplysninger.

3.3.3. Konsekvenser dersom sensitive opplysninger skal håndteres

Enkelte skjema/søknader er lagt opp til å kunne inneholde sensitive opplysninger, mens andre skjema/søknader i utgangspunktet ikke skal inneholde sensitive opplysninger.

3.3.3.1. Ved datafangst

Ved ren datafangst og innsending av opplysninger fra innbyggeren vil ikke innhold av sensitive opplysninger eller ikke gi noen automatisk føringer for kravet til autentisering av innbyggeren. Så lenge transportsikkerhet, datahåndtering hos skjemaleverandør, mottak av data i kommunen etc. er godt nok ivaretatt, så vil ikke sensitive opplysninger automatisk legge føringer for høyere krav til autentisering. Transportsikkerhet, mottak av data i kommunen etc. er uansett forhold som må være ivaretatt fordi det er vanskelig å hindre at en borger for eksempel oppgir sensitive data i et fritekstfelt.

Det kan være at skjema som skal kunne inneholde sensitive opplysninger generelt krever en mer omfattende behandlingsprosess hos kommunen, og at kommunen av slike årsaker ønsker å vite med stor grad av sikkerhet hvem som er avsender. En kommune vil derfor kunne sette krav til autentisering av innbyggeren ved innsending av skjema/søknader som skal kunne inneholde sensitive opplysninger.

3.3.3.2.Ved innsyn

Ved innsyn til egen informasjon vil innsyn til sensitive opplysninger kreve et høyere sikkerhetsnivå med tanke på autentisering av innbyggeren. Ved tilgang til sensitive opplysninger anbefales det autentiseringsløsninger som PKI eller med tilsvarende på sikkerhetsnivå 4.

3.3.4.Hva omfatter datafangsten

Krav til autentisering ved datafangst må sees i sammenheng med den totale informasjon en får tilgang til ved utfylling av et skjema. Eksempelvis kan tilgang til karttjenester med detaljert informasjon gjøre at kravet til autentisering øker i forhold til bare tilgang til et ”tomt” skjema.

Den enkelte kommune må derfor selv vurdere krav til autentisering ved datafangst basert på den informasjonen som skjemautfylleren får tilgang til.

3.3.5.Anbefalinger til autentisering av innbyggeren

Kravet til autentisering må sees i sammenheng med hvordan den totale saksbehandlingen i kommunen foregår. En ”heldigitalisert” saksbehandling hvor all kommunikasjon mellom borger og kommune foregår elektronisk vil sannsynligvis ha større krav til autentisering enn en ”halvdigitalisert” saksbehandling. Dersom for eksempel bare innsendingen skjer elektronisk og videre kommunikasjon med borgeren skjer på vanlig post og/eller fysisk oppmøte vil dette kunne redusere behovet for autentisering i datafangsten.

Det sentrale er at kommunen i løpet av saksbehandlingen må autentisere borgeren slik at kommunen vet med nødvendig grad av sikkerhet hvem den snakker med. Og en slik autentisering kan skje elektronisk allerede ved datafangst eller senere i saksbehandlingen gjennom vanlig post sendt til borger eller krav om fysisk oppmøte.

Skjemaene er i denne sammenhengen delt inn i to grupper hvor skillet er om skjemaene er tenkt å kunne inneholde sensitiv informasjon eller ikke. Anbefalingene er gjort for 15 skjema som har vært prioriterte i prosjektet ”Tjenester på nett”.

3.3.5.1.Gruppe 1 – skjema som ikke skal inneholde sensitiv informasjon

Skjema som det ikke er lagt opp til skal inneholde sensitive opplysninger:

- Rekvisisjon av kartforretning
- Søknad Kulturskole
- Melding om tiltak¹
- Gravemelding
- Svar offentlig høring
- Tilskudd til kulturformål
- Bestilling av avfallsbeholder
- Skjenkebevilling

3.3.5.2.Gruppe 2 – skjema som kan inneholde sensitiv informasjon

Skjema som potensielt kan inneholde sensitive opplysninger (dvs. at skjemaet har fritekstfelter for ”Andre opplysninger” eller lignende):

- Søknad barnehageplass

¹ Dette skjemaet kan krever samtykke/bekreftelse fra E-verket og/eller Televerket

- Søknad SFO
- Lærerstilling/ ledig stilling

Skjema hvor det konkret etterspørres etter sensitive opplysninger:

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

NB: Det er viktig å merke seg at her kan det være lokale variasjoner/forskjeller mellom skjemaene som kan gjøre at inndelingen ovenfor ikke stemmer. Hver enkelt må derfor ha kontroll på hvilke opplysninger som en kan forvente å motta i det enkelte skjema.

3.3.5.3. Metode for å vurdere krav til autentisering

Det er benyttet et rammeverk fra FAD for å vurdere krav til autentisering av innbyggeren. Med bakgrunn i rammeverket har det blitt utarbeidet en egen mal som har vært benyttet for å vurdere kravene til autentisering av innbyggeren. Malen finnes i ”Vedlegg B – Mal for vurdering av krav til autentisering”.

3.3.5.4. Autentisering ved datafangst

Tabell 1 under viser en oversikt over anbefalinger til autentisering av borger ved datafangst. Det er i tabellen også tatt med om det enkelte skjema kan ha vedlegg og om det har felt for fødselsnummer.

Det anbefales her i utgangspunktet at borgeren blir autentisert for en del av skjemaene som sendes inn. Dette gir:

- 1) Trygghet for kommunen om hvem avsender er
- 2) Trygghet for borgeren og kommunen ved at det er mindre risiko for misbruk av skjemaløsningen (falske søknader etc.)

Den enkelte kommune må selv velge om en ønsker å følge anbefalingene i dette dokumentet eller om man velger andre krav til autentisering for de ulike skjemaene. Ved innsending kan det også være aktuelt å bruke et lavere sikkerhetsnivå for autentiseringen enn nivå 3 dersom kommunen/skjemaleverandøren har tilrettelagt for dette. Slike valg må da eventuelt være gjennomtenkte valg fra kommunens side og begrunnet i gjennomførte risikovurderinger. Det kan også være andre skjema som ikke er vurdert i dette dokumentet hvor det ikke er behov for samme grad av autentisering ved innsending.

Tabell 1: Oversikt over krav til autentisering ved datafangst

Skjema	Egenskaper ved skjema		Krav til autentisering ved datafangst (innsending av søknad)		
	Skjema kan ha vedlegg ²	Skjema har f. nr. ³	ingen autentisering	Nivå 3 (f. eks. Minid)	Nivå 4 (f. eks. PKI)
Rekvisisjon av kartforretning			X		
Søknad Kulturskole		X	X		
Melding om tiltak	X		X		
Gravemelding				X	
Svar offentlig høring	X			X	
Tilskudd til kulturformål	X		X		
Bestilling av avfallsbeholder			X		
Skjenkebevilling		X	X		
Søknad barnehageplass		X	X		
Søknad SFO		X	X		
Lærerstilling/ ledig stilling	X		X		
Søknad om sosialstøtte	X	X		X	
Ledsagerbevis		X		X	
Søknad pleie- og omsorgstjenester		X		X	
Parkeringstillatelse med legeattest	X			X	

3.3.5.5. Autentisering ved innsyn

Tabell 2 nedenfor viser en oversikt over anbefalinger til minstekrav til autentisering av borger ved skjemainnsyn. Det tas her utgangspunkt i at innsyn omfatter innsyn til alle data som potensielt kan registreres for et skjema.

Hovedregelen for innsyn er vurdert til at innsyn til kun ikke-sensitive opplysninger krever sikkerhetsnivå 3 (Minid), mens innsyn til data som kan omfatte sensitive opplysninger krever sikkerhetsnivå 4 (for eksempel PKI-løsning).

² Dette feltet angir om et "standardskjema" slik det ser ut pr. i dag er lagt opp til å kunne ha vedlegg knyttet til seg

³ Dette feltet angir om et "standardskjema" slik det ser ut pr. i dag krever fødselsnummer

Tabell 2: Oversikt over krav til autentisering ved innsyn

Skjema	Egenskaper ved skjema		Krav til autentisering ved innsyn		
	Skjema kan ha vedlegg ⁴	Skjema har f. nr. ⁵	Uten autentisering	Nivå 3 (f. eks. Minid)	Nivå 4(f. eks. PKI)
Rekvisisjon av kartforretning				X	
Søknad Kulturskole		X		X	
Melding om tiltak	X			X	
Gravemelding				X	
Svar offentlig høring	X			X	
Tilskudd til kulturformål	X			X	
Bestilling av avfallsbeholder				X	
Skjenkebevilling		X		X	
Søknad barnehageplass		X			X
Søknad SFO		X			X
Lærerstilling/ ledig stilling	X				X
Søknad om sosialstøtte	X	X			X
Ledsagerbevis		X			X
Søknad pleie- og omsorgstjenester		X			X
Parkeringstillatelse med legeattest	X				X

3.4.Skjema som har krav til utfylling fra flere enn en part

Dersom et skjema krever utfylling fra flere enn en part er dette en ekstra utfordring å få til elektronisk. Eksempel på slike skjema er for eksempel ByggSøk og gravemelding. Mulige løsninger kan være både elektroniske/manuelle eller elektroniske:

Mulig elektronisk løsning:

- Den elektroniske løsningen må utformes slik at flere enn den parten som sender inn skjemaet kan gå inn på aktuell del av skjema og fylle ut ”sin del”.
- Det bør da være logiske sjekker slik at for eksempel et skjema ikke kan sendes inn før alle parter har fylt ut sine deler obligatoriske deler.

Mulig manuell løsning:

⁴ Dette feltet angir om et ”standardskjema” slik det ser ut pr. i dag er lagt opp til å kunne ha vedlegg knyttet til seg

⁵ Dette feltet angir om et ”standardskjema” slik det ser ut pr. i dag krever fødselsnummer

- Part nr 2 sender inn sin del av skjemaet på papir med referanse til elektronisk skjema som er innsendt av part nr 1 (krever at kommunen manuelt må koble sammen elektronisk søknad med papirsøknad).

For mer informasjon om utfordringer rundt problemstillingene skissert ovenfor så har Statskonsult utredet disse problemstillingene rundt ByggSøk .

3.5.Krav til elektronisk signatur fra borger

Det er ikke vurdert detaljert i hvilke situasjoner det stilles krav til elektronisk signatur fra borger i henhold til lov- og regelverk. Når det er behov for en elektronisk signatur fra borgeren er i stor grad en juridisk vurdering og dette området har ikke prosjektgruppen hatt ressurser til å behandle i noen særlig grad.

En har i dag i hovedsak tre nivåer av elektroniske signaturer :

- *Elektroniske signaturer*: Alle metoder som knytter en aktør til en handling eller spesifikk informasjon
 - o Aktør (vanligvis person) må være autentisert
 - o Handling (for eksempel innsending) bør være eksplisitt og valgt av aktøren
 - o Logger sørger for sporbarhet
 - o Minid og FEIDE er to løsninger som kan brukes til elektronisk signatur
- *Avanserte elektronisk signaturer*: Sikker knytning mellom signatur og informasjon slik at endringer kan oppdages. Bare signerer skal kunne ha tilgang til signeringsmetode.
 - o Eneste teknologi i dag er digital signatur med PKI-basert eID
 - o Buypass, BankID, Commfides, ZebSign er eID-løsninger i markedet som kan brukes til avansert signatur
- *Kvalifiserte elektronisk signaturer*: Avansert signatur med tilleggskrav til utsteder av eID(kvalifisert eID) og til signeringsutstyr.
 - o Gir Garantert rettsvirkning som håndskrevet signatur etter Esignaturloven
 - o Kvalifisert signatur finnes ikke i det norske markedet i dag, det er ingen godkjente signeringsverktøy. Dvs. i teorien finnes det ikke noe som gir garantert rettsvirkning

Det er i utgangspunktet få formkrav⁶ i regelverket til elektronisk signatur. Det er i stor grad opptil den ansvarlige å vurdere bevisbehovet i forholdet til kravet om elektronisk signatur. Det handler i stor grad om hvor sikker man vil kunne påvise at en bestemt borger har sendt inn en bestemt informasjonsmengde på et gitt tidspunkt (krav til ”ikke-benektning”). Eksempelvis hvor sterke

⁶ Nærings- og handelsdepartementet har i eRegelprosjektet fra 2001 oppsummerert en del om kravene som står i regelverket (<http://www.regjeringen.no/nb/dep/nhd/dep/ansvarsomraader/VideRe-prosjektet.html?id=439402>)

bevis en kommune ønsker å ha dersom det skulle bli en tvist mellom kommunen og innbyggeren (og i verste fall dersom det skulle bli en rettsak).

Elektroniske signaturer er generelt lite utbredt pr. i dag, men innen helsesektoren kreves det bruk av avansert elektronisk signatur for innsending av elektronisk sykmelding blant annet fordi en slik sykmelding utløser et økonomisk ansvar.

På sin enkleste form kan en se for seg at en elektronisk signatur kan være prosessen hvor en borger blir autentisert og sender inn data:

”autentisering → utfylling → bekreftelse → innsending”

Vha. av logger og lignende vil en i ettertid med en slik signaturløsning i hvert fall til en viss grad av sikkerhet kunne legge frem ”bevis” for at en bestemt borger utførte en gitt handling (innsending) og hvilken informasjon som ble sendt inn. For enkle tjenester som for eksempel barnehagesøknad og lignende bør dette være godt nok pr. i dag, men hver enkelt kommune må vurdere hvor sterke bevis de ønsker å legge til grunn for sin saksbehandling. Dersom en kommune ønsker større grad av sikkerhet for hva en borger har sendt inn så vil det kunne kreve bruk av avanserte elektroniske signaturer eller kvalifiserte elektroniske signaturer.

For mer informasjon rundt elektroniske signaturer og elektroniske søknader vises det til rapport fra Statskonsult som har vurdert dette i forhold til elektroniske byggesøknader. Se også Sikkerhetsrammeverk fra faggruppen for sikkerhet for mer informasjon .

Anbefalinger for bruk av elektronisk signatur:

- *Den ansvarlige må i stor grad selv vurdere bevisbehov og andre relevante faktorer og avgjøre når det er behov for elektroniske signaturer og nivået til selve signaturen (jfr. de tre nivåene presentert ovenfor).*
- *Som en generell regel kan det sies at ”Der offentlig myndighet utøver en handling ovenfor en borger, for eksempel at det foretas inngrep i borgers rettigheter eller plikter, og hvor ikke-benektning er av betydning, bør elektroniske signaturer (basert på kvalifiserte sertifikater) benyttes”.*

3.6.Risikovurdering av skjemaløsningene

Når det gjelder risikovurdering av selve skjemaløsningene bør dette gjøres i samarbeid av den enkelte kommune og skjemaleverandøren. Et eksempel på en mal for slik risikovurdering finnes i Vedlegg C – Eksempel på risikovurdering av skjemaløsning hvor det også er vist eksempler på noen aktuelle trusler.

For gjennomføring av risikovurderinger henvises det til Datatilsynet sin veileder for risikovurderinger .

4. Beskrivelse og anbefaling av tekniske løsninger

Dette kapitlet beskriver en generell arkitektur for elektroniske skjemaløsninger. Mange kommuner bruker en egen skjemaleverandør for sine skjemaer på nett, slik at skjemaløsningen ligger som en ASP-løsning hos en ekstern leverandør. Dersom kommunen har skjemaløsningen internt i sitt datanettverk, så vil krav beskrevet i dette kapitlet i utgangspunktet også gjelde kommunen sine løsninger.

Elementer som omhandler dersom løsningen ligger internt hos kommunen er beskrevet i kapittel 4.6.

I beskrivelse av den generelle arkitekturen er det lagt vekt på følgende områder:

- Borgeren skal ha tilgang til å sende inn skjema via Internett
- Skjemaløsningen ligger hos en ekstern ASP-leverandør
- Kommunen skal ta imot data fra skjemaleverandøren
- Borgeren skal tilbakemelding fra kommunen om status på skjema behandling og informasjon om vedtak

4.1. Generelle sikkerhetsprinsipper

Ved datafangst hos skjemaleverandør og ved datakommunikasjon mellom skjemaleverandør og kommunen er følgende hovedregler de viktigste å tenke på for å ha en trygg og sikker løsning:

1. Datafangst fra borger må skje på en trygg og sikker måte (autentisering/signatur av borger og sikker transport av data)
2. Dataene må håndteres og lagres på sikker måte hos skjemaleverandøren
3. Kommunikasjonen mellom skjemaleverandøren og kommunen må være tilstrekkelig sikret og en må ha god kontroll over datakommunikasjonen mellom skjemaleverandøren og kommunen
4. En må sørge for at løsningene er utformet slik (arkitekturen) at dersom for eksempel ondsinnet kode eller uautoriserte personer/systemer får tilgang til løsningene så blir det minimale konsekvenser (skader) av et slikt sikkerhetsbrudd.

De generelle sikkerhetsprinsippene bør planlegges slik at de ivaretar nødvendige krav i henhold til:

- Konfidensialitet: Å sikre at informasjon bare er tilgjengelig for de som skal ha tilgang.
- Tilgjengelighet: Å sikre at informasjon er tilgjengelig innenfor de krav som er satt.
- Integritet: Å sikre at informasjon er korrekt og fullstendig og at informasjonen ikke er endret av uvedkommende
- Sporbarhet: Å ha nødvendig metoder og mekanismer som skal knytte alle endringer av informasjon til den som har utført endringene

Anbefalinger for generelle sikkerhetsløsninger

Løsningene som anbefales her gjelder uavhengig av hvilke transportmetoder og teknologier som brukes og hvordan den enkelte skjemaleverandør/kommune velger å motta sine data på. Hvordan sikkerheten rent teknisk kan ivaretas vil avhenge av hvilke metoder som velges og av arkitekturen hos den enkelte kommune/skjemaleverandør.

4.2. Generelt om transportmetoder

Nedenfor beskriver de vanligste metodene som brukes for datatransport mellom to eller flere parter.

4.2.1. FTP/SFTP

FTP (File Transfer Protocol, altså filoverføringsprotokoll) er en standard, operativsystemuavhengig protokoll for overføring av filer i et TCP/IP-basert nettverk. Overføringen skjer mellom en FTP-klient og en FTP-server. Hvilken maskin som har hvilken rolle, kan i utgangspunktet velges fritt, men vil selvsagt være gitt av oppgaven som skal løses.

FTP-serveren lytter på nettverket etter forespørsler. FTP-klienten kobler til serveren og kan lese og skrive til serverens filsystem, som opp- og nedlasting av filer, sletting, navnebytte etc.

SFTP (Secure FTP) kan benyttes for sikker overføring av filer over usikrede nettverk. SFTP tilbyr omtrent samme funksjonalitet som standard FTP, men da også med muligheter for blant annet kryptering av data og autentisering.

4.2.2. HTTP/HTTPS

HTTP er en forespørsel/respons protokoll mellom klienter og tjenere. En HTTP tjener lytter ofte på en fast port over IP-protokollen (typisk port 80) og venter på at klienten skal sende en forespørselstreng. HTTP er forskjellig fra andre protokoller, slik som for eksempel FTP, på den måten at forbindelser vanligvis termineres så snart en bestemt forespørsel (eller en serie med relaterte forespørsler) har blitt fullført.

HTTPS er en sikker utgave av http (hypertekstoverføringsprotokoll), som er kommunikasjonsprotokollen til World Wide Web. En HTTPS-sesjon blir kryptert enten ved bruk av SSL-protokollen (Secure Socket Layer) eller TLS-protokollen (Transport Layer Security), og tilbyr på denne måten er fornuftig beskyttelse mot «tyvlytting», og at noen endrer på de sendte dataene. SSL/TLS brukes ofte for å verifisere at parten en kommuniserer med er ekte, som oftest er dette serveren og klienten er uautentisert.

4.2.3. E-post

E-post sendes mellom brukere/systemer via e-posttjenere, såkalte SMTP-tjenere, på Internett. Man kan for eksempel sende med filer som vedlegg til e-post.

S/MIME (Secure / Multipurpose Internet Mail Extensions) er en metode for å kunne kryptere og signere innholdet i en e-post. Vha. S/MIME kan man ha sikker transportoverføring via e-post dersom både avsender og mottaker benytter seg av S/MIME.

4.2.4. Webservices

Web-tjenester er små komponenter som kan brukes fleksibelt på tvers av nettstedet og andre tjenester. En komponent i denne sammenheng er programvare som går på en internettsjerver, og utfører helt bestemte operasjoner. Hver slik operasjon har et eget navn, og fungerer alene, eller i sekvens sammen med andre operasjoner.

All kommunikasjon skjer via internett, med en type meldinger som alle programmeringsverktøy snart forstår. Slike meldinger kalles for SOAP (Simple Object Access Protocol) meldinger. SOAP er en protokoll, i dette tilfelle et mønster som definerer hvordan data sendes fra en maskin til en annen.

Sikkerheten i webservices kan blant annet ivaretas ved å benytte PKI-sertifikater eller at webservices brukes over en sikret transportkanal.

4.2.5. ebXML

ebXML (Electronic Business using eXtensible Markup Language), også kalt "e-business XML", er et rammeverk av XML-baserte standarder. Hovedtanken bak ebXML er å tilby en XML-basert infrastruktur som muliggjør bruk av elektronisk kommunikasjon mellom virksomheter med god interoperabilitet, sikkerhet og konsistens. ebXML er mye brukt innenfor B2B (Business-to-business). ebXML-rammeverket omfatter kort fortalt en felles konvolutt for innpakking av elektroniske meldinger samt prosesser for kvittering, pålitelighet i meldingsoverføringen og sikkerhet.

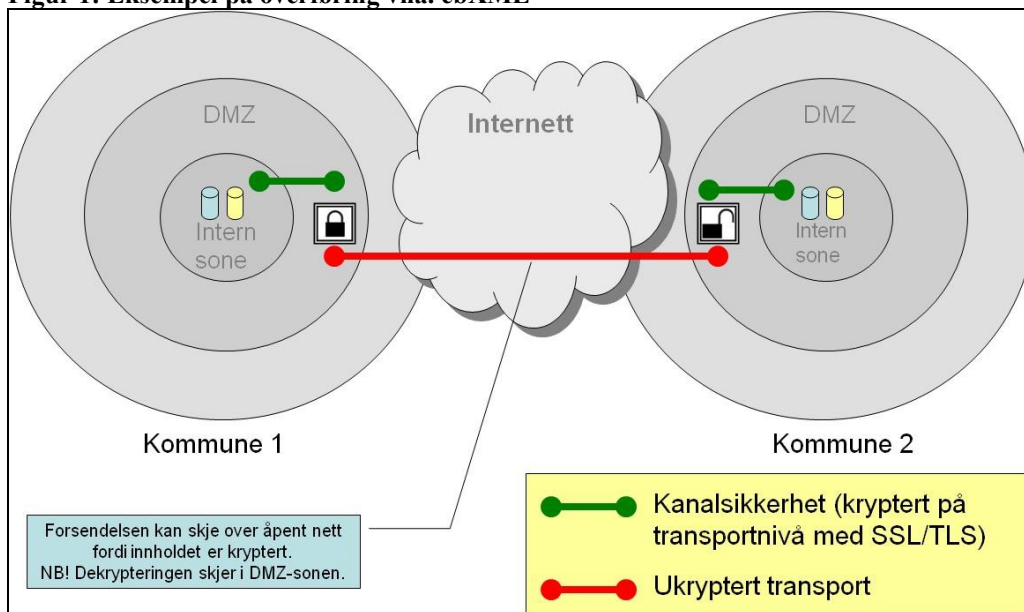
Viktige funksjoner i ebXML er blant annet:

- Støtter sending av flere typer vedlegg
- Har støtte for applikasjonskvittering mellom systemer
- Har også funksjoner for automatisk å sende meldinger på nytt med mindre man har fått kvittering for at meldingen er mottatt, evt. varsle dersom meldingen ikke kommer frem til mottaker

Se Figur 1 for eksempel på bruk av ebXML⁷.

⁷ For forklaring av innholdet i figurene brukt i dette dokumentet, se Vedlegg A – Figurforklaring

Figur 1: Eksempel på overføring vha. ebXML



4.2.6.VPN

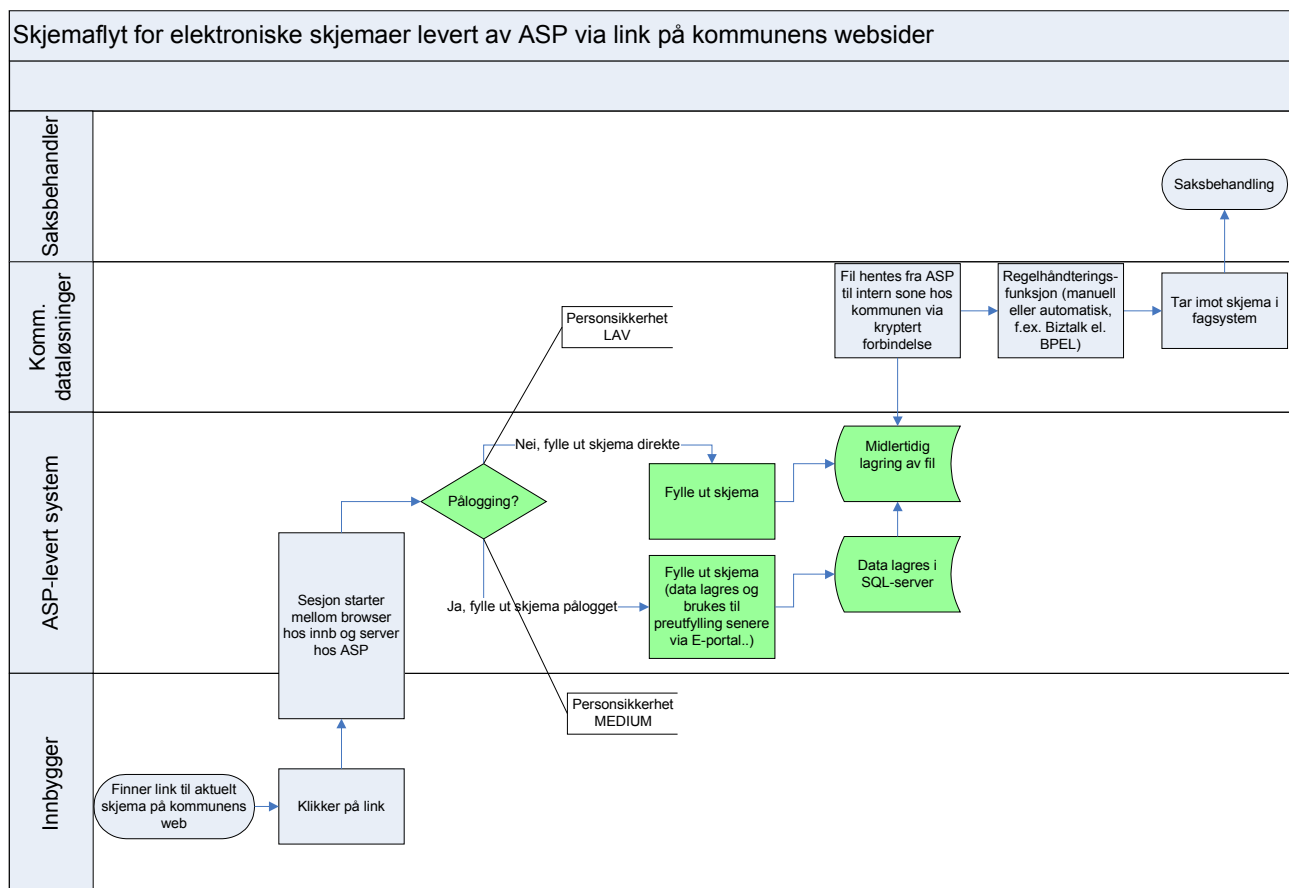
VPN (Virtual private network, på norsk virtuelt privat datanett) er betegnelsen på en datateknikk som anvendes for å skape ”punkt-til-punkt” forbindelser, såkalte ”tunneler”, gjennom et annet datanett (så som internettet). VPN-tunnelen kan være kryptert, noe som er viktig når man ikke kjenner eller er usikker på sikkerheten gjennom et eventuelt offentlig datanett som internettet.

IPSec er en tjeneste som tilbyr autentisering, kryptering og integritetssjekk av datatrafikk på et nettverk. IPSec benyttes ofte i sammen med VPN.

4.3. Sikring av datafangst fra borger

Løsningen for skjemautfylling må utformes slik at minst mulig data blir liggende igjen på den lokale PC-en som brukes av den borgeren som fyller ut et skjema ("tynn-klient" løsning). Borgeren bør heller ikke være avhengig av noen spesiell programvare for å kunne benytte seg skjemaløsningen.

Hvordan datafangsten kan skje med tanke på dataflyt er vist i .Figur 2



Figur 2: Eksempel på skjemaflyt for datafangst

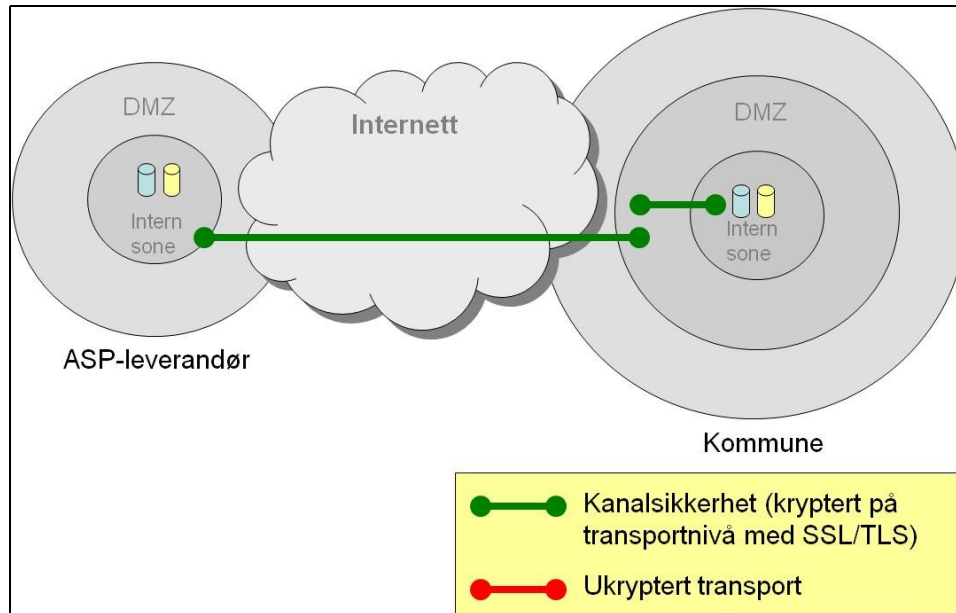
4.3.1. Sikring av datakommunikasjonen

Ved kommunikasjon av sensitiv informasjon er basiskravet i utgangspunktet ende-til-ende kryptering (for eksempel kryptert overføring fra sikker-sone til sikker-sone). Dersom det ikke er praktisk mulig med tilgjengelige løsninger/teknologi å ivareta fullstendig ende-til-ende kryptering må en etablere løsninger som ligger så tett opptil dette kravet som mulig slik at risikoer er minimert i størst mulig grad.

Kryptering skal generelt iverksettes når informasjon er utenfor den databehandlingsansvarliges kontroll. Som generell regel bør en bruke meldingskryptering når innholdet skal inn innom mer enn to parter (for eksempel fra borger, via skjemaleverandør og til kommunen), mens kanalkryptering kan brukes når det kommuniseres direkte mellom to parter (for eksempel fra borger direkte til kommunen).

Transportbasert kryptering

Skjemaløsningen som er tilgjengelig for innbyggeren via Internett må ha tilstrekkelig sikkerhet slik at data kan innhentes på en trygg måte fra innbyggeren og inn til skjemaløsningen. Dette betyr i praksis at informasjon som innbyggeren skriver inn i skjemaer på Internett må transporteres trygt frem til mottaket hos skjemaleverandøren. Å sikre en slik transport på Internett gjøres ofte ved å kryptere transportkanalen mellom nettleseren og serveren med enten SSL (Secure Sockets Layer) eller TLS (Transport Layer Security) SSL/TSL gir også integritetssikring.

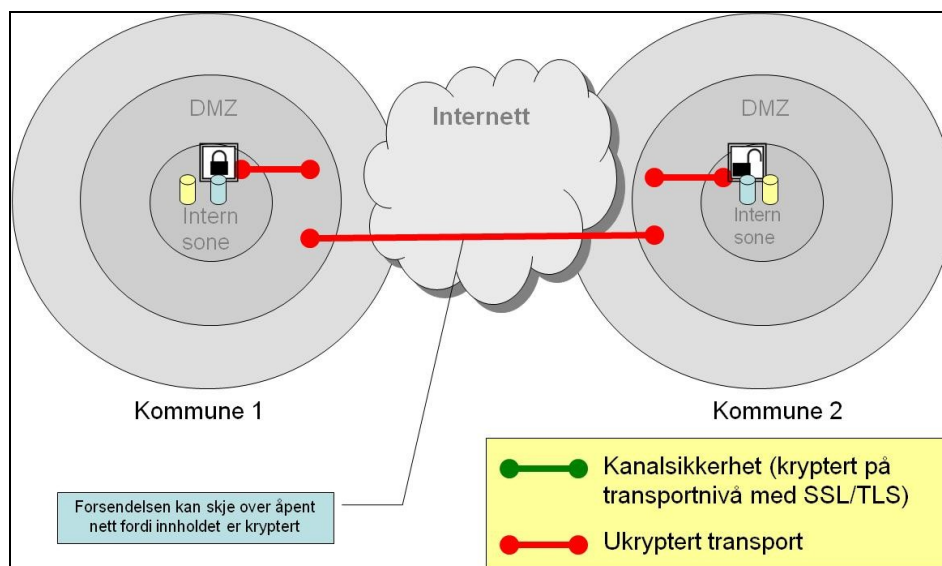


Figur 3: Eksempel på kryptering av transportkanal

Meldingsbasert kryptering

Det finnes teknologi for å kryptere selve informasjonen som alternativ til å kryptere transportkanalen. Meldingene krypteres da slik at det bare er identifisert mottaker som kan dekryptere, og meldingene signeres (digital signatur) av avsenderen. Fordelen med meldingssikkerhet er at meldingene er beskyttet også ved mellomlagring, for eksempel hos en ASP som vil kunne være en skjemaløsningsleverandør. Ett eksempel på meldingssikkerhet er sikker e-post ved bruk av S/MIME standarden.

Meldingssikkerhet krever ofte PKI-baserte mekanismer både hos avsender og mottaker for å få til gode løsninger i dag. De mest brukte PKI-løsningene i det norske markedet, BankID og Buypass, kan brukes til å oppnå meldingssikkerhet, men de støtter ikke sikker e-post. Det går også an å signere, men ikke kryptere, meldingene, og basere seg på en sikker transportkanal (SSL/TLS) for kryptering.



Figur 4: Eksempel på meldingsbasert kryptering med ende-til-ende-sikkerhet

Anbefalinger:

- All overføring av skjemadata anbefales kryptert
- Ende-til-ende kryptering skal brukes så langt dette er mulig dersom det kommuniseres sensitive opplysninger
- Overføringen skal krypteres dersom skjemaene kan inneholde sensitive opplysninger og/eller fødselsnummer
- En må velge mekanismer som også ivaretar nødvendige krav til dataintegritet

4.3.2. Ikke sikret datakommunikasjonen

Dersom man ikke har kryptert datakommunikasjonen hverken med meldingskryptering eller transportkryptering er det begrensning på hvilke skjema man kan tilgjengeliggjøre på Internett. Skjema som er tiltenkt å kunne inneholde sensitive personopplysninger, fødselsnummer eller som har åpne merknadsfelt/kommentarfelt kan da ikke legges ut på Internett.

Anbefalinger:

- Dersom man ikke har kryptert datakommunikasjon kan kun skjema som ikke vil inneholde sensitive opplysninger og/eller fødselsnummer legges ut på Internett

4.3.3. Typer vedlegg som kan sendes ved

Skjemaleverandørene bør i samarbeid med den enkelte kommune bli enige om hvilke typer vedlegg som innbyggeren skal kunne sende inn.

Anbefaling: Alle vedlegg skal overføres kryptert

4.3.4. Teknisk sikring av datafangstløsningen

Datafangstløsningen bør sikres slik at den ikke kan utnyttes til å misbruke datafangsttjenesten på noe vis. Aktuelle sikkerhetstiltak kan for eksempel være:

- Begrensning på hvor mange skjema som kan sendes inn fra samme person/PC slik at dette ikke kan utnyttes av andre til for eksempel å utføre DoS-angrep (Denial-of-Service)
- Tilbakemeldinger til den som fyller ut skjemaet må ikke være av en slik form (må for eksempel ikke oppgi tabellnavn eller feltnavn i databaser) slik at dette kan utnyttes til for eksempel å utføre angrep mot databasene for å få hentet ut informasjon

Det vises også til anbefalinger fra Datatilsynet som er tilgjengelig fra denne siden:
http://www.datatilsynet.no/templates/Page_____2093.aspx.

4.4. Autentisering og bruk av fødselsnummer

Fødselsnummer⁸ skal bare brukes når det er saklig behov, og når det er umulig å oppnå tilfredsstillende identifikasjon ved bruk av andre metoder, som for eksempel navn, adresse, fødselsdato, medlems- eller kundenummer.

Å oppgi fødselsnummer er ikke noen form for autentisering, men fødselsnummer inngår for eksempel som brukernavn i dagens løsning av Minid.

Dersom det benyttes for eksempel Minid til pålogging vil fødselsnummer komme gjennom denne påloggingen. I slike tilfeller vil det være unødvendig å be borger fylle ut fødselsnummer i tillegg på skjemaet dersom man har et legitimt behov for fødselsnummeret.

Anbefaling:

- *Fødselsnummer skal bare brukes når det er saklig behov og 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*

4.4.1. Bruk av fødselsnummer i dag

Flere IT-løsninger i kommunene i dag bruker fødselsnummer som ”logisk oppslagsnøkkel” og unik id. Dette gjør det for eksempel enkelt å kunne følge samme borger vha. fødselsnummeret i både et fagsystem og faktureringsystemet.

Det som gjør fødselsnummer så ”attraktivt” å bruke er i hovedsak to ting:

- 1) Det identifiserer helt entydig den enkelte borger
- 2) Det kan fungere som en global unik ID som kan brukes på tvers av IT-systemer som oppslagsnøkkel

Å innhente fødselsnummer fordi fagsystemet (eller et annet system) av datatekniske årsaker trenger fødselsnummeret til bruk som id eller lignende ansees ikke som en saklig grunn for å innhente fødselsnummer (det skal foreligge et saklig behov).

Dersom fødselsnummer ikke kan brukes kan man se for seg følgende løsninger:

- 1) For å identifisere den enkelte borger kan man bruke for eksempel ”fødselsdato + etternavn”. Dette vil i de aller fleste tilfeller entydig identifisere den enkelte borger innenfor en kommune. Når duplikater dukker opp må man kanskje håndtere disse manuelt ved at man sjekker adresse og lignende før man kan entydig identifisere borgeren

⁸ Fødselsnummer er på 11 siffer og består av *fødselsdato* (6 siffer) + *personnummer* (5 siffer)

- 2) Eventuell autentisering av borgeren vil sikre at kommunen med stor sikkerhet vet hvilken borger som har sendt inn et skjema.
- 3) Innenfor det enkelte IT-system kan en borger få en hvilken som helst unik ID rent datateknisk. Utfordringen er når man må kryssjekke at det er samme borgeren som opptrer i flere systemer. Da vil løsninger for eksempel med bruk av unikt kundenummer innenfor en kommune kunne løse dette problemet.

Med en løsning som beskrevet ovenfor vil tilgang til fødselsnummer kunne begrenses til de tilfeller hvor man i selve søknadsbehandlingen (og ikke av datatekniske årsaker) har legitimt behov for å innhente fødselsnummer til borgeren. Dette kan for eksempel være nødvendig å sjekke fødselsnummeret for kontrollere at det er riktig borger som får utbetalt sosialstøtte.

Anbefalinger:

- *Alle aktuelle systemer må legge til rette for å kunne registrere nødvendig informasjon om en borger uten at dette krever fødselsnummer*
- *Alle aktuelle systemer må ikke legge opp til funksjonalitet som krever bruk av fødselsnummer uten at det er et legitimt behov for å bruke fødselsnummer i den aktuelle situasjonen*

4.5. Datahåndtering når skjema løsning ligger hos en databehandler

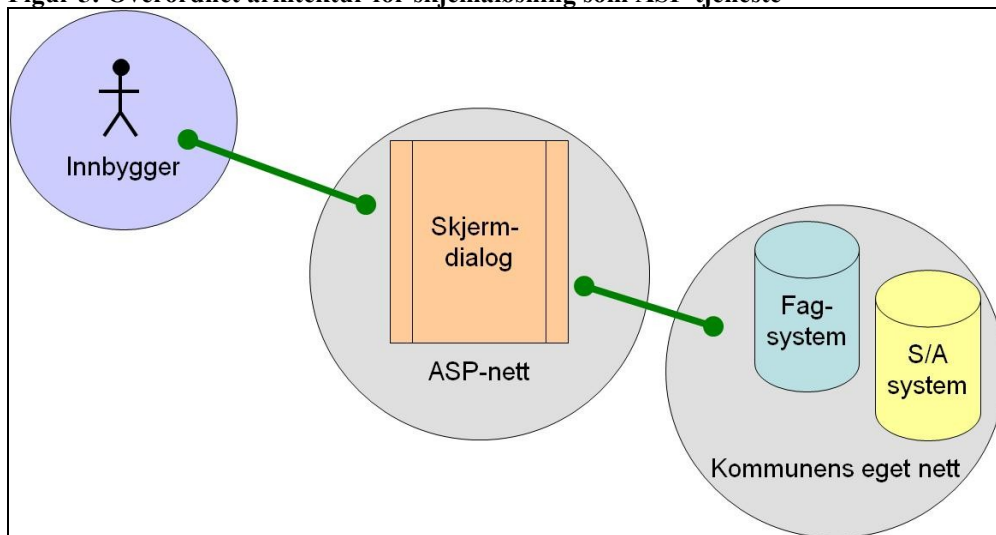
Dersom skjema løsningen ligger eksternt hos en skjemaleverandør (som en ASP-løsning) vil skjemaleverandøren opptre som en databehandler som innhenter data på vegne av kommunen som er behandlingsansvarlig. Ansvarsforholdene mellom databehandler og behandlingsansvarlig må beskrives gjennom en databehandleravtale (se kapittel 5.4). Databehandleravtalen regulerer hvordan databehandler skal håndtere personopplysninger på vegne av behandlingsansvarlig⁹.

Hvordan databehandler kan behandle personopplysninger er beskrevet i personopplysningsloven § 15 (Databehandlerens rådgighet over personopplysninger). Hvordan databehandlingsansvarlige kan behandle opplysninger er blant annet beskrevet i personopplysningsloven § 11 (Grunnkrav til behandling av personopplysninger).

Figur 5 viser eksempel på en overordnet arkitektur for en skjema løsning som ligger hos en ASP-leverandør.

⁹ Eksempel på retningslinjer for en slik databehandleravtale er utarbeidet i forbindelse med Norm for informasjonssikkerhet i helsesektoren: http://www.nhn.no/Tjenester/bransjenormen/filer/faktaark_10_-_bruk_av_ekstern_driftenhet_databehandler.pdf

Figur 5: Overordnet arkitektur for skjemaløsning som ASP-tjeneste



4.5.1. Transaksjonslagring og mellomlagring hos skjemaleverandør

Når skjemaløsningen ligger som en ASP-løsning hos en leverandør er utgangspunktet at leverandøren opptrer som en databehandler som innhenter data ("datainnsamler") på vegne av kommunen (behandlingsansvarlig). Dersom databehandleren skal ha en rolle utover enn en ren "datainnsamler" må dette være i samsvar med blant annet personopplysningsloven § 11 (Grunnkrav til behandling av personopplysninger) og § 15 (Databehandlerens rådighet over personopplysninger). Hva databehandleren skal kunne gjøre av databehandling må også være beskrevet i databehandleravtalen.

Transaksjonslagring

Skjemaleverandør kan foreta transaksjonslagring av de opplysninger som sendes inn fra innbyggeren ved endt datafangst. Slik transaksjonslagring kan gjøres slik at skjemaleverandøren lagrer skjema-dataene borgeren sender inn inntil kommunen kan bekrefte at dataene er korrekt mottatt fra skjemaleverandøren. Skjemaleverandøren kan lagre skjema-dataene i maks 72 timer

etter at en søknad er sendt (72 timer ansees som forvaltningspraksis) slik at det skal være rimelig tid til å oppdage eventuelle (tekniske) feil ved forsendelsen.

Mellomlagring

Skjemaleverandøren (som opptrer som ren datainnsamler og databehandler på vegne av kommunen) har i utgangspunktet ikke grunnlag for å lagre eller behandle personopplysninger på annen måte enn det som er beskrevet ovenfor. Et slikt grunnlag må eventuelt være begrunnet i personopplysningsloven § 11 (grunnkrav til behandling av personopplysninger). Dette betyr for eksempel at mellomlagring av et delvis utfylt skjema ikke kan gjøres så lenge dette ikke kan gjøres med grunnlag i personopplysningsloven § 11 og § 15.

4.5.2.Datahåndtering med og uten autentisering av borger

Skjemaleverandøren og den enkelte kommunen må bli enige om krav til autentisering av innbyggeren. Se mer i kapittel 3.3.5.

4.5.2.1.Retningslinjer vedrørende datafangst

Vi anbefaler følgende retningslinjer for datahåndtering (uavhengig om borgeren er autentisert eller ikke):

- Skjemaleverandøren kan lagre skjemaedata i maks 72 timer etter at en søknad er sendt slik at det skal være rimelig tid til å oppdage eventuelle feil ved forsendelsen
- Data skal slettes hos skjemaleverandør når de er bekreftet korrekt mottatt hos kommunen (for eksempel ved hjelp av applikasjonskvitteringer mellom systemene som kommuniserer)
- Eventuelle vedlegg skal slettes etter at vedlegget er bekreftet korrekt mottatt av kommunen
- Borgeren må få kvittering fra skjemaleverandør ”vist på skjerm” når skjemaet sendes inn fra borgeren
- Skjemaleverandøren kan lagre metadata (”logger”) om skjemaene som er sendt, dette kan for eksempel være id (ikke fødselsnummer), type søknad, tidspunkt.

4.5.2.2.Med autentisering av borger

Dersom borger blir autentisert og samtykker til det kan en ved skjemautfylling tilby ”ekstratjenester” som for eksempel preutfylling av visse typer opplysninger.

Dersom innbyggeren er autentisert og har gitt sitt samtykke kan skjemaleverandøren tilby følgende til borgeren:

- Preutfylling av visse typer veldefinerte opplysninger (for eksempel adresseinformasjon) som hentes fra databehandlingsansvarliges (kommunen) registre
- Hvilke typer opplysninger som innhentes må presenteres for innbyggeren på forhånd og innbyggeren må gi sitt samtykke til dette før slik innhenting kan skje
- Vise logg over ”metadata”, for eksempel tidligere innsendte søknader

4.5.2.3.Uten autentisering av borger

Dersom borgeren ikke er autentisert skal alle data slettes etter at data er bekreftet korrekt mottatt av kommunen. Logg over metadata (id, type søknad, tidspunkt etc.) kan imidlertid lagres.

4.5.2.4.Teknisk lagring hos skjemaleverandør

Skjemaleverandøren må lagre skjemadataene på en sikker måte. Dette betyr blant annet at:

- Det skal være logiske skiller på data tilhørende ulike databehandlingsansvarlige (som i praksis som regel være en kommune).
 - o For eksempel i egne databaser for hver databehandlingsansvarlige
- Sensitiv informasjon skal krypteres ved lagring hos skjemaleverandør.
- Sensitiv informasjon skal lagres i en sikker sone hos skjemaleverandøren

Anbefalinger:

- *Skjemadata kan lagres i inntil 72 timer hos skjemaleverandør, men skal slettes når data er bekreftet korrekt mottatt hos kommunen*
- *Kun metadata om innsendte skjema kan lagres utover 72 timer hos skjemaleverandøren*
- *Preutfylling av visse typer data må skje gjennom at skjemaløsning henter data fra kommunens register*
 - o *Preutfylling krever særskilt samtykke fra innbyggeren*

4.5.3.Kvittering på innsendt skjema

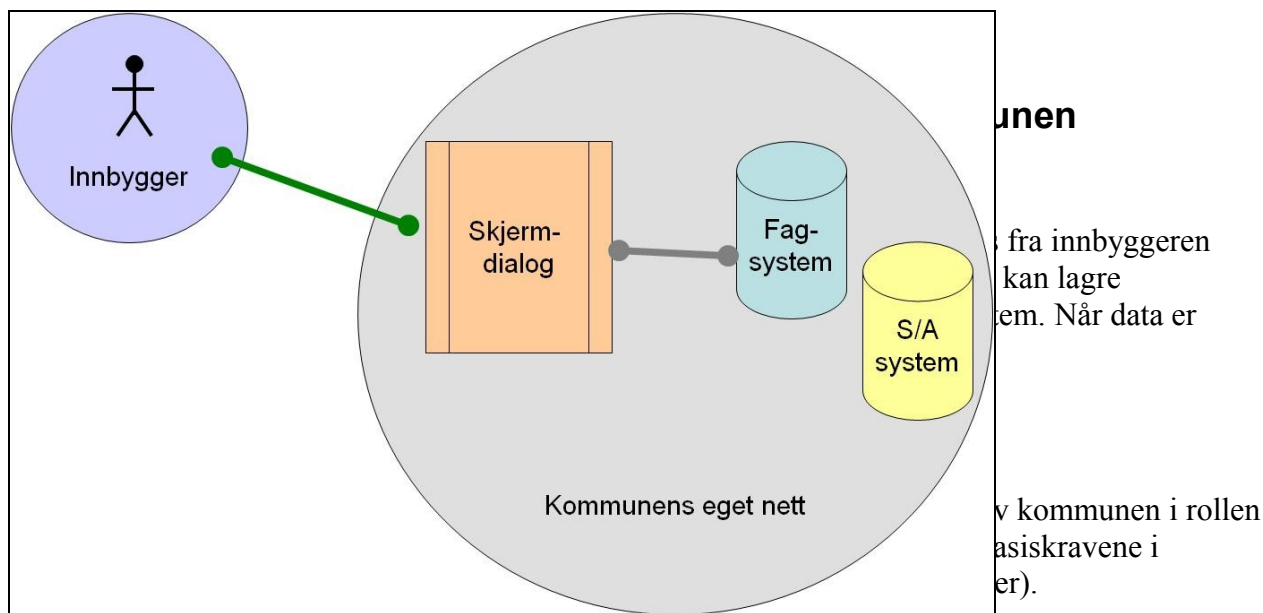
Kvittering ”vist på skjerm” for innsendt skjema kan vises til innbyggeren når skjemaet er sendt inn. Kommunen bør sende også bekreftelse til innbyggeren via e-post når søknad er kommet frem til kommunen. Det bør også være mulig å få slik bekreftelse tilsendt på SMS for den som ønsker det. Kvitteringen må ikke inneholde noen opplysninger fra selve søknaden, men kan for eksempel inneholde et referansenummer til det innsendte skjemaet.

Anbefalinger:

- *Borger bør få kvittering vist ”på skjerm” når et skjema er sendt inn*
- *Borger bør også få en bekreftelse via e-post eller SMS fra kommunen når søknaden er mottatt i kommunen.*
- *Kopi av innsendt skjema (for eksempel i form av en pdf-fil) må **ikke** sendes innbyggeren via e-post for skjema som kan inneholde sensitive opplysninger.*

4.6. Datahåndtering når skjemaløsning ligger hos behandlingsansvarlig

Dersom skjemaløsningen ligger lokalt hos kommunen (dvs. i kommunens nettverk slik at kommunen har full kontroll over datafangsten) vil ikke skjemaleverandøren opptre som noen databehandler på vegne av kommunen. Kommunen vil da både ha rollen som databehandler og databehandlingsansvarlig.



Figur 6: Overordnet arkitektur for skjemaløsning som ligger lokalt hos kommunen

4.6.2. med autentisering av borger

Dersom borger blir autentisert kan en ved skjemautfylling tilby ”ekstratjenester” som for eksempel preutfylling av visse typer informasjon i et skjema.

Dersom innbyggeren er autentisert og har gitt samtykke til kan følgende tilbys innbyggeren:

- Kommunen kan mellomlagre data slik at innbyggeren kan fylle ut et skjema i flere sesjoner (med flere inn- og utlogginger)
 - o Krever autentisering på sikkerhetsnivå 3 eller 4 avhengig av type skjema (se anbefalinger i kapittel 3.3.5)
- Preutfylling av visse typer opplysninger (for eksempel adresseinformasjon) fra kommunens registre
 - o Hvilke typer opplysninger som kan innhentes må presenteres for innbyggeren på forhånd og innbyggeren må gi sitt samtykke til dette.
- Gjenbruke og vise data fra tidligere innsendte skjema dersom innbyggeren samtykker til at kommunen kan beholde kopi av innsendte skjema

¹⁰ Det er viktig å huske på at data innhentet via skjemaløsningen naturligvis skal lagres/arkiveres i aktuelle fag-/arkivsystem etter gjeldene regelverk. Med sletting her menes det at dataene skal slettes fra skjemaløsningen når dataene er mottatt i aktuelle fag-/arkivsystemer i kommunen.

- Krever at innbyggeren samtykker til at kommunen kan lagre kopi av innsendte skjema til senere gjenbruk i skjemaløsningen
- Det må være kjent hvor lenge kommunen kan beholde kopi av innsendte skjema, for eksempel 3 måneder. Kopi av innsendte skjemadata skal da slettes etter angitt tidsrom.
- Dersom gjenbruk av data omfatter sensitive opplysninger må borger autentiseres med en sikkerhetsløsning på sikkerhetsnivå 4. Dvs. at Minid ikke kan benyttes som autentiseringsløsning, men en må benytte for eksempel en PKI-løsning som tilfredsstillende kravene til sikkerhetsnivå 4.

4.6.3.Uten autentisering av borger

Uten innlogging fra innbyggeren skal skjemadata slettes etter at data er mottatt korrekt i kommunens fagsystemer.

4.7.Sikring av datakommunikasjon

For selve transportoverføringen av data mellom skjemaleverandør og kommunen er det flere forhold som bør ivaretas gjennom valgt metode. De viktigste mekanismene beskrives nedenfor.

4.7.1.Sikker datakommunikasjon

Overføringen av data mellom skjemaleverandør og kommune må krypteres for å ivareta krav til konfidensialitet. Kryptering kan i hovedsak skje på to måter:

Kryptert transportkanal

Kryptert transportkanal innebærer at det etableres en sikker overføringslinje mellom skjemaleverandør og kommunen som brukes for å overføre data. Det er viktig å merke seg at data i en slik løsning vil være ubeskyttet når dataene kommer ut av den krypterte transportkanalen. Dersom man for eksempel har en kryptert transportkanal inn til en server i DMZ, så vil dataene ligge ukryptert når det overføres til serveren.

Meldingskryptering

Kryptering av selve informasjonen innebærer at informasjonen som sendes over blir kryptert for eksempel vha. av virksomhets sertifikater i en PKI-løsning. Med slik meldingskryptering vil informasjonen ligge kryptert til man velger å dekode dataene.

Anbefalinger:

- *Overføringen, uansett valgt transportmetode må sikres (krypteres)*
- *Dersom sensitive opplysninger overføres skal disse sikres med ende-til-ende-sikkerhet*

4.7.2. Dataintegritet

Dataintegritet er den egenskapen at data ikke er blitt ødelagt eller endret på en ikke-autorisert måte. Ved datakommunikasjon bør mottageren være i stand til å oppdage om meldinger er blitt endret ved et aktivt inngrep eller ved et uhell. På et stadium må informasjonen forsegles slik at enhver påfølgende endring vil oppdages. Når vi verifiserer dataintegritet forsikrer vi oss om at det ikke har skjedd endringer i informasjonen etter at denne ble forseglet.

Digitale signaturer i en PKI-løsning kan for eksempel brukes til å verifisere at dataintegriteten er intakt.

4.7.3. Kvitteringsmekanismer

Kvitteringsmekanismer skal sørge for at avsender for kvittering for at en melding er kommet korrekt frem til mottaker, eller at det gis feilmeldinger dersom noe har feilet i forsendelsen.

Anbefalinger:

- *En må sørge for sikker og pålitelig transportoverføring som sikrer at data kommer korrekt frem og det er mekanismer for å oppdage for eksempel endring i data eller at data ikke kommer frem*
- *En bør velge en metode kan sørge for kvitteringsmekanismer som sikrer at en får kvittering når en forsendelse er kommet frem eller feilmeldinger når en forsendelse feiler*

4.7.4. Anbefalte transportmetoder

Vi anbefaler alle kommuner å velge en transportmetode som sørger for sikker og pålitelig overføring av data mellom skjemaleverandør og kommunen:

- E-post bør ikke velges som overføringsmetode pga. manglende kvitteringsmekanismer og dårlig sporbarhet
- FTP, http ebXML, eller webservices anbefales som overføringsmetode fremfor e-post fordi disse regnes som mer sikrere og mer pålitelige enn vanlig e-post. ebXML er en kanskje den beste metoden fordi den blant annet har innebygde funksjoner for kvitteringsmekanismer.

Uansett overføringsmetode må denne sikres vha. kryptering, autentisering av systemet etc.

4.7.5. Autentisering av systemene

Ved kommunikasjon mellom to systemer må en være sikker på at det er de riktige systemene som kommuniserer med hverandre. Noen anbefalinger er:

- Det må være autentisering av begge ender som sikrer at det kun er autoriserte systemer som kommuniserer med hverandre
- Autentisering skal skje med sikrere metoder enn bare passord, for eksempel med bruk av sertifikater hos begge parter
- Hos skjemaleverandøren må en sørge for at den enkelte kommune kun får lov til å hente data som tilhører kommunen (dersom dette er aktuelt for valgt overføringsmetode)

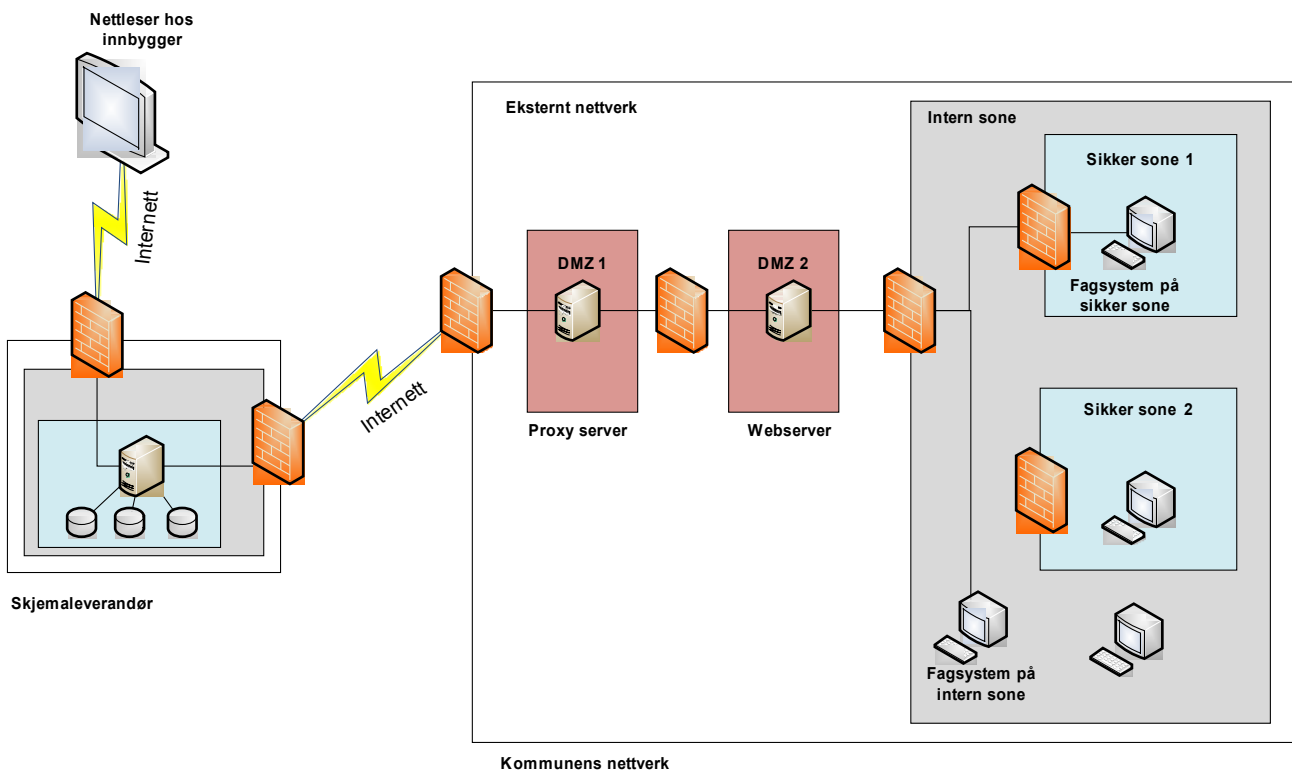
- Skjemaleverandøren må også sørge for at data skrives til riktig kommune (dersom dette er aktuelt for valgt overføringsmetode)
- Hos kommunen må en sørge for at kun skjemaleverandøren får til lov til å overføre data inn til kommunens nettverk (dersom dette er aktuelt for valgt overføringsmetode)

Anbefalinger:

- En må sørge for sikker autentisering av systemene ved overføring slik at ingen uautoriserte systemer får mulighet for datatransport fra/til skjemaleverandør og/eller kommunen

4.8.Datahåndtering hos kommunen

Datatilsynet har retningslinjer og anbefalinger for hvordan en kommune bør utforme sitt nettverk med tanke på sikker informasjonsbehandling . Datatilsynet beskriver blant annet hvordan en kommune bør dele opp sitt nettverk i interne og sikre soner (gjerne kjent som ”tosone-modellen”). Figur 7 under viser et eksempel på hvordan en kommune kan utforme sitt nettverk med tanke på å få til en sikker nettverksarkitektur.



Figur 7: Mulig teknisk nettverksarkitektur for skjemaløsning på nett

Hovedregelen er at sensitiv informasjon skal behandles på et system som ligger i sikker sone, mens ikke-sensitiv informasjon kan behandles på system i intern sone.

I tillegg til soneinndelingen med tekniske sperrer mellom sonene er det også viktig med å sikre tilgangen til tjenestene som ligger på de ulike sonene. Dette kan for eksempel være tilgang til fagsystemer, filområder eller webservice tjenester.

4.8.1. Mottak av data i kommunen

Mottaket av skjema-data må sikres slik at kommunen ikke blir eksponert for unødige trusler knyttet mot datakommunikasjon mot skjemaleverandør:

- Det bør brukes en egen dedikert server som er konfigurert til å ta imot skjema-data fra skjemaleverandøren, jfr. Figur 7.
 - o Det bør vurderes å sikre tilgangen til en slik dedikert server for eksempel ved kun å tillate datakommunikasjon fra IP-adresser hos aktuell skjemaleverandør. I tillegg må det være autentisering av systemene.
 - o Det bør også vurderes å sette mottaket av skjema-data i en egen dedikert DMZ-sone slik tilgang til ”mottaksserveren” ikke kan misbrukes til å få tilgang til andre systemer
- Data må aldri lagres usikret i DMZ. DMZ må kun brukes som en ”mellomstasjon” hvor data kontrolleres og hentes videre inn til intern/sensitiv sone og aktuelle systemer
 - o Data skal krypteres så lenge de er i DMZ
 - o Dekryptering av data skal først skje når data skal hentes videre inn til intern sone, eventuelt at dekryptering skjer når data er kommet på innsiden av DMZ
 - o For sensitiv informasjon som skal til sikker sone er hovedregelen at disse dekrypteres først når data er i sikker sone (jfr. Kommuneveilederen fra Datatilsynet, kapittel 18.3.2)
- Sjekk mot ondsinnet programvare
 - o All innkommende data må kontrolleres for ondsinnet programvare
 - o Skanning bør også skje hos avsender (skjemaleverandør)
 - o Skanning må gjøres etter at en data er dekrypteres for å kunne oppdage eventuell ondsinnet kode
 - o Vedlegg må også skannes
- Kommunen bør som generell regel alltid initiere datatrafikken inn til kommunens nettverk. Dette kan løses på flere måter
 - o Kommunen kan hente data fra skjemaleverandør (for eksempel vha. ftp eller webservices)
 - o Kommunen kan tillate trafikk (for eksempel filoverføring) inn til en dedikert server i DMZ hvor så kommunen henter data videre inn til aktuelle systemer
- Bør ha kvitteringsmekanismer som sendes fra kommunen til skjemaleverandør når skjemaet er mottatt i kommunen
 - o Og e-post til innbyggeren med bekreftelse fra kommunen om mottatt skjema + ev. referansenummer.

Anbefalinger:

- *Kommunen må sikre sitt mottak av skjema-data for eksempel gjennom å bruke dedikerte servere og egne DMZ-soner for dette*
- *Data må aldri ligge usikret i DMZ*
- *All innkommende data må skannes for ondsinnet programvare*

- Dekryptering må skje først når data hentes inn fra DMZ
- Kommunen bør som hovedregel alltid initiere og ha kontroll på datatrafikken inn til kommunens nettverk

4.8.2. Eksempel på teknisk løsning

Eksempel på hvordan trafikken kan settes opp internt fra DMZ og videre innover i kommunens nettverk:

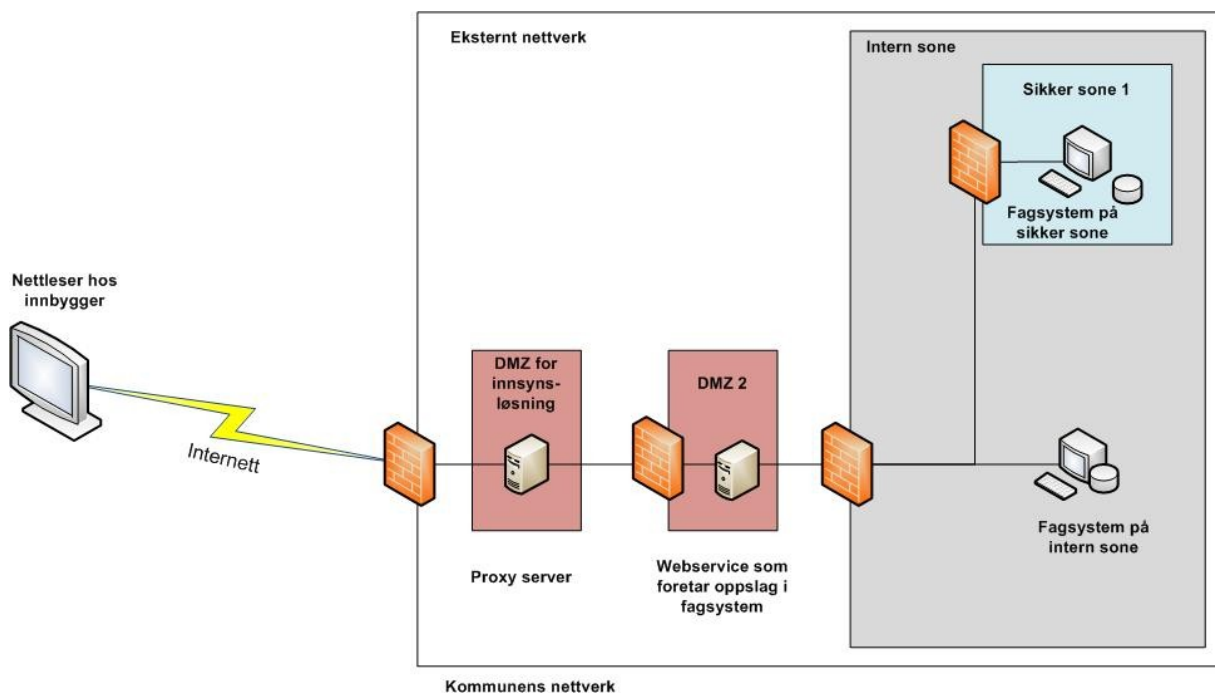
- En setter opp det interne nettverket med to DMZ-soner.
- På det første DMZ nettet setter man inn en reverse proxy. Denne vil da terminere all HTTPS trafikk fra eksterne brukere. Fordelen med dette er at man kun trenger et sertifikat uavhengig av hvor mange web servere på baksiden man ønsker å komme i kontakt med.
- Reverse proxy serveren setter så opp en HTTP forbindelse fra seg selv og videre inn mot webserveren på det andre DMZ nettet. Ved at denne trafikken går i klartekst (HTTP) kan man så benytte Web Security på brannmuren for å sikre seg mot uønsket tilgang.
- Fordelen med å gjøre det på denne måten er at oppsettet på webserveren kan være helt standard HTTP, uten kryptering, som igjen gjør at systemet vil bli enklere å administrere for Kommunen. På den andre siden kan Reverse Proxy'en benyttes som terminering når neste tjeneste skal på luften uten å installere/kjøre nye sertifikater siden dette allerede finnes.

Se også Figur 7 for mulig nettverksarkitektur.

4.9. Tilgang og innsyn i data hos kommunen

Dersom kommunen tillater at data hentes ut fra egne systemer for tilgjengeliggjøring enten i egen innsynsløsning eller via Minside gjelder i utgangspunktet de samme sikkerhetsprinsippene som er beskrevet i kapittel 4.1.

Det blir enda viktigere å ha god kontroll og styring på hvem som får lov til å hente ut data i en slik setting. Dersom en for eksempel har en webservice som henter ut data fra et fagsystem bør en da blant annet sette krav til sterk autentisering vha. sertifikater/PKI-løsning fra den parten som skal benytter webservicen for å hente ut data. En slik webservice må også kjøres i et sikret miljø og være utviklet slik at den som benytter webservicen ikke kan utnytte svakheter i tjenesten til å hente ut mer eller andre data enn det som er tiltenkt.



Figur 8: Eksempel på nettverksarkitektur for innsynsløsning

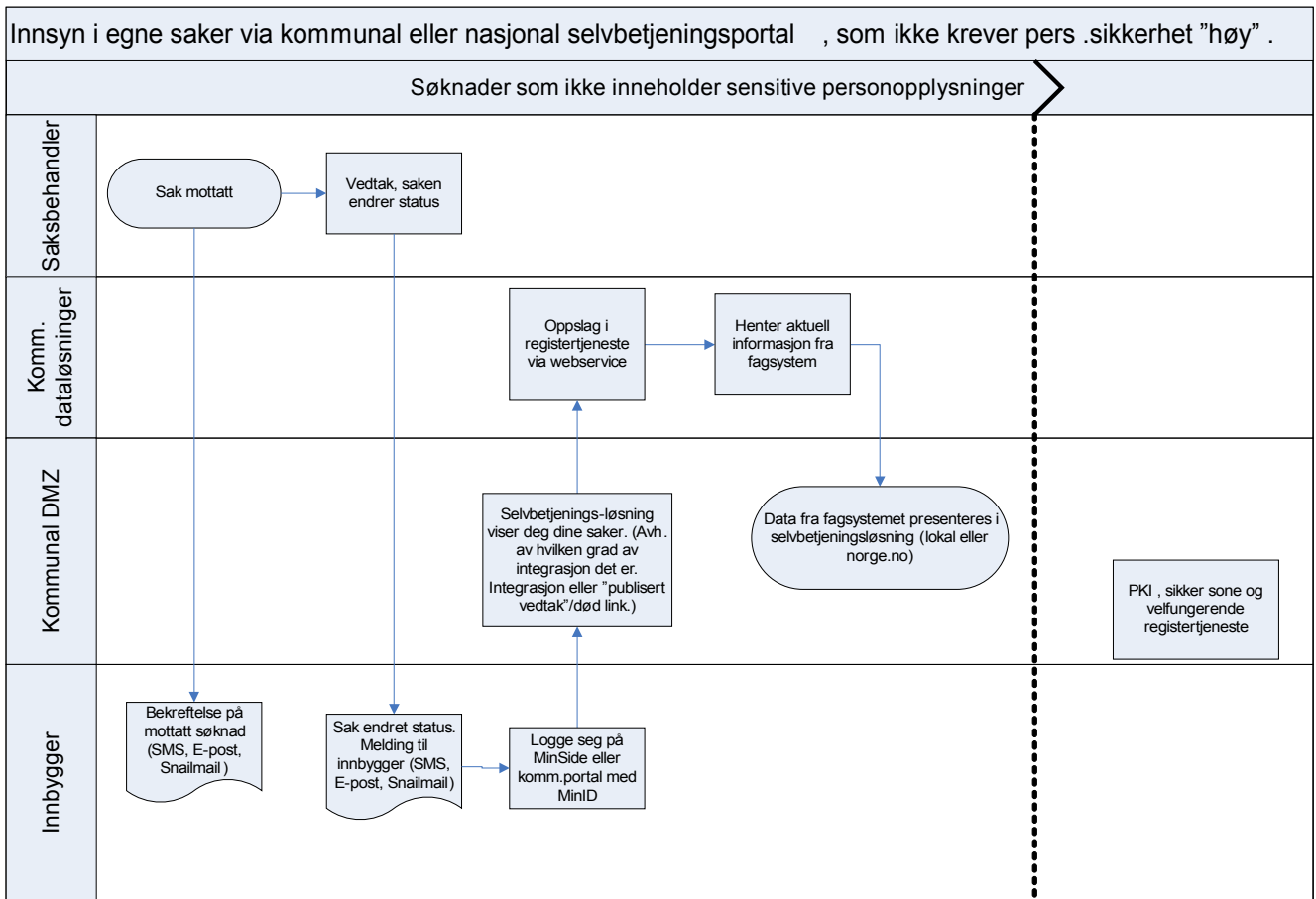
En innsynsløsning må utformes slik at den på en sikker måte henter ut riktige data til autentisert borger (eller et autentisert system):

- Borgeren logger for eksempel på en portalløsning og får innsyn i "sine saker" i henhold til sikkerheten på påloggingen (for eksempel Minid på nivå 3 eller en PKI-løsning på nivå 4)
 - o Informasjonen kan for eksempel være status på behandling av et skjema eller det vedtaket som er fattet
 - o Bruk av autentiseringsløsning på nivå 4 hos borgeren vil kunne gi innsyn til sensitiv informasjon, mens en autentiseringsløsning på nivå 3 hos borgeren vil bare gi tilgang til ikke-sensitiv informasjonen
- Kun den borgeren som er autentisert som avsender kan få elektronisk innsyn i ettertid til samme skjema/sak
- Kommunen må ha god kontroll på hvordan dataene hentes ut
 - o For eksempel at dette skjer gjennom en egen DMZ-sone for innsynsløsningen hvor det er streng kontroll på trafikken inn og ut, jfr. Figur 8.
 - o Kommunen må ved en innsynsløsning ikke unødig eksponere andre interne systemer som eventuelt kan utnyttes av ondsinnede angrep via innsynsløsningen
 - o Innsynsløsningen bør ikke ha muligheter til kommunikasjon mot andre systemer enn det som er nødvendig for å få hentet ut data fra kommunen
 - o Innsynsløsningen bør være så "isolert" så mulig slik at eventuelle ondsinnede angrep får minst mulige konsekvenser

Anbefalinger:

- Kommunen må sørge for sikker autentisering og løsninger som sørger for at data kan hentes ut fra kommunen på en trygg og sikker måte

- Innsynsløsningen må være utformet slik at den ikke unødig eksponerer andre systemer eller annen informasjon enn det som er nødvendig for selve innsynsløsningen



Figur 9: Eksempel på skjemaflyt for innsyn

Videre problemstillinger rundt tilgang og innsyn

En aktuell problemstilling som dukker opp vedrørende innsyn er hvem som skal få innsyn for eksempel til et vedtak. Slike problemstillinger kan for eksempel være:

- Far har elektronisk søkt barnehageplass for et barn, skal mor også få elektronisk tilgang til statusopplysninger og vedtak etc. om søknaden?

Hvordan slike problemstillinger kan løses har både tekniske (hvordan) og juridiske (hva er lovlig) problemstillinger som må vurderes og avklares før slike løsninger kan etableres.

Sikkerhetsgruppen har ikke vurdert slike problemstillinger i prosjektet, men påpeker at dette er et område for videre arbeid.

4.10. Tilbakemelding fra kommune til borger

Informasjon fra kommunen tilbake til borger vedrørende et innsendt skjema kan skje på følgende måter (her kan det være flere løsninger som ikke beskrevet):

Tabell 3: Oversikt over tilbakemeldinger til borgeren

Når	Type tilbakemelding
Ved datafangst	<ul style="list-style-type: none"> - Kvittering vist ”på skjerm” til borger når et skjema sendes inn fra Internett. Mulighet for utskrift bør være tilstede. - Bekreftelse sendt til borger (med referansenummer) via e-post eller SMS når kommunen kan bekrefte at skjemaet er korrekt mottatt i fagsystemet. Dette vil da medføre en forsinkelse før innbyggeren får en slik kvittering på e-post/SMS (forsinkelsen vil avhenge blant annet av valgt overføringsmetode til kommunen)
Under saksbehandling	<ul style="list-style-type: none"> - Tilbakemelding til borger om status på sak kan gjøres via SMS, e-post og vanlig postgang. - Tilbakemelding via usikrede medier (som for eksempel SMS eller vanlig e-post) må ikke inneholde opplysninger om selve saken, men kun et ”statusvarsel”. - Informasjon til borgeren via Minside kan kun omfatte ikke-sensitiv informasjon
Etter at saksbehandling er avsluttet og vedtak er fattet	<ul style="list-style-type: none"> - Informasjon om vedtak må sendes i vanlig postgang og/ eller gjøres tilgjengelig via innsynsløsning hos kommunen/Minside - Dersom innsyn i vedtak innebærer innsyn i sensitive opplysninger krever dette at borgeren autentiseres med sikkerhetsnivå 4. Dvs. at autentisering vha. Minid eller tilgang til opplysningene via Minside ikke kan benyttes. - Innsyn i vedtak som ikke inneholder sensitive opplysninger kan gjøres vha. at borgeren autentiseres på sikkerhetsnivå 3 (for eksempel Minid).

5.Arbeid med informasjonssikkerhet

Arbeid med informasjonssikkerhet er en aktivitet som må drives kontinuerlig i en kommune. Å planlegge og organisere arbeidet kan gjøre det både enklere og mer effektivt å sørge for tilfredsstillende informasjonssikkerhet i en kommune. I tillegg stilles det også flere lovkrav som kommuner må oppfylle, blant annet at må etableres sikkerhetsorganisasjon i samsvar med personopplysningsloven § 13.

5.1.Kommunens ansvar

Aktuelle referanse kilder er blant annet:

- Veileder for kommuner og fylker: http://www.datatilsynet.no/templates/article___890.aspx, her er ”Del II” om ledelsens ansvar spesielt relevant
- Risikovurderinger: http://www.datatilsynet.no/templates/article___888.aspx
- Sikring av fødselsnummer: http://www.datatilsynet.no/templates/article___1594.aspx
- Generelle plikter: http://www.datatilsynet.no/templates/Temaforside___104.aspx
- Kommuner og tilknytning til Norsk Helsenett: <http://www.nhn.no/informasjonssikkerhet/norm-for-informasjonssikkerhet-i-helsesektoren>

5.1.1.Oversikt over behandlinger av helse- og personopplysninger

5.1.1.1.Forvaltning av kommunens opplysninger og systemer

For mange virksomheter kan det være en utfordring å ha oversikt over hvilke behandlinger av helse- og personopplysninger som gjøres i forhold til formål, hjemmel, informasjonssystemer, etc. En slik samlet og oppdatert oversikt over alle behandlinger av helse- og personopplysninger i virksomheten, er et viktig styringsdokument for informasjonssikkerhet, og et praktisk redskap i det gjennomførende arbeidet. Dette vil også kunne være et viktig bidrag til den generelle internkontrollen i virksomheten på dette området.

5.1.1.2.Utforme oversikt over behandlinger og tilhørende formål

Det bør opprettes et oversiktsskjema for de ulike behandlingene av helse- og personopplysninger. Vedlagte skjema kan benyttes som et utgangspunkt og videre tilpasses den enkelte behandlingen av helse- og personopplysninger. Hvilke systemer som inngår i behandling av helse- og personopplysningene bør også inngå som den del av oversikten.

Et oversiktsskjema bør innholde følgende opplysninger:

- Formålet med behandlingen
- Kategori av helse- og personopplysninger
- Juridisk hjemmelsgrunnlag for behandlingen
- Angivelse av system/register/utstyr, og om det er elektronisk eller manuelt

- Beskrivelse av behandlingen av helse- og personopplysninger
- Om opplysningene er sensitive eller ikke-sensitive helse- og personopplysninger
- Konesjonsplikt/meldeplikt/hjemmel for unntak
- Evt. partnere, databehandlere eller leverandører
- Internt ansvarlig for det enkelte system/register/utstyr

5.2. Rutine for ”skjema på nett”

Det bør utarbeides enkle rutiner for ”skjema på nett” som sørger for tilfredsstillende informasjonssikkerhet for skjema som gjøres tilgjengelig på nett. Disse rutineene bør inngå i kommunens styringssystem for informasjonssikkerhet.

Rutineene bør sørge for at:

- Det ikke legges ut nye skjema på nett før det er vurdert at eksisterende løsninger ivaretar tilfredsstillende informasjonssikkerhet (for eksempel at kryptering er på plass for skjema som krever dette). Risikovurderinger skal foretas.
- Det føres oversikt over helse- og personopplysninger som behandles i virksomheten som kommer fra ulike skjema. Det bør angis hvilke systemer og hvilke opplysninger som behandles i de ulike systemene.
- Oversikt over partnere og leverandører skal dokumenteres. Virksomheten skal etablere klare ansvarsforhold mellom partnere og leverandører som beskrives i en særskilt avtale
- Konfigurasjonskart og beskrivelse av den IT-tekniske løsningen skal utarbeides. Løsningen skal baseres på valgt sikkerhetsstrategi og risikovurderinger
- Prosedyrer for informasjonsbehandlingen skal dokumenteres og innføres

5.3. Kommunen må dokumentere tilfredsstillende informasjonssikkerhet

Det er den enkeltes kommune sitt ansvar gjennom sin rolle som behandlingsansvarlig å påse tilfredsstillende informasjonssikkerhet rundt behandling av kommunens data. Dette inkluderer også ansvaret for at skjemaløsningene (og annen bruk av databehandlere) har etablert tilfredsstillende informasjonssikkerhet gjennom planlagte og systematiske tiltak.

Dokumentasjon

Kommunen skal ha dokumentasjon over de system som brukes til å behandle data i tilknytning til ”skjema på nett”

5.4. Bruk av databehandler og databehandleravtale

Personopplysningsloven § 15 (Databehandlerens rådighet over personopplysninger) sier blant annet at *”En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige”*.

En databehandleravtale er en avtale mellom behandlingsansvarlig og databehandler (ekstern driftsenhet). En databehandler er en person eller virksomhet utenfor den databehandlingsansvarliges virksomhet. Databehandleren behandler opplysninger på vegne av den

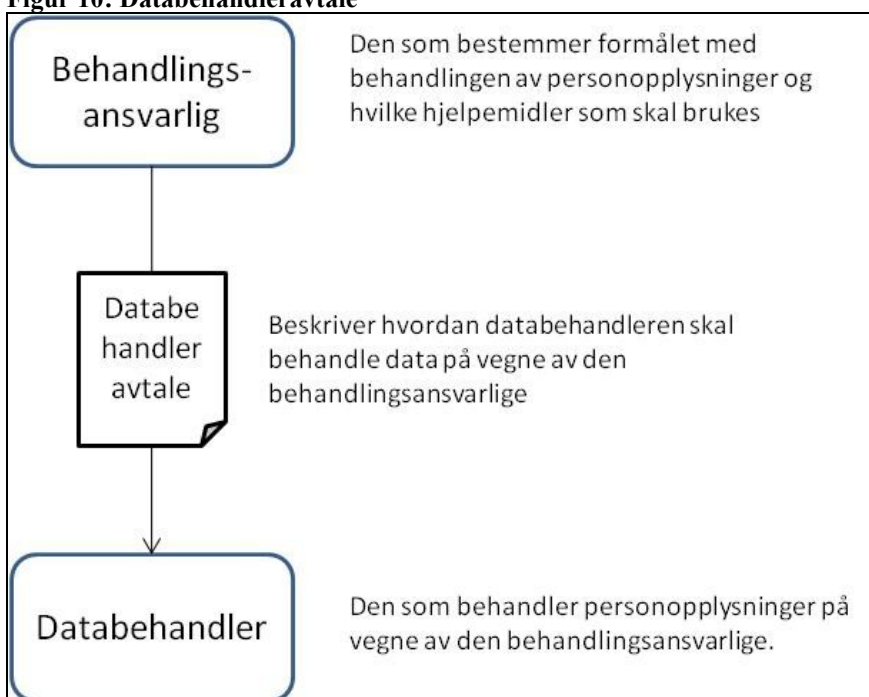
databehandlingsansvarlige. Dette betyr at hvis et kommunens IT-systemer (alle eller noen) blir driftet av en ekstern driftsenhet, er denne eksterne driftsenheten en databehandler. Kommunen skal alltid ha en oversikt over alle eksterne driftsenheter som behandler opplysninger på vegne av kommunen.

Databehandler har et selvstendig ansvar for informasjonssikkerheten etter personopplysningsloven § 13 og personopplysningsforskriften § 2-15.

Her følger punkter som kan være aktuelle for krav til en databehandler og som bør fremgå av avtalen:

- Databehandler skal generelt tilfredsstillende krav som kommunen stiller til behandling av opplysninger.
- Beskriver krav til hvordan dataene skal håndteres av skjemaleverandøren. Dette gjelder blant annet forhold rundt oppbevaring, unødig lagring (jfr. personopplysningsloven § 28), sletting, lover/regler, sikkerhetskopiering etc.
- At databehandler ikke skal behandle opplysninger på annen måte enn det som er avtalt med behandlingsansvarlig.
- Hvis databehandler behandler opplysninger for flere kommuner skal databehandler ved hjelp av tekniske tiltak som ikke kan overstyres av brukerne ivareta at:
 - o det er etablert skiller mellom virksomhetene i henhold til gjennomført risikovurdering, dette både i database hvor data er lagret og i kommunikasjon
 - o ingen andre enn databehandleren, de som arbeider under databehandlerens instruksjonsmyndighet og virksomheten selv har tilgang til opplysningene
- Taushetserklæring

Figur 10: Databehandleravtale



5.5. Informasjonsplikt til borgeren

5.5.1. Informasjonsplikt når det innhentes opplysninger fra borger

Ved innhenting av opplysninger fra borger har en plikt til å informere innbyggeren om den datafangsten som skjer. Basiskravene er beskrevet i personopplysningsloven § 19 ("Informasjonsplikt når det samles inn opplysninger fra den registrerte"). § 19 beskriver at følgende må informeres om:

- a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,
- b) formålet med behandlingen,
- c) opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,
- d) det er frivillig å gi fra seg opplysningene, og
- e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og § 28.

Det må altså klart fremgå for innbyggeren at det er kommunen som er behandlingsansvarlig. I tillegg til krav i § 19 kan følgende retningslinjer også brukes:

- Borgeren bør aktivt godkjenne personvernerklæringen før datafangsten kan avsluttes
- En må gi tilstrekkelig informasjon til innbyggeren til hvordan innsamlingen av data foregår og for eksempel fraråde innbyggeren å bruke Internettkafé-PC eller lignende når det sendes inn opplysninger (fare for ”keyloggere”, at data blir liggende igjen på en ”offentlig” PC etc.)
- Hvilke opplysninger som eventuelt lagres og eventuelt hvor lenge opplysningene lagres

5.5.2.Samtykke fra borger

I tillegg til den generelle informasjonsplikten mot borgeren beskrevet ovenfor kan det være aktuelt å be om særskilt samtykke fra borgeren i visse sammenhenger. Dette kan for eksempel være dersom skjemaløsningen har funksjonalitet for å innhente visse typer informasjon fra kommunens register for preutfylling av visse felter i et skjema.

Datatilsynet har følgende anbefalinger når det gjelder krav til samtykke :

Samtykke til behandling av personopplysninger

Samtykke er et grunnprinsipp i loven. Virksomheter som ønsker å bruke personopplysninger må som hovedregel innhente samtykke før de starter behandlingen.

Krav til samtykket

Personopplysningsloven stiller krav til samtykket. Et samtykke skal være en frivillig, uttrykkelig og informert erklæring fra den opplysningene gjelder, om at hun eller han godtar behandling av opplysninger om seg selv.

Informert samtykke

Samtykket skal være informert. Den som skal registreres må få tilstrekkelig informasjon til å forstå hva samtykket gjelder og hvilke konsekvenser det kan få. Informasjonen til den registrerte skal minst omfatte:

- navn og adresse på den behandlingsansvarlige
- hva opplysningene skal brukes til
- om opplysningene vil bli utlevert til andre, og eventuelt hvem som er mottaker
- om det er frivillig å gi fra seg opplysningene

- informasjon som gjør den registrerte i stand til å bruke sine rettigheter etter personopplysningsloven på best mulig måte, som f.eks. om retten til å kreve innsyn, retting og sletting
- hvor lenge personopplysningene vil bli behandlet eller oppbevart

Frivillig samtykke

Et frivillig samtykke er et samtykke som ikke er avgitt under tvang, verken fra den behandlingsansvarlige eller fra andre.

Det er ikke alltid lett å se om samtykket er frivillig. Eksempler på dette kan være når en virksomhet stiller et samtykke som vilkår for å tilby en eller annen tjeneste eller for å ansette en person. Vil man ha jobben eller forsikringen, må man samtykke. Spørsmålet om samtykket er frivillig eller ikke må avgjøres konkret i det enkelte tilfelle: Hva spørres det etter? Hvor belastende vil et samtykke være? Er konsekvensene uforholdsmessige om man ikke samtykker?

Uttrykkelig samtykke

Samtykket skal være uttrykkelig. Når virksomheten ønsker å behandle opplysninger om en person, må personen foreta seg noe aktivt for å samtykke, som å sende inn en svarslipp eller liknende.

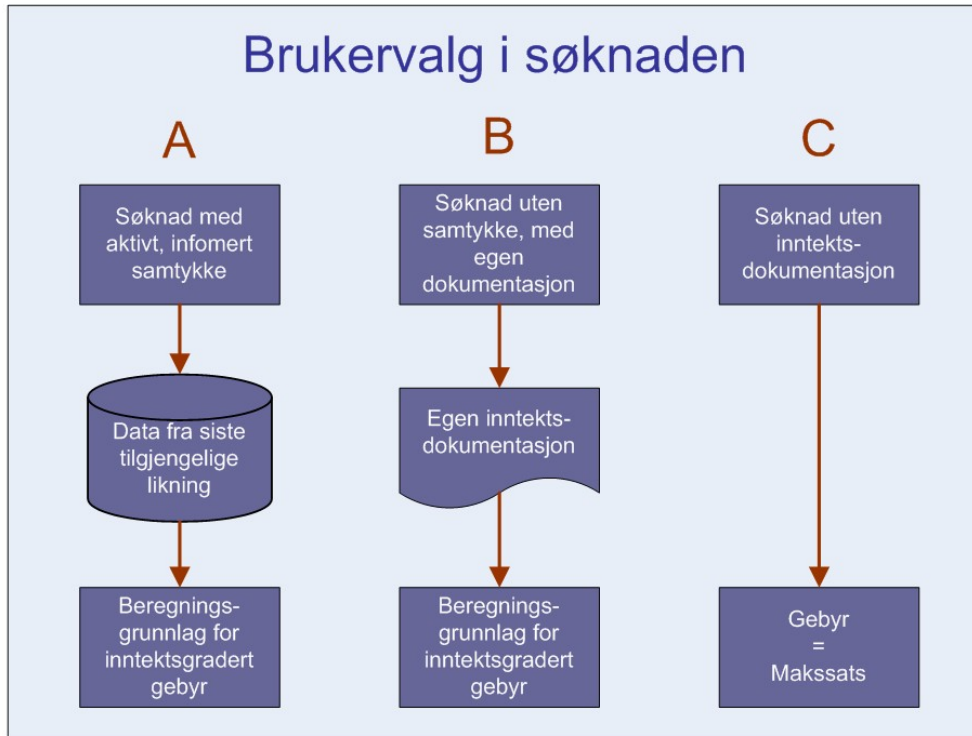
Hvordan skal samtykket gis

Den som skal registreres kan samtykke muntlig eller skriftlig, elektronisk eller på papir. Det må imidlertid gå klart og utvetydig fram:

- at den registrerte samtykker
- hvilke behandlinger samtykket omfatter
- hvilke behandlingsansvarlige samtykket rettes til

Den behandlingsansvarlige skal kunne sannsynliggjøre at samtykket er gitt. Dette er lettere dersom samtykket er gitt skriftlig.

Nedenfor vises det et eksempel på hvordan brukeren kan presenteres for tre ulike valg for samtykke og som resulterer i tre ulike måter for informasjonshåndtering.

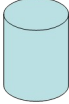









Figur 11: Eksempel på tre ulike valg for samtykke som kan presenteres brukeren (eksempel fra Asker kommune)

Referanseliste

- [1]Fornyings- og administrasjonsdepartementet (FAD): *"Strategi for eID og e-signatur i offentlig sektor"*, versjon 1.0. Vedlegg 1: Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor.
- [2]Prosjektet Tjenester på nett, dokument fra arbeidsgruppen for sikkerhet: *"Sikkerhetsrammeverk for tjenester på nett"*, 20.06.2007.
- [3]Datatilsynet: *"Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven"*, 15.02.2002. Tilgjengelig fra denne siden:
http://www.datatilsynet.no/templates/article___888.aspx
- [4]Datatilsynet: *"Veiledning i informasjonssikkerhet for kommuner og fylker"*, TV-202:2005
- [5]Datatilsynet: *"Samtykke til behandling av personopplysninger"*, hentet fra
http://www.datatilsynet.no/templates/article___876.aspx, 6.2.2008.
- [6]Prosjektet Tjenester på nett, dokument fra arbeidsgruppen "Skjemaer og integrerte tjenester på nett": *"Oppsummering av gruppens arbeider"*, versjon x.xx
- [7]Statskonsult, Rapport 2003:14: *"Signaturkrav, risiko og elektroniske byggesøknader. Rapport om behovet for elektroniske signaturer i ByggSøksystemet, skrevet på oppdrag fra Statens bygningstekniske etat."*
- [8]Ølnes, J: *"Signaturkrav og autentisering"*, innlegg på KS-Workshop om sikkerhetskrav relatert til tjenester på nett, 29.02.2008.

Vedlegg A – Figurforklaring

Fagsyste		Sakssystemer som gir beslutnings-, prosess- eller behandlingsstøtte, men som ikke har egen, godkjent arkiv- eller journalfunksjonalitet.
Sak- / arkivsystem		NOARK-godkjent arkivsystem
Skjema / skjermdialog mot brukeren		
Kryptert forbindelse		HTTP-forbindelser sikret med eksempelvis TSL eller SSL
Ukryptert forbindelse		Usikrede HTTP-forbindelser
Termineringspunkt		Endepunkt for forbindelser
DMZ		Demilitarisert sone
Intern sone		Sikret (lokal-)nettverk
Internett		Usikret (åpen) nettverk
Kryptert informasjon		Informasjon som er sikret vha. PKI
Dekryptert informasjon		Informasjon som er avsikret vha. PKI

Vedlegg B – Mal for vurdering av krav til autentisering

Tabell 4: Mal for å vurdere krav til autentisering og uavviselighet

Vurderingsskjema sikkerhet				Skjema hvor det ikke etterspørres etter sensitive opplysninger og som ikke har "potensielle" felter hvor slike opplysninger kan skrives inn						Skjema som hvor det etterspørres etter sensitive opplysninger eller "Andre forhold", "Begrunnelse" eller lignende og som er "potensielle" felter for sensitive opplysninger																																
Skjema																																										
Vedlegg tillatt? (J / N)																																										
Risiko datafangst og innsyn: Angi risikonivå 1-4 for truslene Feil hender, Falsk avsender, Falske opplysninger	Situasjon	Datafangst	Trussel	Liv og helse	Økonomisk tap	Tap ab renommé	Hindre straffeforf	Uakts. Lovbrudd	Bryderi /ulempe	Liv og helse	Økonomisk tap	Tap ab renommé	Hindre straffeforf	Uakts. Lovbrudd	Bryderi /ulempe	Liv og helse	Økonomisk tap	Tap ab renommé	Hindre straffeforf	Uakts. Lovbrudd	Bryderi /ulempe																					
			Falsk avsender																																							
			Datafangst																			Falske opplysn																				
			Innsyn																			Feil person får tilgang																				
1)	Sikkerhetsnivå datafangst (1 - 4)																																									
	Sensitive data i søknad/vedlegg? (J / N)																																									
2)	Skal behandles i sikker sone? (J / N)																																									
3)	Krav til lagring på skjemahotell																																									
4)	Krav til overføringssikkerhet																																									

5)	Krav til mottakssystem/lagring			
6)	Sikkerhetsnivå for elektronisk tilbakemelding (1-4)			
7)	Sikkerhetsnivå for elektronisk svar fra kunde (1-4)			
8)	Sikkerhetsnivå for innsyn/registeroppslag (1-4)			

Kommentarer:

- 1) Sikkerhetsnivået som vi konkluderer med etter å ha vurdert risiko
- 2) Selv om selve søknaden ikke inneholder sensitive data, skal likevel søknaden behandles i et system som er plassert i sikker sone?
- 3) Beskriv evt. spesielle krav, f.eks. hvis en søknad kan inneholde felter / vedlegg med sensitive data
- 5) Beskriv. Hvis f. eks søknad inneholder sensitive data, hvor må da kommunens mottakssystem ligge, sikker sone?
- 6) Mulig at 6, 7 og 8 ikke skal være med, da tilbakemeldinger og svar vil være egne skjemaer som skal ha en egen kolonne i dette regnearket?
- 7) Mulig at 6, 7 og 8 ikke skal være med, da tilbakemeldinger og svar vil være egne skjemaer som skal ha en egen kolonne i dette regnearket?
- 8) Mulig at 6, 7 og 8 ikke skal være med, da tilbakemeldinger og svar vil være egne skjemaer som skal ha en egen kolonne i dette regnearket?

Tabell 5: Oversikt over risikonivåer i rammeverket

	Risikonivå 1 - ingen	Risikonivå 2 - liten	Risikonivå 3 - moderat	Risikonivå 4 - stor
Konsekvenser for liv eller helse	Det kan ikke forekomme fare for tap av liv og/ eller helseskader	Det kan forekomme mindre helseskader	Det kan forekomme mindre helseskader	Det kan forekomme tap av liv og/ eller store helseskader
Økonomisk tap/ merarbeid/ økte kostnader	Intet økonomiske tap/ merarbeid/ økte kostnader	Det kan føre til et mindre økonomisk tap/ merarbeid/ økte kostnader	Brudd kan føre til moderat økonomisk tap/ merarbeid/ økte kostnader	Brudd kan medføre store økonomiske tap/ merarbeid/ økte kostnader
Tap av renommé (anseelse, tillit og integritet)	Ingen skade på renommé	Eventuelle skader på renommé anses bagatellmessige	Renommé kan bli noe svekket i et kortere tidsrom	Renommé kan bli svekket i et lengre tidsrom, eventuelt varig

	Risikonivå 1 - ingen	Risikonivå 2 - liten	Risikonivå 3 - moderat	Risikonivå 4 - stor
Hindring i straffeforfølgelse	Ingen bidrag til hindring av straffeforfølgning	Minimalt bidrag til hindring av straffeforfølgning	Moderat bidrag til hindring av straffeforfølgning	Det kan forekomme hindringer i straffeforfølgning
Uaktsomt bidrag til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	Det kan ikke forekomme uaktsom bistand til lovbrudd	Brudd kan bidra til uaktsom bistand til lovbrudd
Bryderi/ ulempe	Ingen ulempe eller bryderi	Det kan forekomme noe ulempe eller bryderi	Ikke relevant	Ikke relevant
Bryderi/ ulempe	Ingen ulempe eller bryderi	Det kan forekomme noe ulempe eller bryderi	Ikke relevant	Ikke relevant

Vedlegg C – Eksempel på risikovurdering av skjemaløsning

Med bakgrunn i en tenkt skjemaløsning som vist i Figur 7 er det her vist eksempler på trusler som kan være aktuelle. *Merk at dette bare er et eksempel og hver enkelt må vurdere sin egen løsning for aktuelle trusler, hendelser, sannsynlighet, konsekvens og tiltak.*

Forklaring til koder i skjema for risikovurdering:

Brudd på krav til: **K** = Konfidensialitet **I** = Integritet **T** = Tilgjengelighet **S** = Sporbarhet

Sannsynlighet: (Angitt som antall pr år)	1	Usannsynlig $\leq 1/1$ (En gang pr år eller sjeldnere)	2	Mindre sannsynlig 4/1 (En gang hvert kvartal)	3	Mulig 12/1 (En gang hver måned)	4	Sannsynlig $\geq 52/1$ (ukentlig eller oftere)
Konsekvens:	1	Ubetydelig	2	Moderat	3	Alvorlig	4	Kritisk

Risiko = S x Ko

Risiko > 4 krever vurdering av tiltak

Eksempel på kartlagte risikoer og trusselvurderinger

Tabell 6: Oversikt over alle kartlagte hendelser

Risikovurdering av skjemaløsning							Kontrolltiltak og lederoppfølging	
Nr	K/I / T/S	Uønsket hendelse	S	Ko	R (SxKo)	Mulige konsekvenser	Kommentar / Tiltak	
Hos skjemaleverandør								
1.		Sensitive opplysninger leses av uvedkommende under transport				Konsekvenser: <ul style="list-style-type: none"> Sensitive opplysninger havner på avveie og kan leses av uvedkommende Årsaker: <ul style="list-style-type: none"> Opplysninger sendes ukryptert Borger skriver inn sensitive opplysninger i et skjema som ikke beregnet for dette 	Kommentar: <ul style="list-style-type: none"> Forslag til tiltak: <ul style="list-style-type: none"> 	
2.		Uautorisert tilgang til sensitive opplysninger hos skjemaleverandør				Konsekvenser: <ul style="list-style-type: none"> Årsaker: <ul style="list-style-type: none"> Manglende/dårlige databehandleravtaler Langtidslagring av informasjon Dårlige skiller mellom data fra ulike kommuner 	Kommentar: <ul style="list-style-type: none"> Forslag til tiltak: <ul style="list-style-type: none"> 	
3.		Det skjer teknisk feil ved skriving av data til server i kommunen (ved http-post overføring)				Konsekvenser: <ul style="list-style-type: none"> Årsaker: <ul style="list-style-type: none"> 	Kommentar: <ul style="list-style-type: none"> Forslag til tiltak: <ul style="list-style-type: none"> 	

Risikovurdering av skjemaløsning						Kontrolltiltak og lederoppfølging	
Nr	K/I / T/S	Uønsket hendelse	S	Ko	R (SxKo)	Mulige konsekvenser	Kommentar / Tiltak
4.		E-post sendes feil fra skjemaleverandør				Konsekvenser: <ul style="list-style-type: none"> Årsaker: <ul style="list-style-type: none"> 	Kommentar/etablerte tiltak: <ul style="list-style-type: none"> Forslag til tiltak: <ul style="list-style-type: none">
5.		Feil data sendes fra skjemaleverandør				Konsekvenser: <ul style="list-style-type: none"> Årsaker: <ul style="list-style-type: none"> Dårlige skiller mellom data fra ulike kommuner 	Kommentar: <ul style="list-style-type: none"> Forslag til tiltak: <ul style="list-style-type: none">
6.		Informasjon blir borte under sending til kommunen				Konsekvenser: <ul style="list-style-type: none"> Årsaker: <ul style="list-style-type: none"> Manglende kvitteringsmekanismer for transport 	Kommentar: <ul style="list-style-type: none"> Forslag til tiltak: <ul style="list-style-type: none">
7.		Ondsinnnet kode blir sendt inn i skjemaløsningen				Konsekvenser: <ul style="list-style-type: none"> Årsaker: <ul style="list-style-type: none"> Filer som sendes som vedlegg inneholder ondsinnnet kode 	Kommentar: <ul style="list-style-type: none"> Forslag til tiltak: <ul style="list-style-type: none"> Kun tillate "sikre" filtyper som vedlegg (PDF)
Hos kommunen							
8.		Sensitive opplysninger ligger usikret på server i DMZ i kommunen				Konsekvenser: <ul style="list-style-type: none"> Årsaker: <ul style="list-style-type: none"> Data ligger ukryptert i DMZ 	Kommentar: <ul style="list-style-type: none"> Forslag til tiltak: <ul style="list-style-type: none">

Risikovurdering av skjemaløsning							Kontrolltiltak og lederoppfølging	
Nr	K/I / T/S	Uønsket hendelse	S	Ko	R (SxKo)	Mulige konsekvenser	Kommentar / Tiltak	
9.		Uautorisert tilgang til sensitive opplysninger i kommunen				Konsekvenser: <ul style="list-style-type: none"> • Årsaker: <ul style="list-style-type: none"> • 	Kommentar: <ul style="list-style-type: none"> • Forslag til tiltak: <ul style="list-style-type: none"> • 	
10.		Skjema blir "borte" ved sending til kommunen				Konsekvenser: <ul style="list-style-type: none"> • Årsaker: <ul style="list-style-type: none"> • 	Kommentar: <ul style="list-style-type: none"> • Forslag til tiltak: <ul style="list-style-type: none"> • 	
11.		Det skjer feil i webserviceoverføring						
12.		Det skjer feil ved henting av data fra server hos skjemaleverandør (ftp-overføring)				Konsekvenser: <ul style="list-style-type: none"> • Årsaker: <ul style="list-style-type: none"> • 	Kommentar: <ul style="list-style-type: none"> • Forslag til tiltak: <ul style="list-style-type: none"> • 	
13.		Uautorisert bruk av webservices, ftp eller lignende for å få tilgang til data eller andre systemer i kommunen				Konsekvenser: <ul style="list-style-type: none"> • Årsaker: <ul style="list-style-type: none"> • 	Kommentar: <ul style="list-style-type: none"> • Forslag til tiltak: <ul style="list-style-type: none"> • 	