

**Til** Prosjektet ”Kommunale tjenester på nett”  
**Fra** Faggruppe sikkerhet  
**Dato** 20. juni 2007

## Sikkerhetsrammeverk for ”tjenester på nett”

Notat beskriver et rammeverk for å vurdere sikkerhetskrav for tjenester på nett. Rammeverket beskriver først en del faktorer som påvirket krav til sikkerhet, og til slutt gis det konkrete anbefalinger til sikkerhetsnivå basert på hvilke faktorer som er til stede.

### 1. Ulike tjenester som innbyggeren utfører

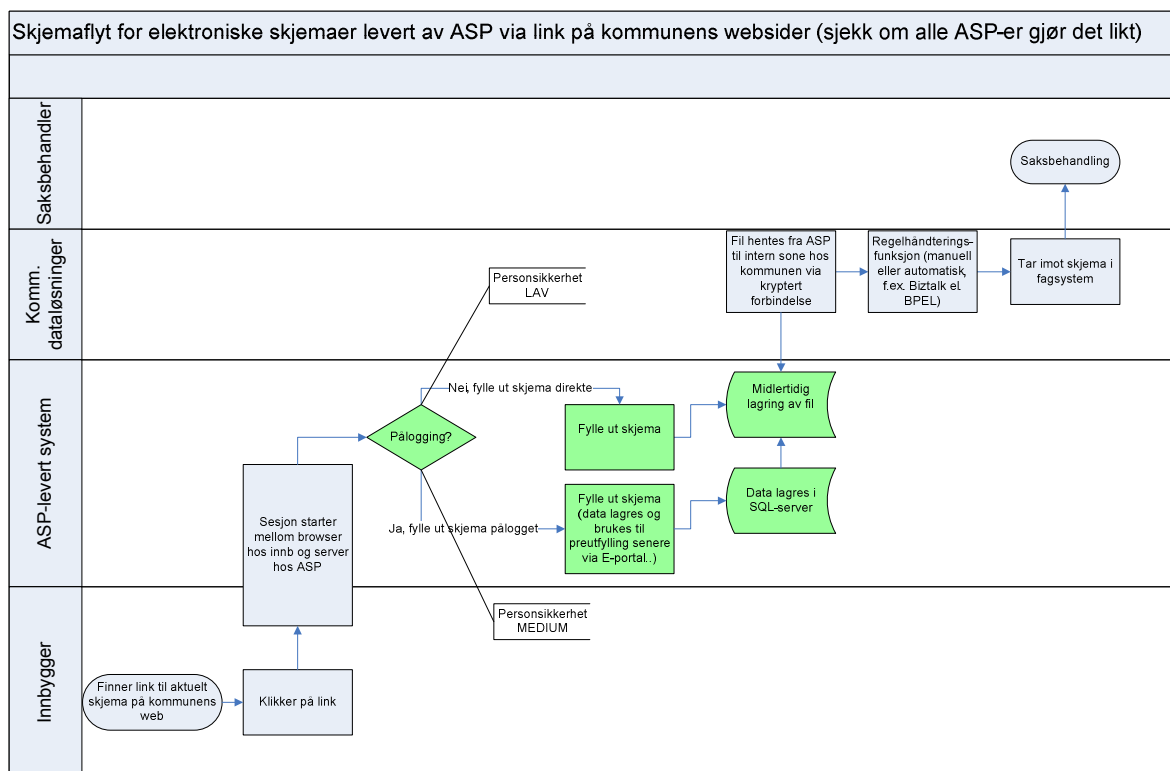
Tabell 1 viser en hovedgruppering av tjenester knyttet til ulike skjema som innbyggeren kan nytte via kommunens portal. Det er beskrevet kort både hva som innbyggeren gjør og hva kommunens IT-løsninger må gjøre med tanke på sikkerhet.

**Tabell 1: Hovedgruppering av ulike tjenester innbyggeren utfører**

	Tjeneste	Innbygger	Kommune
<i>Datafangst</i>	Innsending av skjema	Innbyggeren sender inn et skjema via kommunens portal. Identifiserer seg vha. fødselsnummer.	Kommunen mottar skjema inn i aktuelt fagsystem. Bruker personnr for å registrere innsendt skjema til riktig person.
<i>Dialog</i>	Vise status på skjema	Innbyggeren logger seg inn og får status på aktuelle skjema fra kommunen.	Kommunen viser informasjon fra sine interne systemer om status på for eksempel behandling av innsendt skjema. Krever sikker autentisering av innbyggeren eller at innbyggeren benytter seg av tilsendte referansenummer eller PIN-koder (for eksempel via mobil).
	Referansenr	Innbygger mottar referansenr på for eksempel e-post eller SMS som kan brukes for å logge inn for å få tilgang til for eksempel et tidligere påbegynt utfylt skjema.	Kommunen/skjemaleverandør sender ut et referansenr som gjør at innbyggeren for eksempel kan få tilgang til et tidligere utfylt skjema.
	Innsyn	Innbyggeren får innsyn i opplysninger som er sendt inn til kommunen	Kommunen viser opplysninger fra aktuelt skjema som er innsendt av innbyggeren. Krever sikker autentisering av innbyggeren.

Preutfylling av skjema	Innbyggeren logger seg inn og aktuelt skjema er utfyllt med informasjon fra kommunens systemer (stort sett navn og adresseopplysninger)	Kommunen viser informasjon om innbyggeren fra sine systemer etter at brukeren har logget seg inn. Krever sikker autentisering av innbyggeren.
Aksept av tjeneste/tilbud ("Bekreftelse")	Innbyggeren aksepterer en tjeneste etter tilbud fra kommunen (gir "respons" tilbake til kommunen). Innbyggeren må logge seg inn i portalen for å kunne akseptere tjenestetilbudet. Alternativt kan innbygger gi aksept via e-post eller mobil dersom er tilrettelagt for dette.	Kommunen har behandlet innsendt skjema fra innbyggeren og gir innbyggeren tilbud om aktuell tjeneste.
Signering av skjema	Innbyggeren signerer et elektronisk dokument med en elektronisk signatur.	Kommunen må verifisere at brukeren er den han utgir seg for å være og så koble identitet til aktuelt dokument. Krever sterk autentisering av brukeren og mekanismer blant annet for ikke-benekting.
Sende inn vedlegg	Innbyggeren skal kunne legge ved nødvendige vedlegg til et skjema.	Kommunen må kunne ta imot vedlegg som innbyggeren sender inn.

Figuren under viser en forenklet oversikt over hvordan et skjema blir behandlet.



Figur 1: Enkelt flytskjema for en søknad

## 2. Type informasjon

I hovedsak kan all informasjon grupperes i to ulike kategorier som vil kreve ulike grad av sikkerhetshåndtering, sensitiv og ikke-sensitiv informasjon. De to kategoriene vil kreve ulik grad av sikkerhetsmekanismer.

Tabell 2: To typer informasjon

Informasjon	Beskrivelse
Ikke-sensitiv informasjon (inkl. personopplysninger)	Informasjon som ikke inneholder noen sensitive opplysninger. Ikke-sensitiv informasjon inkluderer også personopplysninger som for eksempel personnummer.
Sensitive personopplysninger (inkl. helseopplysninger)	Informasjon som inneholder sensitive personopplysninger. Dette inkluderer også helseopplysninger. Etter personopplysningsloven § 2. <i>Definisjoner</i> er sensitive personopplysninger opplysninger om: <ul style="list-style-type: none"> <li>• rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning</li> <li>• at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling</li> <li>• helseforhold</li> </ul>

	<ul style="list-style-type: none"> <li>• seksuelle forhold</li> <li>• medlemskap i fagforeninger</li> </ul>
--	---

### 3. Sikkerhetsmekanismer

I tabell 3 under er det beskrevet aktuelle sikkerhetsmekanismer som er aktuelle i forhold til innbyggeren når tjenester legges tilgjengelig på nett. Interne forhold i kommunens IT-infrastruktur som for eksempel soneinndeling og brannmurer er ikke beskrevet her.

**Tabell 3: Aktuelle sikkerhetsmekanismer**

Sikkerhetsmekanismer	Beskrivelse
Kryptering av informasjon og dataintegritet	Gjør informasjon uleselig for alle som ikke er ment å motta informasjonen. Mottaker dekrypterer informasjonen med en nøkkel slik at informasjonen blir leselig. Ivaretar også dataintegritet dersom meldingskryptering benyttes (ok ikke tunellkryptering). Kryptering kan også sikre at informasjon ikke kan endres for eksempel ved oversendelse fra innbygger til kommunen.
Tilsendte referansnr/engangskoder	Gjør at innbyggeren kan få tilgang til statusinformasjon om innsendt skjema (som for eksempel viser behandlingsstatus) ved hjelp av engangskoder tilsendt via mobil, e-post og lignende.
Autentisering lav-nivå	Autentisering av innbygger på en slik måte at er det rimelig grad av trygghet for at brukeren er den som han oppgir å være. Aktuelle mekanismer for dette er først og fremst MinSides PIN-kode autentisering (MinID).
Autentisering høy-nivå (to-faktor)	Autentisering av innbygger på en slik måte at er det stor grad av trygghet for at brukeren er den som han oppgir å være. Aktuelle løsninger for dette er blant annet PKI-løsninger som bank-ID, Norsk Tipping smartkort og Telenor-løsning for PKI på mobilen. Ny offentlig sikkerhetsløsning forventes å ligge på dette sikkerhetsnivået.
Bekreftelse (lav-nivå signering)	Ved hjelp av mekanismene for "autentisering lav-nivå" kan dette brukes til at innbyggeren gir aksept for tilbudt tjeneste fra kommunen. Innbyggeren kan for eksempel bekrefte at han takker ja til tilbudt barnehageplass fra kommunen.
Signering (med PKI)	Elektronisk signering av et dokument slik at det i ettertid ikke kan betviles hvem som signerte og innholdet i det signerte dokumentet.
Uavviselighet	Det skal foreligge rutiner og logger, som gjør at det er rimelig sikkert at kommunikasjonsparten står bak en handling eller et informasjonselement. Kan realiseres for eksempel ved å bruke informasjon fra innlogging eller bruk av signering vha. PKI.

**Merknad:** Autentiseringsløsninger vil senere "harmoniseres" med det som blir endelig anbefalinger fra arbeidsgruppen i FAD for nivå og krav til autentisering.

## 4. Anbefalinger til sikkerhetsnivå ulike tjenester

Her beskrives det tre ulike sikkerhetsnivåer som kan brukes for aktuelle tjenester som den enkelte kommune ønsker å gjøre tilgjengelig via sin "kommuneportal". Felles for alle sikkerhetsnivåene er at vi forutsetter at det skjer via et nettsted (som er kommuneportalen) hvor transportsikkerheten er tilstrekkelig ivaretatt med for eksempel bruk av SSL og tilhørende sertifikater. I tillegg må kommunen ha tilrettelagt sine interne fagsystemer og infrastruktur for å kunne kommunisere elektronisk med innbyggeren på en sikker måte. Tjenester som gjøres tilgjengelige via Internett bør også oppfylle det som er beskrevet i "Forskrift om elektronisk kommunikasjon med og i forvaltningen" [2].

Tabellene for de anbefalte sikkerhetsnivåene leses slik:

- "Tjenester" viser hva innbyggeren kan gjøre innenfor denne sikkerhetsprofilen
- "Informasjon" viser hvilken type informasjon som kan behandles innenfor denne sikkerhetsprofilen
- "Sikkerhetsmekanismer" viser hvilke sikkerhetsmekanismer som kreves innenfor denne sikkerhetsprofilen

### 4.1. Lavt sikkerhetsnivå (identifisering vha. fødselsnummer)

Lavt sikkerhetsnivå tar utgangspunkt i at brukeren ikke logger seg inn, men identifiserer seg ved hjelp av personnummer.

Denne sikkerhetsprofilen egner seg først og fremst til innsending av skjema fra innbyggeren. Kun ikke-sensitiv informasjon kan behandles i denne sikkerhetsprofilen.

Tabell 4: Profil for lavt sikkerhetsnivå - DATAFANGST

	Innhold i sikkerhetsprofil						
Tjenester	Datafangst	Vise status på skjema	Referansen	Innsyn	Gi bekreftelse	Preutfylling av skjema	Signering av skjema
	X		X				
Informasjon	Ikke sensitiv informasjon	Sensitive personopplysninger					
	X	X					
Sikkerhetsmekanismer	Kryptering	Autentisering lav-nivå	Autentisering høy-nivå	Bekreftelse (lav-nivå signering)	Signatur (PKI)	Uavviselighet	
	X						

## 4.2. Medium sikkerhetsnivå ("Person-standard")

Medium sikkerhetsnivå tar utgangspunkt i at innbyggeren logger seg inn vha. autentiseringen i MinSide (MinID). Denne sikkerhetsprofilen kan sammenlignes med det som er definert som "Person-standard" i kravspesifikasjon for PKI i offentlig sektor [1].

I tillegg til innsending av skjema egner denne sikkerhetsprofilen seg også til å vise status på skjema, kunne gi aksept for tilbud om tjeneste og preutfylle informasjon i skjemaer. Kun ikke-sensitiv informasjon kan behandles i denne sikkerhetsprofilen.

**Spørsmål til videre diskusjon:** hvilke krav skal settes til innsending av informasjon som kan inneholde sensitiv informasjon? Er det nok å oppgi fødselsnummer for identifikasjon, skal man kreve innlogging ved bruk av MinID eller skal man kreve bruk av PKI?

**Tabell 5: Profil for medium sikkerhetsnivå - DATAFANGST**

	Innhold i sikkerhetsprofil						
<b>Tjenester</b>	Datafangst	Vise status på skjema	Referansen	Innsyn	Gi bekreftelse	Preutfylling av skjema	Signering av skjema
	X		X				
<b>Informasjon</b>	Ikke sensitiv informasjon	Sensitive personopplysninger					
	X	X					
<b>Sikkerhetsmekanismer</b>	Kryptering	Autentisering lav-nivå	Autentisering høyt-nivå	Bekreftelse (lav-nivå signering)	Signatur (PKI)	Uavviselighet	
	X	X		X		X	

**Tabell 6: Profil for medium sikkerhetsnivå - Dialog**

	Innhold i sikkerhetsprofil					
<b>Tjenester</b>	Datafangst	Vise status på skjema	Innsyn	Gi bekreftelse	Preutfylling av skjema	Signering av skjema
	X	X	X	X	X	
<b>Informasjon</b>	Ikke sensitiv informasjon	Sensitive personopplysninger				
	X					
<b>Sikkerhetsmekanismer</b>	Kryptering	Autentisering lav-nivå	Autentisering høyt-nivå	Bekreftelse (lav-nivå signering)	Signatur (PKI)	Uavviselighet

	X	X		X		X
--	---	---	--	---	--	---

Innhold i sikkerhetsprofil							
Tjenester	Datafangst	Vise status på skjema	Referansen	Innsyn	Gi bekræftelse	Preutfylling av skjema	Signering av skjema
	X	X	X	X	X	X	
Informasjon	Ikke sensitiv informasjon	Sensitive personopplysninger					
	X						
Sikkerhetsmekanismer	Kryptering	Autentisering lav-nivå	Autentisering høy-nivå	Bekreftelse (lav-nivå signering)	Signatur (PKI)	Uavviselighet	
	X	X		X		X	

### 4.3. Høyt sikkerhetsnivå ("person-høyt")

Høyt sikkerhetsnivå tar utgangspunkt i at innbyggeren logger seg inn vha. PKI-løsninger som for eksempel Bank-ID, Norsk Tipping smartkort eller andre tilsvarende løsninger<sup>1</sup>. Denne sikkerhetsprofilen kan sammenlignes med det som er definert som "Person-høyt" i kravspesifikasjon for PKI i offentlig sektor [1].

Denne sikkerhetsprofilen egner seg til alle typer tjenester, også elektronisk signering av skjema i tilfeller hvor det kreves en "juridisk bindende" signatur fra innbyggeren. Også sensitive personopplysninger kan behandles innenfor denne sikkerhetsprofilen.

**Tabell 7: Profil for høyt sikkerhetsnivå – DATAFANGST OG DIALOG**

Innhold i sikkerhetsprofil							
Tjenester	Datafangst	Vise status på skjema	Referansen	Innsyn	Gi bekræftelse	Preutfylling av skjema	Signering av skjema
	X	X	X	X	X	X	X

<sup>1</sup> Blant annet har Telenor en løsning for Bank-ID på mobilen, og dette er en type løsning som godt egner seg for publikumstjenester: <http://www.idg.no/cio/article17935.ece>.

<b>Informasjon</b>	Ikke sensitiv informasjon	Sensitive personopplysninger					
	X						
<b>Sikkerhetsmekanismer</b>	Kryptering	Autentisering lav-nivå	Autentisering høy-nivå	Bekreftelse (lav-nivå signering)	Signatur (PKI)	Uavviselighet	
	X		X		X	X	

Kommentar: Vedlegg er ikke med i tabellene. Det må avgjøres hvorvidt dette vil påvirke krav til sikkerhet.

#### 4.4. Generelle anbefalinger for autentisering fra rammeverket

Dette rammeverket gir altså følgende anbefalinger for autentisering av innbyggeren:

- *kun innsending av skjema*: alle skjema kan sendes uten at det krever pålogging fra innbyggeren
- *Innsyn med MinID autentisering*: kun skjema som ikke kan inneholde sensitive opplysninger
- *Innsyn med nivå PKI autentisering*: skjema som også kan inneholde sensitive opplysninger

Det er viktig å legge merke til at dette kun er generelle anbefalinger og at det er opptil den enkelte kommune å avgjøre sikkerhetsnivå for de skjemaene og tjenestene som innbyggeren kan benytte seg av.

## Referanser

- [1] Moderniseringsdepartementet: *"Kravspesifikasjon for PKI i offentlig sektor"*, versjon 1.02, januar 2005. Tilgjengelig fra denne siden: <http://odin.dep.no/fad/norsk/tema/ITpolitikk/p30007088/050001-990049/>
- [2] FOR 2004-06-25 nr 988 (eForvaltningsforskriften): *"Forskrift om elektronisk kommunikasjon med og i forvaltningen"*, dato: FOR-2004-06-25-988. Tilgjengelig fra denne siden: <http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20040625-0988.html>
- [3] Høringsutkast FAD om eID og eStrategi: *"Høringsversjon Strategi for eID og e-signatur i offentlig sektor, Versjon 1.0"*