

KITH

INFORMASJONSTEKNOLOGI
FOR HELSE OG VELFERD



Fagruppe sikkerhet

Av Magnus Alsaker



Arbeid med sikkerhet

- Mandat og arbeidsoppgaver til faggruppen
 - MinID og kobling til MinSide
 - Vurdere sikkerhetskrav for ulike skjema
 - Sikkerhetsstrategi for "tjenester på nett"

Strategi for eID og e-signatur

- Høringsutkast fra FAD om "Strategi for eID og e-signatur i offentlig sektor"
- Dekker flere områder
 - Status
 - Forsyning av innbyggere med eID
 - Forsyning av virksomheter med eID
 - Samtrafikknv. for bruk av eID og e-signatur
 - Forretningsmodell

Rammeverk for autentisering og uaviselighet ("ikke-benekting")

- Målesetninger er blant annet:
 - Å legge til rette for felles løsninger og gjenbruk av løsninger, for autentisering og uaviselighet på tvers av offentlig sektor.
 - Å gjøre det lettere for offentlige virksomheter å vurdere hvilket sikkerhetsnivå som egner seg for forskjellig type kommunikasjon
- Rammeverket dekker:
 - Autentisering (å verifisere en påstått identitet)
 - Uaviselighet (å bekrefte at en handling eller et informasjonselement er uendret (informasjonsintegritet) og at det kan knyttes til en

4 risikonivåer

	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
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

4 sikkerhetsnivå

N i v å	Krav til Autentiserings faktor(er)	Utlevering til bruker		Sikring av autentiserings faktorer ved lagring	Krav til offentlig godkjenning	Krav til uavviselighet
		<i>Fysiske personer</i>	<i>Juridiske personer</i>			
1	Ingen krav	Ingen krav	Ingen krav	Ingen krav	Ingen krav	Ingen krav
2	Enfaktor	Post til folkeregistrert adresse	Post til enhetsregisterets registrerte adresse. Navnet til den fysiske personen som kan tegne for den juridiske personen, skal stå først på forsendelsen. Alternativt kan det sendes til den som tegners folkeregistrerte adresse.	Både statiske og dynamiske kan være kopierbare	Ingen krav	Det skal foreligge rutiner og logger, som gjør at det er rimelig sikkert at kommunikasjonsparten står bak en handling eller et informasjonselement.
3	Tofaktor, hvorav en er dynamisk	Samme krav som i 2, med tilleggskrav om en eller annen form for sikring av at rette vedkommende tar dette i bruk.	Samme krav som i 2, med tilleggskrav om en eller annen form for sikring av at rette vedkommende tar dette i bruk.	Dynamiske kan være kopierbare Statiske kan ikke være kopierbare	Ingen krav	Det skal foreligge rutiner og logger, som gjør at det er rimelig sikkert at kommunikasjonsparten står bak en handling eller et informasjonselement.
4	Tofaktor, hvorav en er dynamisk	Kravene til registrering og utleveringsprosedyrer er tilsvarende Kravspesifikasjon for PKI ¹⁸ , Person Hoyt. Personlig oppmøte med legitimering, minst en gang.	For juridiske personer skal den fysiske personen som tegner den juridiske, enten møte opp personlig, eller gi fullmakt til en annen som kan møte personlig på personens vegne. Det skal fremlegges legitimasjon for begge, samt sjekkes mot enhetsregisteret. Krav tilsvarende Kravspesifikasjon for PKI, nivå Virksomhet.	Ikke-kopierbare	Løsningen skal være deklartert i henhold til offentlige krav.	En kommunikasjonspart skal kunne verifisere at den andre part står bak en handling eller et informasjonselement, den skal ikke selv kunne produsere eller endre på et slikt bevis i etterkant.

Kobling mellom risiko og sikkerhet

- Anbefalinger til sikkerhetsnivå
 - ▣ Risikonivå 1 → sikkerhetsnivå 1
 - ▣ Risikonivå 2 → sikkerhetsnivå 2
 - ▣ Risikonivå 3 → sikkerhetsnivå 3
 - ▣ Risikonivå 4 → sikkerhetsnivå 4
- Risikonivå avgjøres av utførte risikovurderinger

Sikkerhetsrammeverk utarbeidet av faggruppen

- Utarbeidet før forslag fra FAD forelå, men er ganske sammenfallende
- Tre sikkerhetsnivå
 - 1. Lavt sikkerhetsnivå (identifisering vha. fødselsnummer) – tilsvarer nivå 1 fra FAD
 - 2. Medium sikkerhetsnivå (MinID) – tilsvarer nivå 3 fra FAD
 - 3. Høyt sikkerhetsnivå (PKI) – tilsvarer nivå 4 fra FAD
- Rammeverket fra faggruppen beskriver for hvert sikkerhetsnivå:
 - Hvilke tjenester innbyggeren kan utføre/tilbys

Lavt sikkerhetsnivå

- Identifisering vha. fødselsnummer

	Innhold i sikkerhetsprofil				
Tjenester	Innsending av skjema	Vise status på skjema	Gi bekreftelse	Preutfylling av skjema	Signering av skjema
	X	X ¹			
Informasjon	Ikke sensitiv informasjon	Sensitive personopplysninger			
	X				
Sikkerhetsmekanismer	Kryptering	Autentisering lav-nivå	Autentisering høy-nivå	Bekreftelse (lav-nivå signering)	Signatur (PKI)
	X				

¹ Krever at kommunen har sikkerhetsmekanisme for tilsending av referansenummer, engangskoder eller tilsvarende som kan brukes av innbyggeren for å få tilgang til statusinformasjon.

Medium sikkerhetsnivå

- Bruk av MinID

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

Høyt sikkerhetsnivå

- Bruk av PKI

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

Vurdering av ulike skjema

- Faggruppen skal vurdere og komme med anbefalinger til sikkerhetsnivå for ulike skjema
- Dette gjøres med basis i egenutviklet rammeverk samt rammeverket fra FAD om autentisering og uavviselighet
 - Hvilke skjema kan brukes med MinID og hvilke tjenester kan innbyggeren utføre (innsending, visning etc.)
 - Hvilke skjema og tjenester krever PKI