DET KONGELIGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

Retningslinjer

Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor

Retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett

April 2008

DET KONGELIGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

Retningslinjer

Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor

Retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett
April 2008

Forord

Dette rammeverket for autentisering og uavviselighet er et hjelpemiddel for offentlige virksomheter som skal sikre samhandling på åpne eller lukkede nett. Rammeverket skal bidra til å gjøre det enklere å gjenbruke autentiseringsløsninger på tvers av offentlige virksomheter og gjøre det enklere å knytte sammen tjenester, slik at de fremstår som en enhet for brukeren. Målet er forenkling for brukeren ved at hun trenger å forholde seg til færre autentiseringsløsninger (eID). Gjenbruk av løsninger vil også bidra til reduserte kostnader i offentlige virksomheter.

Dette rammeverket for autentisering og uavviselighet er et teknologinøytralt sett med overordnete anbefalinger rettet mot hele offentlig sektor. Anbefalingene gjelder gjennomføring av risikoanalyse og valg av sikkerhetsnivå ved behov for autentisering av brukere av elektroniske tjenester fra forvaltningen samt brukere i offentlig sektor som kommuniserer internt. Videre inneholder rammeverket overordnede anbefalinger for valg av sikkerhetsnivå ved behov for å knytte en bruker til en elektronisk transaksjon (uavviselighet, "signering").

I 2005 publiserte FAD 1. versjon av Kravspesifikasjon for PKI i offentlig sektor. Dette er en kravspesifikasjon for autentiseringsløsninger (eID) basert på PKI-teknologi. Kravspesifikasjonen dekker i tillegg til autentisering og uavviselighet også til en viss grad konfidensialitet. Kravspesifikasjonen inneholder krav til tre sertifikatklasser eller typer eID, som har definerte sikkerhetsnivå. Det er i Kravspesifikasjonen definert to typer eID for personer – Person Standard og Person Høyt, og én type eID for organisasjoner – Virksomhet.

Kravspesifikasjonen er en forvaltningsstandard som ligger til grunn for anskaffelse i markedet av PKI-tjenester til bruk i offentlig sektor. Standarden er fastsatt med hjemmel i Forskrift om elektronisk kommunikasjon med og i forvaltningen, §27, samt vedtak 2005-10-07 nr 1117 om etablering av koordineringsorgan for forvaltningens bruk av sikkerhetstjenester og -produkter ved elektronisk kommunikasjon med og i forvaltningen. Bruk av standarden er pålagt gjennom instruks i brev av 20. september 2006 fra FAD til alle statlige virksomheter. Bruk av standarden er også anbefalt til kommunesektoren.

I forhold til foreliggende rammeverk vil løsninger som tilfredsstiller krav til Person Standard i Kravspesifikasjon for PKI i offentlig sektor også kunne tilfredsstille krav til sikkerhetsnivå 3. Andre typer teknologiske løsninger enn PKI vil også kunne tilfredsstille krav til sikkerhetsnivå 3 i dette rammeverket.

Løsninger som tilfredsstiller nivå Person Høyt og Virksomhet i Kravspesifikasjon for PKI i offentlig sektor, vil kunne tilfredsstille krav til sikkerhetsnivå 4 i rammeverket. Det er foreløpig ikke avklart hvilke andre løsninger for eID enn de som er basert på PKI som kan tilfredsstille krav til sikkerhetsnivå 4. Det må først utvikles felles kravspesifikasjoner og etableres selvdeklareringsløsninger for slike løsninger. Dette er et arbeid som FAD vil prioritere i forbindelse med det generelle standardiseringsarbeidet innen elektronisk forvaltning.

1. Innledning

1.1 Bakgrunn

Offentlig sektor har en strategi for å tilrettelegge for gode elektroniske tjenester til brukere (innbyggere og næringsliv), og tilrettelegge for god elektronisk samhandling mellom offentlige virksomheter.

Forskrift om elektronisk kommunikasjon med og i forvaltningen[1] krever at en offentlig virksomhet som velger å kommunisere elektronisk, skal tilrettelegge sin kommunikasjon på en måte som ivaretar nødvendig bekreftelse av partenes identitet eller fullmakter (autentisering), at data ikke utilsiktet eller urettmessig endres (integritet), beskyttelse av informasjon mot innsyn fra uvedkommende (konfidensialitet), og at det er mulig å dokumentere henvendelser og aktiviteter og hvem som har sendt eller utført dem (ikke-benekting). Dette skal gjøres i henhold til den offentlige virksomhetens egen sikkerhetsstrategi. Virksomheten skal likevel ikke kreve vesentlig høyere sikkerhet enn det som er nødvendig for den type informasjon som kommuniseres eller den type handling som tilbys utført elektronisk.

Økt elektronisk samhandling fører med seg et behov for å koordinere bruk av metoder for autentisering og uavviselighet på tvers av offentlig sektor. Felles sikkerhetsnivåer for dette i offentlig sektor vil gi mulighet for gjenbruk av sikkerhetsløsninger eller bruk av felles sikkerhetsløsninger, i kommunikasjon med brukere av offentlige elektroniske tjenester. Gjenbruk av løsninger gir økt brukervennlighet for brukerne og fører til besparelser i de offentlige virksomhetene. Felles sikkerhetsnivåer vil også gi økt trygghet for at samhandlende offentlige virksomheter sikrer utvekslet informasjon på en tilstrekkelig måte.

Dette dokumentet er ikke et komplett sikkerhetsrammeverk, men et rammeverk for sikkerhetstjenestene autentisering og uavviselighet. Autentisering er å verifisere påstått identitet. Uavviselighet er å bekrefte at en handling eller et informasjonselement er uendret (informasjonsintegritet) og at det kan knyttes til en bestemt identitet. Uavviselighet er i mange sammenhenger også omtalt som ikke-benekting. Rammeverket gjelder for autentisering og uavviselighet ved behandling av informasjon som er åpen, konfidensiell, taushetsbelagt eller personsensitiv. Det er derimot ikke gjort vurderinger opp i mot informasjon som har krav til konfidensialitet som følger av sikkerhetsloven og beskyttelsesinstruksen.

Det er viktig å være klar over at autentiserings-/ uavviselighetsmekanismen kun er en del av det som utgjør sikkerhetsnivået til en offentlig elektronisk tjeneste. I vurderingen av en tjenestes totale sikkerhet må også mange andre elementer vurderes.

Autorisasjon vil si at en identitet har fått godkjent tilgang til ressurser eller til å utføre en viss type handlinger i et system. Autorisasjon bygger på autentisering, fordi en identitet må verifiseres før tilgang kan gis. Sikkerhetstjenesten autorisasjon er ikke omfattet av dette rammeverket.

Konfidensialitet er egenskapen at informasjon kun kan leses av autoriserte mottakere. Denne egenskapen kan blant annet realiseres ved å kryptere (kode) informasjon på en måte som gjør at kun autoriserte kan dekryptere og lese den. Konfidensialitet bygger på autentisering, fordi

[1] eForvaltningsforskriften, Fornyings- og administrasjonsdepartementet, 2004-06-25, nr 0988.

en identitet må verifiseres før tilgang til konfidensialitetsbeskyttet informasjon kan gis. Dette rammeverket omfatter ikke konfidensialitet. Noen tekniske løsninger som benyttes for autentisering kan også benyttes for kryptering, dette gjelder for eksempel løsninger iht. Kravspesifikasjon for PKI i offentlig sektor.

Dette rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor er utformet for å være teknologinøytralt. Antall risiko- og sikkerhetsnivåer og posisjonering av disse er gjort etter faglig vurdering av arbeidsgruppen som utformet dette rammeverket. Rammeverket anbefaler felles nivåer for risiko og vurderer hvilke sikkerhetsnivåer som egner seg for de forskjellige risikonivåene.

1.2 Målsetning

Hovedmålsetningen med dette rammeverket, er å legge til rette for felles løsninger og gjenbruk av løsninger, for autentisering og uavviselighet på tvers av offentlig sektor. Offentlige virksomheter gjennomfører risiko- og sårbarhetsanalyser ved etablering av nye elektroniske tjenester eller samhandling og ved revidering av eksisterende. I den sammenheng skal virksomhetene kunne vurdere risikonivået i en elektronisk tjeneste opp mot felles definerte risikonivåer i dette rammeverket. Virksomheten kan så finne anbefalte sikkerhetsnivå og implementere en autentiserings-/ uavviselighetsløsning iht. anbefalt nivå.

Det er viktig å merke seg at rammeverket er veiledende. Hver offentlig virksomhet er selv ansvarlig for de vurderinger og valg som gjøres i forhold til å sikre egne elektroniske tjenester/ elektronisk kommunikasjon, og eventuelle følger av disse valgene.

I tillegg skal dette rammeverket bidra til:

- å legge til rette for felles løsninger og gjenbruk av løsninger for autentisering og uavviselighet
- å gjøre det lettere for offentlige virksomheter å vurdere hvilket sikkerhetsnivå som egner seg for forskjellig type kommunikasjon
- å gjøre det enklere for offentlige virksomheter å velge løsninger for autentisering og uavviselighet
- å muliggjøre gjenbruk av løsninger for autentisering og/ eller uavviselighet på tvers av offentlig sektor, for effektivisering internt og for økt brukervennlighet mot brukere av offentlige tjenester
- å understøtte Kravspesifikasjon for PKI i offentlig sektor, samt ordningen forvaltet av Post- og teletilsynet der leverandører kan selvdeklarere egne produkter og tjenester som tilfredsstiller kravspesifikasjonen.

1.3 Målgruppe for rammeverket

Rammeverket er skrevet for de som skal arbeide med vurdering av risiko, valg av sikkerhetsnivå og valg av tekniske løsninger for sikring av autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Dette gjelder offentlige tjenestemenn som arbeider med å vurdere, anbefale, beslutte og implementere slike løsninger.

1.4 Rammeverkets oppbygning

Dokumentet er bygget opp ved at kapittel 2 gir en innføring i begrepene autentisering og uavviselighet. Kapittel 3 forklarer hva dette rammeverket legger i begrepet risikonivå, og definerer fire felles risikonivåer for offentlig sektor. Kapittel 4 forklarer hva dette rammeverket legger i begrepet sikkerhetsnivå, og definerer fire sikkerhetsnivåer, og gir

eksempler på tekniske løsninger som tilfredsstiller de forskjellige nivåene. Kapittel 5 anbefaler hvilke sikkerhetsnivå som egner seg for de forskjellige risikonivåene.

2. Utdypende om autentisering og uavviselighet

2.1 Autentisering

Autentisering er å verifisere en påstått identitet, og dette kan to kommunikasjonsparter velge å gjøre ensidig eller tosidig. Partene som skal autentisere hverandre over nettet kan være av to forskjellige typer:

- En fysisk person (et anskuelig menneske underlagt fysiske lover) på en "klient", for eksempel en PC, mobiltelefon eller annen type kommunikasjonsterminal.
- En juridisk person (et selvstendig rettssubjekt som for eksempel stater, kommuner, aksjeselskap, stiftelse eller forening) på en "tjener", for eksempel en webserver eller et system for meldingshåndtering.

Begge parter må ha maskinvare og programvare med støtte for felles autentiseringsprotokoller og nødvendige brukerdialog. Partenes utstyr må være sikret mot uautorisert tilgang og bruk.

De som skal autentisere seg må også inneha noe som kan bekrefte deres identitet. Dette kalles autentiseringsfaktorer. En bruker kan ha en eller flere av disse avhengig av sikkerheten i løsningen. Det finnes tre forskjellige typer autentiseringsfaktorer:

- Noe personen **vet** - for eksempel et passord
- Noe personen **har -** for eksempel en passordkalkulator
- Noe personen **er** - for eksempel et fingeravtrykk

Autentiseringsfaktoren(e) må på et tidspunkt bli knyttet til en identitet. Denne administrasjonen av brukere kan gjøres av en tredjepart eller av en tjenesteyter selv. Brukeradministrasjonen går ut på å identifisere brukere ved tildeling av brukernavn, se til at riktig bruker får/ har riktig autentiseringsfaktorer og at statusinformasjon om brukere oppdateres og tilgjengeliggjøres.

De delene som ikke regnes som en del av autentiseringsløsningen er blant annet:

- Skallsikringen rundt klient eller tjener.
- Sikringen av autorisasjon og tilgangskontroll til informasjon og ressurser.

2.2 Uavviselighet

Uavviselighet er å bekrefte at en handling eller et informasjonselement er uendret (informasjonsintegritet) og at det kan knyttes til en bestemt identitet. Uavviselighet er i mange sammenhenger også omtalt som ikke-benekting. En løsning for uavviselighet er en løsning som gjør det mulig for en part å innhente tilstrekkelig dokumentasjon for at en annen part ikke kan nekte for å ha gjennomført en handling eller ha valgt å bekrefte / vedstå seg et informasjonselement.
En løsning for uavviselighet er bygget opp på samme måte som løsninger for autentisering som beskrevet over. Forskjellen i denne sammenheng, er at brukeren skal være i stand til ikke bare å bekrefte hvem man er over nettet, men også å legge igjen dokumentasjon som entydig knytter personen til en handling eller et uendret informasjonselement.

"Elektronisk signatur" er et vidt begrep som benyttes for elektroniske løsninger som knytter en person (fysisk eller juridisk) til et dokument eller en handling. I Lov om elektronisk signatur er en elektronisk signatur definert som "data i elektronisk form som er knyttet til

andre elektroniske data og som brukes som autentiseringsmetode". For å lage en elektronisk signatur kan det for eksempel benyttes teknologiske løsninger basert på passord og brukernavn, passordkalkulatorer, biometri eller PKI. Benyttes løsninger som i seg selv ikke sikrer integritet og uavviselighet, men bare autentisering, kreves det sporing av knytningen mellom autentiseringsdata og handling/ dokument. I tillegg må disse sporene sikres forsvarlig mot endring.
Begrepet "digital signatur" er vanligvis kun benyttet når man snakker om en elektronisk signatur basert på PKI.

En "avansert elektronisk signatur" er en elektronisk signatur som:

a) er entydig knyttet til undertegneren,
b) kan identifisere undertegneren,
c) er laget ved hjelp av midler som bare undertegneren har kontroll over, og
d) er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering.[2]

Den vanligste måten å implementere "avanserte elektroniske signaturer" på er ved å benytte PKI, en teknologi som baserer seg på bruk av sertifikater. Et sertifikat er en form for elektronisk identitetsbevis som kan benyttes til å verifisere elektroniske signaturer. Sertifikatet knytter innehavers navn eller pseudonym til informasjon om egenskaper ved innehavers elektroniske signatur som gjør det mulig å verifisere den. Sertifikatet skal være signert av utsteder, som bør være en tredjepart som alle stoler på, slik at sertifikatet kan benyttes til å verifisere en elektronisk signatur, selv om man ikke kjenner den andre part på forhånd. I Lov om elektronisk signatur er sertifikat definert som "en kopling mellom signaturverifikasjonsdata og undertegner som bekrefter undertegners identitet og er signert av sertifikatutsteder".

Et "kvalifisert sertifikat" er et sertifikat som er utstedt iht. bestemmelser i Lov om elektronisk signatur. Bestemmelsene omhandler bl.a. innholdet i slikt sertifikat og krav til utstedere av det.

Lov om elektronisk signatur implementerer et EU-direktiv om elektroniske signaturer gitt i 1999. Forarbeidene og intensjonen for utarbeidelsen av EU-direktivet, og påfølgende norsk lovarbeid gjør det klart at direktivets bestemmelser gjelder kun for fysiske personer og ikke for juridiske personer. Sertifikater utstedt til juridiske personer som for eksempel en bedrift, kan derfor ikke ha status som kvalifisert sertifikat (Jfr. Ot. prp. 82 (1999-2000), særlig s. 49). Dette gjelder for sertifikater på nivå Virksomhet iht. Kravspesifikasjon for PKI i offentlig sektor, selv om det sikkerhetsmessig er satt tilsvarende krav som for kvalifiserte sertifikater på dette nivået.

Lov om elektronisk signatur setter i kapittel 2 krav til "sikre signaturfremstillingssystemer", og godkjenning av slike. Det er i regi av EU utviklet internasjonale standarder som kan benyttes for å verifisere at løsninger i markedet tilfredsstiller disse kravene. Det finnes ingen leverandører i det norske markedet som tilbyr godkjente signaturfremstillingssystemer. Slike løsninger kan dog anskaffes i enkelte EU-land.

En "kvalifisert elektronisk signatur" er en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt ved bruk av et godkjent sikkert signaturfremstillingssystem.

---

[2] Definisjon hentet fra Lov om elektronisk signatur, 2001-06-15 nr 81.

Sertifikatklassen Person Høyt iht. Kravspesifikasjon for PKI i offentlig sektor har tilsvarende sikkerhet som krav til kvalifisert signatur, men kan ikke formelt godkjennes som det. Dersom leverandøren av Person Høyt- baserte sertifikater også kan levere et teknisk system godkjent iht. regelverket som "sikkert signaturfremstillingssystem" vil en slik løsning kunne brukes til å generere kvalifiserte signaturer. Kvalifiserte elektroniske signaturer vil alltid oppfylle formkrav til underskrift gitt i et regelverk som åpner for elektronisk kommunikasjon på et bestemt område, som for eksempel i tinglysing.

I Norge er det med hjemmel i Lov om elektronisk signatur etablert en selvdeklarasjonsordning for løsninger som tilfredsstiller Kravspesifikasjon for PKI i offentlig sektor, på nivå Person Standard, Person Høyt og Virksomhet. Denne selvdeklarasjonsordningen forvaltes av Post- og teletilsynet. Det er imidlertid ikke utpekt noen aktør som kan ivareta rollen som godkjenningsinstans for sikre signaturfremstillingssystemer. Ansvaret for vurdering av samsvar med regelverkets krav ligger derfor i Nærings- og handelsdepartementet, som forvalter av loven.

3. Risikonivåer

Offentlige virksomheter gjennomfører risiko- og sårbarhetsanalyser ved etablering av nye elektroniske tjenester eller samhandling og ved revidering av eksisterende. Virksomheten må da vurdere hvilke konsekvenser forskjellige uheldige hendelser kan få, for brukere av tjenesten, den offentlige virksomheten selv og offentlig sektor som helhet. Deretter må virksomheten vurdere sannsynligheten for at identifiserte konsekvenser vil inntreffe. Produktet av identifisert konsekvens og sannsynligheten for at den inntreffer blir i dette dokumentet beskrevet som et risikonivå.

Her defineres fire felles risikonivåer for offentlig sektor. Offentlige virksomheter skal på bakgrunn av risiko- og sårbarhetsanalyser kunne plassere egne tjenester/samhandling iht. disse felles risikonivåene. Dette skal igjen gi grunnlag for å finne riktig sikkerhetsnivå i neste kapittel, slik at man på bakgrunn av sikkerhetsbehov, og funksjonelle behov, kan velge en egnet løsning for autentisering eller uavviselighet. Den valgte løsning bør gjøre det såpass vanskelig å misbruke tjenesten at den resterende risikoen skal kunne anses som forholdsmessig akseptabel.
Felles risikonivåer er dermed det første steget for å legge til rette for felles løsninger og gjenbruk av løsninger for autentisering og uavviselighet.

3.1 Sannsynlighet

Sannsynlighet beskrives i dette rammeverket ved hjelp av følgende parametere:

- Frekvens — Hvor ofte en sårbarhet historisk blir forsøkt utnyttet.
- Kapasitet — En uautoriserts evne til å utnytte en sårbarhet. Hvor vanskelig det er å utnytte sårbarheten og hvor lett det er å skalere, dvs. øke omfanget av, et angrep.
- Motivasjon/Vinning — Hvor interessant det er å utnytte en sårbarhet.

I dette rammeverket vurderes sannsynlighet kun på bakgrunn av parametrene frekvens (historisk) og motivasjon. Dette fordi en uautorisert persons kapasitet til å utnytte autentiserings- eller uavviselighetsløsningen, først kan vurderes etter den er valgt, og denne vurderingen av risiko gjøres jo nettopp for å velge en slik løsning. Det anbefales imidlertid å gjennomføre en full risikovurdering etter valg av løsning for autentisering eller uavviselighet, der sannsynlighetsberegningen også kan inkludere kapasitet. Da kan virksomheten vurdere

om den resterende risiko er blitt såpass liten at den kan anses som forholdsmessig akseptabel for virksomheten.

På bakgrunn av frekvens og motivasjon vurderes sannsynligheten for at en hendelse inntreffer å være til stede, eller ikke. Enten er sannsynligheten for at en konsekvens inntreffer tilstrekkelig stor - og konsekvensen inkluderes i vurdering av risikonivå, eller den vurderes som så usannsynlig at konsekvensen ekskluderes. (Sannsynligheten settes lik 1 eller 0).

Motivasjonen for å utnytte sårbarheter i en løsning for autentisering eller uavviselighet er større dersom løsningen dekker flere elektroniske tjenester, fordi det er mer innhold og større funksjonalitet som kan utnyttes. Det kan lede til større konsekvenser. Der konsekvensene ved utnyttelse er store vil motivasjonen også kunne være stor. På et moderat nivå vil konsekvensene være av en slik art at selv om man samler mye innhold og stor funksjonalitet, vil motivasjonen som regel fortsatt være begrenset.

3.2 Konsekvens

Konsekvens er resultatet av at en sårbarhet blir utnyttet eller en uheldig hendelse inntreffer, uavhengig av sannsynligheten for at dette skal skje (iboende risiko). Med andre ord "worst case scenario". Det er viktig at den offentlige virksomheten i sin risikovurdering av en tjeneste, vurderer konsekvenser for alle parter, brukere av tjenesten (privatpersoner og næringsliv), den offentlige virksomheten selv og offentlig sektor som helhet.

Følgende sett med konsekvenser er benyttet for å definere risikonivåene i dette rammeverket:

- Konsekvenser for liv eller helse
- Økonomisk tap/ merarbeid/ økte kostnader
- Tap av renommé (anseelse, tillit og integritet)
- Hindring i straffeforfølgelse
- Uaktsomt bidrag til lovbrudd
- Bryderi/ulempe

Det er viktig å presisere at alle disse typer konsekvenser kan gjelde for alle målgrupper – sluttbrukere (personer, virksomheter), offentlige virksomheter og offentlig sektor som helhet. Den offentlige virksomheten som vurderer konsekvenser, må derfor vurdere alle disse konsekvenstypene for hver målgruppe.

Det er viktig å huske på de krav sentrale lover og spesiallovgivningen setter for den virksomheten som bedrives. Disse kravene har stor betydning i forhold til vurdering av konsekvenser.
Listen over er ikke uttømmende, så det kan skje konsekvenser som ikke påvirker de felles definerte risikonivå.

3.3 Risikonivåer

Risikonivåene i rammeverket beskrives i form av konsekvenser. Dette kan gjøres fordi sannsynligheten vurderes binært (1 eller 0, dvs. enten til stede eller ikke til stede). Risikoen, som er produktet av sannsynlighet og konsekvens, blir dermed beskrevet som konsekvenser som er inkludert eller ekskludert avhengig av sannsynligheten.

Det er definert følgende fire risikonivåer i tabellen under. Teksten i tabellen beskriver høyest risiko godkjent på et gitt risikonivå for den type konsekvens.

	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 straffe-forfølgelse	Ingen bidrag til hindring av straffe-forfølgning	Minimalt bidrag til hindring av straffe-forfølgning	Moderat bidrag til hindring av straffe-forfølgning	Det kan forekomme hindringer i straffe-forfølgning
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

”Risikonivå 1 – ingen”, er beregnet på åpen informasjon. Funksjoner og informasjonsutveksling i tilknytning til informasjon som er konfidensiell, taushetsbelagt eller personsensitiv, må legges på de andre risikonivåene iht. hvilke sannsynlige konsekvenser som kan oppstå hvis uheldige hendelser finner sted.

Nedenfor er det eksemplifisert uheldige hendelser som kan lede til konsekvenser i tabellen over:

1. Uautorisert endring av pasientdata.
2. En persons sykdomsdiagnose blir kjent for uvedkommende.
3. Omsetningstall lekker ut før kvartalsrapportering.
4. Feil i utbetalingsgrunnlag av trygd.
5. Feil i utbetalingsgrunnlag for MVA.
6. Uautorisert endring for å påvirke offentlige utbetalinger.
7. Offentlig etat taper renommé etter oppslag i media om datainnbrudd.
8. Bevismateriell blir ødelagt eller kommer på avveie, på grunn av operatørfeil.

9. Uautorisert endring av personadresse som ledd i identitetstyveri.

4. Sikkerhetsnivåer for autentisering og uavviselighet

Sikkerhet i løsninger for autentisering og uavviselighet kan beskrives ved hjelp av forskjellige sikkerhetsparametere. En sikkerhetsparameter er en faktor som påvirker sikkerhetsnivået i løsningen hvis den endres. Et eksempel på slik faktor er "utlevering til bruker". For en passordløsning vil "utlevering til bruker" beskrive hvordan passordet i praksis deles ut til brukeren. Er passordene delt ut til bruker på bakgrunn av fysisk legitimering, er det vanskelig å skaffe seg et passord i andres navn. Deles passordene ut over Internett på bakgrunn av påstått identitet er det lett å skaffe et passord i andres navn. Dette viser at to forskjellige krav til samme sikkerhetsparameter endrer graden av hvor vanskelig det er å kompromittere løsningen.

Sikkerhetsnivåene i dette rammeverket er definert på bakgrunn av følgende sett av sikkerhetsparametere:

- Krav til autentiseringsfaktor(er)
  Beskriver antall autentiseringsfaktorer og deres egenskaper. For eksempel om autentiseringsfaktoren er statisk eller dynamisk. Med statisk menes at dokumentasjonen som presenteres for andre som skal verifisere påstått identitet ikke endres fra gang til gang. Et eksempel på dette er fast passord eller biometriske data. Med dynamisk menes at dokumentasjonen som presenteres for andre som skal verifisere påstått identitet, endres fra gang til gang. Eksempler på slike løsninger er tidsbaserte passordkalkulatorer, som gir nytt passord avhengig av tid, og løsninger basert på PKI, hvor det ved hver autentisering genereres en ny, tilfeldig datastreng som signeres digitalt.
- Utlevering til bruker
  Beskriver hvordan man sikrer knytningen mellom autentiseringsfaktorer og brukeridentiteter. For eksempel om brukeren har måttet møte opp fysisk og legitimere seg selv, eller om brukeren har fått noe tilsendt til folkeregistrert adresse. I dette rammeverket er folkeregistrert adresse definert til å være en av adressene registrert i folkeregisteret (Folkeregisteret har definert tre typer adresser i sitt register).
- Sikring av autentiseringsfaktorer ved lagring
  Beskriver hvordan autentiseringsfaktoren er lagret lokalt, og hvordan den er fysisk og logisk sikret. Et eksempel er forhåndsdefinerte passordlister. Kommer disse på et åpent ark, er de kopierbare. Er passordene beskyttet som skrapelodd, er de ikke kopierbare uten at mottakeren vil oppdage dette.
- Krav til uavviselighet
  Beskriver i hvilken grad det i ettertid er mulig å dokumentere at en bruker står bak et informasjonselement eller har utført en handling.

- Krav til offentlig godkjenning
  Innebærer at det finnes en offentlig kravspesifikasjon (ev. en forvaltningsstandard) for den type løsninger, og at løsningen er deklarert ved en offentlig ordning.

Overforstående sikkerhetsparametere er definert for å være teknologinøytrale. De forskjellige sikkerhetsparametrene er vektet likt på den måten at en løsning som skal tilfredsstille et sikkerhetsnivå, skal oppfylle kravene som er satt for alle sikkerhetsparametrene på det nivået.

Det settet med sikkerhetsparametere som er benyttet i dette rammeverket for å skille mellom sikkerhetsnivå er ikke uttømmende. Det finnes derfor autentiserings- og uavviselighetsløsninger som har andre sikkerhetsparametere som kan ha forskjellig nivå, og som dermed kan oppfattes sikkerhetsmessig forskjellig.

Når en offentlig virksomhet skal velge sikkerhetsnivå på bakgrunn av sitt risikonivå, er det viktig å være oppmerksom på at sentrale systemsjekker i noen tilfeller vil kunne begrense sannsynligheten for at en konsekvens inntreffer og dermed senke kravet til sikkerhetsnivå. For eksempel kan en sentral sjekk om at utbetaling går til en konto i brukers navn senke kravet til utlevering.

Det er definert fire sikkerhetsnivåer som vist i tabellen under.

Nivå	**Krav til Autentiserings faktor(er)**	**Utlevering til bruker**		**Sikring av autentiserings faktorer ved lagring**	**Krav til offentlig godkjenning**	**Krav til uavviselighet**
		Fysiske personer	***Juridiske personer***			
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, men med ett tilleggskrav om at utsendelsesprosedyren skal ha integrert tilleggssikring som sørger for at sannsynligheten for at feil person tar løsningen i bruk minimaliseres. Det er ikke krav om personlig oppmøte.	Samme krav som i 2, men med ett tilleggskrav om at utsendelsesprosedyren skal ha integrert tilleggssikring som sørger for at sannsynligheten for at feil person tar løsningen i bruk minimaliseres. Det er ikke krav om personlig oppmøte.	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[3], Person Høyt. 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[3], nivå Virksomhet.	Ikke-kopierbare.	Løsningen skal være deklarert 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.

[3] Kravspesifikasjon for PKI i offentlig sektor, Moderniseringsdepartementet, januar 2005, og til enhver tid gjeldende versjon av denne.

Praktiske eksempler på løsninger som tilfredsstiller de forskjellige sikkerhetsnivåene
Her gis det eksempler på hva slags tekniske løsninger som vil tilfredsstille de forskjellige sikkerhetsnivåene. Alle løsninger på et høyere nivå vil kunne benyttes på et lavere sikkerhetsnivå.

Sikkerhetsnivå 1
Dette sikkerhetsnivået gir liten eller ingen sikkerhet. Her fungerer helt åpne løsninger. Det finnes også noen sikkerhetsløsninger som vil havne i denne kategorien fordi de ikke tilfredsstiller kravene til sikkerhetsnivå 2. Dette gjelder løsninger som for eksempel:

- Selvvalgt passord og brukernavn over nettet.
- Identifisering med fødselsnummer.

Sikkerhetsnivå 2
På dette sikkerhetsnivået fungerer alle løsninger som tilfredsstiller kravene til sikkerhetsnivå 2, men som ikke tilfredsstiller kravene til sikkerhetsnivå 3. Eksempler på sikkerhetsløsninger som havner i denne kategorien er:

- Fast passord, sendt ut i brev til folkeregistrert adresse.
- Passordkalkulatorer uten passordbeskyttelse, minimum distribuert gjennom folkeregistrert adresse.
- Engangspassordlister distribuert til folkeregistrert adresse.

Sikkerhetsnivå 3
På dette sikkerhetsnivået fungerer alle løsninger som tilfredsstiller kravene til sikkerhetsnivå 3, men som ikke tilfredsstiller kravene til sikkerhetsnivå 4. Eksempler på sikkerhetsløsninger som havner i denne kategorien er:

- Passordkalkulatorer beskyttet med PIN-kode, der første PIN-kode er sendt i separat forsendelse.
- Engangspassord på mobiltelefon, der mobiltelefonen er registrert med en egen registreringskode distribuert til folkeregistrert adresse.
- Person Standard iht. Kravspesifikasjon for PKI i offentlig sektor.
- 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).

Prosedyren for utsendelse til folkeregistrert adresse, skal ha implementert en tilleggssikring for å sannsynliggjøre at ikke en uautorisert tar i bruk løsningen. Eksempler på slik tilleggssikring er:

- utsendelse av kode i et brev brukeren forventer å motta og vil etterlyse,
- bekreftelse på aktivering av sikkerhetsløsning i eget brev,
- sjekk mot mobiltelefon brukerregister, eller
- begrenset levetid på utsendte koder.

Sikkerhetsnivå 4
På dette sikkerhetsnivået vil det, i forhold til dagens situasjon og teknologiske løsninger i markedet, kun være løsninger basert på PKI som tilfredsstiller kravene. I henhold til gjeldende regelverk må løsningene være selvdeklarert 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.
Eksempler på teknologier som kommer, men ikke har tilstrekkelig standardiseringsgrad pr. i dag, er:

- En tofaktorløsning, hvor en av faktorene er dynamisk, hvorav en av faktorene eller en registreringsfaktor er personlig utlevert. Det benyttes en tredjepart til å registrere en logg med knytningen mellom handling/ informasjonselement og identitet. Loggen skal lagres med endringsbeskyttelse.
- En tofaktorløsning, hvor en av faktorene er dynamisk, hvorav en av faktorene eller en registreringsfaktor er personlig utlevert. Det benyttes spesialprogramvare som hindrer brukersted i å generere falsk dokumentasjon over hvem som står bak et informasjonselement/handling og som hindrer operatører å kunne endre logging av informasjonselement/ handlingsbeskrivelse og identitet.

5. Anbefaling om bruk av sikkerhetsnivåer

Hver offentlig virksomhet er selv ansvarlig for å forvalte sine oppgaver på en forsvarlig måte, og er blant annet hva angår personopplysninger definert som behandlingsansvarlig i personopplysningsloven[4]. Hver offentlig virksomhet må derfor selv vurdere hva som er et akseptabelt risikonivå og hvilke sikkerhetsløsninger som gir forholdsmessig akseptabel sikkerhet for virksomheten.

Dette dokumentets anbefalinger om hvilket sikkerhetsnivå som egner seg for de definerte risikonivåer fritar derfor ikke den offentlige virksomheten fra krav til selv å vurdere sikkerhetsbehovet i forhold til den konkrete tjenesten som skal tilbys.

Når en offentlig virksomhet skal kommunisere elektronisk må de gjennomføre en Risiko- og sårbarhetsanalyse. På bakgrunn av den analysen kan de iht. kapittel 3 vurdere hvilket risikonivå som bør tilordnes den aktuelle type elektronisk kommunikasjon. Dette rammeverket gir følgende anbefaling om hvilke sikkerhetsnivåer definert i kapittel 4 som egner seg for de forskjellige risikonivåer definert i kapittel 3:

Risikonivå 1 → Sikkerhetsnivå 1
Risikonivå 2 → Sikkerhetsnivå 2
Risikonivå 3 → Sikkerhetsnivå 3
Risikonivå 4 → Sikkerhetsnivå 4

Dette rammeverket er et generelt verktøy for offentlige virksomheter, som kan brukes til å "plassere" tjenester eller samhandling mht. sikkerhetsnivå og til påfølgende valg av løsning for autentisering eller uavviselighet. Rammeverket kan også brukes til å velge sikkerhetsnivå eller sikkerhetsløsning for offentlige løsninger (portaler) der en autentisering kan gi adgang til flere tjenester. Rammeverket kan også benyttes i forhold til å vurdere gjenbruk av andres sikkerhetsløsninger eller felles sikkerhetsløsninger mot egne tjenester.
Det vil bli utarbeidet en veileder med en mer grundig innføring i risikovurderinger og bruken av dette rammeverket.

[4] Lov om behandling av personopplysninger (personopplysningsloven), Justis- og politidepartementet, 2000-04-14, nr 31.

6. Referanser

1. Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), Fornyings- og administrasjonsdepartementet, 2004-06-25
2. Kravspesifikasjon for PKI i offentlig sektor, Moderniseringsdepartementet, januar 2005
3. NoU 2001:10 Uten Penn og blekk, Arbeids- og administrasjonsdepartementet, mars 2001
4. E-authentication Guidance for Federal Agencies, Office of Management and Budgets, Washington DC 2003 Dec 16
5. Registration and Authentication, e-Government Strategy Framework Policy and Guidelines, September 2002. Office of the e-Envoy, UK
6. Lov om elektronisk signatur (esignaturloven), Nærings- og handelsdepartementet, 2005-06-17
7. Lov om behandling av personopplysninger (personopplysningsloven), Justis- og politidepartementet, 2000-04-14
8. Wikipedia, 2007-01-22
9. www.brreg.no/registrene/enhet/ Brønnøysund, 2007-01-22

Utgitt av:
Fornyings- og administrasjonsdepartementet

Offentlige institusjoner kan bestille flere eksemplarer av denne publikasjonen fra:
Departementenes servicesenter
Post og distribusjon
www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefaks: 22 24 27 86

Oppgi publikasjonskode: P-0945 B

Trykk: Departementenes servicesenter 04/08 - 2000