Justisdepartementet

Utarbeidet av konsulentselskapet Steria AS

Dato: 30.06.2011

Sikkerhet, risiko og sårbarhet for ny dataløsning for vergemål

Innholdsfortegnelse

Figurliste

Tabelliste

1. Oppsummering

Dataløsningen for vergemålsområdet vil realiseres som en webløsning som vil bli tilgjengelig gjennom internett. Det vil derfor stille store krav til sikkerheten og overvåking av løsningen. Det er viktig å ha en sikker autentiseringsløsning som gjør at man er helt sikre på at de brukerne av Vergemålsportalen er den de utgir seg for å være. Ved å ta i bruk den nasjonale felleskomponenten ID-Porten vil løsningen ta i bruk en godt etablert tjeneste som er forankret i det offentlige. I detaljert design er det nødvendig å se på prosessene og klassifisere disse med henhold til konfidensialitet, integritet og tilgjengelighet.

Arkivloven med forskrifter og Personopplysningsloven er viktige føringer for beskyttelse og krav for Vergemålsportalen. Prosjektet må gjennomføre en analyse av beskyttelsesbehovet og klassifisere dette for å kunne definere riktig sikkerhetsnivå. Det vil være hensiktsmessig å definere egne roller der det bestemmes hvilke funksjoner en autentisert bruker skal få utføre, samt hvilken informasjon denne brukeren skal få tilgang til.

I forbindelse med sikkerheten for portalen er det gjort en overordnet risiko- og sårbarhetsanalyse (ROS). Ved å kartlegge sannsynlighet og konsekvenser av uønskede hendelser, som for eksempel tekniske feil,hacker andgrep, datalekasjer, kan man prioritere risikoområder og planlegge tiltak for å forhindre dem eller redusere konsekvensen av dem dersom de skulle oppstå. ROS-analysen er i hovedsak en kvalitativ risikovurdering, bygget på faglig skjønn og erfaring. Det er ikke mulig å gjennomføre en detaljert ROS av sikkerheten for en løsning som ikke er implementert, og en slik ROS analyse krever ofte mye tid og ressurser. Ofte vil resultatet av en analyse – altså den risiko man kommer frem til at en hendelse representerer – bli presentert i en risikomatrise. ROS-analyser bør utføres av arbeidsgrupper bestående av medarbeidere som representerer ulike deler av virksomheten, og gjennom dette bidrar med ulike synsvinkler på feltet som analyseres, samt ulike erfaringer fra praksis. En av de største nytteeffektene med ROS-analyser er at de setter bestemte problemstillinger på dagsorden og fungerer som gode oversikts-, for midlings- og beslutningsverktøy.

1.1. Arbeidsmetode

Vurderinger rundt sikkerhet og risiko er et resultat av arbeidsprosessene og behovsanalysen utført av Steria, offentlig dokumentasjon om lover og regler, samt workshops og oppfølging med følgende deltagere:

- Oddbjørn Vassli, prosjektlededer
- Arild Justnes, Steria
- Ronny Robinsson Stavem, Steria
- Eldbjørg Kluften, Fylkesmannen i Oslo og Akershus
- Stine Røtne, Statens sivilrettsforvaltning
- Ann Kristin Netland, Statens sivilrettsforvaltning
- Bjørn Tore Årøy, Fylkesmannen i Sogn og Fjordane
- Gisle Losnegård Hansen, Fylkesmannen i Hordaland
- Jørgen Tistle, Fylkesmannen i Sogn og Fjordane

2. Referanser

ID	Referanse	Beskrivelse
1	Arkivverket, standard for elektronisk arkiv NOARK 5 http://www.arkivverket.no/arkivverket/lover/elarkiv/noark-5.html	Standard for elektronisk arkiv NOARK 5
2	"Forskrift til arkivloven av 1. desember 1999 nr. 1566 om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver", kapittel IX: Bestemmelser om elektronisk arkivering av saksdokumenter http://www.lovdata.no/for/sf/ku/xu-19991201-1566.html#map059	Forskrifter for arkivering
3	LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger (personopplysningsloven) http://www.lovdata.no/all/hl-20000414-031.html med sentrale forskrifter: http://www.lovdata.no/for/sf/sf-20000414-031.html	Den viktigste rettskilden innen beskyttelse av personvern. Loven gir generelle bestemmelser om behandling av personopplysninger, dvs. opplysninger som direkte eller indirekte kan knyttes til en fysisk person
4	Policy for informasjonssikkerhet	Intern mal som distribueres til alle fylkesmannsembeter. Danner basis for den policy hvert fylkesmannsembete ønsker å innføre.
5	Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, April 2008 http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf	Retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett

Tabell 1: Referanseliste

3. Premisser, lover og forskrifter

Arkivloven med forskrifter stiller strenge krav til elektronisk journalføring og arkivering. Et vesentlig krav er at ALLE dokumenter i en SAK enten skal være Papirbasert eller Elektronisk. Fylkesmannen må siden man har til hensikt å ha en gradvis overgang til en fullstendig elektronisk løsning av saksmapper vurdere om det kan være behov for dispensasjon for å la noen dokumenter i en sak være elektronisk, og noen er i papirformat.

Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver. Fastsatt av Riksarkivaren 1. desember 1999 med hjemmel i forskrift av 11. desember 1998 nr. 1193 om offentlege arkiv § 2-15, § 3-14 siste ledd, § 3-21 annet ledd, § 3-22, § 3-23, § 5-8, § 5-10. Endret ved forskrifter 11 mai 2000 nr. 431, 11 juni 2000 nr. 747, 4 des 2000 nr. 1220 (bl.a. tittel), 1 okt 2002 nr. 1066, 2 juni 2005 nr. 587, 24 april 2007 nr. 442. Forskriften trådde i kraft 1. januar 2000. Samtidig oppheves forskrift av 1. januar 1999 nr. 73 om Riksarkivarens arkivbestemmelser.

Vedlegg 1 viser kravene til Elektronisk arkiv og Vergemålsportalens behov for dekning av disse.

4. Journalføringsplikt i Offentlighetsloven

Formålet med loven er å legge til rette for at offentlige virksomheter er åpne og gjennomsiktig, for slik å styrke informasjons- og ytringsfriheten, den demokratiske deltakingen, rettssikkerheten for den enkelte, tilliten til det offentlige og kontrollen fra allmennheten. Organ som kommer inn under lovens virkeområde, har plikt til å føre journal etter reglene i arkivloven med forskrifter, jfr Offentlighetslovens § 10. Funksjonalitet for journalføring blir implementert i Vergemålsportalen.

4.1. Personvernhensyn

Foreligger det bruk av personopplysninger, dvs. opplysninger og vurderinger som kan knyttes til en enkeltperson, setter personopplysningsloven en rekke krav til behandling av personopplysningene. Behandling av personopplysninger vil si enhver bruk av personopplysninger, for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksområder.

4.1.1. Grunnlag for behandling av personopplysninger etter personopplysningsloven

Det rettslige grunnlaget for behandling av personopplysninger (pol §§ 8 og 9):

- Samtykke
- Lovhjemmel
- Nødvendighetsvurderinger etter pol §§ 8 a-f og 9 c-h)

4.1.2. Type personopplysninger som skal behandles

Vergemålsportalen skal vise oversikt over :

- Inngående og utgående dokumenter
- Personopplysninger fakta bosted, familieforhold
- Brukers utbetalinger
- Kontaktinformasjon (e-post, telefon)
- Inn- og utgående dokumenter for en sak (Journal)

4.1.3. Dokumentmengder og -typer

Vergemålsportalen vil gi tilgang til inngående og utgående dokumenter i et stort omfang.

4.1.3.1. Omfang og tilgang

Vergemålsportalen har en meget stor målgruppe, i utgangspunktet er det:

- Verger
- Fylkesmenn
- Klienter
- Sentral vergemålsforvaltning
- Leger og andre interessenter

4.1.3.2. Ivaretakelse av den registrertes rettigheter

Vergemålsportalens forprosjekt er kjent med innsynsretten (Vedlegg 2). Prosessen for hvordan Vergemålsprosjektet skal håndtere en forespørsel om innsyn fra en registrert (bruker) vil bli beskrevet i brukerveiledning og rutinene.

Vergemålsportalen vil systematisere og forenkle brukers mulighet for innsyn.

Vergemålsportalen skal ha følgende muligheter for innsyn:

- Portalbruker kan, for autorisert tilgang, på en enkel måte få en oversikt over utskrift av loggen over alle henvendelser knyttet til en klient.
- Få oversikt over dokumenter som er tilknyttet en klient, som er lagret i ePhorte, utskrift enkeltvis og journal for klient.

4.2. Bevaring og kassasjon

Dokumenter må lagres så lenge som det er bestemt for den enkelte type dokument.

Det henvises til bestemmelsene i arkivforskriften § 3-20 og § 3-21 og til Riksarkivarens bevarings- og kassasjonsbestemmelser.

Dokumenter som skal avleveres til Riksarkivet og kan ikke slettes før avleveringen er godkjent av Riksarkivet.

Metadata skal ikke slettes i det hele tatt. Disse skal alltid oppbevares. Dette gjelder journaler og andre gjenfinningsregistre.

4.3. Melding til Datatilsynet

Meldeplikten er regulert i personopplysningslovens § 31. Meldeplikten innebærer at den som ønsker å bruke personopplysninger, skal orientere Datatilsynet før behandlingen blir startet. Meldingen skal sendes Datatilsynet senest 30 dager før behandlingen starter (dvs. før systemet/Vergemålsportalen settes i drift)

Hovedregelen er at følgende behandling av personopplysninger er meldepliktige:

- Ikke-sensitive personopplysninger som blir behandlet med elektronisk hjelpemiddel.
- Sensitive personopplysninger som skal føres i et manuelt register.

Den behandlingsansvarlige skal gi melding til Datatilsynet før:

a) behandling av personopplysninger med elektroniske hjelpemidler,

b) opprettelse av manuelt personregister som inneholder sensitive personopplysninger.

Meldingen skal gis senest 30 dager før behandlingen tar til. Datatilsynet skal gi den behandlingsansvarlige kvittering for at melding er mottatt.

Ny melding må gis før behandling som går ut over den rammen for behandling som er angitt i medhold av § 32. Selv om det ikke har skjedd endringer, skal det gis ny melding tre år etter at forrige melding ble gitt.

Kongen kan gi forskrift om at visse behandlingsmåter eller behandlingsansvarlige er unntatt fra meldeplikt, underlagt forenklet meldeplikt eller underlagt konsesjonsplikt. For behandlinger som unntas fra meldeplikt kan det gis forskrift for å begrense ulemper som behandlingen ellers kan medføre for den registrerte."

Meldingen er bare en orientering fra behandler til Datatilsynet, og blir ikke "godkjent" av Datatilsynet.

Det kreves konsesjon fra Datatilsynet for å behandle sensitive personopplysninger. Det gjelder ikke for behandling av personopplysninger i organ for stat eller kommune når behandlingen har hjemmel i egen lov, jf personopplysningsloven § 33 fjerde ledd. Foreligger det lovhjemmel for behandling av personopplysningene er det tilstrekkelig med en melding til Datatilsynet.

5. Systemsikkerhetskrav for Vergemålsportalen

Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor er et rammeverk for autentisering og uavviselighet, og 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”).

Forskrift om elektronisk kommunikasjon med og i forvaltningen 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.

5.1. Autentisering

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.

5.2. Autorisasjon

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.

Det er flere muligheter ved valg av en autorisasjonsmodul. De fleste CMS rammeverk har egne funksjoner for å håndtere dette ved bruk av roller. Og tilganger vil da styres etter hvilke roller en autentisert bruker har. Dette betyr da at autorisasjonsmodulen må tilpasses løsningen. Ved enkle roller og tilgangsbehov kan dette være en fornuftig løsning.

Et annet alternativ er å se på en Identity and Access Management løsning for å håndtere autentisering og tilgangskontroll. Dette er en mer kompleks løsning som vil kreve mye mer enn en enkelt egenutviklet modul. Prosjektet bør gjøre en vurdering av hvilke krav som stilles og hvilken kompleksitet som er nødvendig for tilgangsmodeller. Dette må ses i sammenheng med analysen av beskyttelsesbehovet som må gjennomføres i design fasen.

5.3. Konfidensialitet

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 en identitet må verifiseres før tilgang til konfidensialitetsbeskyttet informasjon kan gis. 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.

6. Risikonivåer

Offentlige virksomheter må gjennomføre 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 , 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.

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

Tabell 2: Risikonivåer

"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 klientdata.
2. En persons sykdomsdiagnose blir kjent for uvedkommende.
3. Uautorisert endring for å påvirke offentlige utbetalinger.
4. Offentlig etat taper renommé etter oppslag i media om datainnbrudd.
5. Bevismateriell blir ødelagt eller kommer på avveie, på grunn av operatørfeil.
6. Uautorisert endring av personadresse som ledd i identitetstyveri.

6.1. Sikkerhetsnivåer for autentisering og uavviselighet

Sikkerhetsnivåene i 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 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 Autentisering s faktor(er)**	**Utlevering til bruker**		**Sikring av autentisering s faktorer ved lagring**	**Krav til offentlig godkjennin g**	**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	Både statiske og dynamiske kan være kopierbare.	Ingen krav.	Det skal foreligge rutiner og logger, som gjør at det er rimelig sikkert at kommunikasjons

			den juridiske personen, skal stå først på forsendelsen. Alternativt kan det sendes til den som tegners folkeregistrerte adresse.			-parten 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 , 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.	Ikke-kopierbare.	Løsningen skal være deklarert i henhold til offentlige krav.	En kommunikasjons-part 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.

			Krav tilsvarende Kravspesifikasjon for PKI nivå Virksomhet			

Tabell 3: Sikkerhetsnivåer for autentisering og uavviselighet

6.2. 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. Løsninger som i dag er godkjente er for eksempel løsinger fra Comfides og BuyPass.

Eksempler på teknologier 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.

7. Krav til klassifisering

7.1. Krav til klassifisering av prosesser

I detaljert design er det nødvendig å se på prosessene og klassifisere disse mht konfidensialitet, integritet og tilgjengelighet.

7.2. Systemer Vergemålsportalen er avhengig av – sikkerhetsbehov

For detaljert sikkerhetskrav for Vergemålsportalen må systemer portalen er avhengig av defineres og klassifiseres med tilhørende krav til konfidensialitet, integritet og tilgjengelighet.

7.3. Lagringsområder som Vergemålsportalen benytter, datatilgjengelighet

For lagringsområder brukt av andre systemer eller portalen selv må det også lagringsområder klassifiseres.

8. Beskyttelsesbehov

8.1. Generelt for behovet

- Konfidensialitet (§2-11 Sikring av konfidensialitet)
  - Vergemålsportalen legger vekt på "uautorisert tilgang" til personopplysninger.
  - Når det gjelder overføring av informasjon i det offentlige telenett vil Vergemålsportalen være tilgjengelig i åpen sone, med eksterne grensesnitt. Beskyttelse av integrasjonspunkter er viktig.

- Integritet (§2-13 Sikring av integritet)
  - Hindre uautorisert tilgang til å endre personinformasjon og dokumenter
  - Videre vil Vergemålsportalen vektlegge å hindre endring av annen informasjon
  - Tiltak mot ødeleggende programvare

- Tilgjengelighet (§ 2-12 Sikring av tilgang)
  - Tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig
  - Sikret tilgang til annen informasjon med betydning for informasjonssikkerhet
  - Alternativ behandling skal forberedes for de tilfeller systemet er utilgjengelig
  - Personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk skal kopieres

9. Sikkerhetskonsept

9.1. Ulike type roller og deres behov for rettigheter

Det vil være hensiktsmessig å definere egne roller der det bestemmes hvilke funksjoner en autentisert bruker skal få utføre, samt hvilken informasjon denne brukeren skal få tilgang til. Nedenfor er det noen eksempler på roller som kan tenke så ha et ulikt informasjonsbehov.

- Saksbehandler hos fylkesmannen
- Saksbehandler hos Sentral vergemålsmyndighet
- Klient
- Verge
- Pårørende

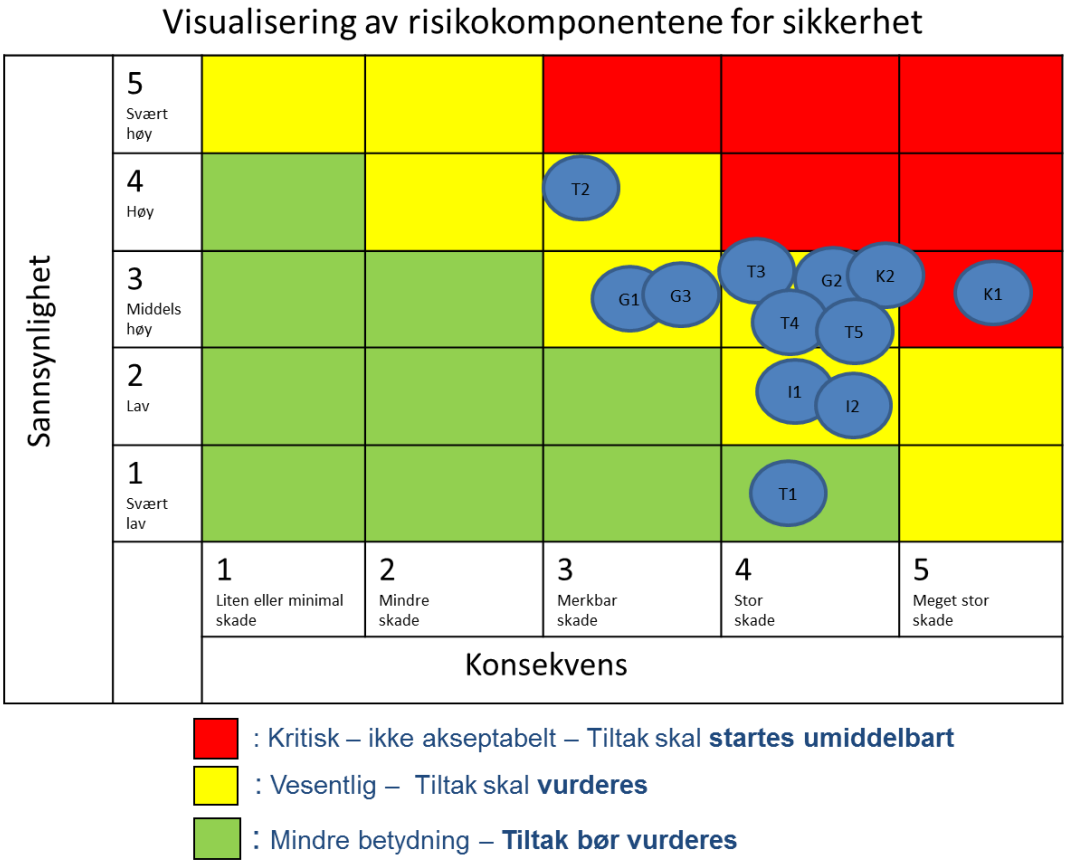
10. Risiko

I en ROS analyse vil det være ønskelig med en vurdering av hyppigheten hvor ofte en sannsynlighet vil inntreffe. Det er sannsynlig at hacker angrep eller forsøk på å angrep vil skje daglig, mens andre usikkerheter vil man ikke kunne si noe om. Ofte er disse vurderingene et resultat av erfaring med implementert løsning og hvordan organisasjonen fungerer. Det er derfor ikke lagt inn vurderinger på forekomstrate i denne overordnede analysen. En mer detlajert ROS analyse må gjennomføres når prosjektet går inn i fasen for detaljert design.

Vurderingene av sannsynlighet og konsekvens for denne overordnede ROS analysen er vurderinger gjort av forprosjektet, og disse har blitt sendt ut til deltagere i sikkerhets-workshopen, som det refereres til under delkapittelet Arbeidsmetode, for en tilbakemelding. Endringer av verdier for sannsynlighet og konsekvens har blitt oppdatert i henhold til de tilbakemeldinger som kom tilbake fra denne utsendelsen.

Denne ROS analysen gjør en overordnet analyse av et system som ikke eksisterer, og det må i etterkant av detaljert design utføres en ROS analyse som analyser risiko mer i detalj enn hva som kan gjøres i denne fasen. Flere av de overordnede risikopunktene kan deles opp i flere risikopunkter med flere detaljer. Dette avhenger av implementering av den faktiske løsningen. Det vil da også bli synliggjort hvorvidt noen av de overordnede punktene vil høre inn under andre risikopunkter, og de vil da i så måte spesifiseres mer i detalj.

10.1. Usikkerhet



Figur 1: Visualisering av risikokomponentene for sikkerhet

10.2. Håndtering av usikkerhet

10.2.1. Generelt

ID	Usikkerhet/ Problem	Mulig(e) konsekvens(er)	Aksjon for å håndtere risiko	Effekt av tiltak	S	K	Grad
G1	Mangelfull informasjonspolicy	Inkonsistent håndtering av overordnede føringer	Forankring av policy med ansvar og roller	Enhetlig håndtering av operative føringer	3	3	
G2	Roller og ansvar for informasjons-sikkerhet ikke blir forankret	Svak og tilfeldig styring av sikkerhet og potensiale for at hendelser ikke	Innføre et styringssystem for informasjonssikkerhet som er felles for alle	Bedre sikkerhet og styring	3	4	

		blir håndtert eller oppdaget.					
G3	Løsningen blir ikke tatt i bruk i tilstrekkelig grad	Det vil bli flere manuelle saker enn hva som formålstjenlig	God kommunikasjon om hvilke gevinster og fordeler bruk av vergemålsportalen vil ha, samt en god opplæringsplan. Krav til at løsningen skal brukes.	Større oppslutning av bruk av løsningen	3	3	

Tabell 4: Generell risiko

10.2.2. Brudd på tilgjengelighet

ID	Usikkerhet/ Problem	Mulig(e) konsekvens(er)	Aksjon for å håndtere risiko	Effekt av tiltak	S	K	Grad
T1	Risiko for at ID-porten ikke er tilgjengelig for autentisering	Det vil da ikke være mulig å komme inn på portalen for saksbehandling	Monitorering av grensesnittene som portalen er avhengig av.	Tidlig varsling av at avhengigheter ikke er tilgjengelig og at dette kan kommuniseres tidlig til brukere av portalen.	1	4	
T2	Risiko for hacker-angrep	Ved evt Service of Denial angrep vil tjenester I Vergemålsportalen blokkeres	Overvåking	Redusert nedetid ved et angrep	4	3	
T3	Teknisk feil og feil i forvaltningsrutiner	Vergemålsportalen blir utilgjengelig	Opprette forvaltningsrutiner og prosedyrer	Redusere sannsynligheten for teknisk svikt som kan føre til nedetid av portalen	3	4	
T4	Risiko for svikt i	Det vil ikke være	Gode testrutiner	En mer stabil	3	4	

	integrasjon mellom Vergemålsportalen og ePhorte (arkiv) slik at dokumenter ikke blir tilgjengelig i portalen	mulig å se/vise dokumenter i Vergemålsportalen	og overvåkings-mekanismer for integrasjon og kommunikasjon mellom portal og endesystemer	løsning			
T5	Portalen er utilgjengelig for brukeren grunnet feil OS, nettleser etter patchnivå.	Tjenestene på protalen eller portalen selv blir utilgjengelig for brukeren.	Informasjon, etablert helpdesk. Testing før utrulling av ny funksjonalitet og oppgraderinger.	En kompatibel portal som er tilgjengelig	3	4	

Tabell 5: Brudd på tilgjengelighet

10.2.3. Brudd på konfidensialitet

ID	Usikkerhet/ Problem	Mulig(e) konsekvens(er)	Aksjon for å håndtere risiko	Effekt av tiltak	S	K	Grad
K1	Hacker-angrep, avlytting, menneskelig svikt, rutinesvikt, utro medarbeider	Sensitive opplysninger kan komme på avveie, og tap av omdømme	Gode overvåkings-mekanismer, og etablering av gode forvaltningsrutiner, opplæring av brukere	Mulig å sette i gang strakstiltak for å stoppe angrepet.	3	5	
K2	Uautoriserte personer får tilgang på sensitiv informasjon	Tap av omdømme og tillit til Vergemålsordningen	Gode autentiserings- og autorisasjonsløsninger som ved implementering av brukeradministrasjon og tilgangskontroll	Informasjon blir tilgjengelig kun for personer som er autorisert for informasjonen	3	4	

Tabell 6: Brudd på konfidensialitet

10.2.4. Brudd på integritet

ID	Usikkerhet/ Problem	Mulig(e) konsekvens(er)	Aksjon for å håndtere risiko	Effekt av tiltak	S	K	Grad
I1	Utro verger eller fylkesmenn endrer opplysninger som ikke må endres	Tap av omdømme og tillit	Innføring av logg og sporingsmekanismer	Opprettholde godt omdømme og tillit av Vergemåls-ordningen	2	4	
I2	Angrep utenfra som prøver å sende inn linker over epost	Uttransportering av data, eller hele eller deler av portalen	Gode sjekkerutiner i kildekode og feilhåndteringsrutiner.	En løsong som ikke lekker data/informasjon	2	4	

Tabell 7: Brudd på integritet

Vedlegg 1: Dekning ift krav om elektronisk arkivering

Denne listen viser Kapittel IX: Elektronisk arkivering av saksdokumenter med en beskrivelse av Vergemålsportalens oppfyllelse av kravene.

Fastsatt av Riksarkivaren 1. oktober 2002 med hjemmel i forskrift av 11. desember 1998 nr. 1193 om offentlege arkiv § 2-13.

Kapittel IX: Elektronisk arkivering av saksdokumenter **A Generelle bestemmelser**	**Vergemålsportal beskrivelse**	**Status (Åpen, Ok, Ikke relevant)**
§ 1-1. Virkeområde		
Bestemmelsene gjelder for alle offentlige organer som omfattes av arkivforskriften.	Omfattes av forskriften	OK
Bestemmelsene omfatter saksdokumenter som lagres på elektroniske medier, og elektroniske systemer som slike dokumenter er knyttet til, herunder journal- og arkivsystemer, saksbehandlingssystemer og spesialiserte fagsystemer.	Omfattes	OK
§ 1-2. *Registrering av elektroniske saksdokumenter*		
Saksdokumenter som lagres elektronisk, skal være knyttet til et journalføringssystem eller annet elektronisk system for registrering av dokumenter, jf. § 2-1 – § 2-3. Systemet skal styre all arkivering av og tilgang til saksdokumentene.	Omfattes Inngående dokumenter vil bli skannet og knyttet til arkivsystemet via portalen	OK Mulig behov for dispensasjon for siste setning hvis ePhorte skal være arkivsystemet.
§ 1-3. *Kassasjon av papirversjoner ved skanning*		
Når dokumenter på papir blir skannet og arkivert elektronisk i tråd med bestemmelsene i dette kapitlet av forskriften her, kan papirversjonen av dokumentene kasseres med mindre lovbestemte formkrav, for eksempel krav om håndskrevet signatur, eller andre juridiske hensyn krever	Det må utarbeides rutiner for sikkerhetsarkiv. Eventuelle behov for tilleggsbevaring av noen dokumenter på papir må bli avklart i detaljert design.	Åpen

at papirversjonen bevares.		
Riksarkivaren kan i enkelttilfeller fastsette at også papirversjonen av dokumentene skal bevares, jf. arkivforskriften § 2-13.	Under detaljert design vil det være behov for å se på hva som skal destrueres og ikke	Åpen
§ 1-4. *Utfyllende bestemmelser for kommuner og fylkeskommuner*		
Innenfor rammen av bestemmelsene i dette kapitlet av forskriften her, kan den enkelte kommune eller fylkeskommune fastsette utfyllende bestemmelser og instrukser.		Ikke relevant
B. Krav til systemer, formater og lagringsmedier		
§ 2-1. *Generelle systemer for journalføring og arkivering*		
Journalføring av elektroniske saksdokumenter skal som hovedregel skje i et system som følger kravene i Noark-standarden og er godkjent av Riksarkivaren, jf. arkivforskriften § 2-9. Dette gjelder enten man benytter et rent journal- og arkivsystem, eller om funksjoner for journalføring iht. arkivforskriften § 2-6 og § 2-7 er integrert i et saksbehandlingssystem eller lignende.	Omfattes ePhorte er lagt fram som forslag som arkivsystem for Vergemålsapplikasjonen. ePhorte har en midlertidig godkjenning mot NOARK 5 standarden.	OK
Ved elektronisk arkivering av saksdokumenter må systemet tilfredsstille de spesifikke kravene til elektronisk arkivering i Noark-standarden og være godkjent av Riksarkivaren for dette formålet.	Se over	OK
Dersom saksdokumenter skal utveksles elektronisk i tilknytning til det elektroniske arkivet, bør systemet også	Det er ikke lagt opp til e-post håndtering for dokumentene	OK

tilfredsstille basiskravene til integrert e-post i Noark.		
Dersom dokumenter skal signeres med elektronisk signatur, bør systemet også tilfredsstille basiskravene til integrert bruk av digital signatur i Noark.	Det er ikke lagt opp til digital signatur i første fase	Ikke relevant
§ 2-2. *Spesialiserte fagsystemer med journalfunksjoner*		
For spesialiserte fagsystemer som har funksjoner for journalføring og arkivering av saksdokumenter, kan det gjøres unntak fra bestemmelsene i § 2-1 dersom systemet er blitt utformet før disse bestemmelsene iverksettes, eller dersom det av andre grunner er urimelig å stille krav om at Noark-standarden skal følges fullt ut. Slike unntak må godkjennes av Riksarkivaren for det enkelte system, jf. meldeplikten i § 4-1.	Omfattes ikke siden dette ikke er relevant for portalen	Ikke relevant
Unntak fra Noark-standarden etter første ledd innebærer at det gis dispensasjon fra arkivforskriften § 2-9 første punktum, jf. arkivforskriften § 1-3. De øvrige bestemmelser om journalføring i arkivforskriften gjelder likevel uinnskrenket, jf. særlig § 2-6, § 2-7 og § 2-10 i arkivforskriften. Dette innebærer bl.a. at alle obligatoriske journalopplysninger skal kunne registreres i systemet. Dokumenter som hører til én og samme sak, eller en annen type gruppering av dokumenter, skal kunne kobles sammen under et felles	Omfattes Under detaljert design må det vurderes hvilken saksbehandling som skal utføres i portalen og hvilke som behandles i bakenforliggende sakssystemer.	OK

nummer.		
Ved eksport for avlevering eller deponering, jf. § 2-4, skal systemet i alle tilfeller kunne produsere et datauttrekk som følger spesifikasjonene i rapporten *Saks- og dokumentoversikt* i gjeldende Noark-standard. I tillegg til denne rapporten kan Riksarkivaren i det enkelte tilfelle bestemme at det skal fremstilles et fullstendig avleveringsuttrekk slik dette er spesifisert i Noark-standarden.	Omfattes Under detaljert design må det vurderes hvilke journaldata som skal avleveres både om sak og journalpost for en avleveringsrapport.	OK
Som ledd i vurderingen av et system kan Riksarkivaren kreve at det blir gjennomført test av prøve på datauttrekk i forhold til spesifikasjonene i Noark-standarden. I denne sammenheng kan organet pålegges å utføre test selv ved hjelp av verktøy som Riksarkivaren distribuerer for dette formålet. Riksarkivaren kan også autorisere andre instanser til å utføre eller administrere slik test.	Omfattes Må innbefattes i testplanen	OK
§ 2-3. *Andre systemer*		
Til elektronisk arkivering av saksdokumenter som ikke kommer inn under bestemmelsene om journalføring i arkivforskriften § 2-6 og § 2-7, kan man benytte systemer som ikke følger Noark-standarden. Systemene må likevel oppfylle de øvrige bestemmelsene i dette kapitlet av forskriften her. Jf. også § 4-1 om meldeplikt.	Trolig ikke relevant	Ikke relevant
§ 2-4. *Eksportfunksjoner*		

Systemet skal kunne eksportere datauttrekk hvor saksdokumentene er tilknyttet overordnede tabeller i samsvar med bestemmelsene i kapittel VIII i forskriften her (for statlige organer) eller kapittel 4 i *Normalinstruks for arkivdepot i kommuner og fylkeskommuner* (for kommunale og fylkeskommunale organer).	Ikke relevant	OK Ikke relevant, se andre ledd.
Bestemmelsene i første ledd gjelder ikke dersom alle dokumenter og opplysninger i systemet tillates kassert etter 10 år eller mindre i medhold av arkivloven § 9.		Ikke relevant
§ 2-5. *Lagringsformater*		
Systemet skal ha funksjoner for å lagre elektroniske saksdokumenter i ett eller flere av de dokumentformater som er spesifisert i Noark-standarden og fastsatt som godkjente arkivformater i kapittel VIII i forskriften her. Kommuner og fylkeskommuner kan gjøre unntak fra denne bestemmelsen dersom andre arkivformater inngår i et samlet opplegg som er godkjent av Riksarkivaren, jf. *Normalinstruks for arkivdepot i kommuner og fylkeskommuner* pkt. 4.1.5.	Omfattes	OK
Bestemmelsene i første ledd gjelder ikke for dokumenter som tillates kassert etter 10 år eller mindre i medhold av arkivloven § 9.		Ikke relevant
§ 2-6. *Lagringsmedier*		
Ved elektronisk arkivering skal det benyttes lagringsmedier	Omfattes	OK

som sikrer at dokumentene blir bevart i tilgjengelig form inntil den formelle avleveringen til offentlig arkivdepot har funnet sted. Når dokumenter arkiveres off-line på bortsatte medier (CD, magnetisk tape), må det foretas kopiering til nye lagringsmedier i god tid før det arkiverte materialet kan bli utilgjengelig eller gå tapt pga. et teknologisk foreldet medium.	Dette må beskrives i kravspesifikasjon for sikkerhet og driftsrutiner når løsningen blir tatt i bruk	
Det skal alltid være minst én ekstra kopi av elektroniske saksdokumenter på en separat lagringsenhet.	Omfattes Krav om sikkerhetskopiering må bli ivaretatt av driftsrutiner	OK
C. Krav til organisering og rutiner		
§ 3-1. *Blandet arkivering av elektroniske dokumenter og papirdokumenter*		
I systemer som følger Noark-standarden, kan det registreres en blanding av elektroniske dokumenter og dokumenter i papirform under forutsetning av	Omfattes	Ok
- at alle journalførte dokumenter innenfor én og samme sak lagres enten elektronisk eller på papir, med visse unntak for vedlegg, jf. Noark	Trolig behov for å søke dispensasjon i en overgangsperiode	Dispensasjon
- og at elektroniske og papirbaserte saker arkiveres i hver sin arkivdel. Dersom det forekommer en blanding av elektroniske dokumenter og papirdokumenter innenfor samme sak, må hele saken arkiveres og avleveres samlet på papir. Sakens	Det vil innebære fysiske saksmapper for saker som ikke har komplett elektronisk arkiv.	Dispensasjon

elektroniske dokumenter regnes da som arbeidskopier. Dersom man praktiserer saksdeling slik det er definert i Noark-standarden, kan man likevel arkivere saksdeler elektronisk selv om saken for øvrig er på papir. Forutsetningen er at slike saksdeler arkiveres i egne arkivdeler som bare har elektronisk materiale.		
I systemer som ikke følger Noark-standarden, skal man bygge på tilsvarende prinsipper. Hovedregelen er at dokumenter som inngår i én og samme sak, eller i en annen type gruppering av dokumenter, jf. § 2-2, skal lagres enten elektronisk eller på papir. Dette gjelder så langt det lar seg gjøre innenfor hensiktsmessige løsninger. Papirbaserte og elektroniske saksdokumenter skal inngå i hver sine klart definerte deler av arkivet (arkivdeler).	Ikke relevant ved bruk av ePhorte	Ikke relevant
All blanding av papirbasert og elektronisk arkivering skal være godt dokumentert i arkivplanen.	Arkivplan må oppdateres under implementeringen	OK
§ 3-2. *Oppbygning og bruk av det elektroniske arkivet*		
Før systemet tas i bruk, skal det være utarbeidet en instruks for organet som beskriver oppbygningen og bruken av det elektroniske arkivet. For bruk av Noark-baserte systemer skal instruksen blant annet spesifisere følgende:	Omfattes Dette må håndteres som en del av instruks eller rutine for arkivering.	OK

1) hvilke kategorier av saker, herunder typer av saksdokumenter, som skal arkiveres elektronisk, og hvilke som eventuelt iht. formkrav i lov- og regelverk eller av andre grunner skal arkiveres på papir, jf. § 3-1	Det må framgå av rutiner som må utarbeides for arkivering	OK
2) hvilke(t) arkivformat(er) som skal brukes	Dokumenter skal inn som PDF	OK
3) dersom dokumenter skal autentiseres med digital signatur: hvilke typer dokumenter som skal autentiseres	Ikke relevant i første omgang	Ikke relevant
4) retningslinjer for å verifisere at skanning av innkomne dokumenter er utført korrekt og komplett, og at dokumentene er lesbare, før det foretas kassasjon av den originale papirversjonen	Dette må være et krav ved innskanning med etterarbeid. Det kan være situasjoner der det er behov for å bestille originaldokument innenfor et bestemt tidsrom	OK
5) retningslinjer for kassasjon av mottatte papirdokumenter som er skannet og arkivert elektronisk	Må legges inn i rutiner	OK
6) en plan for periodisering av arkivet og vedlikehold av det elektroniske materialet inntil det kan avleveres til arkivdepot. For systemer som ikke følger Noark-standarden, skal instruksen oppfylle de samme kravene så langt de er relevante.	Må legges inn i rutiner	OK
Arkivplanen skal inneholde oversikt over arkivstrukturen,	Omfattes	OK

herunder eventuell inndeling i arkivdeler.		
§ 3-3. *Interne ansvarsforhold og rutiner*		
Før systemet tas i bruk, skal det være etablert et apparat og retningslinjer for å administrere og ajourholde brukerrettigheter til systemet. Det skal utarbeides instruks som beskriver følgende ansvarsforhold og rutiner så langt disse er relevante for bruk av systemet:	Omfattes Må spesifiseres i detaljert design og håndteres av autentiseringsmotoren og autorisasjonsmotoren, samt prosessmotor.	OK
1) ansvar for tildeling og ajourhold av brukerrettigheter til registrerings- og arkiveringsfunksjoner	Se over.	OK
2) hvilke spesifikke registrerings- og arkiveringsrettigheter som tildeles ledere og saksbehandlere	Se over.	OK
3) ansvarsforhold og prosedyrer for registrering og arkivering av saksdokumenter som sendes og mottas som e-post	Se over.	OK
4) ansvarsforhold og prosedyrer for konvertering av saksdokumenter til arkivformat, herunder tidspunkt for konvertering	Se over.	OK
5) operatøransvar, arbeidsprosedyre og rutiner for kvalitetssikring ved skanning av innkomne papirdokumenter	Se over.	OK
6) ansvar og rutiner for kvalitetssikring av	Se over.	OK

registreringen og den elektroniske arkiveringen		
7) dersom digital signatur anvendes: regler og rutineopplegg for bruken	Se over.	OK
8) rutiner som definerer opplegg og ansvar for:	Se over.	OK
- fordeling av dokumenter,	Se over.	OK
- retting av registrerte journal- og arkivopplysninger,	Se over.	OK
- avskrivning av ferdigstilte dokumenter,	Se over.	OK
- vurdering av spørsmål vedrørende offentlighet,	Se over.	OK
- registrering av unntak for offentlighet og hjemmel for dette.	Se over.	OK
9) nødprosedyrer for registrering og arkivering til bruk dersom systemet er ute av drift.	Se over.	OK
§ 3-4. *Kopibok*		
For arkivdeler hvor alle egenproduserte dokumenter er lagret elektronisk, kan man sløyfe papirbasert kopibok. For andre arkivdeler skal det føres komplett papirbasert kopibok, jf. arkivforskriften § 3-9.	Ikke relevant	Ikke relevant
Dersom kopiboken i henhold til første ledd sløyfes for en eller flere arkivdeler, skal dette dokumenteres i arkivplanen.	Må beskrives i arkivplan ila prosjektgjennomføringen	OK
D. Rapportering og godkjenning		
§ 4-1. *Meldeplikt for systemer*		
Dersom et offentlig organ planlegger å arkivere elektroniske saksdokumenter i et system som ikke kommer inn	Ikke relevant	Ikke relevant

under godkjenningsordningen etter § 2-1, skal det sendes melding til Riksarkivaren før systemet tas i bruk. Meldingen skal inneholde		
a) systemets offisielle betegnelse (navn)	Se over	OK
b) leverandørens navn og adresse	Se over	OK
c) en kort oversikt over de funksjoner systemet har for registrering og arkivering av elektroniske saksdokumenter	Se over	OK
d) opplysninger om hvilket organ, eventuelt hvilke organer, som skal benytte systemet	Se over	OK
e) opplysninger om formålet med systemet og hvilke saksområder og typer av saksdokumenter det elektroniske arkivet skal omfatte	Se over	OK
f) navn og funksjonsområde for det system som det nye systemet erstatter.	Se over	OK
Riksarkivaren kan i hvert tilfelle kreve å få seg forelagt systemet til godkjenning, jf. § 4-4.	Se over	OK
§ 4-2. *Særskilt rapporteringsordning for statlige organer*		
For statlige organer gjelder meldeplikten etter § 4-1 første ledd også når man tar i bruk systemer som er godkjent etter bestemmelsene i § 2-1. I slike meldinger kan man likevel utelate de opplysninger som er spesifisert under bokstav c.	Omfattes	OK
§ 4-3. *Generell informasjonsplikt*		
Riksarkivaren kan kreve å få seg	Omfattes	OK

forelagt de interne instrukser et offentlig organ har utarbeidet for bruk av elektronisk arkivering, jf. arkivloven § 8.		
§ 4-4. *Godkjenning*		
Dersom systemer eller instrukser som er innrapportert etter bestemmelsene i § 4-1, § 4-2 eller § 4-3, ikke tilfredsstiller kravene i dette kapitlet av forskriften her, kan Riksarkivaren pålegge organet å arkivere sine saksdokumenter på papir.	Omfattes	OK

Vedlegg 2: Innsynsrett

Rett til innsyn i sakens dokumenter.

Fvl. §§ 18 - 21

I tillegg til de opplysningene Vergemålsforvaltningen plikter å fremlegge i henhold til fvl. § 17, kan søkeren /fullmektigen be om å få gjøre seg kjent med sakens øvrige dokumenter. Notater som er gjort i forbindelse med møter, andre samtaler eller telefonsamtaler er å betrakte som vanlige dokumenter, som parten i utgangspunktet har rett til innsyn i.

Formålet med regelen

Innsynsretten (partsoffentligheten) skal sikre at parten får ivaretatt sine interesser, og samtidig gjøre det mulig for han å bidra til at saken blir opplyst.

Begrensninger i innsynsretten

Fra hovedregelen om at det kan kreves innsyn i alle sakens dokumenter, gjør loven flere begrensninger.

- Ifølge fvl. § 18 annet ledd, bokstav a), b) og c) og § 19 er det noen dokumenter søkeren ikke kan kreve innsyn i, men hvor man kan gi parten adgang til dokumentinnsyn.
- Etter § 19 første ledd, bokstav c, har parten ikke rett til å gjøre seg kjent med opplysninger hvor det er utilrådelig av hensyn til hans egen helse eller forhold til personer som står han nær.

I saker om attføringspenger og attføringsstønad vil ofte en legeerklæring om fysisk eller psykisk helse være av sentral betydning. Det kan i enkelte tilfeller være skadelig for personen å få nærmere opplysninger om sin sykdom eller om forholdet til sine nærmeste.

Hva som er "utilrådelig" å la vedkommende få vite, er et skjønnsspørsmål. Det er viktig for parten å kunne gjøre seg kjent med egen sak og de opplysningene vi bygger avgjørelsene på. Vergemålsforvaltningen bør derfor være varsom med å anvende unntaksregelen. Vergemålsforvaltningen kan i tilfelle rådføre seg hos den som har gitt opplysningene, f.eks. behandlende lege. Dersom unntaket anvendes, kan likevel parten be om at en representant får se opplysningene.

Unntaket fra rett til innsyn i fvl § 19 første ledd bokstav c) gir ikke vern om kildens identitet. Vergemålsforvaltningen kan derfor ikke garantere kildevern overfor den som gir opplysninger om en part.

Unntaksvis kan en gi begrenset kildevern etter fvl § 19 annet ledd bokstav b), men dette unntaket gjelder ikke der innsyn er av vesentlig betydning for parten. Det er som regel av vesentlig betydning for en part å kunne kontrollere opplysningenes innhold og kvalitet, herunder opphavet til opplysningene.

Vedlegg 3: Skala for beskyttelsesbehov

Klasse	Kriterier
EKSTRA HØYT **(SAMFUNNS-KRITISK)**	*Samfunnsinteresser* - bortfall av systemer eller tjenester berører i stor grad samfunnets funksjonsevne. Betegnes som *samfunnskritisk.* *Offentlige interesser* - særdeles store økonomiske tap (svarende til ca 1000 mill kroner) *Etatens interesser* - bortfall av systemer eller tjenester har fatale konsekvenser for etatens funksjonsevne på flere virksomhetskritiske tjenesteområder (*kritisk for etaten*). *Personer* - livstruende skader for mange personer eller store belastninger for svært mange
HØYT **(VIRKSOM-HETSKRI-TISK)**	*Samfunnsinteresser* - bortfall av systemer eller tjenester berører i noen grad samfunnets funksjonsevne. Kan betegnes som *mindre samfunnskritisk.* *Offentlige interesser* - meget store økonomiske tap (svarende til ca 100 mill kroner) *Etatens interesser* - bortfall av systemer eller tjenester berører i stor grad etatens funksjonsevne. Betegnes som *virksomhetskritisk*. - langvarig, betydelig svekket renommé og tillit for etaten *Personer* - livstruende skader for flere personer, store belastninger for mange

Klasse	Kriterier
MIDDELS	*Offentlige interesser* - store økonomiske tap (svarende til ca 10 mill kroner) *Etatens interesser* - betydelig skade på etatens renommé - alvorlig skade for etatens arbeid eller effektivitet *Personer* - livstruende skader for en enkelt person - fysisk eller psykisk skade på helse til en gruppe personer - alvorlig belastning for et lite antall personer, for eksempel brudd på taushetsplikt - belastning for mange, men som er av en slik art at personene kan tåle den.
MODERAT	*Offentlige interesser* - middels store økonomiske tap (svarende til ca 1 mill kroner) *Etaten* - skade på etatens renommé - skade for etatens arbeid eller effektivitet *Personer* - mindre skade på fysisk eller psykisk helse - belastning for noen få personer - mindre belastning for mange
LAVT	*Offentlig økonomi* - mindre økonomiske tap (svarende til ca 100 000 kroner) *Etaten* - mindre skade på etatens renommé - mindre skade for etatens arbeid eller ansattes arbeidssituasjon *Personer* - mindre belastning for få, det kan gjelde arbeidsbyrde eller personlig belastning for medarbeidere