Rammeverk for formulering av portable krav til informasjonssikkerhet

Morten Ween

Masteroppgave
Master i informasjonssikkerhet
30 ECTS
Institutt for informatikk og medieteknikk
Høgskolen i Gjøvik, 2005

Masterprogrammet i informasjonssikkerhet
har blitt kjørt i samarbeid med
Kungliga Tekniska högskolan (KTH),
Stockholm, Sverige

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

When information is exchanged in a network, or different entities are accessing the same information through the network, the various actors will manage and describe information security requirements and precautions in different ways. The information itself will, however, maintain the security needs after being transferred or a shared access is opened. For this reason, it is important to be able to transfer knowledge about security requirements for the data. This would contribute to ensure that usage and handling of the data are in accordance with the conditions set prior to transferring the data.

We have suggested a structure for describing metadata for security requirement. Metadata is used to structure elements of the security requirements, services, mechanisms or procedures. A requirement specification is formulated by assembling the wanted security requirements in a unified structure. By using a unified formulation and structure, security requirements from different environments may be made comparable. We have used categories of security requirements based on level of formality, specification type, and requirement type as described in the standard PrENV 13608 for Security for Healthcare Communication, but have extended the uniform structure in the formulation of the security requirements.

Sammendrag

Når data skal utveksles i et nettverk, eller det skal gis delt tilgang til data fra forskjellige systemer tilknyttet nettverket, vil aktører i forskjellige deler av nettet håndtere og beskrive sikkerhetsspørsmål på forskjellige måter, mens dataene vil ha de samme behov for sikkerhet etter at de er overført eller gjort tilgjengelig i det nye systemet. Det er derfor viktig at informasjon om sikkerhetskrav for data kan overføres til andre virksomheter. Det vil det kunne sikre at behandlingen der er i samsvar med forutsetningene for å overføre eller tillate bruk av informasjonen.

Vi foreslår her en struktur for å beskrive metadata for sikkerhetskrav. Metadata brukes for å strukturere elementene i sikkerhetskrav, -tjenester, -mekanismer eller -prosedyrer. En kravspesifikasjon formuleres ved at de ønskede sikkerhetskrav samles i en enhetlig struktur. Ved å benytte en enhetlig formulering og strukturering vil sikkerhetskrav fra ulike omgivelser kunne gjøres sammenlignbare. Vi har benyttet en inndeling av sikkerhetskrav etter formaliseringsnivå, spesifikasjonstype og kravtype som er beskrevet i standarden PrENV 13608 for sikkerhet for kommunikasjon i helsenett. Vår metadatastruktur bruker denne inndelingen, men går videre i å formulere sikkerhetskravene på en enhetlig måte.

Innholdsfortegnelse

Illustrasjonsliste

Tabelliste

1 Introduksjon

Høringsutkast for «Norm for informasjonssikkerhet i helsesektoren»[SHdir]:

> «Stadig mer av arbeidet i helsesektoren er basert på elektronisk behandling av pasientenes opplysninger. Likeledes foregår en stadig større andel av kommunikasjonen mellom virksomhetene elektronisk.
>
> Den økende elektroniske behandlingen av opplysninger gir muligheter, men skaper også utfordringer for informasjonssikkerheten hos virksomhetene. Elektronisk behandling medfører blant annet at opplysningene enklere og raskere kan gjøres tilgjengelig både internt i en virksomhet og eksternt utenfor virksomheten. Dette er en fordel forutsatt at opplysningene kun gjøres tilgjengelig for rett vedkommende til rett tid. Det kan imidlertid få utilsiktede konsekvenser for opplysningenes konfidensialitet, og særskilte tiltak må iverksettes for å sikre at uvedkommende ikke får tilgang til opplysninger som er lagret elektronisk. Det er behov for mekanismer som gir tillit til at alle aspekter ved informasjonssikkerhet er tilfredsstillende ivaretatt hos de aktuelle virksomheter.»

1.1 Bakgrunn

Med en stadig økende elektroniske samhandling i samfunnet vil behovet for å kunne kommunisere egne og forstå andres krav til og implementering av informasjonssikkerhet være stadig større. Sitatet ovenfor illustrerer at opplysninger som tidligere ville bli behandlet i avgrensede omgivelser vil nå kunne overføres til eller nås fra en rekke ulike miljøer. I omgivelser hvor nettverk blir stadig mer integrert, og samhandling mellom systemer og delt tilgang til eller utveksling av data blir stadig mer utbredt, får vi et økende behov for å kunne sikre at data blir gitt en riktig beskyttelse når de flyttes mellom domener med heterogene systemer og ulik implementering av sikkerhetstiltak.

Dette er også påpekt i rapporten «Persondata-utveksling i Norge [daVin]» hvor det sies at «Det er en mangel på oversikt og struktur i persondata på et nasjonalt nivå», og «Bruk av metadata i persondataregistere og i utveksling vil gi nye muligheter til å styre tilgang». Når strukturert informasjon om sikkerhet mangler vil sammenligning av sikkerhet i ulike perspektiver lett bli en ad-hoc øvelse.

Sikkerhetskrav vil være en del av spesifikasjonene i de fleste informasjonssystemer. Som regel beskrives sikkerhetsegenskaper ut fra en «beste praksis» for formulering og definisjoner. Ved anskaffelse eller utvikling av en IT-løsning kan man velge å stole på leverandøren, teste systemet og funksjoner selv, eller man kan få en tredjepart til å gjøre en evaluering. I beste fall er da sikkerhetsfunksjoner beskrevet slik at de kan sammenlignes med kravene. Det finnes flere standarder og anbefalinger som definerer begreper og beskriver krav til håndtering av informasjonssikkerhet. Dette har imidlertid ikke ført til at beskrivelser av informasjonssikkerhet kan sies å være sammenlignbare mellom systemer, organisasjoner og formål i særlig grad. Dersom løsninger må tilpasses eller utvikles for formålet, vil de fleste brukere ha manglende

forutsetninger for å vurdere om løsningen møter kravene [dent]. Det samme gjelder når man knyttes opp mot et nytt nett.

Standarder for evalueringskriterier for informasjonssikkerhet har utviklet seg over flere stadier, fra Orange Book [TCSEC] og ITSEC [ITSEC] til Common Criteria [CC]. Nyere metoder eller standarder for vurdering av krav til sikkerhet har i stor grad sine røtter tilbake i disse. NS-ISO/IEC 17799 [17799] gir anbefalinger for administrasjon av informasjonssikkerhet, og er rettet mot organisasjonens sikkerhetspraksis. Standarden beskriver ikke krav til informasjonssikkerhet eller hvordan sikkerhetskrav skal beskrives. Også OECD har gitt retningslinjer for sikkerhet i informasjonssystemer og nettverk [OECD]. Disse har til hensikt å bidra til å etablere en sikkerhetskultur og å være en referanseramme for forståelse av informasjonssikkerhet.

I helsesektoren, som har et omfattende sett av lover og forskrifter å forholde seg til, er det utarbeidet standarder, normer og anbefalinger for flere ulike aspekter ved informasjonssikkerhet. Det er en rekke aktører, både som leverandør, kunde, pasient, helseforetak, myndighet m.m. som har befatning med eller påvirkes av spørsmål om informasjonssikkerhet. Det er likevel ikke utviklet og tatt i bruk noe enhetlig rammeverk for formulering av sikkerhetskrav på tvers av organisasjoner og systemer. En del eksempler på ulike aktører, systemer og juridiske kilder og deres tilnærming til informasjonssikkerhet og personvern i helsevesenet er beskrevet i Vedlegg A.

1.2 Problemformulering

Når data skal utveksles i et nettverk, eller det skal gis delt tilgang til data fra forskjellige systemer tilknyttet nettverket, vil aktører i forskjellige deler av nettet håndtere sikkerhetsspørsmål på forskjellige måter. De data som behandles vil likevel ha samme behov for sikkerhet etter at de er overført eller er gjort tilgjengelig i et nytt system. Når data overføres til andre steder enn der de opprinnelig har vært registrert eller generert, må det kunne knyttes overførbar informasjon til dataene som sikrer at de blir tilfredsstillende behandlet i forhold til de sikkerhetskrav som gjelder for disse dataene. Overføring av pasientdata mellom sykehus og primærhelsetjenesten er et eksempel på dette. En rekke verktøy og metoder er utviklet for å kunne gjennomføre risikoanalyser. Mangel på en enhetlig struktur for å beskrive sikkerhetsbehov og sikkerhetstiltak gjør sammenligning mellom forskjellige tilfeller vanskelig.

Det juridiske rammeverket for informasjonssikkerhet og personvern er omfattende og komplisert. Det finnes en rekke standarder, anbefalinger og protokoller som er relevante i forbindelse med implementering av sikkerhetstjenester. Selv om lover og forskrifter gjelder for alle aktører innen et område, vil ikke alle anvendelser dekke hele området, og heller ikke vil nødvendigvis alle regler være relevante. Noen aktører vil også kunne ha tilleggsbehov eller behov for unntak fra det normale. Hvilke sikkerhetskrav som gjelder vil da være avhengig av bruksområdet, og det vil være behov for å referere sikkerhetskrav til sikkerhetsbehov med ulike opprinnelser.

Man vil kunne ha behov for å kunne sammenligne sikkerhetskrav for et datasett med implementerte rutiner, tjenester og mekanismer i vertssystemet for å sikre

overensstemmelse. Det kan være behov for å sammenligne alternative systemløsninger for å finne en optimal implementering, med tanke på kost, ytelse, funksjonalitet og brukervennlighet. Det er i dag ikke etablert et felles rammeverk som dekker disse behovene. Både kunder, leverandører og systemansvarlige i forskjellige organisasjoner vil kunne ha nytte av å gjøre slike sammenligninger. De vil kunne ha en felles referanseramme og metode for å beskrive og verifisere sine sikkerhetsbehov eller løsninger og å finne en optimal konfigurasjon.

Vårt overordnete forskningsspørsmål er:

- Hvordan etablere et enhetlig rammeverk for formulering av sikkerhetskrav for informasjon slik at også kravene kan overføres til andre omgivelser når dataene skal overføres?

Underliggende spørsmål er:

- Hvordan definere metadata for elementer i et sikkerhetskrav?
- Kan et datasetts eller systems sikkerhetsprofil uttrykkes gjennom rammeverket?
- Hvordan benytte rammeverket for å sammenligne sikkerhetskrav med sikkerhetspolicy, prosedyrer og sikkerhetstjenester for ulike systemer og omgivelser?

1.3 Mål

Målet med oppgaven er å definere et forslag til rammeverk for å kunne formulere sikkerhetskrav knyttet til de sikkerhetsbehov et sett med, eller en type, data vil ha. Sikkerhetskravene skal kunne overføres til andre omgivelser slik som de data de er ment å spesifisere sikkerheten for. De overførbare sikkerhetskravene skal kunne brukes som referanse i en risikoanalyse for å undersøke om implementerte sikkerhetstiltak i et IT-system og dets omgivelser er tilstrekkelige for å ivareta dataenes sikkerhetsbehov.

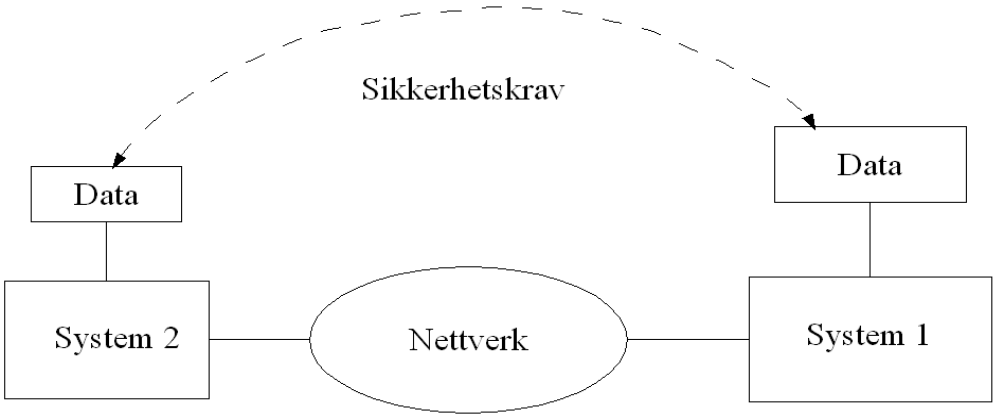
Basert på dette rammeverket skal det kunne utvikles metoder for å sammenligne ulike krav, policyer, implementeringer o.l. for å verifisere overensstemmelse, avdekke avvik eller for å optimalisere eller velge løsninger. Slike metoder vil også kunne være grunnlag for å kartlegge konsekvenser av endringer i krav eller løsning.

selv om det er beskrevet fra ulike perspektiver, for ulike formål og i ulike organisasjoner.

1.4 Formål og omfang

Formålet med undersøkelsen er å kunne formulere informasjon om krav om sikkerhet for en datamengde slik at informasjonen knyttes til de modulene med informasjon som behandles, ikke til systemet som behandler dem. Dette for at sikkerhetskrav skal kunne overføres fra et system til et annet, uavhengig av systemets karakteristika. Sikkerhetskrav knyttet til en datamodul må kunne sammenlignes med et systems

sikkerhetsegenskaper. Spørsmålet om en egnet formulering av sikkerhetskrav er oppgavens kjernespørsmål og er grunnleggende for å kunne gjennomføre en sammenligning av ulike krav og løsninger.



Figur 1: Datasentrisk perspektiv. De samme sikkerhetskrav skal gjelde for et sett med data, enten de behandles i System 1 eller System 2 eller på tvers av nettverket.

Et sett med data vil ha det samme krav på beskyttelse enten det behandles i det ene eller det andre systemet. Når data flyttes i et nettverk med heterogene systemløsninger, eller det er tilgang til dataene fra slike forskjellige systemer, vil det ikke være tilstrekkelig å forsikre seg om at opprinnelsessystemet har tilstrekkelig god sikkerhet. Et sett med data vil også kunne flyttes fra system nummer to og videre til et tredje system hvis dokumentasjon på sikkerhetskravene som er lagret sammen med de definerte dataene kan overføres og sikkerheten kan tilfredsstilles i henhold til disse kravene. Man må da beskrive sikkerhetskrav i et datasentrisk perspektiv.

Alle systemer som skal ha tilgang til et sett med data må tilfredsstille disse dataenes sikkerhetskrav. Andre systemer med tilgang til de aktuelle dataene kan fungere som en sidekanal med et annet sikkerhetsnivå. Man kan da f.eks. tenkes å tillate at et system med strenge sikkerhetskrav likevel tillater at et annet system med mindre strenge sikkerhetskrav får tilgang til eller overført et gitt sett med data, fordi disse dataenes sikkerhetskrav ikke er strengere enn at de likevel tilfredsstilles i det nye systemet. At dette vil kunne representere en sikkerhetsrisiko for systemet og andre data med strengere sikkerhetskrav i det opprinnelige systemet, er et spørsmål som ikke diskuteres her. Det er behandlet i andre sammenhenger, som f.eks. Mandatory Access Control problematikk og flernivåsikkerhet [goll].

De verdier (assets) man ønsker å beskytte er som regel dataene selv, og disse vil avgjøre kravene til sikkerhet gjennom sine sikkerhetsbehov. Hvis man har en eller flere typer data med ulike sikkerhetsbehov, vil man med en enhetlig struktur for kravene kunne sammenligne disse og alternative implementeringer av systemer, policy og rutiner. Dette forutsetter at sikkerhetskrav og sikkerhetsegenskaper kan defineres med felles referanser og i en felles struktur for ulike systemer, anvendelser og

organisasjoner.

Når krav og løsning eller egenskaper kan sammenlignes, vil det være et grunnlag for å velge optimal løsning i implementeringen ut fra de behovene som er identifisert. Slike sammenlignbare fremstillinger vil også kunne benyttes som utgangspunkt for å karakterisere godheten eller styrken i en sikkerhetstjeneste, og sammenligne denne med styrken eller viktigheten i et krav. Dette vil også kunne danne utgangspunkt for å karakterisere og følge løsningers sikkerhetsnivå gjennom definisjon av metrikker.

Sammenlignbare beskrivelser med gradering av krav og egenskaper vil kunne være grunnlag for å dokumentere overensstemmelse med krav, eller mangel på dette. Dette vil kunne gjøres på et detaljert nivå eller aggregeres til en konklusjon på om et gitt sett med data har tilfredsstillende beskyttelse i et gitt system. Sammenlignbarhet og kvantifisering vil gir grunnlag for:

- klarhet i krav med reell enighet uten usikkerhet rundt tolkninger,
- kriterier som kan kontraktfestes,
- prioriteringer og
- evaluering av prosesser, strategier, arkitekturer o.l. som skal understøtte sikkerhetstiltak [gilb].

Vi har i kapittel 4 beskrevet en inndeling av sikkerhetskrav. Kapittel 5 beskriver en metadatastruktur for elementer i et sikkerhetskrav. Kapittel 6 beskriver noen mulige anvendelser av kravspesifikasjoner formulert gjennom et enhetlig rammeverk.

1.5 Avgrensning

Vårt mål er å beskrive et rammeverket med en struktur og en metodikk for å formulere overførbare sikkerhetskrav for et sett med, eller en type, data. Disse kravene skal gjelde selv om dataene flyttes. Vi har ikke forsøkt å definere tilsvarende strukturer for systemer og kommunikasjonskanaler. Vi har tatt utgangspunkt i sikkerhetskrav for personopplysninger uten å teste våre modeller på andre typer datas sikkerhetsbehov, men har ikke begrenset oss prinsipielt til persondata.

Som eksempel på bruk av strukturen og metoden har vi benyttet kildemateriale som er hentet fra helsevesenet, men vi har søkt å unngå å eksempler som ikke vil være relevante utenfor helsevesenet. De sikkerhetskrav vi har inkludert er ikke ment å være utfyllende da det vil finnes et utall ulike behov i forskjellige miljøer og anvendelser. Flere sikkerhetskrav og egenskaper vil derfor måtte tilføres de oversikter vi har foreslått i oppgaven. Vårt mål har vært å finne frem til generiske prinsipper.

Vi har skissert metoder for å sammenligne sikkerhetskrav med egenskaper i systemer eller med hva som kan oppnås gjennom prosedyrer. Dette forutsetter en metrikk eller nivåbeskrivelse av en eller annen type. Det har ikke vært vårt mål å utvikle slike målekriterier. Vi har inkludert dette kun for å illustrere en mulig anvendelse av strukturen for formulering av sikkerhetskrav.

2 Metode

I dette kapittelet diskuteres metodevalg for oppgaven.

Et utvalg av dokumentasjon på forskjellige systemers og organisasjoners informasjonssikkerhet, lover og forskrifter, policyer, kravspesifikasjoner og system- og applikasjonsbeskrivelser vil være et egnet forskningsobjekt for formålet, sammen med standarder og ulike anbefalinger for håndtering av informasjonssikkerhet. Kildematerialer kan finnes hos leverandører av EPJ-applikasjoner[1], sykehus, IT-faglige miljøer, forskningsmiljøer som arbeider med informasjonssikkerhet og helseinformatikk, lover og forskrifter, standardiseringsorganisasjoner, offentlige myndigheter, tidligere master- og PhD-oppgaver og kilder på Internett. Materialet bør hentes fra ulike typer kulturer for å dekke forskjellige behov, og bør representere tverrfaglighet hvor både juss, sikkerhetsledelse og teknologi er med og beskriver sine premisser. Et utvalg eksempler på beskrivelse av sikkerhetskrav trenger ikke nødvendigvis være uttømmende, men må være tilstrekkelig differensiert og dekkende for formålet med oppgaven.

En case-undersøkelse vil kunne være intensiv ved at den går i detalj på de enkelte utvalgte objekter, ser på flest mulig egenskaper og betrakter dem i et helhetsperspektiv. Men ved at også overlappende kilder benyttes, vil undersøkelsen kunne få ekstensive trekk hvor det blir brukt flere objekter av samme type for å identifisere trender eller typiske parametere. For å gjennomføre en ekstensiv analyse må et stort nok utvalg av dokumentasjon av likeartede systemer, applikasjoner eller organisasjoner gjennomgås. Det vil være nødvendig for å kunne trekke generaliserte konklusjoner, og f.eks. etablere et representativt utvalg av objekter i form av ulike standardiserte sikkerhetskrav.

For strukturering av arbeidet vil det være hensiktsmessig å dele dette i flere faser.

- å identifisere, klassifisere og beskrive et eksempelsett med sikkerhetskrav som vil være basis for det videre arbeidet.
- å definere en felles struktur eller pseudosyntaks for å beskrive sikkerhetskravene, selv om disse skulle ha ulik formaliseringsgrad og anvendelse.
- å skissere en metodikk for å kunne vurdere sikkerhetskrav av ulik type opp mot hverandre.
- å gjennomføre en utprøving av om resultatene er anvendbare i reelle eksempler.

For å kunne bekrefte anvendbarheten av resultatene vil det være nødvendig å bruke reelle testtilfeller, f.eks. fra helsevesenet. Helsevesenet har et stort spekter av aktører, behov og mulige løsninger. Helsevesenet har strenge juridiske og etiske krav knyttet til sine aktiviteter, og det er et velutviklet, men komplekst, regulatorisk regime for

1 EPJ – Elektronisk pasientjournal

området. Etablerte norske og internasjonale miljøer har arbeidet med problemstillinger rundt IT i helsevesenet i en årrekke og det er gjennomført flere forskningsprosjekter i miljøene.

Den type kilder som er aktuelle for vårt tema vil inneholde få kvantitative elementer (utover detaljer som f.eks. antall bit i krypteringsnøkler), informasjon finnes som tekst eller referanser til dokumenter og standarder. En undersøkelse vil derfor bli deskriptiv, uten målinger, eksperimenter eller sammenlikninger mellom systemer eller andre data. Intervjuer for utfyllende informasjon om praksis og erfaringer kan være supplerende, men spørreundersøkelser eller innsamling av empiriske data synes ikke å ville gi viktig informasjon med vår avgrensing av oppgaven. En kvantitativ analyse vil derfor være uaktuell, en kvalitativ analyse synes langt bedre egnet for formålet. Kvalitative metoder er i sin natur tolkende[cres] og derfor velegnet for å sammenligne ikke kvantifiserbar informasjon fra og om ulike miljøer. Det vil være et mål å gjøre tolkningsrommet så lite som mulig for å oppnå repeterbare og sammenlignbare formuleringer og et rammeverk som vil fungere disiplinerende, og det vil være ønskelig å finne frem til kriterier eller karaktertrekk som gir mest mulig presise klassifiseringer av de parametere vi behandler.

Når det ved starten av arbeidet er ukjent hva slags struktur for sikkerhetskrav som ville kunne brukes, vil det være en kritisk aktivitet tidlig i analysen å finne frem til en egnet referansestruktur. I en tidlig fase av arbeidet vil en induktiv tilnærming for å identifisere strukturer og karakteristika kunne føre frem til mulige løsninger for de definerte problemene. Når hovedstrukturen er beskrevet, må den så verifiseres til å være presis nok for formålet. Arbeidet vil da anta en mer deduktiv karakter for å supplere strukturen med et rikere utvalg av eksempler på sikkerhetskrav.

Med en anvendbar struktur for å klassifisere og organisere sikkerhetskrav på plass, vil det være nødvendig å beskrive elementene i et krav på en enhetlig måte. Dette må gjøres med et datasentrisk utgangspunkt, en metode må lede frem til å beskrive sikkerhetsbehovene for den informasjonen som skal beskyttes. Valg av struktur vil i seg selv ikke være knyttet til spesielle krav, så lenge de ønskede metadata kan fremstilles slik at de kan brukes som byggestener i en strukturert kravspesifikasjon. Basert på denne strukturen skal en kunne knytte sikkerhetskrav til informasjon som skal kunne benyttes i andre systemer enn der de opprinnelig ble registrert, på en slik måte at forsvarlig behandling og sikkerhet kan ivaretas.

For å kunne dokumentere om f.eks. et tiltak gir god nok sikkerhet i forhold til et gitt krav, eller å kunne sammenligne to systemers sikkerhetsprofiler eller sikkerhetsnivåer, må man kunne sammenlikne sikkerhetskrav med hverandre. Det kan også være egenskaper fremstilt i andre perspektiver eller på andre abstraksjonsnivåer. For dette formålet vil det være nødvendig å definere en metode for å tilordne ulike krav og egenskaper et sikkerhetsnivå. Dette kan så være grunnlag for å bestemme om et krav er dekket eller hvilken løsning som er optimal. Tidligere masteroppgavebesvarelser ved HiG har foreslått forskjellige tilnærminger til å definere metrikker for informasjonssikkerhet. Vårt mål ville ha vært å kunne angi en metode som var

datasentrisk og som kunne brukes for å sammenlikne kriterier med forskjellig grad av formalisme og på forskjellig nivå i et hierarki, men dette ligger utenfor oppgavens ambisjon.

Tradisjonelt har beskrivelse av informasjonssikkerhet vært prosess- eller produktorientert. De fleste risikoanalyser tar utgangspunkt i en «asset», eller verdi, men går så over til å beskrive systemets sårbarheter, trusselbildet og konsekvenser ved eventuelle sikkerhetshendelser for å definere en risiko. For at spesifikasjon av sikkerhetskrav for et datasett skal kunne relateres til beskrivelser av system- og applikasjonssikkerhet, må metodikken kunne overføres til å beskrive såvel krav og behov som løsning i ulike former. Når informasjon flyttes fra en omgivelse til en annen vil fortsatt behovet for å beskytte informasjonen være det samme, men beskrivelsen av hvordan dette ivaretas i miljøet er endret. Dette peker mot en objektorientert, datasentrisk tilnærming, fordi det er informasjonen selv som har et beskyttelsesbehov, men strukturen for formulering av krav må også gi mening i et perspektiv for beskrivelse av systemegenskaper.

3 Kunnskapsfronten – annet arbeid

Dette kapittelet behandler krav til spesifikasjon av informasjonssikkerhet og metoder for dokumentasjon av sikkerhetskrav og -egenskaper. Metrikker eller sammenligning av sikkerhet er i liten grad dekket da det er perifert i oppgaven. Først beskrives eksempler på hvordan sikkerhetskrav og -egenskaper ofte beskrives, og hvorfor dette ikke uten videre vil være anvendbart for vår beskrivelse av datasentrisk sikkerhetskrav. Vi beskriver så relevante arbeider som kan bidra til å løse vårt problem og de begrensninger som ligger i disse arbeidene.

3.1 Beskrivelse av sikkerhet

Krav til dokumentasjon av informasjonssikkerhet finnes i de enkelte virksomheters egne kravspesifikasjoner og gjennom myndighetenes krav i virkemidler som er utviklet som generiske styringsverktøy for myndighetene [scha] og aktivitetsorienterte prioriteringer som operasjonaliseres gjennom IT-politikken [lima]. I tillegg kommer spesiallover og forskrifter som inneholder krav om eller har konsekvenser for håndtering av informasjonssikkerhet. Personopplysningsloven [Pol] og -forskriften [Pof] gir konsekvenser i form av krav til sikkerhet i IT-systemer som behandler personopplysninger. Langt på vei har ikke anbefalte offentlige tiltak for samordning for bedre informasjonssikkerhet vært fulgt opp i regulatoriske pålegg og sanksjoner [haug]. Lovverket inneholder derfor en rekke forskjellige tiltak for de ulike områder av samfunnet. Koordineringsutvalget for informasjonssikkerhet [KIS] har som mål at regelverket skal videreutvikles på en samordnet og oversiktlig måte.

Felles for regulatoriske krav og føringer er at selv om de er bindende for aktørene er de uformelle i sin struktur. Det er derfor nødvendig å fastslå praktiske konsekvenser for de enkelte situasjoner. Heller ikke Sikkerhetsloven [Sikl] og Forskrift om sikkerhetsadministrasjon [Sikf] er detaljerte i å beskrive konkret hvordan tiltak skal gjennomføres for å oppnå tilfredsstillende informasjonssikkerhet, selv om de går langt i å kreve spesifikke tiltak implementert. Det regulatoriske materialet gir få føringer som kan brukes for å holde sikkerhetskrav og tiltak opp mot hverandre i praktiske anvendelser. Metadata for sikkerhet er i begrenset omfang regulert [scha], men berøres i f.eks. arkivforskriften [Arkf] som setter krav til dette for langvarig arkivering.

Tradisjonelt retter mange arbeider innen informasjonssikkerhet seg mot et avgrenset system, men omhandler alt i systemet (data, HW, SW og ulik fasiliteter i systemet) og ikke primært mot den informasjonen som flyter i systemet. Informasjonssikkerheten behandles da i et systemperspektiv eller et organisatorisk perspektiv og ikke et datasentrisk, selv om det primært er dataene som har et beskyttelsesbehov. Dette gjenspeiles i at en sikkerhetspolicy ofte i hovedsak fokuserer på rutiner, personell og fysisk sikring. Militær sikkerhetstenkning har hatt fokus på konfidensialitet fremfor integritet og tilgjengelighet [bygr], og systemets og organisasjonens evne til å sikre konfidensialitet har vært et sentralt kriterium. Kravspesifikasjoner omhandler gjerne systemarkitekturer, kommunikasjonskanaler eller funksjonalitet.

Applikasjonsspesifikasjoner beskriver typisk funksjoner som gir tilgang til sikkerhetstjenester, men uten å spesifisere tjenesten [fire]. For mange anvendelser er dette en egnet tilnærming, hvis det kan omfatte eller være relevant for alle omgivelsene som inngår i en aktørs behandling av data.

Med stadig flere ulike brukere med heterogene nettverk og IT-strukturer som knyttes sammen over en felles infrastruktur, vil det være lite hensiktsmessig å skulle ha en altomfattende sikkerhetspolicy for alle involverte aktører, selv i et så regulert område som helsevesenet, eller å kreve at alle aktører implementerer den samme policyen. Det er derfor behov for strukturering og gjenbruk av spesifikasjoner. Sikkerhetskrav omfatter et sett med subfaktorer med begrenset omfang som til sammen utgjør kravet, og ofte vil mange sikkerhetskrav være lik hverandre selv om applikasjonene er ulike [fire2]. Gjenbruk vil kunne skje på tvers av applikasjoner p.g.a. de generiske subfaktorene i kravene. Han foreslår en mal hvor det gjennomgående angis hva et tiltak består i, hva det skal beskytte, mot hvilken skade, mot hvilken trussel, hvordan det gjennomføres og krav til målbarhet.

Ved en risikoanalyse vil en overordnet gjennomgang av risikobildet normalt gi en kvalitativ beskrivelse av sikkerhetssituasjonen. Kvantitative verdier, som f.eks. frekvens eller sannsynlighet, kan tilordnes de kvalitative konklusjonene [Elvi]. En todimensjonal matrise med verdier for sannsynlighet og konsekvens som uttrykk for en samlet risiko, kan da gi en representasjon av risikonivået gjennom innplassering av den enkelte trussel.

Sannsynlighet \ Konsekvens	4	3	2	1
4				K2.7, K5.1, T1
3			K2.4, T2, T3	K2.2, T4, T5, I1
2			K7.3, K2.1, K2.3, K2.5	
1		K1.1, K1.2, K1.3, K1.4, K1.5, K1.6, K3.3, K5.2, K7.1, K7.4, I5	K1.7, K2.6, K5.3, K6.1, K7.2, I3, I4	K3.1, K3.2, K6.2, K6.3

Figur 2: Eksempel på visning risikonivå som av resultat fra risikoanalyse . Høyt nivå på sannsynlighet og konsekvens gir høy risiko (mørke felt).*(Kilde: NST)*.

Trusler kan beskrives på et generelt nivå eller de kan detaljeres ved f.eks. å knytte dem til en mulig svakhet i systemet [dale]. En slik risikoanalyse gir en systemorientert beskrivelse av sikkerhetsbildet. Et rammeverk for analyse og håndtering av sikkerhetshendelser er beskrevet av [Ell.mf] med utgangspunkt i trusselbilder, respons og motstandskraft mot trusler for å kunne vurdere en arkitekturs motstandsevne mot angrep.

For kommunikasjonsløsninger er sikkerhet ofte knyttet til kryptering, signaturer, algoritmer, loggføring, kvitteringer og nøkkelhåndtering [KITH]. Selv om standarder og metoder er velkjente, er ikke beskrivelse av sikkerhet, implementering og krav standardisert, men angitt i prosa eller oppsett som er forskjellig fra tilfelle til tilfelle. Kravspesifikasjoner for sikkerhet i IT-systemer er en forutsetning for å strukturere, implementere og drifte større nettverk, ofte med flere heterogene løsninger. Spesifisering av slike krav er normal et ansvar for IT-ansvarlig, som f.eks. i [ØNH], og vil være styrende for alle som benytter og har tilgang til systemet eller leverer utstyr og tjenester. Det er ingen normgivende struktur for slike kravspesifikasjoner eller for drifting av IT-systemer. Mange vil regne overensstemmelse med ISO/NS 17799 [17799] som en forutsetning for tilfredsstillende sikkerhetsledelse, uten at det sies hvordan noe skal implementeres. ISO/IEC 10181 Security Framework [10181] beskriver et sikkerhetsrammeverk for åpne systemer som kan benyttes som grunnlag for å utarbeide en sikkerhetsarkitektur eller kravspesifikasjon ut fra behov i systemet. Men standarden angir ikke formater for beskrivelse av sikkerhetsaspekter. Tilsvarende beskriver ASTM [ASTM] et rammeverk for beskyttelse av helseinformasjon som adresserer både lagring og overføring, men uten å behandle formulering av sikkerhetskrav. De gir også en oversikt over en rekke sikkerhetsrelevante standarder, særlig innen sikker kommunikasjon. Den amerikanske Health Insurance Portability and Accountability Act (HIPAA) «Secutity Rules» bygger på publikasjoner fra NIST[2] og beskriver krav til konfidensialitet, integritet og tilgjengelighet på policynivå, men går ikke inn på hvordan dette skal formuleres utover å beskrive hva det skal stilles krav til [NEMA] [HIPAA]. SHdir, Norsk helsenett AS og andre aktører i helsesektoren arbeider med en norm for informasjonssikkerhet i helsesektoren, men denne er i skrivende stund (juni 2005) ikke ferdig.

Beskrivelse av sikkerhet ved overføring av data i nettverk med mobile enheter krever en analyse av leddene i kommunikasjonskanalen med ulike mekanismer og nivåer for sikkerhet [falc]. Behandling i termineringsutstyr og overføringsledd eller faste og mobile terminaler gir forskjellige sikkerhetsutfordringer, men det er ikke etablert en standard for sammenligning eller beskrivelse av sikkerhetsparametere i slike scenarier. RFID er et annet område hvor det vil være nye sikkerhetsutfordringer og behov for å beskrive og vurdere sikkerhetsparametere. RFID i sykehus vil forutsette trådløs overføring av sensitiv informasjon (siden det er data om pasienter) og sikkerhetsegenskapene vil måtte kunne beskrives og verifiseres opp mot krav i en sikkerhetspolicy. Sikkerhetsutfordringer for slike omgivelser beskrives av [ski&sø], men uten å ta stilling til hvordan sikkerhetskrav vil måtte struktureres.

Rollebasert tilgang til systemer, applikasjoner og data er i noen tilfeller nedfelt i krav og standarder. I omgivelser hvor informasjon flyttes vil roller og tilgangsretter være situasjons- og tidsavhengig [has&ut]. Sikker tilgangskontroll er avgjørende for at et system skal kunne overholde de krav som stilles, og må bygges på en veldefinert

2 NIST – National Institute of Standards and Technology

sikkerhetsstrategi [røst]. I distribuerte systemer kan informasjon f.eks. lagres med delt tilgang i sentrale eller distribuert lagre, eller den lagres i separate distribuerte lagre og synkroniseres. For å realisere det må det bygges bro mellom en uformell policybeskrivelse og den faktiske implementeringen av sikkerhetstjenester [pope]. Det kan være nødvendig å hente data fra flere lagre for å få frem et komplett sett med data. Det er utviklet en sikkerhetsarkitektur for å ivareta sikkerheten hos de enkelte aktørene i denne typen omgivelser [moe]. Dette inkluderer ikke en metadatastrukturer for å overføre sikkerhetsparametere som kan gjøre det mulig å verifisere et tilfredsstillende og tillitsverdig sikkerhetsnivå hos flere kommuniserende parter. Dersom flere systemer kommuniserer med hverandre blir kravene til autentisering komplekse å håndtere og kontekstkrav og autentiseringskrav må samordnes [McDa]. Integrasjon av tilgangskontroll og sikkerhetspolicy vil være sentralt for rollebasert tilgangskontroll og brukeraksept [iAccess] [mand]. Slike systemer må også være forberedt på å kunne kommunisere selv om ikke alle systemer er fullt operative til enhver tid [stab].

I PERMIS-prosjektet [PERMIS] behandles tilgangskontroll knyttet til en definert policy beskrevet i XML, og autorisasjon kan besluttes på basis av denne gjennom en «Privilege Management Infrastructure» basert på X.509 attributtsertifikater [chad]. Det er utviklet et rammeverk for autorisasjon av Internettressurser og tjenester for administrasjon av tillit. I rammeverket beskrives tiltak, prinsipaler, policyer, rettigheter og overensstemmelse som grunnleggende komponenter. Andre formater for eller beskrivelser av sikkerhetskrav er ikke behandlet

Sikkerhetsaspekter ved nettbasert tilgang til personinformasjon vil måtte inkludere arkitekturforutsetninger (datavarehus, mellomvareløsning, mobile agenter) og bruk av PKI, katalogtjenester og indekser m.m. [Elvi2]. Nasjonale PKI-løsninger vil være nødvendig, som f.eks. [SEID], og ulike indeksers informasjonsmoduler bør minst inneholde informasjon om hvor data er lagret, á jour-hold, loggføring og om informasjon lagret i et system vil vises som skjermbilder i andre systemer. Det er etablert anbefalinger for felles implementering av PKI-løsninger og sertifikater [KITH2], men dette er avgrenset til f.eks. hvilke protokoller og formater som skal anvendes og hvordan katalogtjenester bør benyttes. Krav til sikkerhetsnivå ved bruk av PKI vil være avhengig av situasjon og lokalisering i nettverk og bruk av sertifikater vil være avhengig av sertifikatenes definerte bruksområder [nhn]. Dette vil kunne knyttes til integrasjonsnivå i nettverk og systemer. PKI-bruk vil kunne knyttes direkte til veldefinerte sett med data. Infrastrukturer for sikker meldingsutveksling er realisert [SESAM], men ikke med definisjoner av felles strukturer for angivelse av sikkerhetskrav. Blant de uavklarte spørsmål er realisering av løsninger som håndterer sikker aksess, roller, autorisasjon for tilgang til informasjon, tilgjengelighet til sentral informasjon i distribuerte systemer.

Det har tidligere vært gjennomført arbeider for automatisert analyse av spesifikasjoner uttrykt i naturlig språk. [NASA] peker spesielt på utfordringer med slike spesifikasjoner som ligger i fare for tvetydigheter, upresise angivelser og inkonsistens.

Svak setningsstruktur kan også forårsake feiltolkninger og begreper kan bli brukt på tvers av gitte definisjoner. De vurderer kvalitet på grunnlag av antall forekomster av sentrale ord og begreper i en spesifikasjon, og estimerer risiko for at ikke programvaren skal fungere etter intensjonene som er forsøkt uttrykt i spesifikasjonen. [heitm] viser at å utvikle formelle kravspesifikasjoner basert på krav beskrevet i prosa er vanskelig, særlig p.g.a. struktur og organisering av dokumentene. Struktur i dokumentet er også påpekt av NASA som en begrensende faktor for ekstraksjon og sammenligning av krav. Et pågående (juni 2005) NIST-prosjekt analyserer verktøy for metrikker, kravregistrering (requirements capture), design, spesifikasjoner m.m. [SAMATE].

For komplekse systemer vil registrering av krav måtte ta hensyn til en rekke interessenter og tilnærminger. [white] har beskrevet en struktur for kravanalyse hvor sikkerhetskrav legges under ikke-funksjonelle krav og dynamiske systemegenskaper. Disse deles videre inn i bl.a. tilgjengelighet, pålitelighet, integritet presisjon, påregnelighet, sårbarhet, overlevelsesevne o.l. Formålet er å strukturere kravene før kravspesifikasjonene modelleres. [patz] presenterer en arkitektur for å uttrykke sikkerhetskrav for store grupper abstrakt. I arkitekturen bestemmes aktørenes aksepterte policyer. Det beskrives en algoritme for å definere hvilke valg som er akseptable for ulike konstellasjoner basert på en «policy level agreement» som uttrykkes gjennom beskrivelse i et «security abstraction layer», og videre til konkret implementering av den enkelte policy. Sikkerhetstjenester bygger på mekanismer, som bygger på implementeringer, men uten at strukturen på kravspesifikasjonene diskuteres.

3.2 Måling og spesifikasjon av sikkerhet

Definisjon av grunnleggende målemetoder for IT og programvare er mangelfull, og dette gjelder også sikkerhetskrav, bl.a. fordi metoder for kvantifisering i liten grad er utviklet [gray].

[gilb] beskriver en metodikk for kvantifisering av sikkerhet. Han sier om behovet for måling av sikkerhet:

> «The systemic advantages of quantifying the security problem:
>
> - We get clarity regarding our requirements
> - We get real agreement, not different interpretations of the requirement
> - We can contract for results
> - We can prioritize security as effectively as other quantified attributes like performance or reliability

- We can more logically evaluate all designs, strategies and architectures that are supposed to help us reach our security requirements».

En måling krever en skala, kategorisering, intervaller eller referanse for måleparametrene. For etablering og vedlikehold av en metrikk for sikkerhet må det defineres et formål, det må beskrives hvilke metrikker man ønsker og disse må defineres. Metoder og rutiner for logging og rapportering må bestemmes. Data må være tilgjengelig, målbare, relevante over tid og må fange opp endringer som skjer. Dette inkluderer behov, mål, definisjoner, ledelse, roller, overvåking, oppfølging, etterprøving o.s.v. En sikkerhetspolicy, som angir retning og strategi, vil ikke nødvendigvis være en referanse med en formalisert beskrivelse eller etterprøvbare mål, og man må identifisere relevante elementer å knytte en metrikk opp mot [wold].

Det kan også være aktuelt å undersøke om en policy er i overensstemmelse med lover og EU-dirketiver [maal]. Både krav og implementering vil være vanskelig å angi med eksakte mål, og et kvalitativt sammenligningsgrunnlag må etableres.

En policy vil være rettet mot et nivå i virksomheten; toppnivå, oppgaveorientert, funksjonsorientert eller målorientert [wies]. Avhengig av nivå og fokus vil også en sikkerhetspolicy være påvirket i ulik grad av forretnings- eller teknologiaspekter og detaljeringsgrad i sine definisjoner. Et rammeverk for administrasjon av sikkerhetspolicy i distribuerte systemer er foreslått av [sloman] for å kunne uttrykke et policykrav presist, og er beregnet på at en policy skal kunne implementeres i systemet basert på beskrivelsen, og at policyen skal kunne analyseres og raffineres.

Sikkehetskrav og egenskaper som skal brukes i sikkerhetsmetrikker må kunne presenteres på en hensiktsmessige måte [NIST]. Disse kravene vil gjelde enten man måler hyppighet eller de kvalitative egenskapene ved et system, som ved metrikk for rutiner og prosedyrer [fag.mfl]. Når metrikken er etablert må resultatene følges opp med analyser og forbedringstiltak [payn]. Dette er viktig i en utviklings- og forbedringssituasjon, og også påpekt i CEN-standarden PrENV 13608 [13608]. Dette ligger utenfor vårt fokusområde, vi vil beskrive aspekter som skal kunne brukes i en metrikk, men er likevel viktig å ha innsikt i som referanse for anvendbarheten av de elementer som skal brukes ved formulering av sikkerhetskrav.

Standarder for evalueringskriterier for informasjonssikkerhet har utviklet seg over flere stadier [goll], fra Orange Book [TCSEC] og ITSEC [ITSEC] til Common Criteria [CC]. Orange Book beskriver en metode for å plassere sikkerhetsprodukter på et nivå på en skala, «Security Classes». Evalueringskriterier knyttes til et «Target of Evaluation» som vil være et produkt eller system. Nyere metoder vil i stor grad ha sine røtter i Orange Book og denne filosofien. Orange Book skiller mellom sikkerhetsanalyser for evaluering av systemer, sertifisering av produkter og akkreditering for bruk. Evalueringen må sikre repeterbarhet og reproduserbarhet. En metode kan være prosessorientert eller produktorientert og relatert til funksjonalitet, effekt for sikkerhet eller omfanget av analysen. Orange Book definerer klasser for sikkerhetsnivå, hvor den øverste klassen krever formelle spesifikasjoner med bevisbar sikkerhet. ITSEC innfører beskrivelse av sikkerhetsmål (hvorfor),

sikkerhetsfunksjoner (hva gjøres) og sikkerhetsmekanismer (hvordan) som verktøy for å beskrive sikkerhetsfunksjonalitet. I ITSEC kan et sett med aspekter trekkes med i sikkerhetsevalueringen av Target of Evaluation:

- sikkerhetsmål (kan ofte utledes av systemsikkerhetspolicy);
- beskrivelse av systemomgivelsene;
- antagelser om testobjektets omgivelser;
- sikkerhetsfunksjoner,
- hensikten med sikkerhetsfunksjonene;
- påkrevde sikkerhetsmekanismer;
- påkrevd evalueringsnivå;
- påstått minimumsstyrke for sikkerhetsmekanismer.

CC ble utviklet for å muliggjøre konsistent evaluering av sikkerhetsprodukter og -systemer. En Protection Profile skal gjøre det mulig å beskrive krav og ønsker, slik at leverandøren kan verifisere sitt produkt opp mot denne profilen. En Common Criteria (CC) Protection Profile (PP) består av fem seksjoner: Beskrivende elementer, rasjonale, funksjonelle sikkerhetskrav, utviklingskrav og evalueringskriterier. CC definerer en struktur og krav for lenking av elementene som brukes i en PP, som er sikkerhetsfunksjoner for produkter, programvare og systemer. Strukturer for sikkerhetsparametere beskrives ikke. Det kan være aktuelt å benytte CC for å beskrive de omgivelser som skal behandle det sett med data som vi betrakter i en risikoanalyse gjennom å utvikle en PP.

To sikkerhetspolicyer kan være forenlige eller uforenlige. En algoritme for å identifisere uforenlig krav er vist av [McDa.mf]. Det forutsettes et formalisert språk og at formelle krav er spesifisert, f.eks. for kryptering for kommunikasjonssekvenser som i Internet Key Exchange (IKE). Algoritmen søker å finne om minimumskrav er tilfredsstilt, ikke om to policyer er like.

EU-prosjektet CORAS var rettet mot risikoanalyse og har flere verktøy og metamodeller for beskrivelse av risiko, trusler og tiltak og evaluering av disse opp mot hverandre. UML kan benyttes som verktøy for modellbasert risikoanalyse [CORAS]. Det er utviklet UML-profiler for identifisering og analyse av sikkerhetsrisiko. Metamodeller brukes for å beskrive bl.a. kontekst for risikoanalyse [lund]. I sikkerhetsanalysen i CORAS benyttes grafiske modeller for å oppnå presis innmating av informasjon og på et riktig abstraksjonsnivå. Metoden tillater modellering av konteksten for analysen. For å lette kommunikasjonen mellom systemutviklere, beslutningstakere og systemansvarlige kan det benyttes ikoner tilpasset ulike kontekster og ontologier og som supplerer diagrammer, tabeller o.s.v. Alle elementer på et høyere nivå må være i overensstemmelse med strukturer på lavere nivå. UML-profiler kan på denne måten skapes som lagdelte metamodeller. Data kan ekstraheres fra modellene gjennom å merke aktuelle elementer. Videre arbeid pågår for å kunne bruke grafisk UML-lignende språk for spesifikasjon av policy og sikkerhetsanalyse[ENFORCE].

I åpne arkitekturer og agentbaserte systemer tilstrebes åpne dataformater for utveksling av data, og det kreves sporbarhet av krav. Registrering av sikkerhetskrav må gjøres tidlig i prosessen og det bidireksjonale forholdet mellom utvikling og krav må vedlikeholdes, slik at det planlagte systemet vil kunne møte organisasjonens mål. For design av multi-agent systemer er det utviklet metoder for å sikre at utviklingsprosesser håndterer dette [TROPOS]. Dette inkluderer imidlertid ikke beskrivelse av hvordan sikkerhetskravene i seg selv skal ivaretas.

Ved bruk av mobil eller komponentbasert SW og programvaremoduler som skal kunne kjøres uten at systemomgivelsene på forhånd er kjent, vil det være behov for å forutsette en grad av tillit til vertssystemet. Det må derfor knyttes sikkerhetsforutsetninger til programvarekomponenter som skal kunne overføres mellom systemer, f.eks. gjennom en tilstandsavhengig tillit. En metrikk basert på en informasjonstjeneste for tillit vil kunne gi et rammeverk for å måle dette basert på en komponentspesifikk sikkerhetspolicy [jøs&kn]. Informasjonstjenesten vil samle data over tid. Det er ikke beskrevet hvordan dette skulle kunne relateres til spesifikke datas sikkerhetskrav.

Ved Centre for Quantifiable Quality of Service in Communication Systems [q2s] pågår et prosjekt om sikkerhetstjenester i dynamiske nettverk. I prosjektet adresseres etablering av sikkerhetstjenester, det er ikke fokus på formulering og strukturering av sikkerhetskrav [knap].

Angivelse av tillit og tillitsverdighet er et område som i forbindelse med sertifikater og nøkler er brukt i «Web of trust [PGP]» for aksept av sertifikater. I en bredere sammenheng pågår arbeid [ENFORCE] for å utvikle verktøy for formalisering, analyse og gjennomføring av en policy for å sikre tillit basert på et bredt perspektiv med informasjonssikkerhet, lover og forskrifter og etiske aspekter. Dette prosjektet dekker ikke spesifikasjon av sikkerhetsparametere, men beskrivelser av policy ville kunne være relevant når det blir tilgjengelig resultater. Språklige og syntaktiske konstruksjoner vil også kunne tenkes gjenbrukt for andre anvendelser.

KITH beskriver bruk av og krav til indikatorer for måling av informasjonssikkerhet i helsevirksomheter og hvilket informasjonsgrunnlag som kan danne basis for indikatorer [KITH3], men det gis ingen beskrivelse av mulige datastrukturer for enhetlig formulering av sikkerhetskrav. Vi har heller ikke funnet andre egnede, eksisterende formater for vårt behov for å beskrive sikkerhetskrav og egenskaper.

4 Inndeling og beskrivelse av sikkerhetskrav

I dette kapittelet viser vi hvordan sikkerhetskrav og -egenskaper kan grupperes ut fra formaliseringsgrad, hvilken sammenheng et krav beskrives i og hvilken type krav vi har. Sikkerhetskrav og -egenskaper vil i denne sammenheng være kontekstuelle ved at de er definert i en gitt sammenheng. Egenskaper og karakteristika vi ser etter er:

- Hva som beskrives. Er det et krav, en policy, en sikkerhetstjeneste eller -funksjon, en standard eller protokoll?
- Grad av formalisme i beskrivelsen. Er kravet eller egenskapen formelt definert slik at det kan bevises eller verifiseres overensstemmelse med en premiss, eller er det en semiformell eller uformell utforming?
- Hva som ønskes oppnådd med kravet eller egenskapen. I hvilken kontekst stilles kravet?

4.1 Kontekstuelle sikkerhetsbehov

Som fundament for å strukturere sikkerhetskrav er deler av standarden «PrENV 13608: Sikkerhet for kommunikasjon i helsevesenet»[13608] brukt som referanse. Standarden beskriver en arkitektur for en enhetlig policymodell som benyttes for å definere en policyprofil eller beskyttelsesprofil for kommunikasjonsløsninger. Standarden er konsistent med ISO/OSI 7498-2 Basic Reference Model – Part 2: Security Architecture [7498].

PrENV 13608 tar utgangspunkt i et brukebehov og skal benyttes for å gi en beskrivelse av sammenhengen mellom brukerkrav eller en sikkerhetspolicy og en teknologisk løsning. Dette skal til sammen danne en Communication Protection Profile (CPP), eller alternativer for en CPP, for kommunikasjonsløsninger i helsenett. En CPP vil metodisk beskrive koplinger mellom: Hva CPP'en omhandler – Hvorfor kravet er relevant – Hvilken sammenheng det gjelder og hvem er ansvarlig – Hvordan det kan implementeres. PrENV 13608 beskriver også en prosess for å oppnå en tilnærming mellom brukerbehov og implementert løsning. Gjennom en CPP skal det defineres en felles terminologi og basis for policysammenligning, og gjennom en iterativ prosess skal man oppnå en tilpassing av og enighet om felles kommunikasjonspolicy for to parter som skal kommunisere. Metoden skal brukes for å kunne etablere en á priori tillit til at implementering av en gitt teknologisk standard eller løsning gir en ønsket sikkerhetseffekt.

Vi vil ikke her benytte den prosessen PrENV 13608 beskriver, vi vil kun benytte de inndelinger som er definert for:

- Formelle, semiformelle og uformelle krav
- Globale, konseptuelle og kontekstuelle sikkerhetsbehov, og
- Kravspesifikasjoner, prosedyrer, tjenester og mekanismer.

I den iterative prosessen PrENV beskriver, detaljeres behandlingen av krav,

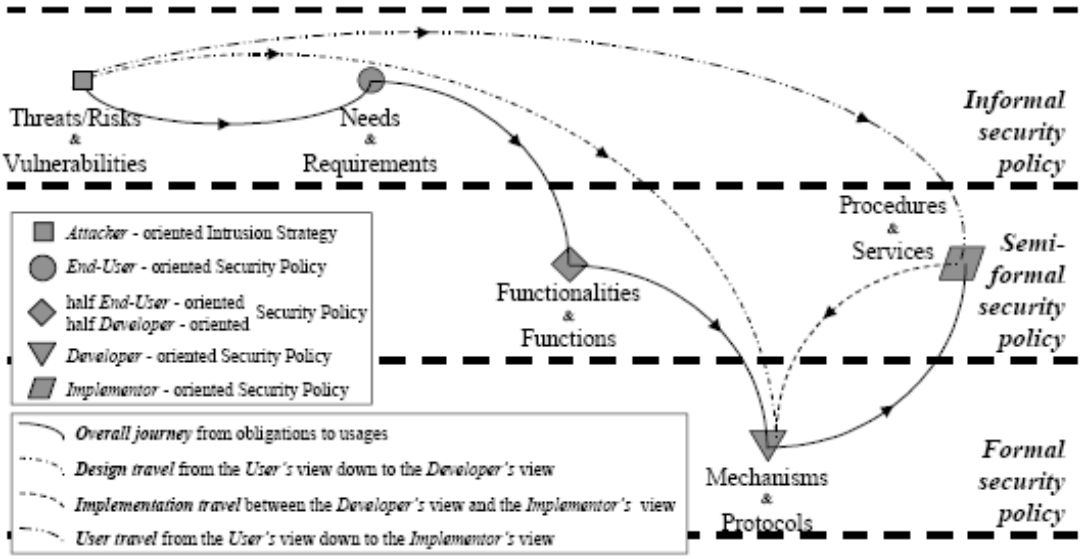
prosedyrer, tjenester og mekanismer videre. Den detaljeringen har ikke vært hensiktsmessig i vår kontekst og for vårt behov for å formulere sikkerhetskrav for et sett med data.

4.1.1 Uformelle, semiformelle og formelle krav

En CPP beskrives med tre lag; med formelle, semiformelle og uformelle beskrivelser av sikkerhetskrav:

- Det øverste av de tre lagene i en CPP består i en uformelt beskrevet sikkerhetspolicy, lovkrav og krav fra en sikkerhetsinstruks eller norm o.l. som typisk vil uttrykkes som uformelle krav.
- Det neste, semiformelle, laget beskriver sikkerhetsfunksjoner og funksjonalitet og sikkerhetsprosedyrer og -tjenester. Prosedyrer og rutiner i en organisasjon og funksjoner, funksjonalitet og egenskaper som tilbys i et system vil typisk uttrykkes som semiformelle krav.
- Det mest detaljerte laget er formelle angivelser av sikkerhetsmekanismer og protokoller. Disse vil være forankret i standarder eller formaliserte beskrivelser.

Semiformelle funksjoner, prosedyrer og tjenester skal betjene de uformelle kravene. Det trenger ikke være en en-til-en sammenheng mellom krav og tjeneste eller prosedyre og det vil da være behov for krysskoplingsoversikter for å sikre at et krav er dekket. Prosedyrer skal sørge for at de som behandler personopplysninger gjør dette slik kravene beskriver, mens tjenester tilbys gjennom IT-systemer og IKT infrastruktur, inkludert drift (systemsikkerhet, systemarkitektur, segmentering, systeminteraksjon). Gjennom beskrivelser av prosedyrer og tjenester synliggjøres prosesser og hendelseshåndtering og aktørenes ansvar for og innvirkning på sikkerheten.



Figur 3: Formelle, semiformelle og uformelle sikkerhetskrav. (*Kilde: CEN)*

Formelle beskrivelser av sikkerhetsmekanismer skal referere til protokoller og bruk av standarder som beskriver hvordan sikkerhetsmekanismer implementeres. Her beskrives realisering og teknisk kontekst for web, logiske komponenter, databaser, kommunikasjon o.l. Ofte vil ikke krav om bruk av en bestemt algoritme være et eksplisitt sikkerhetskrav for bestemte data, men det kan være aktuelt i forbindelse med arkivering, bruk av PKI, standardisering mellom virksomheter o.l.

4.1.2 Globale, konseptuelle og kontekstuelle krav

Sikkerhetsbehov som beskrives i de ulike lagene kan kategoriseres på tre ulike nivåer:

- det **globale**/overordnete sikkerhetsbehov: tilgjengelighet, integritet, konfidensialitet, etterprøvbarhet (T-I-K-E)
- det **konseptuelle**: T-I-K-E for objekter, subjekter og hendelser o.l., og
- det **kontekstuelle**: T-I-K-E for protokoller, applikasjoner, meldinger o.l..

De **konseptuelle sikkerhetsbehov** brukes for å strukturere de kontekstuelle sikkerhetsbehovene. De konseptuelle sikkerhetsbehovene som angis i PrENV13608 er:

Tilgjengelighet:

- Objekttilgjengelighet
- Subjektpålitelighet

Integritet:

- Objektintegritet
- Subjektintegritet

Konfidensialitet:

- Transportkonfidensialitet (behandlingskonfidensialitet)
- Kontekstuell konfidensialitet

Auditerbarhet/etterprøvbarhet:

- Klareringskontroll (inkl. sikring av hjemmel for behandling av persondata)
- Avsenderkontroll
- Mottakerkontroll
- Utvekslingskontroll

Objektintegritet og -tilgjengelighet skal ivareta de enkelte dataelementene i systemet, men subjektintegritet og -pålitelighet skal ivareta systemet, protokoller og applikasjoner. Kontekstuell konfidensialitet er i PrENV 13608 beskrevet som selektiv, implisitt eller eksplisitt.

Kontekstuelle sikkerhetsbehov beskrives i krav, policyer og funksjoner o.l. for systemer, applikasjoner og organisasjoner. Teknologi og løsninger knyttes opp mot

disse behovene gjennom beskrivelse av formelle mekanismer og protokoller og semiformelle prosedyrer og tjenester. Kontekstuelle krav kan være uformelle, semiformelle eller formelle. I det kontekstuelle perspektiv uttrykkes f.eks. sikkerhetsbehov relatert til roller og ansvar med beskrivelse av hva sikkerhetsbehovet er, hvorfor og hvem som er ansvarlig for å møte dem.

Del 2 og 3 av PrENV13608 angir krav til kryptering og protokollbruk og sikring av datakanaler og dataobjekter som overføres basert på «meldingsparadigmet». Dataenes karakter behandles altså ikke, kun deres konfidensialitet og integritet inkludert autentisering av partene o.l. Disse delene av standarden brukes ikke i strukturen nedenfor.

Kontekstuelle, uformelle krav utformes eller finnes bl.a. som regulatoriske krav (med personopplysningsloven, personopplysningsforskriften og spesiallover), men vil ofte også dekkes av veiledninger, normer og standarder eller gjennom en sikkerhetspolicy. De vil inneholde både funksjonelle og sikkerhetsmessige elementer, som tilgang, sikring av data, kommunikasjon, autentisering, sporbarhet o.s.v. og angivelse av interessenter ved bruk av f.eks. EPJ. Funksjonelle krav som vil forutsette sikkerhetsfunksjoner behandles ikke som sikkerhetskrav i denne sammenhengen.

4.2 Krav, prosedyrer, tjenester og mekanismer

I eksemplene i dette kapittelet er referansestrukturen fra PrENV13608, med inndelingene på det globale og konseptuelle nivået, benyttet direkte, men begrepet «transport» erstattes av «behandling» (inkludert lagring) siden det ikke er sikkerhet for en kommunikasjonskanal som skal beskrives. Eksemplene på krav og egenskaper beskrives på det kontekstuelle nivået og viser hvordan de kan grupperes inn i samme overordnede rammer selv om de beskrives fra ulike perspektiver.

I denne første oversikten har vi inkludert krav og egenskaper som beskriver sikkerheten og sikkerhetsbehov ved behandling, overføring og lagring av data i systemer, applikasjoner og kommunikasjonskanaler uten å avgrense dette. Oversikten er delt inn i kontekstuelle krav, prosedyrer, tjenester og mekanismer (protokoller, standarder).

Hver oppføring kan gis en ID/kode som kan brukes som referanse i andre oppsett. Mer utfyllende lister basert på kildemateriale fra helsevesenet er vist i vedlegg B, C og D. Oversikten ikke er ment å skulle være et endelig sett med entydig definerte krav og egenskaper, men å vise hvordan de kan grupperes i forhold til konseptuelle sikkerhetsbehov.

4.2.1 Kontekstuelle krav

Kontekstuelle krav finnes normalt i lover, forskrifter, sikkerhetspolicy, normer, standarder, instrukser eller kravspesifikasjoner. De kontekstuelle kravene uttrykker brukerens behov for sikker behandling av data. I tabellen er sikkerhetskrav inndelt etter de konseptuelle sikkerhetsbehovene. Kravet beskrives kort, men ikke nødvendigvis utfyllende, og med en angivelse av bakgrunn eller opprinnelse for

kraveksempelet. Kravene vil ikke ha en formalisert utforming. Et uformelt krav vil som regel være nøytralt i forhold til hvordan en prosedyre blir utformet eller en funksjon implementeres.

Kontekstuelle krav (K)	***Kilde***
Objekttilgjengelighet (OT)	
Pasientinnsyn: Rett til innsyn i egen journal.	Pasientrettighetsloven kap. 3, §5-1. Helsepersonelloven §41
Nødvendig tilgjengelighet skal sikres	Personopplysningsforskriften §2.12
Subjektpålitelighet (SP)	
Beskyttelse mot ødeleggende programvare skal etableres	Personopplysningsforskriften §2.13
Objektintegritet (OI)	
Det skal sikres at ikke personopplysninger er endret eller ødelagt	HIPAA §164.312. Personopplysningsforskriften §2.13
Subjektintegritet (SI)	
Tilstrekkelig sikring av data med tilkoplingssikkerhet og fysisk sikkerhet. Autorisert tilkopling og tilgangskontroll	ØNH[3]. Personopplysningsforskriften §2.13 HIPAA §164.312
Behandlingskonfidensialitet (BK)	
Konfidensialitet skal sikres	Personopplysningsforskriften §2.11 Helsepersonelloven §5, 21
Kontekstuell konfidensialitet (KK)	
Tilgang kun til relevant info, nødvendig for aktuel behandling	Segmentert, rollestyrt tilgang til opplysninger. EPJ std.
Mottaker (M)	
Informasjon skal gis tilstrekkelig dokumenterbar sikkerhet.	Personopplysningsloven.
Utveksling (U)	
Hjemmel for utveksling. Samtykke fra pasient eller hjemmel i lov	Grunnlag for utveksling skal sikres. Helseregisterloven §5, 2

Tabell 1: Kontekstuelle sikkerhetskrav

4.2.2 Kontekstuelle prosedyrer

Prosedyrer beskrives gjerne i virksomhetenes internkontrollsystemer. Det kan f.eks. være sikkerhetspolicyer eller sikkerhetsinstrukser. Prosedyrene vil beskrive hvordan organisasjonen som behandler en informasjon skal fungere, og utrykker de tiltak brukeren iverksetter i egen organisasjon for at den skal fungere best mulig med tanke

3 ØNH – Østnorsk helsenett

på sikkerhet i databehandlingen. Prosedyrer er beskrevet i en semiformell form og vil kunne verifiseres gjennom at faktiske handlinger utføres.

Prosedyrer og tjenester er ikke nødvendigvis formulert som krav i utgangspunktet, men det kan stilles krav om at visse tjenester eller prosedyrer skal etableres eller være tilgjengelig for å ivareta den informasjonssikkerheten som kreves for å behandle et aktuelt sett med data.

Kontekstuelle prosedyrer (P)	***Bakgrunn, hensikt***
Objekttilgjengelighet (OT)	
Det skal være forberedt for tilgang i akuttsituasjoner.	UUS[4] sikkerhetsinstruks. HIPAA §164.312
Rutine for håndtering av manuell oppringing.	Opprette alternativ tilgang ved feil, hvis Internettilgang er blokkert. NST.
Subjektpålitelighet (SP)	
IT driftsprosedyrer	Pålitelig drifting av systemer, IT-avdeling
Objektintegritet (OI)	
Helsepersonell sjekker importerte data manuelt.	Fanger opp åpenbart gale overføringer. Nasjonalt Senter for Telemedisin
Subjektintegritet (SI)	
Opplæring av brukere.	Hindre brudd på sikkerhetsinstruks, hindre brukerfeil.
Oppdatering av sikkerhetspatcher. Vedlikehold av SW og systemkonfigurasjoner.	Vedlikehold av sikkerhetsnivå. ØNH kravspec
Dokumentasjon av sikkerhetsrutiner. Ref. personopplysnings- lov og forskrift m.m.	Sikkerhetsprosedyrer. Personopplysningsloven
Risikoanalyse skal gjennomføres	Sikre eget forvaltet IT-system. ØNH kravspec
Kontekstuell konfidensialitet (KK)	
Avdelingsoverlege skal avgjøre autrorisasjon for tilgang til pasientdata	UUS sikkerhetsinstruks
Klareringskontroll/hjemmel (KH)	
Filer skal merkes med sensitiv/ikke sensitiv	Klassifisering av meldinger og filer. ØNH kravspec

Tabell 2: Kontekstuelle sikkerhetsprosedyrer

4.2.3 Kontekstuelle tjenester

«Tjenester» vil beskrive hvilke egenskaper, funksjonalitet og funksjoner IT-systemet

4 UUS – Ullevål universitetssykehus

skal ha. Kontekstuelle sikkerhetstjenester er tjenester eller funksjonalitet som systemet eller applikasjonen tilbyr for å ivareta sikkerheten. De spesifiseres typisk i system-, arkitektur- eller applikasjonsbeskrivelser. Sikkerhetsfunksjoner beskrives på en semiformell form og vil benyttes automatisk når gitte funksjoner utføres.

Kontekstuelle tjenester (T)	***Beskrivelse***
Objekttilgjengelighet (OT)	
Tilgang ved akuttbehov skal være mulig	Blålystilgang, aktualisering
Objektintegritet (OI)	
Digital signering av sendt informasjon	Signering av melding eller konvolutt
Subjektintegritet (SI)	
Kun Java med sertifisert opphav. Ikke ActiveX.	Sikring av soner. ØNH
Automatisk logoff etter time-out	HIPAA §164.312
Behandlingskonfidensialitet (BK)	
Sperre mot kopiering av data til andre systemer	Ikke lokal lagring. Pasientinfo ikke cachet
Personopplysninger skal kunne krypteres	HIPAA §164.312
Kontekstuell konfidensialitet (KK)	
Tilgang skal gis basert på rolle eller funksjon. Rollebasert aksesskontroll	Kontekstavhengig tilgang til relevant informasjon. Intern PKI. ØNH
Det skal skilles logisk mellom identitet og andre personoplysninger	EPJ-standarden
Klareringskontroll/hjemmel (KH)	
Klassifisering av meldinger og filer	Merking sensisitiv, ikke sensitiv. ØNH
Mottakerkontroll (M)	
Ikkebenekting	PKI-basert (Elektronisk sykemelding)
Utvekslingskontroll (U)	
Logg av hendelseskronologi	Juridisk, oppgaver, system, revisjon. For rekonstruksjon av forløp

Tabell 3: Kontekstuelle sikkerhetstjenester

4.2.4 Kontekstuelle funksjoner og mekanismer

«Mekanismer» vil beskrive hvordan en tjeneste er implementert. Funksjoner og mekanismers implementering beskrives gjennom at det defineres hvilke formelle standarder og protokoller som benyttes og eventuelt hvordan tjenester konfigureres. Dette vil kunne verifiseres på et systemmessig lavt nivå. Slike parametere beskrives i spesifikasjoner for grensesnitt, systemer og applikasjoner, og i noen tilfeller i kravspesifikasjoner. I tabellen er kun standarder angitt, ikke hvilke verdier parametere

skal gis eller andre valg som må gjøres ved implementering.

Funksjon, mekanismer (M)	*Protokoll, standard, teknologi*
Objekttilgjengelighet (OT)	
Byte padding for interoperabilitet med eldre EDI	DES
Notifikasjon for innkomne meldinger	GSM, MIME
SSO for felles pålogging	Kerberos
Subjektpålitelighet (SP)	
Databaseagenten sender melding hvis server er nede, systemmonitorering	SOAP-objekter
Fjernsupport gjennom brannmur	Port nn
Objektintegritet (OI)	
Meldingsautentisering ved offentlig nøkkel kryptering	X.509, LPAD, Crypto API, S/MIME (RSA/3DES/SHA-1)
Meldingsautentisering ved signering	ebXML, XML-Dsig, PKCS#12
Godkjenning av EPJ ved påføring av digital signatur	SKCF7, SHA-1, X.509
Subjektintegritet (SI)	
Administratortilgang til webserver begrenset	SSH
Autentisering ved meldingsoverføring	SMTP/POP
Segmentering: adskilt autentisering for web, applikasjon og database	IIS, ASP.NET, SQL server
CRL-adminstrasjon og sertifikatverifisering	RFC 2459, 3280, 2560
Autentisering av personsertifikat	ETSI TS 101 826 v.1.2.1, X.509 v.3
WLAN pålogging	RADIUS
NAT sikkerhetsbarriere	RFCxxx
Behandlingskonfidensialitet (BK)	
Kryptering webutveksling server – pasient	HTTPS, SSL m/128 bits nøkkel
Krypterte meldinger server – EPJ	S/MIME, RFC 2633, 3369, 2632
Kryptert kommunikasjon	AES, 3DES, RC6, =<2048 bits nøkkel
PKI-basert autentisering	ebXML

Tabell 4: Kontekstuelle sikkerhetsmekanismer

4.3 Sikkerhetskrav i et datasentrisk perspektiv

Normalt vurderes sikkerheten ved informasjonsbehandling ut fra et systems sikkerhetsbilde, som trusselbilde, sårbarhet, konsekvenser ved sikkerhetshendelser,

risiko o.s.v. I et IT-system er det informasjonen som er samlet og behandles i systemet som er det verdifulle. Det ikke er IT-systemet i seg selv som er verdifullt, det er systemets evne til å behandle og sikre informasjonen slik som ønsket.

I oversiktene tidligere i dette kapittelet er vist sikkerhetsrelevante krav og egenskaper som gjelder generelt for bruk av IT-systemer. Når data overføres til et annet system enn der de først ble behandlet, eller det skal gis delt tilgang for flere aktører i et nettverk av flere ulike systemer, vil en beskrivelse av de systemavhengige sikkerhetsegenskaper for opprinnelsessystemet ikke lenger være tilstrekkelig for å sikre informasjonen i det nye systemet.

Sikkerhetskrav man stiller for behandling av de aktuelle dataene må være overførbare, og det må kunne etterprøves om de er oppfylt i det nye systemet. Dette kan være krav som vil være forskjellig for personopplysninger i forhold til andre data, som informasjon om produkter, kunder, offentlige tjenester, underholdning o.s.v. Ulike typer data vil ha ulike sikkerhetsbehov, og det stilles ulike sikkerhetskrav til systemene som skal behandle informasjonen.

Det vil da være naturlig å beskrive sikkerhetskravene i et datasentrisk perspektiv. Sikkerhetskrav og innføring av tiltak kan da naturlig knyttes eller refereres til «sak» eller «dokument» eller «fragment» i dokument, ikke til et system. For å identifisere de datasentriske kravene må vi inkludere de krav som kan knyttes til en modul med data eller type data som skal overføres mellom to parter, og som vil gi mening både i det avgivende og det mottagende IT-system.

Hvis to parter som ikke har forhåndsklarerte forbindelser med hverandre skal utveksle informasjon, må de vite noe om hverandre. De må da kunne forsyne motparten med nok opplysninger til at tillit kan etableres. Dersom dette tillitsnivået er avhengig av hva slags data som skal overføres, må det finnes informasjon om påkrevd sikkerhetsnivå i tilknytning til dataene. For informasjon i f.eks. en EPJ er det ingen slik klassifisering, men det kan likevel tenkes at personalia som navn og telefonnummer kan overføres med en «gradering» mens sensitive opplysninger kan gis en annen gradering. ebXML [ebXML] gir f.eks. muligheter til å ta hensyn til en organisasjons rolle i en transaksjon.

I PrENV 13608 er sikkerhetskrav som er relevante for en kommunikasjonskanal og partene som deltar i kommunikasjonen beskrevet gjennom en CPP – Communication Protection Profile, en sikkerhetsprofil for kommunikasjonskanalen. Standarden beskriver således ikke primært sikkerhetskrav og -egenskaper knyttet til de data som overføres, men egenskapene til det systemet som overfører data. Data som transporteres tar ikke med seg kunnskap om kanalen, men det vil stilles krav til kanalen for de data som skal overføres. Når en CPP inneholder både sikkerhetskrav og prosedyrer og informasjon om sikkerhetstjenester og implementering av sikkerhetsmekanismer som forholder seg til et felles rammeverk basert på en kontekstuell inndeling, kan krav og egenskaper lettere holdes opp mot hverandre på tvers av de ulike perspektivene. Dette brukes som utgangspunkt for å etterprøve om en aktuell implementering tilfredsstiller en kravspesifikasjon, og for å forbedre løsningen der det er nødvendig. Man kan også forhandle frem felles krav til implementering av

kommunikasjonskanalen gjennom denne prosessen, og gjennom en iterativ detaljering og tilpassing av beskrivelsene for kanaler og nettverk for ulike systemer.

I et datasentrisk perspektiv vil en del krav falle ut av sin kontekst og ikke gi mening. Beskrivelsen av sikkerheten i en kommunikasjonskanal vil f.eks. normalt ikke ha betydning for sikkerheten i et system etter at en overføring er avsluttet, dersom dette er transparent slik at informasjon om overføringen ikke lagres sammen med dataene i ettertid. Det er derfor ikke gitt at det skal stilles som et krav at en gitt kryptering skal benyttes ved overføring av data for at den nye parten skal få lov til å behandle overførte persondata. Slike krav vil kunne ha likeverdige alternativer og det vil ikke alltid være et naturlig krav i en gitt kontekst. De kan likevel inngå i aktuelle implementeringer og være blant mulige alternativer til løsning, valg av protokoller som oppfyller kravene knyttet til informasjonen vil være et forhandlingsspørsmål mellom partene.

Formelle krav og bruk av standarder vil kunne kreves i tilknytning til autentiseringstjenester. F.eks. vil signaturer som er lagret sammen med dataene måtte kunne gjenskapes. Da er det knyttet til dataenes objekttilgjengelighet og -integritet.

I det følgende vil sikkerhetskrav og -egenskaper settes opp i et datasentrisk perspektiv, ikke relateres til kommunikasjonskanalen eller IT-systemet. Vi vil bruke betegnelse Data Protection Profile (DPP) på kravspesifikasjonen. Referansestrukturen søkes lagt så nær opp til PrENV 13608 struktur for kanalsikkerhet som mulig, men for å beskrive det globale behovet for «etterprøvbarhet» vil vi erstatte de konseptuelle kategoriene som brukes i PrENV 13608 med «klarering/hjemmel» og «utvekslingskontroll». Disse kategoriene vil være bedre egnet når hensikten er å diskutere sikkerhetskrav for behandling av informasjon. Vi skal samle krav om hva som vil kreves for at opplysninger skal kunne overføres eller gjøres tilgjengelig i et nytt system, og for at mottagende og avgivende part skal verifiserer overfor hverandre hvilke sikkerhetskrav som vil gjelde.

Krav om bruk av funksjoner og mekanismer i form av spesifiserte protokoller og standarder er ikke tatt med i dette eksempelet. Men det vil kunne være aktuelt å knytte krav om bruk av f.eks. en spesifisert type sertifikater til det å behandle personopplysninger i en gitt sammenheng og ha sin naturlige plass i spesifikasjonen. Spesifisering av f.eks. digitale signaturer vil kunne bli inkludert i spesifikasjonen for hvordan et system ivaretar sikker lagring av persondata.

Tabellen nedenfor skal vise hvordan sikkerhetskrav som gjelder en avgrenset mengde eller type data kan struktureres etter konseptuelle kategorier som vi har beskrevet. Sikkerhetsbehov spesifisert gjennom uformelle krav, krav til implementering av sikkerhetstjenester og prosedyrer.

Konseptuell gruppe/ kravtype	*Datasentriske kontekstuelle krav*	*Kommentar, referanse*
Objekttilgjengelighet		
Uformelle krav	Pasienten har på forespørsel rett til innsyn i egen EPJ	Pasientrettighetsloven, pasienten må autentiseres
Uformelle krav	Helsepersonell skal ha tilgang til informasjon etter behov i forbindelse med besluttet tiltak	Rollebasert, avgrenset, må autentiseres
Prosedyrekrav	Det skal finnes sikkerhetskopi.	Pers.oppl.forskr. §2-12
Krav om sikkerhetstjenester	Det skal finnes alternativ tilgang ved systemfeil	Pers.oppl.forskr. §2-12
Subjektpålitelighet		
Uformelle krav	Personopplysnings-forskriftens krav	Ref. Pers.oppl.forskr. §2
Objektintegritet		
Uformelle krav	Formål for registrering av data skal angis, beslutning om behandlingstiltak nødvendig	Gir informasjon om anvendelse av data
Prosedyrekrav	Det skal finnes rutiner for retting, sletting, sperring, signering, låsing.	Intern instruks
Subjektintegritet		
Uformelle krav	Tilstrekkelig sikring av data og system. Tilkoplingssikkerhet og fysisk sikkerhet	Autorisert tilkopling og adgang, tilgangskontroll
Prosedyrekrav	Etablering av sikkerhetsprosedyrer	Personopplysnings-forskriften §2-13 m.m.
Krav om sikkerhetstjenester	Registrering av forsøk på uautorisert bruk	Pers.oppl.forskr. §2
Behandlings-konfidensialitet		
Uformelle krav	Tilstrekkelig sikring av data i systemet, tilkoplingssikkerhet og fysisk sikkerhet	Autorisert tilkopling og adgang, tilgangskontroll
Krav om sikkerhetstjenester	PKI-basert autentisering	Krav til systemet om ebXML e.l.
Kontekstuell konfidensialitet		
Uformelle krav	Taushetsplikt, kun autorisert tilgang når personell deltar i behandling eller foretar tilsyn	Segmentert, rollestyrt tilgang til opplysninger
Prosedyrekrav	Det skal være etablert prosedyrer for tildeling av roller og tilgangsrettigheter	Intern instruks. Gjelder både vanlig bruk og aktualisering

Konseptuell gruppe/ kravtype	*Datasentriske kontekstuelle krav*	*Kommentar, referanse*
Klarering, hjemmel for behandling av opplysninger		
Uformelle krav	Offentlig lisens for helsepersonell	Pers.opl.forskr. §7-26 (unntak fra kons.krav)
Krav om sikkerhetstjenester	Klassifisering av meldinger og filer, merking sensisitiv/ikke sensitiv	Synliggjøring av beskyttelsesbehov
Utvekslingskontroll		
Uformelle krav	Registrering ved avgivelse av informasjon	Spredning, sporing
Uformelle krav	Hjemmel for utveksling. Samtykke fra pasient eller hjemmel i lov	Grunnlag for utveksling skal sikres
Prosedyrekrav	Det skal bestemmes en informasjonseier	EPJ-ansvarlig hos mottaker
Krav om sikkerhetstjenester	Logg av hendelseskronologi: Juridisk, oppgaver, system, revisjon	For rekonstruksjonav forløp

Tabell 5: Datasentriske kontekstuelle sikkerhetskrav

I eksempelet er det hovedsaklig uformelle krav og krav om semiformelle sikkerhetstjenester som er inkludert som krav, men noen krav om implementering av prosedyrer er også tatt med. Implementeringsavhengige elementer, som funksjoner og protokoller, vil brukes i IT-systemet for å møte kravene. En risikoanalyse vil måtte inkludere alle disse aspektene, bl.a. for at en part som gir fra seg personopplysninger skal kunne få bekreftelse på at mottakers system kan håndtere de krav som stilles og som definerer påkrevd sikkerhetsnivå. Oversikten foran er bygget på eksempler fra ulike typer kildemateriale. Strukturen muliggjør synliggjøring av en sammenheng mellom krav og egenskaper på ulikt formaliseringsnivå.

Utover Personopplysningslovens og -forskriftens krav om etablering av prosedyrer og rutiner, som alltid vil gjelde for all behandling av personopplysninger, er det beskrevet få kontekstavhengige lovkrav om etablering av prosedyrer for selve behandlingen av data. Det kan forklares ved at bruk av IT-systemer i seg selv ofte påtvinger et bruksmønster som ikke krever ytterligere rutiner siden systemet setter krav og begrensninger. For behandling av personopplysninger vil Personopplysningsloven føre til at man alltid vil måtte innføre passende rutiner likevel. Lovens krav dekker både konfidensialitet, tilgjengelighet og integritet og krever at det etableres rutiner for å sikre dette. Bestemmelsenes spesifikke konsekvenser for konkrete anvendelser er f.eks. i helsesektoren dekket gjennom andre og mer detaljerte lover, normer og standarder som helhetlig gjenspeiler lovens og forskriftens bestemmelser og intensjon.

4.3.1 Alternativer for strukturer

Andre strukturer for sikkerhetskrav har vært presentert, bl.a. innen fagområdet «requirements capture» og gjennom CC. Som beskrevet i kapittel 3 konsentrerer disse tilnærmingene seg hovedsaklig om innhenting av sikkerhetskrav eller behandling av systemsikkerheten. Dette gjelder også en PP i CC for f.eks. e-handel, databaser eller PKI.

I [fire] defineres en rekke typer sikkerhetskrav. disse kan grupperes inn under de konseptuelle kravtypene spesifisert tidligere, og vil kunne innplasseres i henhold til de konseptuelle kategoriene vi har brukt:

Identification Requirements	Objektintegritet, skal sikre rettmessig tilgang til objekter
Authentication Requirements	Objektintegritet, skal sikre rettmessig tilgang til objekter
Authorization Requirements	Objektintegritet, skal sikre rettmessig tilgang til objekter Subjektintegritet, skal sikre mot uautorisert systemtilgang
Immunity Requirements	Subjektintegritet, skal sikre pålitelig operasjon
Integrity Requirements	Objektintegritet, evt. subjektintegritet
Intrusion Detection Requirements	Subjektintegritet, skal sikre pålitelig operasjon
Nonrepudiation Requirements	Etterprøvbarhet, skal sikre korrekt utveksling av data
Privacy Requirements	Behandlingskonfidensialitet, skal verne data
Security Auditing Requirements	Subjektintegritet, skal ivareta systemsikkerhet og vedlikehold
Survivability Requirements	Subjektpålitelighet, skal også sikre objekttilgjengelighet
Physical Protection Requirements	Subjektintegritet, skal sikre pålitelig drift
System Maintenance Security Requirements	Subjektintegritet, skal sikre pålitelig drift

Tabell 6: Kryssreferanse mellom ulike inndelinger av typer sikkerhetskrav

Konkrete krav formuleres så på det kontekstuelle nivået. Dette viser at strukturen har fleksibilitet nok til å at andre inndelinger også kan formuleres innenfor definisjonene som er gitt, selv om det kan være at f.eks. to forskjellige krav av typen Integrity Requirements vil falle inn under hver sin konseptuelle kategori.

5 Beskrivelse av elementer i sikkerhetskrav

I dette kapittelet foreslår vi en struktur for å beskrive elementer i et sikkerhetskrav i en enhetlig metadatastruktur. De enkelte sikkerhetskrav bygges opp av slike elementer. Hvordan en kravspesifikasjon kan settes sammen av et samlet sett med sikkerhetskrav vises i kapittel 6.

Det må stilles krav til både kvalitet og til at strukturen tillater alle ønskede krav å bli beskrevet gjennom strukturen og metadataelementene. Hvor god kvalitet en kravspesifikasjon har vil som oftest være subjektivt vurdert. Kvalitetsindikatorer vil kunne grupperes i to kategorier [NASA]:

– Spesifikke kravformuleringer kan vurderes etter bruk av imperativer, utdypende beskrivelser, presiseringer, valgmuligheter og mer vage formuleringer.

– Spesifikasjonen som helhet vurderes etter størrelse, detaljeringsgrad, lesbarhet og struktur.

Beskrivelsen av enkeltelementer i en kravspesifikasjon for sikkerhet bør understøtte disse kvalitetsindikatorene. Elementer som f.eks. spesifikasjonens størrelse og antall subjekter som omtales vil kunne si noe om formål og omfang av temaer som skal dekkes og detaljeringsgrad i beskrivelsene. Forholdet mellom slike størrelser bør stå i et rimelig forhold til hverandre hvis man har en godt strukturert og formulert spesifikasjon.

5.1 Metadata for sikkerhetskrav

Metadatastrukturer er egnet for å lette søk etter informasjon, administrasjon av innhold og ved deling av informasjon [DC]. En metadatabeskrivelsele for sikkerhetskrav vil kunne gjøre sammenligning av ulike krav og løsninger lettere gjennom at det blir lettere å finne frem til ønsket informasjon. Informasjon om sikkerhet vil kunne ses på som metadata om opplysninger i en datafil. Samtidig vil det være behov for metadata om sikkerhetsparametere for å strukturere og bevare informasjon om forutsetninger for de sikkerhetskrav og egenskaper som angis.

En formalisert metadatabeskrivelse må bygges på en konsistent begrepsbruk og et gitt sett med valgmuligheter. Fremstilling i f.eks. UML-format er en vanlig metode som gir grunnlag for en semantisk interoperabilitet. Dette krever forhåndsdefinisjon av kategorier og mulige valg. Dette er gjort for pasientdata i KITHs[5] EPJ-standard [KITH4] og PrENV 13606 [13606] hvor strukturen for informasjon er definert i UML. Dette er nødvendig for kompatibilitet mellom forskjellige systemer som skal kunne ha tilgang til dataene eller for å kunne utføre krysskopling mellom datakilder (crosswalk). Sikkerhetskrav må skilles ut eller markeres i slike datastrukturer.

5.1.1 En struktur for å beskrive metadataelementer for sikkerhet

Når sikkerhetskrav skal formuleres vil vi basert på metadatadefinisjoner kunne

5 KITH - Kompetansesenter for IT i helsevesenet

beskrive og karakterisere hvert enkelt krav. Samtidig vil vi kunne systematisere kravene slik at vi kan etablere profiler for et ønsket formål, f.eks. en Data Protection Profile (DPP) for persondata. Vi har foreslått en pseudosyntaks og regler for å angi innholdet og variablene. Ulike anvendelser vil kreve forskjellig form og detaljeringsgrad i dokumentasjonen, men det er også nødvendig at form og innhold gir strukturer som letter sammenligning mellom ulike krav og egenskaper.

I elementstrukturen har vi valgt å benytte et antall forhåndsdefinerte metadataelementer med faste navn, og i noen tilfeller «subnavn». Informasjonen i elementene består dels av fritekst, dels av data med et fast format eller av predefinerte valg samlet i en liste for det enkelte aktuelle kravelementet. Dette er angitt i formatet for «content» i tabellene nedenfor. For andre elementer vil fritekst være mest hensiktsmessig, og en kvalitativ vurdering vil måtte være grunnlag for beskrivelsen.

Metadatastrukturen angir hvordan de enkelte elementer i sikkerhetskrav eller egenskaper skal beskrives. En «sikkerhetsprofil» vil kunne beskrives som et sett med krav og ønskede egenskaper og benyttes som samlebetegnelse på en samling krav, egenskaper, spesifikasjoner el.l. I beskrivelsen av enkeltelementene for formulering av sikkerhetskravene er det tre typer informasjon: Navn, formålet med elementet og beskrivelse av hvordan data formateres i elementet.

Navn på element	" hoved.sub-navn "	content= " format på informasjonen"
Metainformasjon om kravelementet. Fritekst.		
Formatert informasjon: *Liste med forhåndsvalg eller data med fast format (f.eks. for dato)*		

Figur 4: Struktur for beskrivelse av elementer i sikkerhetskrav

Valg av krav og strukturering og sammensetting av metadataelementer vil gjøres ut fra de aktuelle behov. Vi har ikke her en ambisjon om å foreslå en ordlyd som skal sikre at kravene i seg selv er presist beskrevet og det er ikke her et mål å vise en komplett struktur og utvalg av metadataelementer. Vi vil vise at metodikken er anvendbar for det formålet vi beskriver.

Nedenfor er et sett med foreslåtte metadataelementer definert. Hvert enkelt metadataelement er beskrevet for seg. Senere brukes disse for å sette opp ulike profiler for sikkerhetskrav eller -egenskaper. Noen metadataelementer vil naturlig omfatte hele settet med sikkerhetskrav, som «tittel», «type», «opprettet», «dato», «anvendelse», «ansvar» og «språk». Disse brukes da én gang for en sikkerhetsprofil. «Tittel» vil være en identifikator for kravsettet. Hva som vil være et hensiktsmessig utvalg av metadataelementer vil måtte tilpasses på praktiske behov for bruk av metodikken. Utvalget vi foreslår her er basert på at det skal kunne dekke eksemplene på ulike krav, egenskaper m.m. som er vist i vedlegg E og F.

Tittel	"tittel"	content= " "
Navn på den sikkerhetsprofilen som beskrives		

Type	"type"	content= " ordliste "
Type sikkerhetsprofil (sikkerhetspolicy, kravspesifikasjon, applikasjon o.s.v.).		
Format, ordliste: *Policy, kravspec, produktspec, arkitektur, risikoanalyse, metrikk, regelverk, prosedyre.*		

Opprettet	"opprettet"	content= " URL "
Identifikator for institusjon eller virksomhet som har opprettet sikkerhetsprofilen, kravspesifikasjonen el.l.		
Format: *URL, evt. epostadresse*		

Dato	"dato.opprettet"	content=" dato "
	"dato.endret"	content=" dato "
	"dato.overført"	content=" dato "
	"dato.gyldighetsperiode"	content=" dato "
Dato for opprettelse, endringer, overføring til annet system eller gyldighetsperiode		
Format: *YYYY-MM-DD*		

Anvendelse	"anvendelse"	content= " ordliste "
Kontekstavhengige begrensninger. Bruksområde, gyldighetsbegrensninger, peiode o.l.		
Format, ordliste: *Generisk, innleggelse, fastlege, individuell plan, forskning, observasjon, nettverkstilgang, intern, kreditinformasjon, medlemskap, EPJ, kunde*		

Ansvar	"ansvar"	content= " ordliste "
Angivelse av hvem som har rett til å bestemme sikkerhetskrav, dennes funksjon.		
Format, ordliste: *Pasient, pårørende, daglig leder, avdelingsleder, databehandler, forsker, tilsynsperson, systemansvarlig, sikkerhetssjef.*		

Språk	"språk"	content=" ISO639-2[6] "
Angivelse av hvilket språk spesifikasjonen er skrevet på.		
Format, std.: *Språk, se ISO 639-2*		

Relasjon	"relasjon"	content= " ordliste "
Angir kopling eller referanse hvis sikkerhetsparametere beskrevet på forskjellige steder vil være avhengig av eller påvirke hverandre. Kilde eller lenke for relaterte beskrivelser av sikkerhetskrav, lover e.l..		
Format, ordliste: *Kopiert til, kopiert fra, lenke fra (underordnet), lenke til (overordnet), synkroniseres med (sist endret), lov, forskrift, norm, kravspesifikasjon*		

Figur 5: Elementer for beskrivelse av et sett med sikkerhetskrav

Beskrivelse av de enkelte sikkerhetskrav i en kravspesifikasjon gjøres med metadataelementer som brukes én gang for hvert krav som skal beskrives, men bare de elementene som er relevante tas med for hvert krav. Til sammen vil metadataene identifisere og definere den policy, implementering el.l. som skal beskrives for en datamengde, datafil eller datatype. Metadataelementene vi foreslår for å beskrive de enkelte kravene er «konsept» som angir konseptuel tilhørighet, og de kontekstuelt bestemte elementene «beskrivelse», «metrikk» og «referanse».

6 www.loc.gov/standards/iso639-2/langhome.html.

Konsept	"konsept.objekttilgjengelighet"	content= " ordliste "
	"konsept.subjektpålitelighet"	content= " ordliste "
	"konsept.objektintegritet"	content= " ordliste "
	"konsept.subjektintegritet"	content= " ordliste "
	"konsept.behandlingskonfidensialitet"	content= " ordliste "
	"konsept.kontekstkonfidensialitet"	content= " ordliste "
	"konsept.behandlingshjemmel"	content= " ordliste "
	"konsept.utvekslingsansvar"	content= " ordliste "
Konseptuel tilhørighet for kravet velges gjennom å angi «subnavn». Formaliseringsgrad, som vil være knyttet til type krav, for kravet velges fra ordliste.		
Kravtype, ordliste: *Krav (uformell), prosedyre (semiformell), tjeneste(semiformell), mekanisme (formell)*		

Beskrivelse	"kontekst.beskrivelse"	content=" ordliste "
Tekstlig beskrivelse av kontekstuelt krav. Detaljering med beskrivelse av teknologivalg, standarder, protokoller, referanse til kravtabeller o.l. **<Tabell> kan være en forhåndsdefinert oppstilling som refererer til forhåndsgodkjente krav som kan inngå.*		
Format, ordliste: *DES, 3DES, AES, RSA, SHA-1, RC6, SOAP, S/MIME, ebXML, SSH, SSL, GSM, RADIUS, HTTPS, SKCF7, X.509, Crypto API, IIS, ASP.NET, SQL Server, <tabell>**		

Metrikk "kontekst.metrikk" content=" ordliste "
Angir viktighet, sannsynlighet, konsekvens, styrke el.l. og bakgrunn for eller hensikt med kravet. Bruk av skala vil avhenge av anvendelse, som f.eks. risikoanalyse, metrikk, optimalisering av løsningsvalg m.m. I tillegg angis hvordan verdien er fremkommet (metrikk). Vi forutsetter at en metrikk lar seg definere, men går ikke inn på hvordan dette kan gjøres.
Format, ordliste: *Low - 1, medium - 2, high - 3*

Figur 6: Elementer for beskrivelse av enkelte sikkerhetskrav

En ordliste vil inneholde forhåndsdefinerte valgmuligheter for de metadataelementer som det er definert valgmuligheter for. Ordlisten vil defineres og fylles ut for aktuelle behov, bare én felles ordliste brukes for de profiler som skal sammenlignes. Skal man ha kompatibilitet mellom systemer må det være enighet om en felles ordliste for disse. En ordliste med kontekstuelle sikkerhetskrav eller egenskaper vil kunne defineres ut fra behov som finnes for tabellene i kapittel 4 eller vedlegg B – F.

Beskrivelsen av metadataelementene ovenfor sier ikke hvordan elementene skal settes sammen i et sikkerhetskrav eller hvordan flere sikkerhetskrav skal settes sammen til en kravspec. Vi har her kun beskrevet hva de ulike elementene skal forstås som hver for seg. Nedenfor vil vi vise eksempler på hvordan dette kan benyttes.

5.1.2 Eksempel på formulering av enkeltstående sikkerhetskrav

Modellen er her illustrert med et enkelt eksempel basert på et frittstående krav i en kravspec og en funksjon i en applikasjon. De er først beskrevet med bruk av metadatastrukturen. Deretter er sikkerhetsegenskapene holdt opp mot hverandre i et enkelt metrikkoppsett som f.eks. en del av en risikoanalyse.

Krav: En pasient skal ha innsynsrett i sin EPJ.

Tittel	***Innsynsrett pasient***	
Type	Krav i intern instruks	Kravspec
Opprettet av	UUS – Ullevål universitetssykehus	www.ullevaal.no
Dato	opprettet	11.4.2005
Anvendelse	Gjelder all pasientinformasjon	Generisk
Ansvar		Sikkerhetssjef
Språk		Nor
Relasjon	Pasientrettighetsloven	Lov
objekttilgjengelighet		Krav, uformelt
beskrivelse	pasient skal på forespørsel ha innsyn i EPJ	OT.K#
referanse	Pasientrettighetsloven, §-- www.lovdata.no/all/hl-19990702-063.html	www.lovdata.no
metrikk	Lovkrav	Høy: 3

Figur 7: Formulering av et sikkerhetskrav

Tiltak: Applikasjonen har implementert rollebasert tilgangsstyring.

Tittel	***Rollebasert tilgang***	
Type	Applikasjon	Produktspec
Opprettet av	DIPS	www.dips.no
Dato	opprettet	11.4.2005
Anvendelse	Behandling av pasientinformasjon	EPJ
Ansvar		Systemansvarlig
Språk		Nor
Relasjon	EPJ-standarden	Norm
objekttilgjengelighet		tjeneste; semiformell
beskrivelse	Autorisering av tilgangsrett. Enkeltpersoner kan gis tilpassede rettigheter i systemet	OT.T#
referanse	KITH: www.kith.no/templates/kith_WebPage____834.aspx	www.kith.no
metrikk	risikoanalyse	styrke: 2

Figur 8: Formulering av en sikkerhetstjeneste

For å definere en Data Protection Profile for et datasett eller en applikasjon må de sikkerhetskrav eller -egenskaper som til sammen skal utgjøre profilen samles i en DPP. Et verktøy for å beskrive metadatastrukturer hierarkisk vil kunne implementeres i UML, et databaseverktøy som Access el.l.

6 Sammenligning av sikkerhetskrav

En hovedhensikt med å formulere sikkerhetskrav i et enhetlig rammeverk er at det skal være mulig å sammenligne ulike kravprofiler, løsninger og systemers sikkerhetsegenskaper. I dette kapittelet vises en mulig anvendelse av strukturert formulerte sikkerhetskrav til å sette opp en kravprofil for sikkerhet for et sett med data, og hvordan strukturert formulerte og grupperte krav kan være grunnlag for å sammenligne krav i forskjellige spesifikasjoner. Begge deler forutsetter at det er mulig å definere et kvantifiserbart nivå for de enkelte sikkerhetskrav.

Vi vil ikke her gå inn på hvordan sikkerhetsnivåer best kan måles eller hvordan det kan etableres gode metrikker, det er beskrevet mange andre steder [ragl] [NIST2] [gray], og [gilb] som viser hvordan risikoanalyse kan brukes som grunnlag for å kvantifisere f.eks. integritet. Vi vil legge til grunn at det lar seg gjøre for de tilfeller man ønsker å tallfeste eller gradere sikkerhet. Vår hensikt er å vise at dersom man har tilgjengelig resultatene fra en slik måling, eller et estimat på hvor sterkt et krav er eller hvor god en løsning er, kan man bruke det til å vise en profil for kravspesifikasjon eller et systems implementerte sikkerhetsegenskaper.

6.1 Sikkerhetsnivå og -profil

For å sammenligne krav til sikkerhet og tiltak som implementeres for å ivareta sikkerhet vil det være hensiktsmessig å kunne gradere eller måle sikkerheten med en felles skala. Det er da naturlig å se på overordnede krav og behov og bryte disse ned for å finne enkeltindikatorer som forteller noe om hvordan disse behovene ivaretas gjennom en form for monitorering eller måling. Hvis dette skal gjøres over tid, f.eks. for å registrere effekt av endringer, er etablering av en metrikk en egnet metode. En metrikk skal baseres på indikatorer som forteller om utviklingen i sikkerhetsnivået er tilfredsstillende eller hvordan en sikkerhetsparameter forholder seg i forhold til en referanse.

Ved sammenligninger i en statisk tilstand, som hvis en sikkerhetskravprofil skal holdes opp mot en systemsikkerhetsprofil i forkant av oppstart eller oppgradering av et system, har man ikke anledning til å basere seg på en dynamisk tilnærming gjennom logging av informasjon for å registrere om et sikkerhetsbehov er dekket. De krav og egenskaper man ønsker å holde opp mot hverandre må velges og beskrives slik at validitet og reliabilitet for vurderingsmetoden blir tilfredsstillende, men kriteriene må velges ut fra et øyeblikksbilde, spesifikasjoner eller empirisk oppsamlet informasjon fra tidligere aktiviteter. Det må kunne vises at et tiltak som implementeres har en effekt i forhold til det kravet man stiller.

Vi vil her skissere en struktur som et verktøy til bruk når man skal vurdere om en valgt eller implementert løsning har egenskaper som vil kunne forventes å møte et sett med gitte sikkerhetskrav. En mulig måte å strukturere et metrikkoppsett for et statisk sikkerhetsnivået for personopplysninger på, er å ta utgangspunkt i de kontekstuelle sikkerhetsparametrene gruppert etter konseptuel tilhørighet. Tiltakene (funksjoner,

mekanismer, tjenester eller prosedyrer) må analyseres opp mot kravene slik at det kan bestemmes om de vil ha den effekten som ønskes. Dette kan så gis poeng og vekting, og det kan gis en verdi for tillitsverdighet i forhold til forventet eller påkrevd sikkerhetsnivå. I de fleste systemer vil det være enkelte vitale hendelser som ikke skal inntreffe, eller absolutte krav som skal overholdes. Det bør derfor være mulig å markere terskelverdier som skal overholdes i tillegg til veide verdier for mer helhetlige beskrivelser, eller å gi enkelte krav en høy verdi slik at det kreves sterke tiltak for å tilfredsstille dem.

I KITHs forprosjektrapport om bruk av PKI i helsevesenet [KITH5] beskrives forslag til PKI sikkerhetsprofiler med sikkerhetstjenester. Profilene er tilpasset tre sikkerhetsnivåer, høy, medium og lav slik det er skissert i «Uten penn og blekk» [2001:10]. For kritiske anvendelser anbefales å minst bruke sikkerhetsnivå 2, medium, mens sikkerhetsnivå 3, høy, er nødvendig for å oppnå ubetinget rettslig binding. Vi vil ikke drøfte disse sikkerhetsnivåene, men benytter dem som en etablert referanse som kan være egnet for vår metode. Vi definerer for vårt eksempel:

- Nivå 1 representerer krav eller tiltak for å hindre at tilfeldige eller utilsiktede sikkerhetsbrudd oppstår, enten fra interne eller eksterne hendelser eller handlinger. Anbefalt, men ikke obligatorisk.
- Nivå 2 representerer krav eller tiltak som skal gi sikker beskyttelse av personopplysninger, dersom det ikke er utro tjenere som bevisst forsøker å bryte sikkerhetssperrer. Bør tilfredsstilles, men vurderes i helhetlig sammenheng.
- Nivå 3 skal gi beskyttelse mot bevisste forsøk på å bryte sikkerhetssperrer og skal aksepteres som tilstrekkelig tiltak i rettslig forstand. Ufravikelig krav.

Disse sikkerhetsgraderingene er et eksempel for å illustrere en metode, og kan brukes i f.eks. risikoanalyser. De kan erstattes av andre definisjoner av nivåer for andre formål, som f.eks. en vekting med fem nivåer basert på konsekvenser eller trusselnivå som brukt av [simo], eller sikkerhetsklasser fra Common Criteria [CC].

6.2 Sikkerhetsprofil

Ved å tilordne de kontekstuelle sikkerhetsegenskapene eller kravene individuelle nivåer for sikkerhetsstyrke og ordne dem i forhold til den konseptuelle inndelingen, kan det etableres en sikkerhetsprofil for de datamoduler som skal beskyttes, en Data Protection Profile - DPP.

En DPP for en EPJ vil kunne vises som nedenfor. Tabellen viser sikkerhetskrav hentet fra materiale innen helsevesenet, med angivelse av hva slags type krav eller egenskap som beskrives (krav, prosedyre, tjeneste, mekanisme). Eksempelet viser hvordan kravstyrken kan vise hva som vektlegges i denne kravspesifikasjonen. Kun et begrenset utvalg parametere er tatt med, og vi har brukt metadatadefinisjonene til å vise kravet og kravstyrken for hvert krav, og organisert kravene etter formalitetsnivå og

konseptuelle grupper. Oppsettet for tabellen er forskjellig fra tabellene i kapittel 5 for å unngå redundant informasjon, men elementene baseres på de definisjonene som er gitt i kapittel 5. Verdiene for kravstyrker som brukes er ikke basert på reelle vurderinger eller anbefalinger, men brukes kun for å illustrere prinsippet. De vil f.eks. kunne bestemmes ut fra en risiko- eller konsekvensanalyse. Angivelse av «metrikk» viser bakgrunnen for kravet og gir med det premisser for hvordan kravoppfyllelse må verifiseres, men beskriver ikke metrikken og vil utfylles mer detaljert hvis krav er spesifisert. Referanse til nummererte (#) valgbare, predefinerte **K**rav, **P**rosedyrer hhv. gitt gjennom OT.K#, OT.P# for **O**bjekt**T**ilgjengelighet o.s.v. , men vi har ikke utarbeidet slike komplette referansetabeller her. Det enkelte krav er vist samen med et etterfølgende forslag til kravstyrke og grunnlaget for denne. Se også Vedlegg E for et mer utfyllende utvalg av sikkerhetskrav for informasjon i pasientjournaler.

Tittel	***Sikkerhetskrav for pasientopplysninger***	***DPP***
Type	Krav til beskyttelse av persondata	Kravspec
Opprettet av	HiG	www.hig.no
Dato	Opprettet	28.5.2005
Anvendelse	Gjelder all pasientinformasjon	EPJ
Ansvar	Gjennomføring delegert til sikkerhetssjef	Dagl.leder
Relasjon	Personopplysningsloven, Pasientrettighetsloven	Lov
Objekttilgjengelighet		
Krav, uformelt	Pasienten har på forespørsel rett til innsyn i egen EPJ, dersom ikke journalansvarlig gir begrunnet avslag.	OT.K#
Metrikk	Lovkrav: Pasientrettighetsloven	Middels: 2
Prosedyrekrav, semiformelt	Det skal finnes sikkerhetskopi av informasjonen.	OT.P#
Metrikk	Lovkrav: Pers.oppl.forskr. §2-12	Høy: 3
Subjektpålitelighet		
Krav, uformelt	Personopplysningsforskriftens krav skal oppfylles	SP.K#
Metrikk	Lovkrav: Pers.oppl.forskr.	Middels: 2
Objektintegritet		
Krav, uformelt	Formål for registrering av data skal angis, beslutning om behandlingstiltak nødvendig	OI.K#
Metrikk	Lovkrav: Pers.oppl.lov, Helseregisterloven	Lav: 1
Prosedyrekrav, semiformelt	Det skal finnes rutiner for retting, sletting, sperring, signering, låsing.	OI.P#
Metrikk	Krav i standard og sikkerhetsinstruks.	Høy: 3
Subjektintegritet		
Krav om sikkerhetstjenester, semiformelt	Forsøk på uautorisert bruk skal registreres	SI.T#
Metrikk	Lovkrav: Pers.oppl.forskr. §2	Middels: 2

Tittel	*Sikkerhetskrav for pasientopplysninger*	*DPP*
Krav om sikkerhetstjenester, semiformelt	Logging av aksess skal gjøres: Tid, ID, kontekst	SI.T#
Metrikk	Krav i standard	Høy: 3
Behandlings-konfidensialitet		
Krav om sikkerhetstjenester, semiformelt	Sperre mot kopiering av data, lokal lagring ikke tillatt	BK.T#
Metrikk	Krav i standard	Lav: 1
Kontekstuell konfidensialitet		
Krav, uformelt	Tilgang gis kun til relevant info, tilgang skal være nødvendig for aktuell behandling	KK.K#
Metrikk	Krav i standard	Lav: 1
Prosedyrekrav, semiformelt	Det skal være etablert prosedyrer for tildeling av roller og tilgangsrettigheter	KK.P#
Metrikk	Krav i standard. Intern instruks	Middels: 2
Klarering, hjemmel for behandling av opplysninger		
Krav, uformelt	Formål med behandling skal finnes. Vedtak om tiltak	KH.K#
Metrikk	Lovkrav: Helseregisterloven	Lav: 1
Krav, uformelt	Kilde for data angis. Autorisert registrering og registreringsmåte	KH.K#
Metrikk	Krav i standard	Middels: 2
Krav om sikkerhetstjenester, semiformelt	Klassifisering av meldinger og filer, merking sensisitiv/ikke sensitiv i systemet	KH.T#
Metrikk	Krav i intern instruks	Lav: 1
Utvekslingskontroll		
Krav, uformelt	Registrering ved avgivelse av informasjon når oversendt andre	U.K#

Tittel	*Sikkerhetskrav for pasientopplysninger*	*DPP*
Metrikk	Krav i standard	Lav: 1
Krav om sikkerhetstjenester, semiformelt	Informasjon som er referert andre steder må ikke slettes	U.T#
Metrikk	Krav i standard	Lav: 1
Krav om sikkerhetstjenester, semiformelt	Logg av hendelseskronologi: Juridisk, oppgaver, system, revisjon	U.T#
Metrikk	Krav i standard	Høy: 3

Tabell 7: Sikkerhetskravprofil for persondata, Data Protection Profile – DPP.

Denne eksempelprofilen samler sikkerhetskrav som stilles for å kunne behandle et sett med pasientdata i et system. Profilen kan overføres mellom parter som ønsker å dele informasjon. Dersom alle krav gis samme vekt og alle konseptuelle kategorier gis samme vekt vil profilen kunne sies å ha en kravstyrke på:

$$[(2+3)/2 + 2 + (1+3)/2 + (2+3)/2 + 1 + (1+2)/2 + (1+2+1)/3 + (1+1+3)/3]/8 = 1{,}75.$$

Det er også mulig å veie de forskjellige parametrene. Det er neppe mulig å si at et enkelt gjennomsnittstall vil være representativt for en slik sikkerhetsprofil, da utvalget av parametere vil ha mye å si for hvilket styrketall som kommer ut til slutt. Det kan imidlertid være en indikator på endringer i en og samme profil slik at tallet kan inngå i en metrikk for å monitorere hvordan endringer i krav slår ut over tid.

6.2.1 Bruk av sikkerhetsnivå

Gjennomsnittstall vil ha liten verdi alene, men vil kunne gi en indikasjon på hvor to løsninger står i forhold til hverandre, eller om en profil styrkes eller svekkes gjennom endringer som gjøres. Sikkerhetsstyrken for de enkelte konseptuelle kategoriene vil kunne gi noe mer interessant informasjon om en profil. Eksempelprofilen over vil da beskrives med verdiene:

2,5 – 2 – 2 – 2,5 – 1 – 1,5 – 1,3 – 1,7.

En slik tallrekke vil illustrere kravenes profil og vi ser at i dette eksempelet er det tilgjengelighet og integritet som tillegges størst vekt, men det settes svakere krav til konfidensialitet og etterprøvbarhet. Her vil objektilgjengelighet kunne sies å tillegges en kravstyrke, eller viktighet, på 2,5 basert på snittet av de to parametrene som er inkludert. Klareringskontroll ville ha en kravstyrke på 1,3.

For å vurdere om omgivelsene og systemet møter de krav som er satt opp, kan tilsvarende analyser gjøres for implementerte prosedyrer, sikkerhetstjenester og mekanismer. En prosedyreprofil vil kunne utarbeides ved å analysere organisasjonens evne og beredskap for å håndtere sikkerhetsspørsmål. Tilsvarende vil en sikkerhetsegenskapsprofil kunne beskrives for et IT-system ved å beskrive sikkerhetstjenester og mekanismer. Prosedyrer, tjenester og mekanismer grupperes i henhold til den konseptuelle inndelingen som er brukt for sikkerhetskravene

I tabell 8 er det foreslått en oppstilling for sammenligninger av sikkerhetskrav, tiltak og egenskaper. Tallene brukt i tabellen er kun illustrasjoner, de er ikke basert på reelle eksempler, men skal illustrere bruk av tabellen. Avvik indikerer, etter en helhetlig vurdering (risikoanalyse), om systemet og organisasjonen samlet sett tilbyr tilfredsstillende sikkerhet for data som har sikkerhetskrav som angitt i den aktuell DPP. Her vil man f.eks. kunne konkludere med at sikkerhetsnivået for systemet ikke er tilfredsstillende selv om snittallet for prosedyrer, tjenester og mekanismer er høyere enn for kravene, fordi manglene på klarering og utveksling er for alvorlige. Bruk av sikkerhetsnivå og tall i en DPP vil ikke gi et svar direkte, men kan være et støtteverktøy for analyse.

Styrkematrise - DPP	***Sikkerhets-krav***	***Prose-dyre***	***Tjeneste***	***Meka-nisme***	Avvik
Objekttilgjengelighet	2,5	2,5	2,75	2	+
Subjekttpålitelighet	2	2	2,9	2,5	+
Objektintegritet	2	1,5	2	2,5	+
Subjektintegritet	2,5	1,5	2,7	2,9	+
Behandlingskonfidesialitet	1	2,75	2,5	2,5	+
Kontekstuell konfidensialitet	1,5	2,5	1,5	1,5	+
Klarering	1,3	2	1	1	-
Utvekslingskontroll	1,7	1,5	1	1	-
Sikkerhetsstyrke, snitt	**1,75**	**2**	**2**	**2**	

Tabell 8: Nivåmatrise.

En egenskapsprofil for et system vil bygge på andre parametertyper enn en kravprofil, og en en-til-en sammenligning vil ikke nødvendigvis la seg gjennomføre direkte. Det vil trolig likevel være relevant å forvente at sikkerhetsstyrken for et system bør ligge på et tilsvarende eller høyere nivå enn for kravene. Man kan få en første indikasjon på om

et system vil tilby et tilstrekkelig sikkerhetsnivå, men tallverdier på konseptuelt nivå i profilene vil ikke alene være nok til å konkludere på om et system møter de krav som stilles. Det kan først gjøres ved å undersøke i hvilken grad hvert enkelt sikkerhetskrav dekkes av et eller flere tiltak i systemet eller organisasjonen. Sammenligning av tallrekkene for to systemer vil også kunne gi noen innledende indikasjoner på disse systemenes relative styrker.

Både prosedyreprofilen og egenskapsprofilen vil bidra til å dekke kravprofilen, og prosedyrer og egenskaper vil kunne forsterke hverandre gjensidig. Det må imidlertid vurderes for hvert enkelt krav, og reliabilitet og validitet må slås fast. Svakheter i en sikkerhetstjeneste i systemet vil kunne kompenseres for gjennom implementering av egnede prosedyrer, og omvendt.

Hvilket detaljeringsnivå man vil kunne beskrive omgivelsene på vil naturlig nok være avhengig av hvor mye informasjon som er tilgjengelig om systemene og applikasjonene som benyttes. Normalt vil det være noe informasjon tilgjengelig på alle formaliseringsnivåer. Det vil da være mulig å vise hvordan sikkerhetskravene dekkes gjennom en samlet oppstilling av profilene.

6.3 Sammenligning av sikkerhetsnivå

For å kunne gjennomføre sammenligningene av sikkerhetsnivåer som er forutsatt ovenfor, må det etableres et strukturert grunnlag for å sammenligne tallparametere som er estimert fra ulike typer utgangsparametere. Vi vil her indikere hvordan det kan være mulig å gjøre slike sammenligninger, men vil ikke beskrive hvordan man vil kunne tallfeste og kvalitetssikre de tallene for krav og sikkerhetsnivå som brukes.

En struktur for å beskrive indikatorer i en metrikk for sikkerhet i prosedyrer og rutiner etter mønster av NIST 800-55 [NIST] er beskrevet av Fagerjord m/fl [fag.mfl]. Vi har her gitt parametrene et noe annet innhold og forenklet og tilpasset strukturen, men prinsippet for oppsettet er tilsvarende. Vi vil ikke her angi en måling av ytelse eller oppførsel i forhold til et kriterium, men vil vise en struktur for hvordan man kan gjøre en vurdering av i hvilken grad et tiltak har potensial til å støtte et ønsket krav. Vurderingen vil da hovedsaklig være kvalitativ, men resultatene vil representeres med tallverdier for lettere å kunne foreta sammenligninger og dokumentere konklusjonene.

En vurdering av validitet og reliabilitet må inngå som en del av grunnlaget for konklusjonene for å kunne bestemme om tilstrekkelig sterke tiltak er inkludert, men vi vil ikke her gå inn på dette utover å forutsette at manglende reliabilitet eller validitet vil trekke verdien av tiltaket ned. Dersom konklusjonen er at man ikke oppnår ønsket sikkerhet må et tiltak styrkes eller suppleres. For en virksomhet vil dette kunne medføre en kostnad, men beregning av det har vi ikke inkludert som en del av denne metoden. Elementene i strukturen er beskrevet i tabellen nedenfor.

Indikator-navn	***Indikatorbeskrivelse***
Policy, krav	**Krav**: Defineres av et sikkerhetskrav. Et krav gis en styrke i henhold til hvor kritisk det er at kravet overholdes, konsekvenser og hvordan trusselbildet vurderes å ville være.
Funksjon, implementering	**Tiltak**: Defineres av den prosedyren, funksjonaliteten, sikkerhetstjenesten, mekanismen eller protokollen som skal ivareta sikkerhetsbehovet. Det kan knyttes et eller flere implementerte tiltak til hvert krav. Tiltak må ha effekt innen det konseptuelle området som skal beskyttes. Tiltakets styrke vurderes.
Reliabilitet, Validitet	**Reliabilitet** uttrykker om sikkerhetsvurderingen av krav og tiltak vil være repeterbar, og om implementeringen av et tiltak gir samme effekt dersom det gjentas. **Validitet** uttrykker om årsakssammenhengen mellom krav og tiltak er gyldig. Disse forholdene bestemmes ut fra en vurdering av årsakssammenhenger, systeminformasjon og informasjon om brukeromgivelsene og rutiner. Det kan være nødvendig å gjennomføre en risikoanalyse for å kunne konkludere vedrørende validitet og reliabilitet.
Styrketest	De enkelte krav og tiltak gis et styrkenivå, f.eks. 1 – 3, som beskrevet. De enkelte tiltaks effekt og bidrag i å understøtte et krav vurderes. Dersom et tiltak vurderes å være tilstrekkelig sterkt og med tilstrekkelig reliabilitet og validitet vil det gis poeng på nivå med kravet det dekker. Dersom reliabilitet eller validitet mangler, reduseres tiltakets styrke med 1 pr. mangel.
Tiltak, mangler	Beskriver mangler eller mulige tiltak dersom det er gap mellom krav og tiltakenes antatt evne til å dekke kravene.

Tabell 9: Styrkesammenligning

Et eller flere tiltak eller egenskaper settes opp mot et krav som skal dekkes. Styrken for krav og tiltak estimeres ut fra de kriterier som er definert for anvendelsen, disse holdes så opp mot hverandre og må ses i sammenheng. En nødvendig, men ikke tilstrekkelig, forutsetning for at et krav og en egenskap eller tiltak skal kunne vurderes mot hverandre, er at de begge tilhører samme konseptuelle kategori sikkerhetsparametere. Et krav som hører inn under «objekttilgjengelighet» må møtes av et tiltak som man kan vise at har en effekt på objekttilgjengeligheten. Hvis ikke vil manglende validiteten tilsi at tiltaket ikke vil ha noen effekt, og det kan derfor ikke tillegges noen verdi.

Dersom det er et gap mellom krav og oppnådd beskyttelse, må tiltak styrkes eller legges til og oppdatert analyse må gjennomføres for å teste om tiltakene nå gir ønsket beskyttelse.

Som eksempel kan vi se på kryptering av EPJ-filer med AES og 2048 bits nøkkellengde som tiltak for å sikre et system mot at helsepersonell leser journaler til pasienter de ikke deltar i behandlingen av. AES-kryptering kunne isolert gis sikkerhetsstyrke 3, da det ikke er kjente angrep som vil kompromittere algoritmen. Kryperingen vil imidlertid ikke ha noen betydning som beskyttelse mot uautorisert lesing dersom journalen kan dekrypteres og leses av personell med generell tilgang til systemet, og det var forutsatt at konfidensialitet var basert på at disse ikke ulovlig ville forsøke å lese journaler som ikke skulle leses av dem. Tiltaket mangler validitet, og da blir det i dette tilfellet også vanskelig å påvise noen reliabilitet. Vi reduserer derfor sikkerhetsstyrken med to nivåer og tiltaket får verdi 1 i forhold til det gitte kravet. Det forhindrer ikke at krypteringen kan gis full styrke som tiltak mot andre krav, men mot uautorisert lesing må andre tiltak enn kryptering settes inn.

I forrige kapittel ble et sikkerhetskrav fra en kravspec og en funksjon i en applikasjon beskrevet i metadatastukturen. Begge omhandler objekttilgjengelighet, og hører inn under samme konseptuelle kategori. Dersom krav og tiltak vurderes mot hverandre kan vi innpasse dem i strukturen som er definert ovenfor. Kravet vurderes til nivå 2 som innebærer at ikke uvedkommende utenfra eller personell uten behov for å gå inn i denne journalen skal kunne få tilgang.

Indikator-navn	***Indikatorbeskrivelse, objekttilgjengelighet***
Pasient-innsynsrett	**Krav**: På forespørsel skal pasienten ha innsyn i egen EPJ, dersom dette ikke er avslått av journalansvarlig.
Rollebasert tilgang	**Tiltak**: Det er implementert en rollebasert tilgangsstyring for EPJ-systemet som gir anledning til å la pasienten få leserettighet til egen EPJ.
Reliabilitet, Validitet	**Validitet**: Tiltaket har en funksjonalitet som direkte møter kravet og har derfor nødvendig validitet. **Reliabilitet**: Implemetering av tiltaket er ikke kjent, reliabilitet kan ikke fastslås. Tiltaket vil ha effekt, men er ikke komplett da bl.a. autentiseringskrav ikke er beskrevet.
Styrke	Krav om tilgang: Medium sikkerhet påkrevd (nivå 2) Funksjonalitet for tilgang: Medium sikkerhetsnivå (nivå 2), men manglende reliabilitet reduserer vekten til «Lav» (nivå 1).
Tiltak, mangler	Tiltak har ikke tilstrekkelig vekt til alene å sikre pasienten sikker lesetilgang til egen EPJ. Autentisering av pasient må beskrives for å dokumentere reliabilitet.

Tabell 10: Nivåsammenligning, eksempel

Å fastsette sikkerhetsstyrke nøyaktig vil være et omfattende arbeid. Det kan være vanskelig å påvise reliabilitet og validitet kun gjennom en analytisk vurdering av et tiltaks evne til å møte et krav. Det vil som regel være for få bevisbare sammenhenger mellom ulike parametere til å kunne føre formelle bevis. Empirisk verifisering av en sikkerhetsstyrke vil ta lang tid, hvis det i det hele tatt lar seg gjennomføre. Det kan være problematisk å skulle sammenligne et systems sikkerhetsegenskaper med en sikkerhetskravspesifikasjon uten å kunne måtte basere seg på uformell personlig erfaring, empiriske data fra lignende systemer og andre forutsetninger.

Videre analyse av sikkerhetsnivå og hvordan sikkerhetskrav og sikkerhetsegenskaper skal sammenlignes eller metrikker og måleparametere skal defineres ligger utenfor denne oppgavens ambisjon.

7 Diskusjon, konklusjoner og videre arbeid

Vi vil her diskutere noen erfaringer fra vårt arbeid og endringer i forhold til opprinnelig plan, de resultater vi har fremstilt, konklusjoner i en kort oppsummering og forslag til videre arbeid innenfor temaet.

7.1 Erfaringer fra arbeidet

Vi begynte vår undersøkelse som en case-undersøkelse rettet mot å skulle utarbeide en enhetlig beskrivelse av sikkerhetsparametere i helsenett. Utgangsantagelsen var at med mange aktører og ulike tilnærminger til sikkerhetsproblematikk ville det være et behov for samordning av hvordan sikkerhetskrav og -løsninger beskrives. Vi erfarte etter hvert at området langt på vei var standardisert og styrt av premisser for EPJ slik at dette ikke var en konstruktiv vei, men det var et rikholdig kildemateriale som kunne være grunnlag for den oppgavedefinisjonen vi nå har endt opp med. Vi vurderte også andre alternativer, som å utarbeide en mer rikholdig eksempeloversikt av krav fra kravspesifikasjoner og analysere denne, men la det til side da vi ikke hadde et godt definert formål med dette. Kildemateriale inkluderer regulatoriske krav og føringer, etablerte standarder og dokumentasjon fra aktører både på brukersiden og leverandørsiden. Dette ga bredde og mangfold med varierende struktur, detaljeringsgrad og tilnærming til beskrivelse av informasjonssikkerhet.

7.2 Diskusjon, oppnådde resultater

Her diskuteres i hvilken grad vi har oppnådd de resultater vi ønsket og kvaliteten av disse.

7.2.1 Tilfredsstilles krav til en spesifikasjon?

For en Communication Protection Profile (CPP) [13608] er det definert følgende hensikter med beskrivelsen: *Hva CPP'en omhandler – Hvorfor kravet er relevant – Hvilken sammenheng det gjelder og hvem er ansvarlig – Hvordan det kan implementeres*. I den strukturen for sikkerhetskrav (DPP) som vi har satt opp, vil disse kravene være ivaretatt eller dokumenterbare:

- Hva DPP'en omhandler er beskrevet av bl.a. elementene «type», «bruksområde» og «opprinnelse».
- For å fastslå om et krav er relevant må det ses i sammenheng med hva slags data som skal beskyttes. Dette kan f.eks. gjøres ved å referere til lover eller forskrifter for den aktuelle typen data gjennom metadataelementer som angir slike referanser.
- Ansvar og i hvilken sammenhengen DPP'en gjelder og er også ivaretatt i egne metadataelementer.
- Implementering av tiltak som skal gi den ønskede beskyttelse må vises gjennom en sammenligning av krav og tiltak. For å kunne gjøre dette må strukturer tilsvarende kravformuleringen etableres for prosedyrer og systemegenskaper.

Inndelingen etter de konseptuelle gruppene gjør at krav og egenskaper på ulike nivåer og med ulik formaliseringsgrad vil kunne holdes opp mot hverandre. Vi har vist hvordan slike sammenligninger kan settes opp, men vi har ikke gjennomført reelle sammenligninger.

[NASA] setter som mål at en spesifikasjon skal være:

- Complete – tilstrekkelig og presis, ikke unødvendige krav
- Consistent – ikke motstridende beskrivelser
- Correct – tilstander, transisjoner, grensesnitt
- Modifiable – relasjoner må være synlige og sporbare
- Ranked – sentrale krav må kunne identifiseres
- Testable – vurderingskriterier må kunne utledes fra spesifikasjonen
- Traceable – unik identifikasjon av krav
- Unambiguous – ikke flere tolkningsmuligheter
- Understandable – meningen må kunne oppfattes av leseren
- Verifiable – konsistens på tvers av abstraksjonsnivåer

Da vi ikke har hatt som målsetting å spesifisere de enkelte krav blir det ikke relevant å vurdere om en spesifikasjon i seg selv er komplett, konsistent, korrekt, modifiserbar, sporbar og utvetydig. Men gjennom en strukturert fremstilling vil forutsetningene for å oppnå dette generelt være tilstede gjennom den oversiktlighet dette gir. Vår struktur inkluderer også elementer som tillater en rangering av krav og beskrivelse av grunnlag for testoppsett. Dette gir også grunnlag for verifiserbarhet og for å kunne formidle kravene på en forståelig måte. I motsatt retning kan det trekke hvis en struktur ikke tillater tilstrekkelig fleksibilitet og utdyping av krav. Dette har vi forsøkt å unngå ved å tillate fritekst for noen elementer, ved å la ordlistene kunne bygges ut og ved å kunne referere til andre kilder som lover og standarder. Dette vil kunne utvides gjennom å tillate kommentarer i form av fritekst knyttet til f.eks. dato for endringer.

En målsetting har vært å kunne formulere sikkerhetskrav som kan definere de sikkerhetsbehov dataene har, uavhengig av hvordan dette implementeres, og at sikkerhetskravene skal kunne overføres fra et system til et annet. I vår struktur og definisjon av metadataelementer er kravformuleringen system- og applikasjonsuavhengig, men det er ikke en syntaks eller andre strukturelle forhold som garanterer at ikke systemspesifikke krav blir definert. Det blir da en kvalitetssikringsoppgave å garantere at kravformuleringen blir korrekt, f.eks. gjennom å etablere forhåndsvalgte kravdatabaser.

7.2.2 Fleksibilitet i forhold til andre strukturer

Sikkerhetskrav bør kunne formuleres inn i den foreslåtte strukturen selv om de opprinnelig er definert inn i andre organiseringer. Ulike klassifiseringer av

sikkerhetskrav har vært lansert[7]. Men dersom det er mulig å kategorisere de enkelte krav inn i en av de konseptuelle gruppene i vår modell, vil det ikke være grunnleggende motsetninger som hindre denne modellen i kunne brukes, selv om det vil kunne være nødvendig å velge eller beskrive prinsipper for å plassere inn hvert enkelt krav på en konsistent måte. Vi har valgt vår klassifisering ut fra en standard, men valget av klassifisering er ikke avgjørende for metodikken.

Strukturen og definisjonen av metadataelementene bør være i overensstemmelse med etablerte definisjoner og bruk av terminologi. Vår struktur er bygget på de tre klassiske, «globale» sikkerhetskravene tilgjengelighet, integritet og konfidensialitet, med etterprøvbarhet som en fjerde gruppe. Selv om det er alternative måter å gjøre det på, vil de fleste krav la seg kategorisere etter denne inndelingen og de underliggende konseptuelle gruppene. I den strukturen som er beskrevet er ikke sikkerhetsrevisjoner gitt en egen kategori under f.eks. etterprøvbarhet. Krav som gjelder revisjoner og logging er lagt sammen med integritetskravene. Det vil ikke alltid være entydig hvordan et element i et krav skal formuleres eller grupperes. F.eks. vil tilhørighet under enten konfidensialitet eller integritet ofte være et valg man må gjøre når begge muligheter er relevante, men man ikke ønsker redundante krav.

Det er få begrensninger i hvordan definisjonen av de valgbare kontekstuelle kravene gjøres, noe som gir en fleksibel struktur for formulering av kravene. Formuleringen av enkeltkrav bør også ta hensyn til de behov man vil ha hvis et sikkerhetskrav skal sammenlignes med et systems sikkerhetsegenskaper. Dette vil kunne begrense friheten i hvordan krav formuleres, men er et område vi ikke har undersøkt.

En DPP kan være utgangspunkt for forbedringsarbeid i organisasjonen. Strukturering i de ulike konseptuelle kategoriene og angivelse av styrken i sikkerhetsbehov eller løsning kan være et verktøy for å velge rett ambisjonsnivå og å optimalisere valg av løsning. Metodikken vil kunne fungere som dokumentasjon på eget sikkerhetsnivå.

7.2.3 Begrensninger og ikke oppnådde mål

Vi har ikke laget strukturer for hierarkisk innordning eller lenking av krav. Dette vil i mange tilfeller kunne gi mer lesbare, gjenbrukbare eller komprimerte strukturer uten unødvendig redundans, men kan i noen grad kompenseres gjennom hvordan data om sikkerhetskravene presenteres.

Vår struktur gir ikke uten videre målbare eller etterprøvbare kravformuleringer. Det vil kunne være nødvendig med en risikoanalyse eller systemanalyse for å avgjøre om et krav tilfredsstilles eller ikke. Men strukturen er et verktøy for å systematisere en slik prosess siden de konseptuelle kategoriene er gjennomgående som sorteringsnøkkel. Mer detaljerte krav vil være lettere å sammenligne med andre krav eller egenskaper, selv om disse ikke har samme detaljeringsgrad.

Det er også mulig å sammenligne en DPP for sikkerhetskrav med tilsvarende

7F.eks. [fire] som bruker: identification, authentication, authorization,immunity, integrity, intrusion detection, nonrepudiation, privacy, security auditing, survivability, physical protection og system maintenance security requirements.

formulering av sikkerhetsegenskaper for systemer og organisasjoner. En slik sammenligning er vanskelig gjennomførbar som en en-til-en prosess p.g.a. ulik formaliseringsgrad i beskrivelsen og fordi man inntar ulike perspektiver for formuleringene. En sammenligning må derfor baseres på risiko- og sikkerhetsanalyser. Det er likevel mulig å benytte DPP-modellen for å danne basis for å avgjøre hvorvidt en partnere har en sikkerhetspolicy som passer de sikkerhetskrav som stilles for dataene.

En intensjon med PrENV 13608 er å kunne gi en løsning á priori tillit, basert på overensstemmelse mellom sikkerhetskrav og implementerte tiltak i kommunikasjonskanalen. Vi må da spørre: Kan vi á priori gi et system tillit hvis det er implementert visse tjenester for å ivareta informasjonssikkerheten? Vi kan ikke med grunnlag i vårt arbeid si at det er etablert et grunnlag for det. Dette er fordi det vil kreve en undersøkelse av et antall faktiske eksempler, og fordi en sammenligning av sikkerhetskrav og tilsvarende tiltak som skal møte kravene vil kreve omfattende sikkerhetsanalyser. Dette er det ikke tid til i denne oppgaven.

En DPP kan være basis for definisjon av en metrikk for å angi en løsnings godhet i forhold til et krav. Den nivåbeskrivelsen som er benyttet er ikke eksakt og vil kreve en kvalitativ vurdering av behov, implementering, reliabilitet og validitet. Metodikken angir likevel en enhetlig struktur for å formulere slike aspekter, og dermed legge grunnlag for at beskrivelser med ulike perspektiver kan sammenlignes.

Hvis krav skal knyttes til et sett med data vil ikke krav som relateres til brukssituasjoner, som f.eks. EPJ, skulle inkluderes. Hvis man definerer er krav om 99,9% oppetid vil ikke det nødvendigvis være et krav for alle som skal behandle informasjon fra denne datamengden. Statistikkuttrekk vil f.eks. ikke kreve en slik oppetid. Slike krav knyttes mer naturlig til den aktuelle applikasjon eller brukssituasjon. Dette kan ivaretas gjennom et metadataelement som beskriver bruksområdet for kravspesifikasjonen. Et annet sikkerhetskrav som vil kunne stilles, og som vil sette krav til systemet er f.eks. et krav om at ingen data skal gå tapt ved uforutsette eller planlagte driftsforstyrrelse, ytre eller indre angrep. Risikoen for slike situasjoner vil være svært forskjellig for forskjellige systemer, men sikkerhetskravet er definitivt knyttet til de dataene som behandles.

7.2.4 Test case – EPJ

Vi har sett på beskrivelser av sikkerhetskrav for elektroniske pasientjournaler (EPJ), og har undersøkt i hvilken grad kravene lar seg passe inn i strukturen vi har beskrevet tidligere. Innholdet i en EPJ vil typisk kunne være opplysninger som kan overføres, og hvor sikkerhetskravene for å kunne behandle pasientdata vil gjelde i flere systemer knyttet opp mot helsenettet. En nærmere beskrivelse av sikkerhetskrav og applikasjoner for EPJ finnes i Vedlegg E og F. Noen aktuelle problemstillinger for EPJ, som illustrerer behovet for å knytte sikkerhetskrav til et gitt sett med data, er:

- Behov for akutt tilgang til opplysninger i forbindelse med nødsituasjoner, såkalt blålysfunksjon, er et tilleggsaspekt i vurdering av såvel tilgjengelighet som

autentisering, og må kunne knyttes til moduler av opplysninger og ikke bare til systemet.
- Det vil kunne være behov for å kunne gjøre utvalgte journalopplysninger tilgjengelig, gjerne i form av ett eller flere dokumenter, etter forespørsel fra helsepersonell i annen virksomhet eller et forsikringsselskap. Det er da nødvendig med samtykke fra pasienten eller å sikre et annet gyldig rettslig grunnlag.
- Det kan i prinsippet opprettes forbindelser til komponenter i EPJ for samme pasient hos annen virksomhet og det kan opprettes lenker til komponenter i andre pasienters EPJ. I tillegg kan det være behov for å kunne sende forespørsel om overføring av journalinformasjon.

Sikkerhetskrav for EPJ har en rekke opprinnelser:

- **Lover**: En oversikt over lover som stiller krav til beskyttelse av pasientopplysninger er gitt i Vedlegg A. Lovene skal være teknologinøytrale og gir bare unntaksvis føringer som kan koples direkte til implementering av løsninger.
- **Standarder**: EPJ-standarden [KITH3] beskriver en kravstruktur med funksjonelle krav og krav til tabeller og attributter. Kravene skal følges ut fra hva som er relevant for virksomhetenes behov. Kravene klassifiseres i tre nivåer: Obligatoriske krav, avanserte krav og anbefalinger.
- **Instrukser og prosedyrer**: Sykehusene har interne rutiner og instrukser som sier hvordan pasientinformasjon skal håndteres [UUS].
- **Kommunikasjon**: I Østnorsk helsenetts[8] kravspesifikasjon for nettverkssikkerhet settes krav til systemet, ikke til beskyttelse av data [ØNH].
- **PKI**: Forprosjektrapporten [KITH5] beskriver forslag til PKI sikkerhetsprofiler med sikkerhetstjenester for ikke-benekting, autentisering, kryptering og integritetssikring.
- **Applikasjoner**: Disse vil ikke inneholde sikkerhetskrav, de skal være utviklet med egenskaper og tjenester som møter kravene.

Vi har i eksempelet i vedlegg F inkludert krav fra kilder som beskrevet ovenfor. I denne strukturen kan en komplett kravspesifikasjon for et datasett formuleres og overføres til andre systemer, samtidig som historiske krav kan bli ivaretatt.

7.3 Konklusjoner

Vårt primære forskningsspørsmål var å undersøke hvordan vi kunne etablere et enhetlig rammeverk for formulering av sikkerhetskrav for en avgrenset mengde eller type data, slik at kravene kan overføres til andre omgivelser uten å være bundet til et system. Sikkerhetskravene skulle kunne brukes som referanse for sikkerhetsprosedyrer, -tjenester og -mekanismer i ulike omgivelser.

8 Østnorsk helsenett er nå en del av Norsk helsenett AS.

Vi har:

- beskrevet en metadatastruktur for å definere elementer i et sikkerhetskrav på en enhetlig måte.
- vist hvordan sikkerhetskrav formulert med bruk av metadataelementene kan representere en kravspesifikasjon og en sikkerhetsprofil for et gitt sett med data.
- vist eksempler på kravspesifikasjoner og applikasjonsegenskaper formulert gjennom bruk av metadataelementene.
- vist at sikkerhet i ulike perspektiver som sikkerhetskrav, sikkerhetsegenskaper, prosedyrer el.l. kan beskrives strukturert slik at de kan sammenlignes med tanke på kravstyrke eller sikkerhetsstyrke.

Vi har brukt flere dimensjoner i vår fremstilling av sikkerhetskrav:

- gruppering etter konseptuelle kriterier: objekttilgjengelighet, subjektpålitelighet, objektintegriet, subjektintegritet o.s.v.
- grad av formalisering: formell, semiformell, uformell etter anvendelse for h.h.v. mekanismer, prosedyrer, sikkerhetstjenester og kravspesifikasjon.
- metadataelementer for oppbyggingen av krav

De to første av disse dimensjonene brukes hovedsaklig for å gruppere sikkerhetskravene, men metadataelementene formulerer og definerer kravet. Formuleringen tar også vare på informasjon om grupperingen og sier med det noe om kravets karakter.

Vi har gjennom dette nådd hovedmålsettingen med vårt arbeid ved å beskrive en kjernestruktur. Det gjenstår imidlertid vesentlig både teoretisk og praktisk arbeid for å plassere dette inn en en anvendbar og konsistent sammenheng sammen med andre behov, kravfremstillinger og systemomgivelser.

7.4 Videre arbeid

Med vår struktur er det mulig å formulere datasentriske, portable sikkerhetskrav, men for å oppnå uavhengighet av system, applikasjon, organisasjon og situasjon må det utarbeides databasegrunnlag for de forhåndsvalg som skal være mulig. Vi har gjort dette for et svært begrenset utvalg sikkerhetskrav og egenskaper som hovedsaklig er hentet fra helsesektoren, men for en generalisering av bruken må andre sektorer som f.eks. finans, tjenester og offentlig administrasjon inkluderes. Generell bruk av strukturen vil måtte inkludere valgmuligheter tilpasset alle typer data. Det kan også være aktuelt å se på situasjonsbetingede krav, selv om disse ikke er rent datasentriske.

For å kunne sammenligne dataenes sikkerhetsbehov med den implementerte sikkerheten i et system, må systemsikkerheten fremstilles basert på en tilsvarende struktur. Dette har vi beskrevet på et innledende nivå. Beskrivelse av systemers sikkerhetsnivå er derfor nødvendig å inkludere i rammeverket. Det må da defineres nødvendige metadataelementer for dette og databaser med valgmuligheter for

systemegenskaper må utarbeides.

Det må utvikles metoder for sammenligning av et sikkerhetskrav med den sikkerhet implementeringen av en prosedyre, tjeneste eller mekanisme gir, basert på kvantifiserbare kriterier. Dette inkluderer et tiltaks sikkerhetsstyrke og styrken i et sikkerhetskrav. Vi har antydet dette i vårt arbeid, men ikke utviklet slike metoder. Flere tidligere arbeider har berørt dette temaet, men det er ikke etablert normative standarder for slike sammenligninger. Til dette arbeidet hører også prinsipper for vekting av krav og egenskaper og utvikling av metrikker for å observere utviklingen av sikkerhetsnivået med hensyn på de krav og egenskaper som er beskrevet.

Utvikling av kravprofiler eller sikkerhetsprofiler for nettverk, applikasjoner, organisasjoner og systemomgivelser vil være en bekreftelse på anvendbarheten av rammeverket. For dette bør det utvikles hjelpeverktøy i f.eks. UML eller Access. Bedre fremstilling av sikkerhetsstrukturen med tanke på lesbarhet og lett forståelige krav må også utvikles videre. Videre bør det gjøres sammenligninger mellom denne metoden å angi sikkerhetskrav på i forhold til andre metoder med tanke på opplæring, bruk og de kvalitetskriterier som settes for kravspesifikasjoner, hvorav noen er nevnt i oppgaven. Flere kommersielt tilgjengelig applikasjoner tilbyr verktøy for kravspesifisering og systemmodellering, f.eks. gjennom beskrivelse av sikkerhetsrisiko i UML use cae eller misuse case for angrep på systemet, som beskrevet i [Telel]. En undersøkelse av slike verktøys egenskaper opp mot vårt behov ville kunne gi svar på om hvor egnet de er for å definere portable sikkerhetskrav for data.

Bibliografi

Artikler

Ell.mf R.J.Ellison, A.P.Moore, L.Bass, M.Klein & F.Bachmann: "Security and Survivability Reasoning Frameworks and Architectural Design Tactics", Technical Note CMU/SEI-2004-TN-022, Carnegie Mellon Univ. 2004

Elvi E.Henriksen & E.Skipenes: "Sikkerhetsaspekter ved nettbasert tilgang til pasientinformasjon", Delrapport fra Elviraprosjektet, Nasjonalt Senter for Telemedisin, 2001,www2.telemed.no/publikasjoner/ nedlastbare/sikkerhetsaspekter.pdf

Elvi2 Bellika m.fl.: "Nettbasert pasientinformasjonssystem - Hovedrapport fra Elviraprosjektet", Nasjonalt Senter for Telemedisin, 2001

falc E. Falck: "Sikker kommunikasjon for ambulerende medisinske enheter", NTNU, 2004,www.q2s.ntnu.no/annualreport2004.pdf

fire D.G.Firesmith: "Engineering Security Requirements", 2003,www.jot.fm/issues/issue_2003_01/column6

fire2 D.G.Firesmith: "Specifying Reusable Security Requirements", 2004,www.jot.fm/issues/issue_2004_01/column6

gray M.Gray: "Applicability of Metrology toInformation Technology", Volume 104, Number 6, Journal of Research of the National Institute of Standards and Technology, 1999

has&ut Hasle og Uthaug: "Dynamisk tilgangsstyring ved bruk av roller i helseinformasjonssystemer", NTNU, 2002,www.idi.ntnu.no/grupper/su/su-diploma-2002/ hasle-TilgangsstyringHelseinfoSystemer.pdf

heitm C.Heitmeyer: "Applying Practical Formal Methods to the Specification and Analysis of Security Properties", Naval Research Laboratory, 2001

jøs&kn A.Jøsang, S.J.Knapskog: "A Metric for Trusted Systems", NISSC 98, 1998

knap Knapskog, Årnes og Gaup: "Security services in dynamic network environments for mobile users", NTNU, 2005,www.q2s.ntnu.no/project-sservicesmobile.php

lima Berit Lima: "Elektronisk pasientjournal og personvern i allmennlegetjenesten", Universitetet i Oslo, 2002,www.afin.uio.no/forskning/hovedfag/BeritLima_OK_DT.pdf

lund	Lund m.fl.: "UML profile for security assessment. Technical report STF40 A03066", SINTEF, 2003
mand	K.D.Mandl, P.Szolovits & I.S.Kohane: "Public standards and patients' control: how to keep electronic medical records accessible but private", 2001
McDa	P. MacDaniel: "On context in Authorization Policy", AT&T Labs - Research, 2003
McDa.mf	P. McDaniel og A. Prakash: "Methodes and Limitations of Security Policy Reconciliation", AT&T Labs - Research, 2002
moe	N.B.Moe m.fl.: "Sikkerhetsarkitektur for planbasert samarbeidsjournal", SINTEF, 2004
maal	Ole Kristian Maalbakken, "Towards meassuring Legal Compliance", HiG, 2004
NASA	W.M.Wilson, L.H.Rosenberg & L.E.Hyatt: "Automated Quality Analysis Of Natural Language Requirement Specifications", NASA Software Assurance Technology Center, 1996, satc.gsfc.nasa.gov/support/PNSQC_OCT96/pnq.html
NIST2	L.Carnahan, G.Carver, M.Gray, M.Hogan, T.Hopp, J.Horlick, G.Lyon & E.Messina: "METROLOGY FOR INFORMATION TECHNOLOGY (IT)", NIST, 1997, www.itl.nist.gov/lab/nistirs/ir6025.htm
patz	G.Patz, M.Condell, R.Krishnan & L.sanchez: "Multidimensional Security Policy Management for Dynamic Coalitions", BBN Technologies, 2001 IEEE,0-7695-1212-7
payn	Shirley C. Payne: "A Guide to Security Metrics", SANS, 2001, www.sans.org/n/papers/index.php?id=55
pope	B.C.Popescu, B.Crispo, A.S.Tanenbaum & M.Zeeman: "Expressing security policies fpr distributed objects applications", Vrije Iniversiteit, Amsterdam, 2004
ragl	B.Ragland: "Measure, Metric, or Indicator: What's the Difference?", Software Technology Support Center, 1995
røst	L.Røstad: "Sikring av helseinformasjon i distribuerte systemer", NTNU, 2002
SamPro	L.Røstad, Ø.Nytrø, N.B.Moe, E.Stav & G.Skylstad: "Sikkerhetsarkitektur for PlanBasert Samarbeidsjournal SPBS v.2.0", SINTEF, 2004, www.sampro.no
simo	G.Simonsen: "En prosess for Sikkerhets Metrikk Program (SMP)"; HiG, 2004

ski&sø	Skinnes og Sørvik: "Anvendelsesområder og sikkerhetsløsninger for RFID-teknologi i helsesektoren", Høgskolen i Agder, 2004
sloman	M.Sloman, N.Dulay & B.Nuseibeh: "SecPol: Specification and Analysis of Security Policy forDistributed Systems", Impreial College, dpt. of Computing, 1998
white	S.White: "Requirements Capture and Analysis Prior to Modeling", ATDC Northorp Grumman Corporation, 1997, IEEE, 0-81867889-5
wies	René Wies: "Using a Classification of Management Policies for Policy Specification and Policy Transformation", University of Munich, 1995
wold	Gullik Wold: "Key Factors in making Information Security Plicies effective", HiG, 2004
	Bøker
cres	John W. Creswell: "Research Design", Sage Publications, 2002,0-7619-2442-6
dale	Daler, Gulbrandsen, Hole, Melgård, Sjølstad: "Håndbok i datasikkerhet", Tapir, 2002,82-519-1785-9
goll	Dieter Gollmann: "Computer Security", John Wiley & Sons, 2001,0-471-97844-2
scha	Dag Wiese Schartum og Arild Jansen: "Informasjonssikkerhet, Rettslige krav til sikker bruk av IKT", Fagbokforlaget, 2005,82-450-0274-7
	Premissgivende dokumenter
Arkf	Forskrift om offentlege arkiv, KKD, 1998, www.lovdata.no/for/sf/sf-19921204-126.html
ASTM	ASTM D 3565, "E2085-00a Standard Guide on Security Framework for Healthcare Information", ASTM International
CC	"Common Criteria", ISO/IEC 15408, ISO, 1998, www.commoncriteriaportal.org/
ITSEC	"ITSEC - Information Technology Security Evaluation Criteria", CEC, 1991
KITH	A.Vestad: "Krav til kommunikasjonssikkerhet for EDI-løsninger", KITH, 2002,82-7846-128-7,www.kith.no/rapportarkiv/edisikk.pdf
KITH2	Arnstein Vestad: "Anbefalinger og standarder for PKI i helsesektoren, R13-04", KITH, 2004
KITH3	M.Alsaker: "Indikatorer for informasjonssikkehet, 04/08", KITH, 2004,82-7846-225-9
KITH4	T. Nystadnes: "EPJ-standard: Arkitektur, arkivering og tilgangsstyring",

	KITH, 2001, www.kith.no/templates/kith_WebPage____834.aspx
KITH5	B.Aksnes, A.Vestad, E.Henriksen, E.Skipenes, I.E.Kvaase m.fl.: "Forprosjektrapport for PKI i helsevesenet, KITH rapport 3/02", KITH, 2002,82-7846-127-9
nhn	Arbeidsgruppe: "Implementering av PKI i norsk helsevesen - Forslag til utrullingsplan for helseforetakene", Nasjonalt helsenett, 2004
NIST	"Special Publication 800-55, Security Metrics Guide for Information Technology Systems", NIST, 2003
OECD	"OECD rettningslinjer for sikkerhet i informasjonssystemer og nettverk: Mot en sikkerhetskultur", OECDs råd, 2002,webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase
Pof	Forskrift om behandling av personopplysninger (personopplysningsforskriften), Moderniseringsdepartementet, 2000,www.lovdata.no/for/sf/mo/mo-20001215-1265.html
Pol	Personopplysningsloven: LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger, Justis- og politidepatementet, 2000,www.lovdata.no/all/hl-20000414-031.html
RTV	PKI-prosjektet, "Rammeavtale for PKI-løsning, Bilag 1 - Avtaleforvalters formål og kravspesifikasjon", Rikstrygdeverket, 2003
SHdir	"Norm for informasjonssikkerhet i helsesektoren, versjon 1 (Høringsutkast)", Sosial- og helsedirektoratet, 2005,www.shdir.no/index.db2?id=15003
SHdir2	"Kryssreferansetabell - Forskrift til personopplysningsloven og Norm for informasjonssikkerhet", SHdir, 2004
Sikf	Forskrift om personellsikkerhet, Forsvarsdepartementet, 2001,www.lovdata.no/for/sf/fo/fo-20010629-0722.html
Sikl	LOV 1998-03-20 nr 10: Lov om forebyggende sikkerhetstjeneste, Forsvarsdepartementet, 1998,www.lovdata.no/cgi-wift/ldles?doc=/all/nl-19980320-010.html&5
TCSEC	"Orange Book, Trusted Computer Security Evaluation Criteria" DOD 5200.28-STD, US Department of Defence, 1985,0-1302-9386-5
UUS	H.Thorstesen: "Gjennomføring av konsesjon/melding ved behandling av personopplysninger", Ullevål Universitetssykehus, 2003
WELLA	"Pasientintensiv informasjon over Internett på en sikker måte", WellDiagnostics, 2004,www.well.no
WELLC	"En komplett og moderne kommunikasjonsløsning", WellDiagnostics, 2004,www.well.no

ØNH	"Kravspesifikasjon for etablering av østnorsk helsenett", Helse Øst, 2001
10181	"ISO/IEC 10181-1:1996 Information technology - Open systems interconnection - Security frameworks for open systems: Overview", ISO, 1996
13606	prENV 13606-1: Health informatics - Electronichealthcare record communication, CEN/TC 251/WG I, 1999
13608	PrENV 13608: Sikkerhet for kommunikasjon i helsevesenet, CEN/TC251, CEN, 1999
17799	NS-ISO/IEC 17799, "Information technology - Code of practice for information security management", ISO
2001:10	"Uten penn og blekk", NOU 2001:10, 2001, www.odin.dep.no/mod/norsk/publ/utredninger/NOU/002001-020005/dok-bu.html
7498	ISO/OSI 7498-2 Basic Reference Model - Part 2: Security Architecture, ISO
	Annet materiale
bygr	Lee Bygrave: "Legal Aspects of Information Security in the Nordic Countries", Nordiske Seminar- og Arbejdsrapporter 1993:613, Appendix 1, Nordic Council of Ministers, 1993
chad	David Chadwick: "The PERMIS X.509 Based Privilege Management Infrastructure", University of Salford, 2002,sec.isi.salford.ac.uk/download/aaarch-Permis-00.txt
daVin	"Persondatautveksling i Norge", daVinci Consulting, 2004www.enorge.org/modules/module_111/news_item_view.asp?iNewsId=2603&iCategoryId=153
dent	Alex Dent, "Standards and Evaluation Criteria - Presentation", Royal Halloway University of London, Information Security Group, 2005, www.isg.rhul.ac.uk/msc/modules/opt7.shtml
fag.mfl	Fagerjord, Kosmerlj & Ween: "Security Metrics for Procedures and Routines", 2003
haug	Are Vegard Haug, "Rettslig regulering av informasjonssikkerhet", IKT SOS Workshop/Seminar, UiO/AFIN, 2005
iAccess	Ø.Nytrø: "Prosjektbeskrivelse, iAccess", NTNU, 2004
KIS	Koordineringsutvalget for informasjonssikkerhet, Moderniseringsdepartementet, 2004,odin.dep.no/nhd/norsk/024101-070050/dok-bu.html
MAFI	"The MAFIIA Handbook - An Architectural Description Framework

	forInformation Integration Systems", SINTEF (Intern), 2003
NEMA	"Security and Privacy: An Introduction to HIPAA", The Privacy and Security Committee, Medical Imaging Informatics Section, NEMA, 2001
stab	T.Stabell-Kulø & F.Dillema: "PENNE - the pesto of security, reliability and robustness", UiT, 2005
CORAS	Ketil Stølen: "CORAS project", 2004,coras.sourceforge.net
DC	Dublin Core, "Dublin Core Metadata Initiative", dump 2005,dublincore.org
DIPS	"DIPS-systemen" (Webdump mai 2005), DIPS, 2003, www.dips.no/dipsnew.nsf/Display/Dipssystemene
ebXML	About ebXML, OASIS, www.ebxml.org
ENFORCE	K.Stølen, "ENFORCE project web pages", UiO, 2005,heim.ifi.uio.no/~ketils/enforce/enforce.htm
gilb	T.Gilb: "Quantifying Security", 'Practical software quality and testing' (PSQT), 2004,www.abelia-innovasjon.no/pub/config/dir_struc_root/2012_1101989770_GilbQuantifyingSecurityINCOSENOv16_04.pdf
HIPAA	Tom Grove: "Summary Analysis: The Final HIPAA Security Rule", HIPAA advisory, 2003, www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm,
Infodoc	Omtale av Infodoc, mai 2005, Infodoc, 2005, www.kith.no/templates/kith_WebPage____1115.aspx
PERMIS	PERMIS Project: "Permis - PrivilEge and Role Management Infrastructure Standards Validation", 2002, www.permis.org/en/index.html
PGP	Web of Trust - PGP, www.cam.ac.uk.pgp.net/pgpnet/
q2s	Centre for Quantifiable Quality of Service in Communication Systems, NTNU, 2005, www.q2s.ntnu.no
SAMATE	P.Black: "NIST Software Assurance Metrics and Tool Evaluation (SAMATE) project", NIST, 2005, www.itl.nist.gov/lab/nistirs/ir6025.htm
SEID	"SEID-prosjektet har levert anbefaling om norsk sertifikatprofil", Moderniseringsdepartementet, 2004 odin.dep.no/mod/modernisering/tverrgaendeprosjekter/pkiorgan/aktuelt-pki/p30005007/002001-991452/dok-bn.html
SESAM	Bjarte Aksnes: "Sikker Elektronisk SAMhandling i helsesektoren", KITH, 2001, www.kith.no/informasjonssikkerhet_prosjekter/11112/
Telel	Ian Alexader: "Why I use DOORS/DXL for System Modelling", Easyweb,

2002, easyweb.easynet.co.uk/~iany/consultancy/why_doors_dxl.htm

TROPOS TROPOS project, Requirements-driven development for Agent SW, University of Trento, 2004, www.troposproject.org

Vedlegg A: Offentlige føringer og juridisk rammeverk for behandling av personopplysninger i helsenett

Regulatoriske krav

En rekke sikkerhetsparametere på overordnet nivå bestemmes av regulatoriske forhold gitt i lover og forskrifter. Dette er parametere som er styrende for alle de angår, men som ofte har rom for ulike fortolkninger og implementering. Flere offentlige organer har gjennom veiledninger og standarder spesifisert sikkerhetskrav som ikke nødvendigvis er pålagt av myndighetene, men som likevel vil være obligatoriske gjennom at aktører vil måtte inngå avtaler med offentlig eide virksomheter som krever at disse standardene overholdes. Dette vil i praksis fungere som et pålegg bransjen vil være nødt til å overholde.

Relevante lover og forskrifter med tanke på informasjonssikkerhet ved deling og overføring av persondata er både de lovene som gjelder all elektronisk behandling av persondata, som Personopplysningsloven, Arkivloven og Forvaltningsloven, og de lovene som er rettet mot helse som virksomhetsområdet, som Helsepersonelloven, Pasientrettighetsloven og Helseregisterloven, med forskrifter. Videre er det gitt krav som må tilfredsstilles ved bruk av spesielle typer løsninger i lover som Elektronisk signatur loven og tilhørende forskrifter og anbefalinger eller i KITHs EPJ-standard. Lovene, forskriftene og andre relevante standarder og anbefalinger beskriver ikke alltid først og fremst sikkerhetsforhold, men behandler også rettigheter, plikter og funksjonelle forhold som skal ivaretas.

Aktuelle lovebestemmelser[9]

Et stort antall bestemmelser er en utfordring, bl.a. p.g.a. et tidvis stort tolkingingsrom og at flere bestemmelser må ses i sammenheng. Lover og forskrifter som har bestemmelse med direkte følger for behandling av persondata i helsenett (pasientdata) er:

- Pasientrettighetsloven
- Helsepersonelloven
- Journalforskriften
- Helseregisterloven
- Personopplysningsloven, Personopplysningsforskriften
- Kommunehelseloven
- Spesialhelsetjenesteloven
- Psykisk helsevernlov
- Forskrift om individuelle planer
- Arkivloven
- Forvaltningsloven
- Eforvaltningsforskriften
- Elektronisk signaturloven

9 Kilde: Nystadnes, KITH, 9.11.2004 og [lima]

Pasientrettighetsloven angir rett til tilpasset informasjon og innsyn i journalen. Loven beskriver bruk av helseopplysninger med eller uten samtykke fra pasienten og pasientens rett til å kreve sletting eller retting behandles også.

Helsepersonelloven angir hvilken dokumentasjonsplikt helsepersonell har, hvem som omfattes av denne med lovbestemte roller i forhold til pasienten, hva slags handlinger som skal dokumenteres, journalansvar og krav til føringen av journalen. Pasientens muligheter og begrensninger til å bestemme over hvem som skal kunne få del i opplysninger er angitt, samt forhold rund krav om retting og sletting av journalopplysninger.

Journalforskriften beskriver krav til journalens innhold og forhold til andre dokumenter, som arbeidsdokumenter med opplysninger som ennå ikke er ført inn i journalen. Helsepersonelloven gir anledning til å opprette en forskrift for EPJ. Dette er ikke gjort, men pasientjournalforskriften har bestemmelser som er relevante for EPJ. I utgangspunktet skal én pasient ha én EPJ, men dette kravet er ikke absolutt hvis faglige eller organisatoriske forhold gjør at en virksomhets enheter fremstår som separate. Samtidig kan forskjellige virksomheter ikke ha felles EPJ. Overføring av EPJ til annen virksomhet vil være aktuelt f.eks. ved bytte av fastlege eller hvis en virksomhet opphører. Forskriftens krav til tilintetgjøring gjelder også EPJ og får konsekvenser f.eks. ved utskifting av EDB-utstyr.

Helseregisterlovens formål angir både at personvernhensyn skal ivaretas og at helseforvaltning og helsetjenesten skal ha tilgang til nødvendig kunnskap for forsvarlig og effektiv helsehjelp. Loven bygger på EUs personverndirektiv (95/46/EC)[10]. Bestemmelser i helseregisterloven går foran bestemmelser i personopplysningsloven, men ikke foran helsepersonelloven.

Helseregisterloven slår fast at det skal fremgå hvem som har registrert opplysninger i EPJ, og dette kan gjøres ved elektronisk signatur eller tilsvarende sikker dokumentasjon. Virksomheten som tar i bruk EPJ vil være databehandlingsansvarlig.

Helseregisterloven gir også anledning til å opprette regionale, lokale eller sentrale helseregistre, enten gjennom forskrift eller med direkte hjemmel i loven. Slike registre vil kunne ha andre krav til samtykke ved bruk av helseopplysninger enn en EPJ dersom opplysninger er avidentifisert eller behandles pseudonymt eller gjennom lovhjemmel.

Som for annen bruk av personregistre skal også behandling av helseregistre ha et uttrykkelig formål og behandlingen av helseopplysninger skal være relevant og nødvendig for formålet. Også sammenstilling av opplysninger fra flere EPJ om samme pasient tillates etter samme krav om formål, relevans og nødvendighet. Helseregisterloven sier, i tillegg til kravet om tilfredsstillende informasjonssikkerhet,

10 Et forslag til en metrikk for å måle overensstemmelse med EU-direktivet er beskrevet av Målbakken, HiG/NISlab 2004 [maal].

at det skal etableres internkontrollsystem for å sikre at kravene overholdes og at Datatilsynet skal gis detaljert melding om formål, innhold, kilde, utlevering, sikkerhetstiltak m.m., noe som også gjelder EPJ.

Kommunehelsetjenesteloven sier at kommunehelsetjenesten skal utarbeide en individuell plan for visse pasientgrupper, og samarbeide med andre tjenesteytere for å etablere et helhetlig tilbud for pasienten. Denne planen vil inngå i pasientens EPJ, og omfattes således av de krav som gjelder for EPJ.

Spesialhelsetjenesteloven sier at helseforetaket ska utarbeide en individuell plan for visse pasientgrupper. Institusjonen pålegges å gi pasienten informasjon og å sørge for forsvarlig bruk av IT-systemer.

Psykisk helsevernloven gir også krav om individuell plan for hver pasient som er underlagt psykisk helsevern. Det kreves samtykke hvis helsevernet er frivillig.

Forskrift om individuelle planer etter helselovgivingen definerer pasientens rett til og kommunens og helseforetakets ansvar for å få utarbeidet en individuell plan. Dersom både helse- og sosialtjenester er en del av behovet må begge deler være del av samme plan.

Arkivloven m/forskrifter gjelder også for pasientjournaler i offentlig virksomhet. Dette gjelder bl.a. bevaring, kassaksjon, avlevering til arkivdepot og arkiveringstid. For EPJ skal det utarbeides dokumentasjon som sier hvordan det er mulig å benytte materialet etter at ordinær bruk er avsluttet. Det må benyttes godkjent lagringsmedium og formatet skal være egnet for avlevering til arkivdepot.

Personopplysningsloven inneholder de grunnleggende bestemmelser for all behandling av personopplysninger og gjelder som utfyllende bestemmelse i forhold til Helseregisterloven.

Personopplysningsforskriften inneholder flere bestemmelser som er viktige for EPJ, særlig kravene til internkontroll og informasjonssikkerhet og sikkerhet hos andre virksomheter. Personopplysninger kan kun overføres til andre virksomheter hvis de oppfyller kravene i forskriften.

Sikkerhetsbestemmelsene angir også krav til styringssystem, og gjennom det til sikkerhetsledelse, risikovurdering og sikkerhetsrevisjon. Den behandlingsansvarlige skal forsikre seg om at sikkerheten i samarbeidende organisasjoner er tilfredsstillende og kan dokumenteres og at virksomhetens egne medarbeidere får tilstrekkelig opplæring.

Sikkerhetskravene i loven og forskriften skal også være grunnlag for harmonisering av sikkerhetsnivået og gjenkjennbare sikkerhetsnivåer på tvers av sektorer. Dette vil også omfatte nettverk, f.eks. når et system brukes til flere applikasjoner eller administrative eller private formål.

Elektronisk signaturloven har som formål å legge til rette for sikker og effektiv bruk av elektroniske signaturer. Loven inneholder bestemmelser om fremstilling (gjennom krav til avanserte signaturer og kvalifiserte signaturer og sertifikater) og

rettsvirkning for disse.

Forvaltningsloven har bestemmelser om klager, søknader, kommunikasjon m.m. med helsevirksomheter .

Eforvaltningsforskriftens formål er å legge til rette for effektiv bruk av elektronisk kommunikasjon med og i forvaltningen og gir grunnlag for at henvendelser kan skje elektronisk dersom forholdene ligger til rette, men elektronisk kommunikasjon av vedtak kan bare gjøres med mottakers samtykke. Det kan stilles formkrav og krav til informasjonssikkerhet må ivaretas. Forskriften har også anbefalinger og krav angående bruk og behandling av sertifikater og behandling av krypterte og signerte meldinger og arkivering av slike.

Norm for informasjonssikkerhet i helsesektoren

I SHdirs høringsutkast til norm for informasjonssikkerhet i helsesektoren[SHdir] er kravene i forskriftens §2 som omhandler informasjonssikkerhet lagt til grunn og normen beskriver de konsekvenser forksriftens krav har for aktørene i helsesektoren. Normen er en konkretisering av forskriften på områder som er relevante for informasjonssikkerheten, og kopling mellom forskriften og normen er gitt ved kryssreferanser. De fleste av normkravene angir heller ikke spesielle sikkerhetsmekanismer, men stiller krav til organisasjon, tiltak, rutiner og dokumentasjon i virksomhetene som er utdypet i forhold til forskriften. Det er utarbeidet veiledere og faktaark i tilknytning til normen[SHdir2].

EPJ-standarden

EPJ-standarden[KITH3] spesifiserer i begrenset grad konkrete sikkerhetskrav, men har mange krav som fordrer innføring av sikkerhetsmekanismer for håndtering av sikkerhetsspørsmål, særlig for implementering av tilgangskontrollfunksjoner og roller. Overføring av informasjon fra et EPJ-system til et annet vil ha både integritets- og konfidensialitetskonsekvenser. Det er derfor begrensninger i hva som tillates av slike operasjoner både i det å eksportere informasjon og i behandling av informasjon som hentes inn fra en annen EPJ.

Flere forskjellige metoder, som vil ha ulike tilnærminger til å beskrive sikkerhetskrav, kan i prinsippet benyttes ved utveksling av journalinformasjon, f.eks:

- En kan benytte tradisjonelle EDI-meldinger.
- En kan gi de som har legitimt behov direkte tilgang til journalene der de blir ført.
- En kan "publisere" de journaldokumenter som etterspørres på WEB, og la de som har legitimt behov selv hente disse.
- En kan overføre den journalinformasjon som skal kunne deles, til en felles "journal" hvor alle med legitimt behov selv kan hente den.

Krav til bruk – intern instruks

Ullevål Universitetssykehus interne instruks[UUS] inneholder i liten grad krav til EPJ,

men beskriver krav til hvordan brukerne skal behandle opplysninger i EPJ. Instruksen gjelder ved all bruk av personopplysninger der UUS er kilde og der UUS vil kunne bli oppfattet som ansvarlig for opplysningene. Den angir også interne regler om roller og hvem som skal ha ansvar for oppgaver hvor EPJ brukes.

Kravspesifikasjoner – nettverk og systemer

Krav til basissikkerhet i et nettverk og systemer angis gjennom bl.a. indre og ytre sikkerhetsbarrierer, viruskontroll, bruk av VPN, åpen og sikker epost, sertifikatbruk (PKI) og sikker tilgang til Internett fra sikre soner. Mot indre trusler kreves at det ikke blir lett å gjøre feil i vanvare, uvitenhet og ved å ignorere retningslinjer, eller at informasjon med ulikt sikkerhetsnivå blandes.

PKI

Formålet med å bruke PKI i helsenett er å kunne oppnå sikker autentisering og identifisering av parter og sikker informasjonsoverføring og ikke-benekting ved elektronisk samhandling. I en prosjektrapport om PKI i helsenett (KITH 2004, Vestad) klassifiseres behov og krav til elektronisk signatur:

- internt i virksomheter
- ved samhandling mellom virksomheter med meldinger og epost
- ved samhandling mellom helsepersonell og pasient
- ved nettbasert tilgang til EPJ
- for å gi pasienten tilgang til egen EPJ, og evt. for samtykkefunksjon
- ved bruk av sertifikater i nettinfrastruktur

I tillegg er det sett på faktorer som type informasjon, behov for løsninger, signaturens rolle, sikkerhetsnivå og tillitsnivå og hvem som kommuniserer.

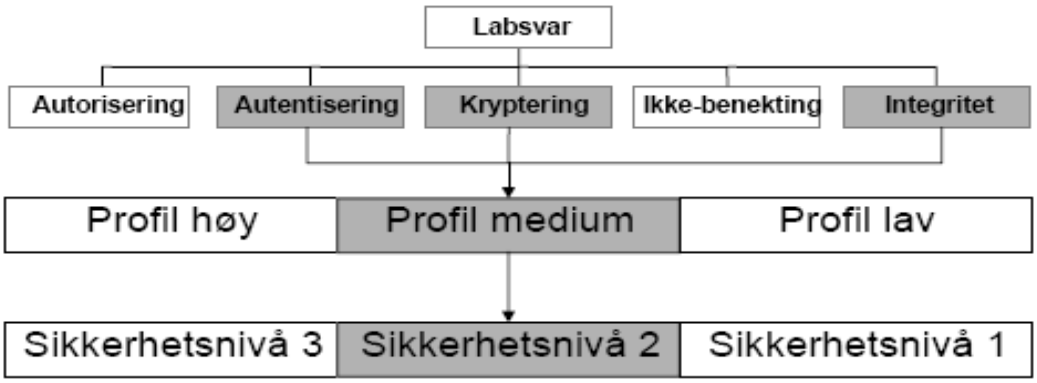
I telemedisinanvendelser vil digitale signaturer kunne gi tilfredsstillende autentisering og kryptering for å sikre konfidensialitet og integritet. Eksempler er fjernkonsultasjon, fjernvisitt, kollegakonsultasjon og i diskusjonsfora. Ved melding til sentrale helseregistre eller i kommunikasjon med pleie- og omsorgs- primærhelsetjeneste må informasjon krypteres og signeres og autentisering må sikres, og det kan være aktuelt med ikke-benekting. Ved nettbasert tilgang til EPJ er autentisering og kryptering viktig, og samtykke fra pasienten en forutsetning. Dersom det skal etableres en blålysfunksjon skal være tilgjengelig over Internett, i tilfeller hvor sertifikater ikke er tilgjengelig, vil det måtte håndteres av aksesskontrollsystemet.

Rikstrygdeverkets kravspesifikasjon for bruk av PKI[RTV] skal forenkle vurderinger rundt valg av sikkerhetsmekanismer. Kravspesifikasjonen dekker elektronisk ID, signatur og kryptering i Altinn og helsenett. Den spesifiserer funksjonelle krav til leverandørenes løsninger, krav til at sikkerhetsmekanismer skal være implementert og krav til sikkerhetsnivå og støtte for PKI, men ikke hvordan dette skal gjøres utover å referere til standarder for bl.a sertifikater og nøkkelhåndtering. I tillegg til

obligatoriske krav er opsjoner for bl.a. tidsstempling, langtidslagring, høy tilgjengelighet, sikkerhetsportal, kvalifiserte sertifikater o.l. beskrevet.

KITH har utarbeidet anbefalinger og standarder for bruk av PKI i helsesektoren[KITH2]. Rapporten angir standarder for meldingsutveksling og bruk av PKI på applikasjonsnivå, konvoluttnivå og nettverks/transportnivå.

Forprosjektrapporten for PKI i helsevesenet[KITH5] og Utrullingsplanen for bruk av PKI i helseforetakene[nhn] angir sikkerhetsmekanismer og beskriver både begrensninger og mulighetene for bruk av PKI avhengig av sertifikattype og nøkkelhåndtering. Det beskrives en anbefalt inndeling i sikkerhetsnivåer ut fra behov for rettsvirkning, trusselbildet, konsekvenser, risikovurdering, sikkerhetsnivå, sensitivitet, aktører, brukeromgivelser, personlig binding til signatur, kompleksitet og kostnader. Forprosjektrapporten beskriver forslag til PKI sikkerhetsprofiler med sikkerhetstjenester for ikke-benekting, autentisering, kryptering og integritetssikring. Profilene er tilpasset tre sikkerhetsnivåer, høy, medium og lav. Kritiske anvendelser bør minst bruke sikkerhetsnivå 2, medium.



Figur 9: Eksempel på bruk av sikkerhetsprofil. *(Kilde: KITH)*

RFID

RFID kan benyttes som et alternativ til strekkoder for øket identitetssikring og kvalitetskontroll ved f.eks. prøvetaking. Det vil innebære at resultater fra RFID-merkede prøver vil overføres til EPJ, og informasjonen må sikres som for annen personinformasjon i helsenett.

Bruk av RFID må ses på som et usikret nett og krever sikkerhet mot avlytting, og da gjennom kryptering i hvert fall av deler av informasjonen, og sikker autentisering av brikke og bruker må garanteres. Siden RFID kan inngå i automatiske on-line prosesser og verken er kontaktbasert eller krever fri sikt, møter man nye sikkerhetsutfordringer ved bruk.

ebXML og XML-Dsig

Meldingstjenesten i ebXML beskriver en tjeneste for å utveksle elektroniske meldinger mellom partnere på en standardisert, sikker og pålitelig måte uavhengig av selve

kommunikasjonssystemet[11]. ebXML håndterer bl.a sikkerhetsfunksjoner som kryptering, signering, autentisering, autorisasjon, kvitteringer og ikke-benekting for de kommuniserende parter og meldingene som overføres.

XML-Dsig kan brukes for signering, autentisering og ikke-benekting på applikasjonsnivå av dokumentet (EPJ) som skal overføres.

11 KITH: R25-02, Rammeverk for meldingsutveksling

Vedlegg B: Generelle kontekstuelle sikkerhetskrav

Kontekstuelle krav	***Vilkår, forutsetning, kilde***
Objekttilgjengelighet (OT)	
Pasientinnsyn: Rett til innsyn i egen journal på forespørsel, dersom ikke anmodning er avslått av journalansvarlig.	Pasientrettighetsloven kap. 3, §5-1. Helsepersonelloven §41 Pasienten må autentiseres.
Tilgang for helsepersonell ved behov. Den som yter helsehjelp skal ha skrivetilgang.	Skal være i forbindelse med besluttet tiltak. Rollebasert, avgrenset etter behov, må autentiseres. EPJ-std.
I akuttsituasjoner skal helsepersonell kunne tilegne seg tilgang	Såkalt blålystilgang, gjøres av forhåndsklarert personell.
Nødvendig tilgjengelighet skal sikres	Personopplysningsforskriften
Alternativ tilgang ved feil skal sikres	Personopplysningsforskriften
Subjektpålitelighet (ST)	
Pålitelig systemtilgang skal sikres	Oppetid, avbrudd. Vil avhenge av type virksomhet
Akseptabel responstid	Situasjonsbetinget: Akutt, planlagt. F.eks. 99% oppetid, <1 t avbrudd (NST)
Tilgang til relatert informasjon skal sikres	Personopplysningsforskriften
Beskyttelse mot ødeleggende programvare skal etableres	Personopplysningsforskriften
Objektintegritet (OI)	
Autorisasjon nødvendig for skriving, sletting og retting	Skal være autorisert personell som skriver. Skal ha ansvaret og være kvalifisert. Helsepersonelloven §§42-44
Det skal sikres ikke personopplysninger er endret eller ødelagt	HIPAA §164.132
Journalansvarlig skal oppgis	EPJ std
Sikker overføring mellom to parter. Ende-til-ende beskyttelse av data	Datatilsynet krever ende-ende kryptering
Formål for registrering av data skal angis	Beslutning om behandlingstiltak, gir informasjon om anvendelse av data. EPJ std.
Kilde for data skal angis	Personopplysningsforskriften
Integritet skal sikres	Personopplysningsforskriften

Kontekstuelle krav	*Vilkår, forutsetning, kilde*
Elektronisk overføring skal sikres med kryptering	Personopplysningsforskriften
Det skal føres oversikt over type personopplysninger	Personopplysningsforskriften
Opplysninger skal sikres mot uautorisert endring	Personopplysningsforskriften
Ved bruk av elektronisk signatur skal signaturinformasjon være entydig	EPJ-stnadarden
Tilgang skal kunne gis for kvalitetssikring	EPj-standarden
Subjektintegritet (SI)	
Tilstrekkelig sikring av data Tilkoplingssikkerhet og fysisk sikkerhet	Autorisert tilkopling og adgang, tilgangskontroll. ØNH
Det skal opprettes unike brukeridentiteter	HIPAA §164.312
EPJ skal beskyttes mot utilsiktet sletting	EPJ std
Skal kunne gjenskape slettet informasjon hvis data skulle ikke vært slettet	EPJ std
Etablering av sikkerhetsprosedyrer. Norm for informasjonssikkerhet skal følges.	Personopplysningsloven og Person-opplysningsforskriften. SHdir
Systemet skal ha tilgangskontrollsystem	Person-opplysningsforskriften HIPAA §164.132
Revisjonskontroll for endringer i EPJ	EPJ std
Sikkerhetsprosedyrer og internkontroll skal etableres. Sikkerhetsstrategi skal beskrives.	Personopplysningsloven
Sikkerhetsrevisjon skal gjennomføres	Personopplysningsloven
Avvikshåndtering skal etableres	Personopplysningsforskriften
Akseptabel risiko skal fastsettes, risikoanalyse skal gjennomføres	Personopplysningsloven
Autorisasjon skal være underlagt styring	Personopplysningsloven
Tiltak mot utro tjenere skal innføres	Personopplysningsloven
Konfigurasjonskontroll skal være underlagt styring	Personopplysningsloven
Behandlingskonfidensialitet (BK)	

Kontekstuelle krav	*Vilkår, forutsetning, kilde*
Tilstrekkelig sikring av data i systemet. Tilkoplingssikkerhet og fysisk sikkerhet	Autorisert tilkopling og adgang, tilgangskontroll
Taushetsplikt skal hindre uautorisert tilgang	Helsepersonelloven §5, 21
Konfidensialitet skal sikres	Personopplysningsforskriften
Personopplysninger skal kunne krypteres	HIPAA §164.312
Kontekstuell konfidensialitet (KK)	
Taushetsplikt, kun autoriserte skal ha tilgang	Deltar i behandling eller tilsyn Alle pasientdata betraktes som sensitive. EPJ std.
Tilgang kun til relevant info, nødvendig for aktuel behandling	Segmentert, rollestyrt tilgang til opplysninger
Rollebasert tilgang skal kunne gis	EPJ std
Informasjonskategori skal angis for å kunne beslutte behov for tilgang, segmentert tilgang	EPJ std
Forskningsdata skal lagres på egen server	UUS
Ved avsluttet bruk skal lagringsmedier slettes	Personopplysningsforskriften
Uautorisert bruk skal hindres	Personopplysningsforskriften
Forsøk på uautorisert bruk skal logges	Personopplysningsforskriften
Klarering, hjemmel (K)	
Konsesjon for EPJ	Formål for behandling av pasientdata oppgis Krav for opprettelse av EPJ. Personopplysningsloven.
Hjemmel for tilgang til personopplysning	I lov, ved samtykke, ved behov. Må være gyldig i aktuel situasjon. Personopplysningsloven.
Databehandlingsansvarlig skal ha gitt fullmakt/autorisasjon	Skal hjemles i styringssystem Virksomheten er ansvarlig for personopplysningene. Helseregisterloven.
Databehandler skal ha fullmalt. Ansvarsforhold skal beskrives.	Ansvarsstruktur. Skal få tildelt ansvar. Helseregisterloven, EPJ std.
Formål med behandling skal angis	Vedtak om tiltak
Opprinnelse (O)	

Kontekstuelle krav	*Vilkår, forutsetning, kilde*
Kilde for data angis	Autorisert registrering og registreingsmåte Kontekstbegrenset gyldighet
Ansvar for opprinnelse angis	Bevaring av signatur og info om organisasjon. Referanse
Registrering om at informasjon er oversendt andre	EPJ std
Mottaker (M)	
Tilstrekkelig dokumenterbar sikkerhet	Persondata skal gis tilstrekkelig beskyttelse. Skal møte krav fra opprinnelsessystemet
Utveksling (U)	
Hjemmel for utveksling. Samtykke fra pasient eller hjemmel i lov	Grunnlag for utveksling skal sikres. Helseregisterloven §5, 2
Skal fremgå hvem som har opprettet EPJ og når	EPJ std
Krav om innsyn skal logges	EPJ std

Tabell 11: Kontekstuelle sikkerhetskrav

Vedlegg C: Generelle kontekstuelle sikkerhetstjenester

Kontekstuelle tjenester (T)	***Beskrivelse***
Objekttilgjengelighet (OT)	
Tilgang ved akuttbehov	Blålystilgang, aktualisering
Tilgang til opplysninger fra andre enheter. Tillate autorisert utveksling	Overføring mellom sikre soner
Sending av sensitiv epost. Forhåndautorisering av mottakere	Ruting til forhåndsdefinerte adresser. ØNH
Sikkerhetslagring av slettet informasjon	Slettet informasjon blir lagret, men skjult. For å kunne gjenopprette slettet informasjon. NST
Systemet skal tilby sikkerhetskopiering	EPJ-standarden
Refererte opplysninger skal ikke kunne slettes	EPJ-standarden
Tilgang skal kunne gis basert på hjemmel i aktuelle lover	EPJ-standarden
Subjektpålitelighet (SP)	
Sikkerhetskopiering	Regelmessig backup. Håndteres av IT-avd. EPJ std.
Kommunikasjon mellom virksomheter	VPN, lukket IP-nett. Settes opp mellom faste samarbeidspartnere. ØNH
Kommunikasjon mellom sikre soner på samme nivå	Autorisert utveksling av data. ØNH
Sikker Internettilgang	Aksess via tynnklient fra sikker sone. ØNH
Integrasjon av systemfunksjoner	Felles primær lagring, reduserer redundans
Systemmonitorering, videresending av feil og advarsler	Sikre stabil drift og tilgjengleighet
Objektintegritet (OI)	
Korrekt utveksling mellom EPJ og epostsystem	Integrasjon av tjenester. Data utveksles mellom ulike systemer. ØNH
Autolagring. Skriving av melding avbrytes ikke	Timeout skal ikke stoppe skriving. Well

Kontekstuelle tjenester (T)	***Beskrivelse***
Digital signering av sendt informasjon (Laboratoriesvar, respeter)	Signering av melding eller konvolutt
Kontroll av sertifikater og nøkler på PKI	Informasjon i EPJ verifiseres mot sertifikat. F.eks. nøkler eller opprinnelse. ØNH
Alle endringer i registreringer skal kunne logges	EPJ-standarden
Redundans p.g.a. dobbeltlagring skal redusere til et minimum	EPJ-standarden
Kilde for informasjon skal angis	EPJ-standarden
Godkjent dokument skal ikke kunne endres	EPJ-standarden
Registrert informasjon skal ikke kunne overskrives av importert informasjon	EPJ-standarden
Kodet informasjon skal velges fra preregistrert liste	EPJ-standarden
Subjektintegritet (SI)	
Regulering av informasjonsflyt	Nettverks- og applikasjonskontroll. Overgang mellom soner. ØNH
Nøkkeladministrasjon	Kryptert nøkkel, lagret på proxy, key-frasing passord ved boot. Nøkkel lagres kun i RAM
To-lags forsvar. Beskyttelse av ytre server	Skille mellom web-server og proxy, brannmurer
Autentisering	Autentiseringsserver i sikker sone: ID, passord, IP-adresse
Aksesskontroll. Beskyttelse mot sniffing	Engangspassord
Signatur- og sertifikatverifisering	PKI-baserte tjenester
Predefinert oppringt samaband	ØNH
Kun Java med sertifisert opphav. Ikke ActiveX.	Sikring av soner. ØNH
Informasjonseier skal registreres	EPJ-standarden
Gyldighetsperiode skal registreres	EPJ-standarden
Automatisk logoff ettet time-out	HIPAA §164.312
Behandling av personopplysninger skal kunne logges	HIPAA §164.132
Behandlingskonfidensialitet (BK)	

Kontekstuelle tjenester (T)	***Beskrivelse***
Kryptering/dekryptering	Beskyttelse når data forlater sikker sone. Tvungen kryptering. ØNH
Autorisasjonssjekk, tilgang krever autorisasjon	Sjekk om mottaker er autorisert for lesing. For ikke-kryptert informasjon
Sendig og mottak av sikker epost. Skal ikke kopieres eller blandes	Skille fra åpen epost. ØNH
Etablering av sikker sone. Sensisitv informasjon behandles innenfor sikker sone	Beskyttelse med to barrierer. ØNH
Sperre mot kopiering av data til andre systemer	Ikke lokal lagring. Pasientinfo ikke cachet
Sikring mot overvåkings-SW	Filsjekk. Nettleserkontroll
Autentisering kreves	To-trinns innlogging, engangspassord, SSO. Aksesskontrollister, validering av ID
Sikring av krypteringsnøkler	Bruk av smartkort for oppbevaring av nøkler (ikke bundet til data?)
Kontekstuell konfidensialitet (KK)	
Anonymisering av data ved ukryptert overføring	Kople ID fra informasjon. ØNH
Tilgang skal gis basert på rolle eller funksjon. Rollebasert aksesskontroll	Kontekstavhengig tilgang til relevant informasjon. Skille mellom behandlingssituasjoner. Intern PKI. ØNH
Tilgang skal baseres p åbehov. Adegang kun til relevante data	Adgangskontroll på datanivå. Segmentering av data
Tilgang skal baseres på samtykke	Identifiserte personer kan nektes eller gis tilgang. Må innhente samtykke
Ingen skal ha tilgang til informasjon de ikke er autorisert for	EPJ-standarden
Det skal skilles logisk mellom identitet og andre personoplysninger	EPJ-standarden
Informasjonskategori og formål fo rbruk av informasjon skal angis	EPJ-standarden
Klareringskontroll/hjemmel (KH)	
Klassifisering av meldinger og filer	Merking sensisitiv, ikke sensitiv. ØNH

Kontekstuelle tjenester (T)	*Beskrivelse*
Validering av ID	Autorisasjon bekreftes. I stedet for/tillegg til rolle
Logging av aksess	Tid, ID, kontekst. Sporing i ettertid
Opprinnelse (avsender) (O)	
Responsverifikasjon	Bekreftelse på korrekt mottak. Mottaker kan mangle autorisasjon
Det skal registreres når informasjon overføres andre	EPJ-standarden
Mottakerkontroll (M)	
Ikkebenekting	PKI-basert (Elektronisk sykemelding)
Utvekslingskontroll (U)	
Logg av hendelseskronologi	Juridisk, oppgaver, system, revisjon. For rekonstruksjon av forløp
Overføring av EPJ	En EPJ skal flyttes. PKI-basert autentisering og signering
Sikker kommunikasjon	Sende melding over ebXML (ikke bundet til data?)
Det skal være mulig å følge referanser mellom systemer	EPJ-standarden

Tabell 12: Kontekstuelle sikkerhetstjenester

Vedlegg D: EPJ-applikasjoner; sikkerhetstjenester

Her er vist et sett med sikkerhetsegenskaper som er oppgitt for noen EPJ-applikasjoner, gruppert etter de konseptuelle sikkerhetsbehovene.

WellDiagnostics: WellArena/Communicator/Multimedia

WellArena [WELLA] er en løsning for å overføre pasientsensitiv informasjon over internett. WellCommunicator [WELLC] tilbyr kommunikasjon som skal tilfredsstille krav til sikkerhet, lagring, logging og integrasjon for forskjellige meldingstyper, formater, transport og konvertering.

DIPS – sikkerhetsmekanismer

For journalsystemet DIPS [DIPS] beskrives sikkerheten gjennom adgangskontroll og autentiseringsmekanismer på funksjons- og datanivå og knyttes til hendelser og kategorisering av data. Sikkerhetsfunksjoner omhandler først og fremst bruksmiljø og brukeromgivelser.

Infodoc

Infodoc [Infodoc] har et frittstående rutinesett for dokumentutveksling mellom aktørene i helsesektoren. Informasjon sendes fra en sertifisert aktør til en annen uten innholds- og format-bearbeiding.

PlanPro/SamPro

Sikkerhetsarkitekturen for SamPro [SamPro] støtter samhandling om individuelle planer for pasientbehandling, og skal muliggjøre sikker kommunikasjon av sensitiv helseinformasjon over åpne nettverk. Sikkerhetsarkitekturen relateres til en referansearkitektur (MAFIIA [MAFI]).

Sikkerhetsfunksjonalitet, EPJ-applikasjoner	***Tjeneste, Mekanisme***
SamPro, DIPS, WellDiagnostics, Infodoc	[WELLC][DIPS][SamPro]
Objekttilgjengelighet (OT)	
Single sing-on for felles pålogging	Kerberos (Mek)
Byte padding for interoperabilitet med eldre EDI	DES (Mek)
Blålystilgang i nødsituasjoner	(Tjeneste)
Mulig å delegere tilgangsretter	(Tjeneste)
Resending av meldinger	(Tjeneste)
Notifikasjon på innkommende meldinger	GSM, MIME (Mek)
VPN tunnel	DES 128 (Mek)
Bakgrunnslagring av sikkerhetskopi	(Tjeneste)

Sikkerhetsfunksjonalitet, EPJ-applikasjoner	***Tjeneste, Mekanisme***
Subjektpålitelighet (SP)	
Databaseagenten sender melding hvis server er nede, systemmonitorering	SOAP-objekter (Mek)
Fjernsupport gjennom brannmur	IP, Port nn (Mek)
PKI-støtte	SA-tre, rotsertifisering, katalogtjenester (Tjeneste)
Sikre soner (LAN, WAN)	Tynnklientstøtte, terminalserver, klient/tjener (Tjeneste)
Objektintegritet (OI)	
Normaliserte datamodeller for integrering av systemer og redusert redundans i lagret informasjon	(Tjeneste)
Automatisk logging av endringer og oppslag i data	(Tjeneste)
Samtidig editering mulig uten å ødelgge integritet	(Tjeneste)
Autolagring ved langvarig editering	(Tjeneste)
Bruk av PKI for autentisering og digital signering	(Tjeneste)
XML Signature og PKCS7 for kryptering og kvittering	(Tjeneste)
Støtte for X.509 baserte sertifikater	(Tjeneste)
Støtte for CRL og LDAP katalogoppslag	(Tjeneste)
Import ov private nøkler og sertifikater fra MS CryptoAPI	(Tjeneste)
Logg av inn- og utgående meldinger	(Tjeneste)
Autentisering for SMTP og POP3	(Tjeneste)
Meldingsautentisering ved offentlig nøkkel kryptering	X.509, LPAD, Crypto API, S/MIME (RSA/3DES/SHA-1)
Meldingsautentisering ved signering av melding	ebXML, XML-Dsig, PKCS#12
Godkjenning av EPJ ved påføring av digital signatur	SKCF7, SHA-1, X.509
Subjektintegritet (SI)	
SSL-kommunikasjon til webservere, mot nett og mot applikasjonsserver	(Tjeneste)
Adskilt autentisering for hver server	(Tjeneste)
To-lags forsvar, web-server og proxy skilt	(Tjeneste)
Brukernav og passord lagres kun på autentiseringsserver	(Tjeneste)

Sikkerhetsfunksjonalitet, EPJ-applikasjoner	***Tjeneste, Mekanisme***
Kun administrator kan endre rettigheter og konfigurasjon	(Tjeneste)
Logging av alle konfigurasjonsendringer	(Tjeneste)
Passord overføres aldri i klartekst	(Tjeneste)
All informasjon skal sikres i henhold til Datatilsynets krav	(Tjeneste)
Automatisk utlogging etter gitt periode med inaktivitet	(Tjeneste)
Administratortilgang til webserver begrenset	SSH (Mek)
Autentisering ved meldingsoverføring	SMTP/POP (Mek)
Segmentering: adskilt autentisering for web, applikasjon og database	IIS, ASP.NET, SQL server (Mek)
CRL-adminstrasjon og sertifikatverifisering	RFC 2459, 3280, 2560 (Mek)
Autentisering av personsertifikat	ETSI TS 101 826 v.1.2.1, X.509 v.3 (Mek)
WLAN pålogging	RADIUS (Mek)
NAT sikkerhetsbarriere	RFCxxx (Mek)
Behandlingskonfidensialitet (BK)	
To-trinns autentisering	(Tjeneste)
Tilgangsstyring skilt ut i egen modul	(Tjeneste)
Nettkommunikasjon med SSL og minst 128 bits nøkkelllengde	(Tjeneste)
Symmetrisk kryptering (AES, 3DES, RC6)	(Tjeneste)
Kryptering webutveksling server – pasient	HTTPS, SSL m/128 bits nøkkel (Mek
Krypterte meldinger server – EPJ	S/MIME, RFC 2633, 3369, 2632 (Mek)
Kryptert kommunikasjon	AES, 3DES, RC6, =<2048 bits nøkkel (Mek)
PKI-basert autentisering	ebXML (Mek)
Kontekstuell konfidensialitet (KK)	
Adgangskontroll basert på hendelser og kategorisering av data	(Tjeneste)

Sikkerhetsfunksjonalitet, EPJ-applikasjoner	***Tjeneste, Mekanisme***
Adgangskontroll på funksjons- og datanivå	(Tjeneste)
Adgangsstyring til enkeltelementer	(Tjeneste)
Samtykkebasert tilgang til personopplysninger	(Tjeneste)
Rollebasert tilgangskontroll	(Tjeneste)
Kun temporær lagring av data på klient, slettes etter bruk	(Tjeneste)
Klareringskontroll, hjemmel (KH)	
Validering av pasient ID, gyldighetssjekk	(Tjeneste)
Logging av aksess til sensitive data	(Tjeneste)
Responssjekk: svar lest, manglende svar	(Tjeneste)
Ikkebenekting	(Tjeneste)
Logging av hendelseskronologi: Jurdisk, oppgaver, system, revisjon.	(Tjeneste)

Tabell 13: Applikasjonsegenskaper i DPP-struktur.

Vedlegg E: Systemsikkerhet

I fremstillingene nedenfor vises krav til systemsikkerhet struktureret i forhold til inndelingen i konseptuelle grupper.

Østnorsk helsenett[12] – kravspesifikasjon nettverkssikkerhet

	Kravspesifikasjon - ØNH
Type	Sikkerhetskrav for nettverk
Opprettet av	ØNH
Dato, opprettet	12.5.2005
Anvedelse	Norsk helsenett
Ansvar	IT-sjef
Språk	Nor
Relasjon	www.norskhelsenett.no/...
Tilgjengelighet	krav: semiformell, uformell
objekttilgjengelighet	Kommunikasjon på tvers av sikkerhetssoner skal kunne gjennomføres med meldingsutveksling på sikker måte
objekttilgjengelighet	Sikker oppkopling mot interne nettverk
objekttilgjengelighet	Pålitelig kommunikasjon og nødvendig båndbredde
objekttilgjengelighet	Tilgang til Internett via tynn klient
subjektpålitelighet	Tjenester og protokoller skal holdes på et minimum
Integritet	krav: semiformell, uformell
objektintegritet	Virussjekk av e-post og vedlegg skal gjøres
objektintegritet	Det skal ikke være lett å gjøre feil i vanvare
objektintegritet	Sertifikater skal kunne brukes for autentisering eller å bekrefte opprinnelse
objektintegritet	All aktivitet skal kunne logges på aktivitetsnivå
subjektintegritet	Eksterne aktører skal ikke trenge inn i virksomhetens nettverk
subjektintegritet	Ingen trafikk tillates initiert fra ekstern nett direkte inn på interne nett

12 Østnorsk helsenett er nå en del av Norsk helsenett AS.

	Kravspesifikasjon - ØNH
subjektintegritet	Nettverk skal ha en sikkerhetsarkitektur med etablering av sikre soner. Sensitive personopplysninger skal behandles og lagres i sikre soner.
subjektintegritet	Bruker skal ikke kunne overstyre innlagte begrensinger.
subjektintegritet	Det skal være to sikkerhetsbarrierer mellom Internett og sikker sone.
subjektintegritet	Det skal være minst én sikkerhetsbarriere mellom sikker og intern sone.
subjektintegritet	Nettverkskontroll skal regulere informasjonsflyt mellom nettverk, soner og applikajsoner
subjektintegritet	Applikasjonskontroll skal beskytte applikasjoner og verifisere korrekt bruk
subjektintegritet	Komplekse datastrukturer skal kontolleres og filtreres ut dersom det er fare for at de kan forårsake skade. Alle inkommende filer sjekkes, også pakkede. Disketter/CD skal sjekkes automatisk.
subjektintegritet	Sikkerhetsbarrieren skal begrense funksjonaliteten om nødvendig.
subjektintegritet	Sikkerhetsbarrieren skal foreta autentisering og autorisering før bruk av tjenester. Sikkerhetsbarrierene skal ha brukerprofiler.
subjektintegritet	Kun Java-applets med kjent og anerkjent opphav skal benyttes
subjektintegritet	Sikkerhetspatcher skal oppdateres kontinuerlig. Virusprogramvare oppdateresjevnlig.
subjektintegritet	Tjenester og protokoller som ikke er eksplisitt tillatt, er forbudt
subjektintegritet	SIkkerhetsbarrieren skal generere alarmer ved sikkerhetskritiske hendelser
subjektintegritet	Ondsinnet kode skal ikke kunne sende ut informasjon, slette informasjon eller ta kontroll over interne nettverk
subjektintegritet	Tjenester og brukere skal skilles i systemer
subjektintegritet	Brudd på plicy skal logges
subjektintegritet	Kun tillate tjenester initiert fra sikker sone til intern sone
subjektintegritet	Trafikk skal ikke initieres fra intern sone mot sikker sone

	Kravspesifikasjon - ØNH
subjektintegritet	Hver sikker sone etableres på eget nettverkssegment
subjektintegritet	Active X skal ikke tillates mot sikker sone eller ytre sikkerhetsbarriere
subjektintegritet	Innkommende epost sjekkes ved ytre sikkerhetsbarriere
subjektintegritet	Ekstern epost skal sikres slik at det ikke gir åpning i sikkerhetsbarrierer
subjektintegritet	Innkommende og utgående epost sjekkes for virus på DMZ
subjektintegritet	Åpning for trafikk initiert mot VPN-tjener kun når nødvendig for VPN funksjonaliteten
subjektintegritet	VPN-enhet plasseres på eget ben på indre sikkerhetsbarriere, skilt fra sikre tjenester
subjektintegritet	Indre sikkerhetsbarriere skalbare slippe gjennom trafikk fra forhåndsdefinert sett av VPN-klienter
subjektintegritet	Utdyping av krav for sikkerhet i VPN, se:
subjektintegritet	NAT benyttes for å skjule indre ressurser
subjektintegritet	VPN-klienten skal kun brukes til kommunikasjon motØNH
subjektintegritet	OS skal beskyttes mot uautorisert tilgang
subjektintegritet	Informasjon og utstyr fra sikkerhetsleverandør skal håndteres sikkerhetsmessig tilfredsstillende.
Konfidensialitet	krav: semiformell
behandlingskonfidens	Kommunikasjons skal være avlyttingssikker
behandlingskonfidens	Ekstern overføring av personopplysninger krever kryptering
behandlingskonfidens	VPN-trafikk skal minst ha DES128 styrke kryptering
behandlingskonfidens	Ukryptert trafikk fra sikker sone kun når initiert fra tynnklient i DMZ på indre sikkerhetsbarriere
behandlingskonfidens	Informasjon skal ikke kunne kopieres mellom applikasjoner
kontekstuell konfidens.	Ikke autorisert mottaker skal ikke kunne lese inforasjon
kontekstuell konfidens.	Åpen og sikker epost skal ikke blandes
kontekstuell konfidens.	Tvungen kryptering av persondata ved utgang av sikker sone

	Kravspesifikasjon - ØNH
kontekstuell konfidens.	Kommunikasjon skal skje mellom parter på samme sikkerhetsnivå
kontekstuell konfidens.	Sikkerhetspolicy for epost
kontekstuell konfidens.	All epost sjekkes på DMZ, kun åpen epost sendes ut
Etterprøvbarhet	krav: semiformell
klareringskontroll	Samarbeidende virksomheter må ha tilstrekkelig sikkerhet
klareringskontroll	Overføring av ukryptert video krever anonymisering

Tabell 14: Nettverkskrav i Østnorsk helsenett – ØNH.

PKI og kryptering

	Krav ved bruk av PKI	
Type	Krav og anbefalinger ved bruk av PKI	Krav-spesifikasjon
Opprettet av	KITH, Norsk helsenett, RTV m.fl.	
Dato, opprettet	12.5.2005	
Anvendelse	Offentlig sektor	
Ansvar	IT-sjef	
Språk	Nor	
Relasjon		
Tilgjengelighet	policy: semiformell	styrke: 3
objekttilgjengelighet	Sertifikatkatalog skal være tilgjengelig som LDAP v.3	KITH 3.3
objekttilgjengelighet	Katalogtjeneste skal gi svar innen 1 sekund pr. oppslag	RTV 2.6.1.3
objekttilgjengelighet	Sperretjeneste skalgi svar innen 1 sekund pr. forespørsel	RTV 2.6.2.3
objekttilgjengelighet	Katalog- og sperretjenester skal ha en oppetid på 99,9%	RTV 2.6.5.1
subjektpålitelighet		
Integritet	mekanismer, protokoller: formell	styrke: 3
objektintegritet	XML Dsig skal brukes for digital signatur på applikasjonsnivå	KITH 1.3, 2.2
objektintegritet	XML Dsig skal brukes for signatur på konvoluttnivå, signatur med virksomhetssertifikat	KITH 1.3, 2.2
objektintegritet	Ved ikke-benekting skal eget nøkkelpar dedikeres for formålet	KITH 2.1
objektintegritet	For kvalifiserte sertifikater skal ETSI TS 101 862 v 1.2.1 x.509 v.3 «Qualified Certificate Profile» (RFC 3739) benyttes.	KITH 2.1.1
objektintegritet	Sertifikater skal baseres på «Internet x.509 Public Key Infrastructure Certificate og CRL Profile» (RFC 3280)	KITH 5.5

	Krav ved bruk av PKI	
objektintegritet	Kvalifiserte sertifikater skal følge kravene i ETSI TS 101 456 «Policy requirements for certification authorities issuin qualified certificates»	KITH 3.1
objektintegritet	Overføring av nøkler gjøres i PKCS #12-format	KITH 3.2
objektintegritet	Sertifikater skal inneholde entydig identifikator	KITH 2.1.1
objektintegritet	For virksomhetssertifikater benyttes RFC 2459 som hovedformat	KITH 2.1.2
objektintegritet	Revokering skal gjøre i henhold til RFC 2459 (CRL) og RFC 2560 (OCSP)	KITH 3.4
objektintegritet	Signaturgenerering gjøres i henhold til CWA 14170 «Security requirements for signature creation applications»	KITH 4.2
objektintegritet	Dokumenter som signerees skal ikke inneholde aktiv kode eller skjulte felt.	KITH
	SAertifikater skal ha gyldighetstid på 2 år	RTV 2.2.2
subjektintegritet		
Konfidensialitet	policy: semiformell	styrke: 3
behandlingskonfidens.	SSL/TLS skal benyttes for for kryptering ved overføringer	KITH 1.3
behandlingskonfidens	VPN skal benyttes for kryptering på nettverksnivå	KITH 1.3
behandlingskonfidens	Asymmertisk nøkkellengde >= 1024 bits, RSA	KITH 2.1
behandlingskonfidens	Signering av epost med S/MIME Version 3 Message Specification (RFC 2633), Cryptographic Message Syntax (RFC 3369) og S/MIME Version 3 Certificate Handling (RFC 2632)	KITH 2.3
Etterprøvbarhet	policy: semiformell	styrke: -
klareringskontroll		

Tabell 15: Krav ved bruk av PKI i DPP-struktur.

Vedlegg F: DPP for EPJ, eksempel

Tittel	***Sikkerhetskrav ved behandling av pasientopplysninger***	***DPP***
Type	Krav til beskyttelse av persondata	Kravspec
Opprettet av	HiG	www.hig.no
Dato	Opprettet	28.5.2005
Anvendelse	Gjelder all pasientinformasjon	
Ansvar	Ansvar delegert til sikkerhetssjef	Dagl.leder
Relasjon	Personopplysningsloven, www.lovdata.no	Lov
Relasjon	Personopplysningsforskriften, www.lovdata.no	Lov
Relasjon	Pasientrettighetsloven, www.lovdata.no	Lov
Relasjon	EPJ-standarden, www.kith.no	Standard
Relasjon	Sikkerhetsinstruks, www.ullevaal.no	Instruks
Relasjon	PKI-anbefaling, www.kith.no	Norm
Relasjon	Applikasjonsbeskrivelse: www.dips.no, www.well-diagnostics.no	Applikasjon
Objekt-tilgjengelighet		
Krav, uformelt	Pasienten har på forespørsle rett til innsyn i egen EPJ, dersom ikke journalansvarlig gir begrunnet avslag. Pasienten må autentiseres.	Pasient-rettighets-loven
Prosedyrekrav, semiformelt	Det skal finnes sikkerhetskopi. (Pers.oppl.forskr. §2-12)	Lovkrav
Krav, uformelt	nødvendig tilgjengelighet skal sikres	Lovkrav
Krav, uformelt	alternativ tilgang ved feil skal sikres	Lovkrav
Krav, uformelt	systemet skal tilby sikkerhetskopiering	EPJ-std
Krav, uformelt	refererte opplysninger skal ikke kunne slettes	EPJ-std
Krav, uformelt	tilgang skal kunne gis for nødaksess	EPJ-std
Krav, uformelt	Pasientopplysninger kan gis til samarbeidende personell når nødvendig	Instruks

Tittel	*Sikkerhetskrav ved behandling av pasientopplysninger*	*DPP*
Krav, uformelt	Helsepersonell skal ha tilgang til informasjon etter behov, skal være i forbindelse med tiltak. Rollebasert, avgrenset, må autentiseres	EPJ-standarden
Krav om sikkerhetstjenester, semiformelt	Sikkerhetslagring av slettet informasjon. Slettet informasjon blir lagret, men skjult for brukeren. For å kunne gjenopprette informasjon slettet ved en feil.	EPJ-standarden
Krav om sikkerhetstjenester, semiformelt	Alternativ tilgang ved systemfeil. Pers.oppl.forskr. §2-12	Lovkrav
Subjektpålitelighet		
Krav, uformelt	Personopplysningsforskriftens krav (Gjelder alltid)	Lovkrav
Krav, uformelt	tilgang til relatert informasjon skal sikres	Lovkrav
Krav, uformelt	beskyttelse mot ødeleggende programvare skal etableres	Lovkrav
Prosedyrekrav, semiformelt	Ref. Pers.oppl.forskr. §2	Lovkrav
Objektintegritet		
Krav, uformelt	Formål for registrering av data skal angis, beslutning om behandlingstiltak nødvendig	OT.K#
Prosedyrekrav, semiformelt	Det skal finnes rutiner for retting, sletting, sperring, signering, låsing. (Intern instruks)	OT.P#
Krav, uformelt	integritet skal sikres	Lovkrav
Krav, uformelt	elektronisk overføring skal sikres med kryptering	Lovkrav
Krav, uformelt	oversikt over type opplysninger skal føres	Lovkrav
Krav, uformelt	opplysninger skal sikres mot uautorisert endring	Lovkrav
Krav, uformelt	alle endringer i registreringer skal logges	EPJ-std
Krav, uformelt	redundans p.g.a. dobbeltlagring skal reduseres til et minimum	EPJ-std
Krav, uformelt	ved bruk av elektronisk signatur skal signaturinformasjon være entydig	EPJ-std
Krav, uformelt	kilde for informasjon skal angis	EPJ-std
Krav, uformelt	et godkjent dokument skal ikke kunne endres	EPJ-std

Tittel	*Sikkerhetskrav ved behandling av pasientopplysninger*	*DPP*
Krav, uformelt	tilgang skal kunne gis til kvalitetssikring	EPJ-std
Krav, uformelt	registrertinformasjon skal ikke overskrives av importert informasjon	EPJ-std
Krav, uformelt	kodet informasjon skal velges fra preregistrert liste	EPJ-std
Prosedyre, semiformelt	Avdelingsoverlege avgjør autorisasjon	Instruks
mekanismer, protokoller: formell	Endringer i journalen skal være sporbare	Instruks
Prosedyre, semiformelt	Kun autorisert personell skal kunne gjøre endringer	Instruks
mekanismer, protokoller: formell	XML Dsig skal brukes for digital signatur på applikasjonsnivå	KITH 1.3, 2.2
mekanismer, protokoller: formell	XML Dsig skal brukes for signatur på konvoluttnivå, signatur med virksomhetssertifikat	KITH 1.3, 2.2
mekanismer, protokoller: formell	Ved ikke-benekting skal eget nøkkelpar dedikeres for formålet	KITH 2.1
mekanismer, protokoller: formell	For kvalifiserte sertifikater skal ETSI TS 101 862 v 1.2.1 x.509 v.3 «Qualified Certificate Profile» (RFC 3739) benyttes.	KITH 2.1.1
mekanismer, protokoller: formell	Sertifikater skal baseres på «Internet x.509 Public Key Infrastructure Certificate og CRL Profile» (RFC 3280)	KITH 5.5
mekanismer, protokoller: formell	Kvalifiserte sertifikater skal følge kravene i ETSI TS 101 456 «Policy requirements for certification authorities issuin qualified certificates»	KITH 3.1
mekanismer, protokoller: formell	Overføring av nøkler gjøres i PKCS #12-format	KITH 3.2
mekanismer, protokoller: formell	Sertifikater skal inneholde entydig identifikator	KITH 2.1.1
mekanismer, protokoller: formell	For virksomhetssertifikater benyttes RFC 2459 som hovedformat	KITH 2.1.2
mekanismer, protokoller: formell	Revokering skal gjøre i henhold til RFC 2459 (CRL) og RFC 2560 (OCSP)	KITH 3.4

Tittel	*Sikkerhetskrav ved behandling av pasientopplysninger*	*DPP*
mekanismer, protokoller: formell	Signaturgenerering gjøres i henhold til CWA 14170 «Security requirements for signature creation applications»	KITH 4.2
mekanismer, protokoller: formell	Dokumenter som signerees skal ikke inneholde aktiv kode eller skjulte felt.	KITH
prosedyre, semiformell	Sertifikater skal ha gyldighetstid på 2 år	RTV 2.2.2
mekanismer, protokoller: formell	XML Signature og PKCS7 for kryptering og kvittering	WellComm.
mekanismer, protokoller: formell	Støtte for X.509 baserte sertifikater	WellComm.
mekanismer, protokoller: formell	Støtte for CRL og LDAP katalogoppslag	WellComm
mekanismer, protokoller: formell	Import av private nøkler og sertifikater fra MS CryptoAPI	WellComm
Subjektintegritet		
Krav om sikkerhetstjenester, semiformelt	Registrering av forsøk på uautorisert bruk. (Pers.oppl.forskr. §2)	Lovkrav
Krav om sikkerhetstjenester, semiformelt	Logging av aksess: Tid, ID, kontekst	EPJ-std
Krav, uformelt	informasjonseier skal registreres	EPJ-std
Krav, uformelt	gyldighetsperiode skal registreres	EPJ-std
Krav, uformelt	akseptabel risiko skal fastsettes	Lovkrav
Krav, uformelt	autorisasjon skal være underlagt styring	Lovkrav
Krav, uformelt	sikkerhetsrevisjon skal gjennomføres	Lovkrav
Krav, uformelt	sikkerhetsstrategi skal beskrives	Lovkrav
Krav, uformelt	konfigurasjonsvedlikehold skal være underlagt styring	Lovkrav
Krav, uformelt	risikoanalyse skal gjennomføres	Lovkrav
Krav, uformelt	utstyr skal skjermes med fysisk sikring	Lovkrav
Krav, uformelt	tiltak mot utro tjenere skal innføres	Lovkrav
Krav, uformelt	det skal etableres internkontroll	Lovkrav

Tittel	*Sikkerhetskrav ved behandling av pasientopplysninger*	*DPP*
Krav, uformelt	avvikshåndtering skal etableres	Lovkrav
Krav, uformelt	All informasjon skal sikres i henhold til Datatilsynets krav	SamPro 2.2.1
Krav, uformelt	Tilstrekkelig sikring av data og system. Tilkoplingssikkerhet og fysisk sikkerhet. Autorisert tilkopling og adgang, tilgangskontroll	Lovkrav
Krav, uformelt	Skal være mulig å gjenskape slettet informasjon ved feilsletting	EPJ-std
Krav, uformelt	Etablering av sikkerhetsprosedyrer for overensstemmelse med Personopplysningsloven. Personopplysnings-forskriften §2-13 m.m.	Lovkrav
Krav, uformelt	Dokumentasjon av sikkerhetsrutiner. Pers.oppl.forskr. §2-3--8, 2-16	Lovkrav
Behandlings-konfidensialitet		
Krav om sikkerhetstjenester, semiformelt	Sperre mot kopiering av data, lokal lagring ikke tillatt. Pasientinfo ikke cachet	Applikasjon
Krav, uformelt	medarbeidere har taushetsplikt	Lovkrav
Krav, uformelt	konfidensialitet skal sikres	Lovkrav
Krav, uformelt	informasjon skal ikke kunne kopieres til andre systemer	EPJ-std
Krav, uformelt	tilgang krever autorisasjon	EPJ-std
Krav, uformelt	tilgang krever autentisering	EPJ-std
Krav, uformelt	Helsepersonell har taushetsplikt	Instruks
Krav om sikkerhetstjenester, semiformelt	To-trinns autentisering	SamPro
Prosedyrer, semiformell	Tilstrekkelig sikring av data i systemet, tilkoplingssikkerhet og fysisk sikkerhet. Autorisert tilkopling og adgang, tilgangskontroll	EPJ-std
Krav om sikkerhetstjenester, semiformelt	PKI-basert autentisering (Krav til systemet om ebXML e.l.)	Applikasjon

Tittel	*Sikkerhetskrav ved behandling av pasientopplysninger*	*DPP*
Kontekstuell konfidensialitet		
Krav om sikkerhetstjenester	Adgangsstyring til enkeltelementer, rollebasert aksess. Mulig systemkrav om bruk av SQL rel.database	DIPS-systeme
Krav om sikkerhetstjenester	Anonymisering av data, kople ID fra informasjon, Ved statistisk behandling av data	EPj-std.
Krav, uformelt	Samtykkebasert tilgang til personopplysninger	SamPro 2.1.4
Krav, uformelt	Tilgang gis kun til relevant info, tilgang skal være nødvendig for aktuel behandling	KK.K#
Prosedyrekrav, semiformelt	Det skal være etablert prosedyrer for tildeling av roller og tilgangsrettigheter. Gjelder både vanlig bruk og aktualisering (Intern instruks)	KK.P#
Krav, uformelt	sletting av medier ved avsluttet bruk	Lovkrav
Krav, uformelt	uautorisert bruk skal hindres	Lovkrav
Krav, uformelt	forsøk på uautorisert bruk skal logges	Lovkrav
Krav, uformelt	tilgang skal gis basert på rolle eller funksjon	EPJ-std
Krav, uformelt	tilgang skal gis basert på behov, Tilgang gis kun til relevant info, tilgang skal være nødvendig for aktuel behandling Segmentert, rollestyrt tilgang til opplysninger	EPJ-std
Krav, uformelt	tilgang skal baseres på samtykke	EPJ-std
Krav, uformelt	ingen skal ha tilgang til informasjon de ikke er autorisert for	EPJ-std
Krav, uformelt	det skal skilles logisk mellom identitet og helseopplysninger	EPJ-std
Krav, uformelt	informasjonskategori og formål for bruk av informasjon skal angis	EPJ-std
Krav, uformelt	Opplysninger kan gis videre basert på pasientens samtykke	Instruks
Krav, uformelt	Elektronisk behandling av helseopplysninger til forskning skal skje i avgrenset og beskyttet system	Instruks

Tittel	*Sikkerhetskrav ved behandling av pasientopplysninger*	*DPP*
Krav, uformelt	Tilgangsrettigheter avgjøres av rolle i behandlingen. Taushetsplikt, kun autorisert tilgang når personell deltar i behandling eller foretar tilsyn	Instruks
Klarering, hjemmel		
Krav, uformelt	Formål med behandling skal finnes. Vedtak om tiltak	KH.K#
Krav, uformelt	Kilde for data angis. Autorisert registrering og registreringsmåte. Mulig kontekstbegrenset gyldighet/kvalitet	KH.K#
Krav om sikkerhetstjenester, semiformelt	Klassifisering av meldinger og filer, merking sensisitiv/ikke sensitiv i systemet	KH.T#
Krav, uformelt	overført data til tredjepart skal gis likeverdig beskyttelse. Tilstrekkelig dokumenterbar sikkerhet. Skal møte krav fra opprinnelsessystemet	Lovkrav
Krav, uformelt	det skal registreres når informasjon oversendes andre	EPJ-std
Krav, uformelt	det skal være mulig å følge referanser mellom systemer	EPJ-std
Krav, uformelt	Overføring av ukryptert video krever anonymisering	EPJ-std
Krav, uformelt	Offentlig lisens for helsepersonell krav for behandling av pasienter. Pers.opl.forskr. §7-26 (unntak fra kons.krav)	Lovkrav
Prosedyre, semiformel	Hjemmel for tilgang til personopplysning i lov, ved samtykke, ved behov. Må være gyldig i aktuel situasjon. Hjemmel for utveksling. Samtykke fra pasient eller hjemmel i lov	Lovkrav
Prosedyre, semiformel	Det skal bestemmes en informasjonseier. Databehandler skal ha fullmalt fra databehandlingsansvarlig. Fullmakt/autorisasjon skal hjemles i styringssystem	Instruks
Utvekslingskontroll		

Tittel	*Sikkerhetskrav ved behandling av pasientopplysninger*	*DPP*
Krav, uformelt	Registrering ved avgivelse av informasjon når oversendt andre	EP-std
Krav om sikkerhetstjenester, semiformelt	Informasjon som er referert andre steder må ikke slettes	EP-std
Krav om sikkerhetstjenester, semiformelt	Logg av hendelseskronologi: Juridisk, oppgaver, system, revisjon	EP-std
Krav om sikkerhetstjenester, semiformelt	Responsverifikasjon, ikkebenekting, bekreftelse på korrekt mottak	EP-std
Krav om sikkerhetstjenester, semiformelt	Skal kunne bekrefte rett mottak, ikkebenekting. PKI-støtte	EP-std
Krav, uformelt	Ansvar for opprinnelse angis. Bevaring av signatur og info om organisasjon. Referanse, opprinnelig informasjonseier	EP-std

Tabell 16: Sikkerhetskravprofil for pasientdata, Data Protection Profile – DPP.