RÅDET FOR IT-SIKKERHED

Pervasive computing – it-sikkerhed og privacy

1 Indholdsfortegnelse

2 Sammenfatning

I forbindelse med pervasive computing bliver sikringen af privatlivets fred (privacy) ofte omtalt som den største it-sikkerhedsmæssige hindring for, at den almindelige forbruger vil have tillid og tryghed til teknologien. Et naturligt spørgsmål er om denne frygt er begrundet og evt. i hvilket omfang, men bestemt også hvilke andre it-sikkerhedsproblemer pervasive computing kan afstedkomme. I "Ting der tænker" fra Teknologisk Fremsyn anbefales det således, at Rådet for it-sikkerhed gennemfører en analyse for at afdække hvad de *reelle* it-sikkerhedsproblemer ved pervasive computing er.

Denne rapport indeholder en analyse og kortlægning af de vigtigste it-sikkerhedsproblemområder ved pervasive computing, samt en undersøgelse af, hvorvidt persondataloven sikrer en fornuftig balance mellem muligheden for registrering af informationer og den nødvendige beskyttelse af personlige rettigheder og privatlivets fred.

Rapportens hovedkonklusioner er, at de primære kortsigtede it-sikkerhedsproblemer er relateret til sikring af privatlivets fred samt brugbarhed. Hvad angår den retlige analyse konkluderes, at persondataloven er egnet til at sikre privatlivets fred, givet at den praktiske udfyldning af lovens regler løbende opdateres således at disse er realistiske i den teknologiserede virkelighed.

På længere sigt forventes det, at den forbedrede teknologi dels vil hjælpe med at løse nogle af disse problemer, dels vil danne baggrund for mere avancerede anvendelser af personlige agenter. Dette introducerer nye sikkerhedsmæssige problemer, relateret til indgåelse af bindende aftaler mellem agenter og håndtering af tillid til andre personers agenter.

På baggrund af analysen gives en række anbefalinger til håndtering af de centrale problemer:

- Udarbejdelse af en kodeks for brug af rfid i detailhandlen.
- Klarhed over behovet for stærk kryptering af følsomme persondata - specielt i forbindelse med anvendelse af enheder med begrænset kommunikationsrækkevidde.
- Anvendelse af anerkendte sikkerhedsprotokoller.
- Igangsættelse af et "proof-of-concept"-projekt som skal illustrere hvorledes nogle af de identificerede problemer kan håndteres.
- Undersøgelse af retlig status for aftaler indgået af personlige agenter.
- Nedsættelse af ekspertgruppe til at følge udviklingen af it-sikkerhed inden for pervasive computing.
- Videreføre og kombinere den danske tradition for forskning inden for it-sikkerhed og brugbarhed af it-løsninger.

3 Introduktion

3.1 Baggrund

Denne rapport er udarbejdet for Rådet for it-sikkerhed som opfølgning på rapporten "Ting der tænker"[1], hvori det anbefales at lave en analyse af sikkerhedsproblemer forbundet med pervasive computing.

Ifølge "Ting der tænker" skal denne rapport bidrage til, at der skabes tillid og tryghed ved brug af pervasive computing hos forbrugerne, idet rapporten skal vurdere hvilke problemer relateret til sikkerhed, der er reelle, for derved at muliggøre en kvalificeret diskussion, så tillid og tryghed kan skabes på et solidt fundament. Rapporten har derfor ikke som sådan til formål at give en teknisk eller juridisk fuldstændig dækkende fremstilling af området, men at udgøre et seriøst fagligt funderet bidrag til den tekniske og juridiske diskussion af de it-sikkerhedsmæssige aspekter af pervasive computing. Dette skal specielt ses i lyset af, at området både industrielt og inden for forskningen er i rivende udvikling.

Den fremtidige anvendelse af pervasive computing er blandt andet beskrevet ved en række scenarier, hvoraf nogle er en realitet i dag, mens andre næppe er sandsynlige foreløbigt – og måske aldrig bliver det. Vurderingen af sikkerhedsaspekterne ved pervasive computing vil tage udgangspunkt i disse konkrete scenarier, idet den hermed kommer tæt på den forventede anvendelse af pervasive computing.

3.2 Pervasive computing

Pervasive computing betyder, at der er computere overalt, og den danske oversættelse er meget passende it-i-alt[2]. Vi støtter os til den uformelle definition i "Ting der tænker" og fastholder det engelske navn pervasive computing.

Kort fortalt handler pervasive computing om, at der er computere overalt (heraf navnet it-i-alt), hvilket muliggøres af den teknologiske udvikling, hvor chips hele tiden bliver mindre og billigere. "Ting der tænker" lister forskellige eksempler på pervasive computing:

- Interaktive rum. Udover forbrugerelektronik i private hjem omfatter dette fx kontorstole som husker højdeindstilling, intelligente køleskabe som ved om mælken er for gammel, og gulvvarme som automatisk slås til når vejrudsigten lyder på koldt vejr.
- Tøj. Dette kan fx være jakker med indbyggede mp3-afspillere, sportstøj med indbygget pulsmåler og briller med indbygget skærm. Andre eksempler inkluderer intelligent arbejdstøj, fx til brandmænd[3].
- Healthcare. Kunne være intelligente bandager, som kan fortælle hvordan skaden har det, og videokonferencer med læger, så syge kan behandles hjemme. Et andet eksempel er døre som automatisk åbnes, så redningspersonalet kan komme ind til en patient med insulinchok.
- Detailhandel og produktion. En lang række eksempler findes inden for detailhandlen, fx tyverisikring som fungerer ved at varen sladrer hvis den forlader butikken, automatisk

[1] [TDT].
[2] Relaterede begreber er ubiquitious computing og ambient intelligence. Ubiquitious computing handler om computere, som forsvinder, dvs. er alle steder men usynlige, og ambient intelligence går skridtet videre og kikker på hvorledes dette kan udnyttes af "intelligente" applikationer. I denne rapport forsøger vi at favne alle tre begreber under en hat.
[3] Se fx [IpFireFighter].

optælling af varelageret, og kasseapparater uden kassedamer hvor indkøbsvognen køres igennem en scanner som registrerer varerne. Der arbejdes også med tanker om at bruge fx rfid til advarsler til allergikere, fødevaresikkerhed, affaldssortering og meget mere.
- Biler. Computerstyrede bremser og dvd-film og spil til passagererne er allerede udbredt ligesom brugen af GPS og vejvisning. Løsninger som tilbyder automatisk alarm mod glatte steder på vejen via kommunikation med andre biler og trafiksikkerhedstiltag er også på vej.
- It. Her tilbyder pervasive computing nye løsninger som fx offentlige printere, som kan benyttes via mobiltelefonen og automatisk lagring af personlige data som fx digitale fotos. Brugen af chips i pas er et andet eksempel.
- Militær. Endeligt findes en lang række militære anvendelser som fx ubemandede fly, kampvogne og operationsstuer, våben som kun kan affyres af rette ejermand mm.

Alle disse anvendelser er baseret på de mange nye enheder med indbyggede computere og kommunikationsmuligheder, hvor vi formodentlig kun har set toppen af isbjerget. Det er karakteristisk at pervasive computing involverer enheder med begrænset it-kapacitet, dvs. begrænsede ressourcer i form af cpu-kraft, hukommelse, båndbredde og batteri. Blandt de mest prominente repræsentanter herfor er de såkaldte rfid-tags (også kendt som elektroniske stregkoder), men listen af almindeligt udbredte pervasive computing-teknologier er allerede lang og indeholder ting som mobiltelefoner, PDA'er, BlueTooth og meget mere.

Som supplement kan også nævnes et par eksempler på moderne it, som er placeret i periferien af pervasive computing[4]: Almindelige tjenester på internettet, hvor man tilgår informationer fra en central database som fx diverse netbank-løsninger; brug af traditionelle pc-baserede programmer til regnskab, grafik, spil osv. I denne rapport betragter vi ikke sådanne løsninger.

I "Ting der tænker" præsenteres en internet-inspireret opdeling fra Forrester[5] i "the executable internet": "*Intelligent applications that execute code near the user to create rich, engaging conversation via the net.*", som vi vil kalde *services-i-alting*, og i "the extended internet": "*Internet devices and applications that sense, analyze, and control the real world.*", som vi vil kalde *agenter-i-alting.* En fundamental forudsætning for dette er, at enheder (inkl. tøj, lamper osv.) er på nettet, og vi kan derfor passende supplere ovenstående med *id-i-alting*: at alle mulige genstande og enheder er på nettet og dermed kan kommunikere elektronisk med andre enheder. Dette betyder specielt, at hver enkelt enhed kan identificeres[6]. Listet efter stigende teknologisk kompleksitet:

- Id-i-alting er karakteriseret ved anvendelsen af passive enheder, forstået derhen at enhederne kun kan afgive deres id og evt. rå sensorinput. Alle beregninger, som ikke vedrører afsendelse af id, er placeret i den infrastruktur, der kommunikeres med. Eksempler herpå er fx anvendelsen af rfid til tyverisikring af tøj, online termometre og webcams og en række andre "passive" enheder.
- Services-i-alting er karakteriseret ved anvendelsen af mere aktive enheder, som selv kan udføre beregninger og påvirke omgivelserne. Som eksempler kan nævnes en lang række services tilgængelige via elektronisk kommunikation, som fx køleskab, varmemåler, motoren i bil osv.

[4] I praksis kan det være svært at give en præcis afgrænsing af begrebet pervasive computing. Ofte vil mere traditionelle løsninger været tæt integreret med pervasive computing-løsninger. Ligeledes er det fx heller ikke oplagt om et traditionelt computerspil afviklet på en mobiltelefon falder ind under begrebet pervasive computing.
[5] Se [Forrester].
[6] Ikke nødvendigvis en entydig identifikation i global forstand. Vi vil behandle dette nærmere nedenfor.

- Agenter-i-alting er karakteriseret ved, at enhederne ikke alene er aktive, de er også autonome, dvs. sender data og påvirker omgivelserne på eget initiativ. Eksempler er softwareagenter, som automatisk leder efter din yndlingsvin og automatisk bestiller og betaler den (efter at have spurgt flasken – for den er også på nettet – direkte om fx dens temperatur igennem dens levetid).

3.3 It-sikkerhed

I forbindelse med it-sikkerhed betragtes følgende tre fundamentale egenskaber[7]

Integritet
Integritet er en bekræftelse af, at der ikke er sket ændringer i sendt, modtaget eller gemt data. Sikring af integritet kræver, at kun brugere/enheder med adgangsret til data/systemer kan ændre data. Dermed vil autenticitet af information, som sikrer, at pågældende information oprinder fra den angivne kilde, ligeledes blive central.

Fortrolighed
Fortrolighed er en beskyttelse mod, at udenforstående får adgang til fortrolige informationer.

Tilgængelighed
Systemer og data skal være tilgængelige og fungere på trods af mulige forstyrrelser. Forstyrrelser kan fx være angreb, uheld, strømafbrydelser og naturkatastrofer.

En implicit forudsætning for at opbygge sikre it-systemer i henhold til disse begreber er, at man kan foretage en sikker adgangskontrol til it-systemer – fysisk såvel som logisk. I forbindelse med integritet må adgang til skrivning/ændring af data kontrolleres, og i forbindelse med fortrolighed skal adgangen til at læse data kontrolleres.

Adgangskontrol omfatter dels identifikation (autentificering) af de brugere/enheder, som ønsker adgang, dels autorisation til at tilgå de ønskede data. Identifikation skal her forstås bredt, idet dette eksempelvis kan være entydig fysisk identifikation, genkendelse i en givet kontekst (fx ved brug af pseudonymer) eller bevis for at man besidder de rettigheder, der kræves for at opnå den ønskede adgang. Identifikation, som brugt i denne rapport, er derfor ikke nødvendigvis i en entydig forstand, men derimod *til formålet*.

Identifikation af en person foregår ofte ved brug af PIN-koder (eller password), biometriske metoder eller engangspassword (fx ved hjælp af specielle tokens). Denne identifikation kan enten ske direkte mod det system, hvortil brugeren ønsker adgang, eller ved en to-trins proces: brugeren identificerer sig først mod en lokal enhed, som efterfølgende udfører en identifikation mod systemet på brugerens vegne. Dette vil typisk gøres ved hjælp af kryptografiske mekanismer så som digitale signaturer eller specielle identifikations-protokoller beregnet til dette formål. I dette andet trin vil enheden således optræde som en betroet, idet det implicit forudsættes, at den kun vil fuldføre trin 2, hvis trin 1 forløb med succes. Fordelen ved to-trins processen er, at den identifikations-protokol, som enheden anvender, kan være meget sikker og samtidig kan enheden potentielt sættes op, så den kun identificerer brugeren i den udstrækning, det er nødvendigt for at få den ønskede adgang.

[7] Se [RFITS].

En implicit antagelse i forbindelse med brugeridentifikation er, at brugeren opfører sig (nogenlunde) som forventet. Er dette ikke tilfældet, kan det få alvorlige konsekvenser for opretholdelsen af de ønskede sikkerhedsegenskaber. Sættes eksempelvis en papirlap med password på skærmen, er værdien af adgangskontrollen allerede drastisk reduceret. Et vigtigt element af sikkerhed er derfor, at de dele, som kræver interaktion med brugeren, er brugbare, dvs. at brugeren er i stand til at bruge dem på en naturlig måde, således at normale arbejdsgange fx ikke ændres. Brugbarhed betyder også, at brugeren har forståelse for sikkerhedsrelaterede problemer, såsom at password er personlige osv.

Integritet og fortrolighed sikres ved en række mekanismer varierende fra fysisk adgangskontrol over sikkerhedsprocedurer til anvendelse af kryptografi. I forbindelse med pervasive computing, hvor der ofte kun kan anvendes fysisk beskyttelse i begrænset omfang, vil mekanismer baseret på brugen af kryptografi ofte blive anvendt.

I forbindelse med fortrolighed skal det allerede her nævnes, at forhold omkring sikring af privacy allerede har været debatteret meget, og privacy-problemer er i medierne og litteraturen omtalt som akilleshælen ved pervasive computing[8]. Vi skal her betragte tre niveauer af privacy:

- anonymitet (eller fortrolighed af identitet)
- beskyttelse mod location tracking, som giver fortrolighed af hvor man har været
- linking eller data-aggregering ("data aggregation"), som er sammenkædning af forskellige stumper data, som i sig selv er uskyldige, men som tilsammen er afslørende[9].

Location tracking er et specialtilfælde af linking, og de to begreber kaldes under en fælles dansk betegnelse for sporing. Det kan i mange tilfælde ikke udelukkes, at et succesfuldt sporings-angreb kan lede til identifikation af personen, idet sammenkædning af en række begivenheder vil karakterisere personen entydigt.

Det skal her bemærkes, at opsætning af systemer, som fx giver øget sikring af integritet og fortrolighed, ofte medfører en risiko for forringet tilgængelighed. Hvis data eksempelvis krypteres af hensyn til fortrolighed, vil disse ikke være tilgængelige, hvis nøglen mistes. Ligeledes kan adgang til data mistes, såfremt et påkrævet password glemmes. I praksis løses sådanne problemer med passende procedurer, fx for backup af nøgle-materiale og mulighed for at få et nyt password. Et andet eksempel er anvendelsen af PUK-koder i mobiltelefoner til åbning af telefonen, hvis man har glemt PIN-koden.

3.4 Retlig regulering

Ret og sikkerhed hænger sammen i den forstand, at de begge er midler til at opnå bestemte mål, eksempelvis beskyttelse af identitet (anonymitet). Retlig regulering kan dog også indebære krav til teknologien og den med denne forbundne sikkerhed. Retlige krav til pervasive computing kan forudsætte, at bestemte former for sikkerhed foreligger.
De retlige krav har først og fremmest være forbundet med værnet af privatlivets fred (privacy) og det enkelte individs personlige integritet. Disse retlige krav omfatter en række delkrav. Der må være åbenhed/transparens om anvendelsen af teknologien. Åbenhed angår her ikke de tekniske detaljer,

[8] Se [IEEEPervasive].
[9] En artikel i [SPC] nævner fx hvorledes man kan spore vha. af det trådløse netværkskort på en bærbar: Udfra at computeren ses på en bestemt postadresse hver aften og en bestemt arbejdsplads hver dag, kan ejerens identitet med stor sikkerhed bestemmes; ses samme bærbare computer nu regelmæssigt hos fx en psykolog kan man drage sine konklusioner – vel at mærke udfra tre stykker information som hver for sig er uskyldige.

men information om at teknologien, fx rfid-tags, bliver anvendt. Et andet krav er, at det enkelte individ skal have mulighed for at udøve kontrol med teknologien. Denne kontroladgang må dog afvejes overfor andre legitime hensyn, der kan være fastsat ved lov[10]. Et tredje krav er, at teknologien kun anvendes, når dette er sagligt og i overensstemmelse med god skik. Bedømmelsen heraf vil variere fra område til område, men af betydning er bl.a. formålet og at opsamlede data ikke spredes bredt, hvilket sikkerhed kan bistå med at hindre. Et fjerde krav er, at oplysninger ikke bruges til at skabe profiler, som fx kan bruges til overvågning af borgerne. Krav af denne type kan opfyldes på forskellig måde, jf. bilag 2 og 3.
Det tilføjes, at der kan være retlige krav, der ikke er forbundet med teknologiens anvendelse i forhold til identificerbare borgere, idet sådanne krav ofte vil kunne opfyldes uden at der stilles særlige sikkerhedskrav.

[10] Bliver det bestemt at pengesedler skal forsynes med rfid vil den enkelte borger ikke kunne have så meget kontrol, at vedkommende kan vælge at bruge sedler uden rfid. Et andet eksempel kan være pas forsynet med rfid.

4 Scenarier og cases

Begrebet pervasive computing spænder vidt og rækker fra ren science fiction til dagligdags ting som mobiltelefoner. En sikkerhedsanalyse er en meget konkret vurdering af værdier og trusler mod disse, og for at få begrebet pervasive computing "ned på jorden", så konkrete værdier og trusler kan identificeres, tager analysen i denne rapport udgangspunkt i konkrete scenarier og cases. Disse er samlet fra forskellige forskningsprojekter, tænketanke og industrielle anvendelser inden for pervasive computing.

Scenarier og cases falder i de tre grupper beskrevet i afsnit 3.2:

- Id-i-alting
- Services-i-alting
- Agenter-i-alting

De fuldstændige scenarier og cases er præsenteret i bilag 4. I dette afsnit beskrives essensen af disse.

Et gennemgående element i de beskrevne scenarier og cases er, at de sjældent eksplicit inddrager it-sikkerhed. Det betyder ikke, at sikkerhed ikke er vigtigt i disse scenarier. Tværtimod, ISTAG-scenarierne (som er af typen agenter-i-alting) nævner eksempelvis sikkerhed som et vigtigt element[11], og det er derfor en implicit antagelse i de beskrevne cases og scenarier, at sikkerheden kan opretholdes i ønskelig grad på en måde som ikke i det væsentlige ændrer brugen. Med andre ord, så må introduktion af sikkerhed ikke reducere brugbarheden.

4.1 Id-i-alting

Dette niveau er allerede kommercielt udbredt. Basalt set tilbydes en facilitet, hvor en enhed kan identificere sig passivt (aflæses af scanner) eller aktivt (sender et signal – evt. kontrolleret af brugeren). Det mest omtalte eksempel er anvendelsen af rfid-tags i detailhandlen og i produktionsstyring. Cases med konkrete applikationer inkluderer:

- Tyverisikring, se fx på [electronics.howstuffworks.com/question601.htm].
- Logistik. Ideen er dybest set at sætte et rfid-tag på en vare eller fx bare en palle med varer for derved at kunne styre logistikken omkring butikkernes varebeholdning. En sådan anvendelse hos Walmart har været meget omtalt, men også engelske Tesco [www.rfidjournal.com/article/articleview/658/1/1/] og danske Kims har gjort lignende tanker.
- Tracking af personer. KidSpotter [www.kidspotter.com], som anvendes i Legoland, er et godt eksempel. Her får børn et armbånd med et tag, og hvis et barn bliver væk, kan forældrene via en SMS-service få opgivet, hvor i Legoland de er.
- Identifikation af personer. Det mexicanske retssystem byder på et mere eksotisk eksempel, hvor ansatte hos den mexicanske statsadvokat har fået indopereret en chip som reelt er et almindeligt rfid-tag fra firmaet VeriChip, som benyttes til at identificere ansatte i forbindelse med deres adgang til fortrolige dokumenter [www.nytimes.com/2004/10/14/technology/14implant.html]. Et mindre vidtgående eksempel er anvendelse af chips i kort, der giver adgang til at bruge lift på skisportssteder.

[11] Se fx de "socio-political issues" i forbindelse med scenariet "Maria – road warrior".

Derudover findes og forskes der i mange andre anvendelser som fx automatiske kasselinjer hvor alle varer automatisk scannes, når man kører sin indkøbsvogn forbi kasseapparatet, og måske trækkes beløbet endda automatisk fra køberens kreditkort.

Selvom ovennævnte udvalg af cases fokuserer på anvendelser af rfid-teknologien, er dette langtfra er den eneste repræsentant for dette område. En lang række andre teknologier er ligesom rfid bærere af information om identitet, fx magnetkort, smart cards (som de nye Dankort), SIM-kort (teknisk set også smart cards) som sidder i mobiltelefoner og BlueTooth-enheder. Disse teknologier har en bredere anvendelse, der behandles som en del af services-i-alting nedenfor.

I forhold til privacy har de her nævnte teknologier og anvendelser den umiddelbare svaghed, at de alle involverer entydig identifikation, hvilket kunne lede til den fejlagtige konklusion, at entydig identifikation er et nødvendigt element. Det er det ikke. Der findes mange forslag til løsninger, som ikke involverer entydig identifikation, blot er deres kommercielle anvendelse mindre udbredt.

Det centrale element ved id-i-alting er, at enheder kan identificeres ved aflæsning, altså en afbildning af fysiske objekter – det være sig genstande eller mennesker, eller genstande som repræsenterer eller er knyttet til mennesker, som fx en togbillet – ind i det virtuelle rum.

4.2 Services-i-alting

På dette niveau er enheder ikke bare på nettet, de er også udstyret med sensorer, aktuatorer og forskellige applikationer, hvorved enhederne kan tilbyde forskellige former for services via nettet. Grundlæggende kan man sige, at systemer på dette niveau assisterer brugeren i dennes handlinger. Denne teknologi er delvist en realitet, fx via PDA'er, digitalkameraer og meget andet som kan kommunikere, og dermed er på nettet i en eller anden forstand.

Som repræsentanter for services-i-alting haves tre scenarier fra aktuelle forskningsprojekter:

- EPCiR. Handler om hjemmebehandling af diabetespatienter med fodsår[12]. Patienten er udstyret med en "intelligent" bandage, som sender forskellige data til en database, og derudover foretages videokonsultationer af en speciallæge på et sygehus ved en besøgende sygeplejerskes mellemkomst.
- The European Service Network (ESN) fra eu-Domain[13] handler om vvs-folk, som er online via deres biler (som automatisk betaler for parkering, bropenge etc.), som bruger virtual reality-briller til at studere varmepumper (som sender data om deres tilstand til brillerne, vvs-mandens PDA mv.), og som når han mangler en reservedel kan lokalisere den nærmeste forhandler eller kollega, der kan sælge ham en sådan reservedel og elektronisk kan indgå købsaftale her og nu.
- Healthcare for tomorrow (også fra eu-Domain) handler som ESN-scenariet om en mobil arbejder, men er her en sygeplejerske, hvilket minder lidt om EPCiR-scenariet. Her benyttes fx rfid til at holde tal på patientens insulinbeholdning, og sygeplejersken får automatisk adgang til patientens hjem, hvis patienten ikke svarer, når sygeplejersken ringer på døren (og patienten vel at mærke er hjemme).

[12] Dette er et alvorligt problem, fordi diabetikeren ikke kan føle såret, hvilket betyder, at der ofte kommer komplikationer fx i form af infektion. I Danmark foretages årligt mange – potentielt unødvendige – amputationer af denne grund.

[13] Eu-Domain er navnet på det forskningsprojekt sponseret af EU, som ESN- og Healthcare for tomorrow-scenarierne stammer fra. Udover selve scenarierne indeholder bilag 4 også en reference til dette projekts hjemmeside.

Samlende for disse scenarier er, at vi har tre typer enheder i spil. Sensorer (fx på varmepumpen) som sender data. Aktuatorer som modtager instruktioner (fx om at låse døren op eller tænde lyset). (Delvist) centrale enheder, som fx en PDA eller såkaldt gateway[14] i vvs-mandens bil. Forskellige enheder kan have et, to eller alle tre egenskaber og kan kommunikere via centrale punkter eller decentralt (dvs. direkte med hinanden). De fleste enheder kan tilgås af brugeren enten direkte eller via andre enheder. Derudover er der stor dynamik i forhold til hvilke enheder, som skal snakke med hinanden, fx når sygeplejersken slutter et videokamera til i patientens hjem. Generelt er systemerne dog relativt lukkede, således at det på forhånd vides hvilke (typer af) enheder som vil forekomme, og disse enheder vil kunne forberedes på at skulle deltage i systemet. Et lidt gammeldags, men meget udbredt, eksempel, som ikke er nævnt i scenarierne, er fjernbetjeninger til alskens elektronisk udstyr. Typisk er fjernbetjeninger netop en del af et lukket system, idet de netop er konstrueret til at kommunikere med en bestemt type enheder.

Det skal bemærkes, at brugbarhed nævnes sjældent eller slet ikke i disse scenarier. Det betyder dog ikke at det ikke er vigtigt, snarere tværtimod, idet grænsefladen mellem systemet og brugeren antages (implicit) at være af en sådan kvalitet, at de beskrevne arbejdsgange kan foregå uden videre problemer. Dette betyder specielt også, at de dele af systemet, som kan henføres til sikkerhedskrav også formodes at være naturlige i deres brug, fx brugerautentifikation, ligesom de mekanismer, der skal til for at understøtte fx tilslutningen af sygeplejerskens medbragte videokamera.

Ud fra et teknologisk perspektiv har denne samling af scenarier den begrænsning, at de har fokus på gateway-baserede løsninger, dvs. kommunikation via en *central* enhed. Dette kan skyldes, at de projekter, scenarierne er taget fra, har relativt kort tidshorisont, og på kort sigt lader det til at løsninger baseret på gateways er tættest på kommerciel realisering. Nedenstående agenter-i-alting-scenarier behandler til gengæld også decentrale løsninger.

Gateways og en lang række af andre aktuelle teknologier, som kan og vil være med til at danne den tekniske platform for pervasive computing, er beskrevet i bogen "Pervasive Computing"[15].

4.3 Agenter-i-alting

Denne sidste gruppe er beskrevet ved fire scenarier udarbejdet af en tænketank under EU. Disse scenarier er tænkt som et muligt kik ind i fremtiden i overensstemmelse med EUs vision om ambient intelligence.

- Maria – road warrior. Maria behøver ikke vise pas når hun rejser, systemet udfører automatisk id-checks via hendes intelligente armbånd. Hendes lejede bil står automatisk klar et anvist sted, når hun ankommer. Maria gemmer en krypteret udgave af en præsentation på et fremmed firmas netværk. Den dekrypteres, når hun har brug for den, og 1 1/2 minut efter at præsentationen er slut, slettes den krypterede udgave. Under præsentationen er hendes telefon lukket ned, så kun meget vigtige opkald kommer igennem.
- Dimitrios – Digital Me. Dimitrios har en agent, Digital Me, som håndterer mange beslutninger for ham. Fx udleverer den data om det nærmeste apotek til en anden persons agent, fordi den anden person mangler samme type medicin som Dimitrios bruger; i denne forbindelse beslutter agenten, at den ikke vil udlevere information om hvem Dimitrios

[14] En gateway er populært sagt en computer, som forstår en lang række kommunikationsprotokoller, både kort- og langtrækkende, dvs. den kan fungere som bindeled mellem enheder med kort rækkevidde og resten af verden.
[15] [PC].

faktisk er til den anden persons agent; på den ene side sikrer dette Dimitrios' anonymitet, men på den anden side forhindrer det også en uddybende personlig (menneskelig) samtale. Dimitrios agent besvarer også telefonopkald med en stemme, der lyder som Dimitrios', og lader kun de opkald komme igennem som den ved Dimitrios ønsker.

- Carmen – traffic, sustainability & commerce. Carmens agent finder kørelejlighed for Carmen ved at kontakte andre bilisters agenter. Mens Carmen bliver kørt på arbejde, finder hendes agent de varer hun noterede om morgenen og bestiller og betaler dem til levering ved hendes lokale kiosk, så Carmen blot kan hente dem på vejen hjem. Agenten falder over et godt tilbud på Carmens yndlingsvin og præsenterer dette for Carmen, som beslutter sig for, at den også skal købes.
- Annette and Solomon – the Ambient for social learning. "The Ambient" er overalt i det lokale, hvor Annette og Solomon følger et undervisningsforløb. The Ambient kommunikerer vha. talesyntese og formidler kommunikation mellem forskellige deltagere i undervisningsforløbet via noget som kunne minde om videokonferencer; dette indebærer kommunikation over få meter til flere tusind kilometer.

På nær det sidste minder disse scenarier om services-i-alting-scenarier. Den store forskel ligger – for de tre første scenarier – i udbredelsen, både globalt og lokalt, samt den fundamentale forskel at beslutningsansvar i stort omfang overdrages til teknologien. Globalt i den forstand at teknologien findes uanset hvor man rejser hen i verden, og lokalt i den forstand at teknologien findes overalt: I armbånd, i den lokale kiosk, i fødevarer, i biler osv. I sandhed pervasive computing! Overdragelsen af ansvar består i, at en lang række beslutninger i disse scenarier træffes af såkaldte agenter. Dette inkluderer simple opgaver som modtagelse af telefonopkald og kalenderfunktioner, men også økonomiske transaktioner og vurderinger om udlevering af personlige data.

På det teknologiske område vil en række af de beskrevne funktionaliteter kunne løses med de samme teknologier som under services-i-alting. De beskrevne systemer er dog ikke længere "lukkede" i samme forstand, dvs. man kan ikke længere begrænse sig til fx at skulle kommunikere med enheder, som er tilsluttet et "lokalt" system, som det fx er tilfældet i EPCiR-scenariet. Desuden vil fremtiden måske byde på større anvendelse af ad-hoc-netværk, som modsat gateways mv. er en decentral netværksstruktur.

5 Analyse af retsgrundlaget og de retligt orienterede hensyn og krav

Med henblik på at sikre, at pervasive computing anvendes på en samfunds- og hensigtsmæssig måde til gavn for borgere og virksomheder, er der ud over gode sikkerhedsløsninger behov for retlig regulering, som kan understøtte dette mål. Denne retlige regulering kan være af forskelligartet karakter, men angår dog hovedsageligt spørgsmålet om privatlivets fred, som det følgende og den mere detaljerede redegørelse i bilag 2 derfor er centreret om. Behovet for at sikre tilstrækkelig privacy har betydning for borgernes accept og modtagelse af de nye teknologier og dermed ligeledes for den erhvervsmæssige udnyttelse af disse teknologier.

Et hovedspørgsmål for den retlige analyse er på denne baggrund hvorledes det kan sikres, at det enkelte menneske ved udbredelsen af pervasive computing undgår at blive transparent eller informatorisk nøgent, fx ved at data om online personen bliver tilgængelige for enhver. Hvorledes sikres autonomi og en samfundsmæssig forsvarlig selvbestemmelsesret for den enkelte person. Det er denne problemstilling, der må anses for den centrale under det retlige perspektiv, som dermed er knyttet til den grundlæggende ret til privatlivsbeskyttelse i Den Europæiske Menneskerettighedskonventions artikel 8.

Ved vurderingen af denne problemstilling er det vigtigt at skelne mellem to situationer. I den første indebærer brug af pervasive computing, at der opnås viden om eller sker overvågning af personer, hvis identitet ikke er kendt, medens der i den anden sker behandling af oplysninger om identificerbare personer. Uanset den fortsatte udbredelse af identificeringsteknologi vil den første situation fortsat forekomme, og for at forebygge en generel oplevelse af at være overvåget, er det ønskeligt, at der fastsættes regler, der både i den offentlige og den private sektor indebærer en forpligtelse til i almindelighed at informere om, at sådanne former for pervasive computing bliver anvendt. Den anden situation påkalder sig dog størst interesse, og det følgende vedrører derfor denne.

I dag er problemstillingen reguleret i persondataloven (samt en række sektorlove), og spørgsmålet er om denne regulering, der i det væsentligste beror på direktiv 96/46 EF, fortsat er tilstrækkelig, når it er i alt. Med andre ord om loven er fremtidssikret[16]. Loven tager ikke stilling til, hvem der ejer persondata, men derimod til på hvilken måde den, der har persondata i sin besiddelse, må behandle disse data. Selvom det for en umiddelbar betragtning kunne være tiltalende at antage at den enkelte person ejer sine egne data, er dette reelt en kompleks problemstilling, der på ingen måde alene er knyttet til pervasive computing. Konsekvenserne af en regel, hvorefter personen ejer sine data, er nærmest uigennemskuelige, hvorfor det i denne sammenhæng er bedst at basere den retlige analyse på den indfaldsvinkel, der er lovens.

Et væsentligt spørgsmål bliver herefter om det i en situation, hvor it er overalt, herunder stadig mere i online-verdenen, fortsat er muligt med sikkerhed at fastslå hvem der i konkrete situationer er den dataansvarlige, der skal opfylde lovens krav. Det stigende flow af data vil givet på dette punkt skabe vanskeligheder, og vil ligeledes i nogle tilfælde kunne gøre det mindre rimeligt at fastholde dataansvaret hos en oprindelig dataansvarlig. Dette begrebs udfyldning i praksis bør derfor overvejes fremover.

[16] Ved vurderingen heraf er der ikke taget hensyn til den lidt fjerne fremtid, "agenter-i-alt".

En justering af praksis kunne, som det vil fremgå nedenfor, ligeledes være aktuel i forhold til andre af lovens regler uden at dette betyder, at disse formelt skal ændres. Årsagen hertil er dels at de gældende regler er udformet teknologineutralt, dels at de i mange tilfælde har karakter af retlige standarder, der kan tilpasses en ændret teknologisk virkelighed.

Dette gælder således for de almindelige principper, herunder om saglighed/god skik, formålsbestemthed, proportionalitet, datakvalitet og tidsbegrænsning. Disse principper, som udgør databeskyttelsens forfatning, er velegnede i forhold til pervasive computing, men de sættes samtidig under pres af denne udvikling. Det kan eksempelvis blive vanskeligere at sikre, at det oprindelige indsamlingsformål styrer dataanvendelsen, således at der er den ønskelige transparens, eller at sikre at persondata ikke i nye sammenhænge benyttes, således at de giver et vildledende billede af personen. Pervasive computing stiller krav om øget opmærksomhed i forbindelse med princippernes overholdelse.

Af central betydning vil fremover være princippet om sikkerhed. I loven er der fastsat et generelt krav om sikkerhed. Det kan konstateres, at dette for den offentlige forvaltning er uddybet i en bekendtgørelse og vejledning, hvilket derimod ikke er tilfældet for den private sektors vedkommende, hvilket kan give anledning til en vis undren. I praksis antages dog, at disse regler også gælder for denne sektor. Der er grund til at fremhæve, at en dataansvarlig har pligt til at fastsætte adæquate sikkerhedsregler, der løbende skal opdateres, at der skal udvises særlig opmærksomhed, når oplysninger transmitteres, idet eksempelvis følsomme data, fx helbredsdata, skal underkastes stærk kryptering baseret på en anerkendt algoritme, og at der ligeledes skal være særlig opmærksomhed, når persondata behandles uden for et professionelt miljø, fx hjemme. Det må betragtes som ønskeligt, at de retligt fastsatte sikkerhedskrav løbende tilpasses den teknologiske situation, dels søges formidlet på den mest effektive måde.

I almindelighed er det ønskeligt, at den enkelte person er informeret om at persondata behandles ved hjælp af it. I loven er det fastsat, at der skal gives information, når oplysninger enten direkte eller indirekte indsamles. Når it kommer i alt, kan det blive vanskeligt at sikre, at denne forpligtelse altid opfyldes ved den indirekte indsamling, der vil finde sted i stadig større udstrækning. Reglen kan komme til at virke ressourcebelastende, men er i og for sig god nok, idet der dog må forventes at blive et stigende behov for tilsyn med dens overholdelse.

Et centralt spørgsmål er om borgerens muligheder for at kontrollere brugen af persondata retligt er tilstrækkeligt sikret. Det kan konstateres, at loven muliggør behandling af persondata på grundlag af et samtykke, men at et sådant samtykke kun i få tilfælde er obligatorisk. Det er vanskeligt at vurdere adgangen til samtykke, fordi et samtykke på den ene side er udtryk for selvbestemmelsesret, men på den anden side kan prisgive de svage borgere. På denne baggrund bør en samtykkeret ikke stå alene, idet staten fortsat må have en pligt til at sikre borgernes privacy.

Alt i alt er den retlige analyses konklusion, at den retlige opgave består i at sikre, at pervasive computing bliver en realitet på en måde, der fortsat sikrer beskyttelsen af privacy. Persondataloven er et egnet instrument hertil, men det vil være nødvendigt løbende at opdatere den praktiske udfyldning af lovens regler, således at disse er realistiske i den teknologiserede virkelighed.

6 Analyse af it-sikkerhedsproblemer

Som nævnt indledningsvist tager analysen af sikkerhedsaspekterne omkring anvendelse af pervasive computing udgangspunkt i de scenarier, som er skitseret i afsnit 4. For scenarierne vil potentielle sikkerhedstrusler blive beskrevet, og mulige metoder til beskyttelse mod nogle af disse vil blive skitseret.

En traditionel sikkerhedsanalyse har til formål at identificere trusler og prioritere dem på baggrund af den risiko de udgør. En sådan risikovurdering kan fx tage udgangspunkt i to dimensioner: 1) hvor alvorlige konsekvenser vil en realisering af en given trussel have; og 2) hvor ofte skønnes realisering af truslen at forekomme. Jo alvorligere og jo oftere, jo større siges risikoen at være. Sådanne vurderinger vil ofte være kraftigt afhængige af den anvendte teknologi samt empiriske studier, og da denne rapport undersøger fremtidige teknologier og forestillede anvendelser, er disse input ikke tilgængelige. Derfor vil risikovurdering blive baseret på ekstrapoleringer fra aktuelle it-anvendelser og på vurderinger af hvor svær realiseringen af en given trussel vurderes at være.

Vurderingen af mulige trusler vil blive foretaget med baggrund i eksisterende metoder til analyse af it-sikkerhed i organisationer og konkrete it-systemer. Som beskrevet i Octave[17] kan en trussel karakteriseres ved

- Den værdi som trues (fx personlige oplysninger)
- Adgangen til værdien (fysisk eller logisk)
- Den aktør, som truer værdien
- Aktørens motiv
- Udfaldet af truslen (som kan være kompromittering af integritet, fortrolighed eller tilgængelighed)

Det vil være for omstændeligt her at karakterisere hver enkelt trussel i overensstemmelse med disse karakteristika, men de vil blive anvendt som ledetråd i vurderingen af scenarierne. Den følgende beskrivelse fokuserer på udfaldet af de identificerede trusler, da dette giver den mest homogene præsentation. I afsnit 6.4 gives en oversigt over de identificerede trusler.

Én type aktør fortjener dog særlig opmærksomhed, nemlig den almindelige bruger, fordi trusler af denne oprindelse ikke fremtræder tydeligt i de beskrevne scenarier. Brugere, som ikke opfører sig fornuftigt i forhold til it-sikkerheden, kan få en ellers velgennemtænkt sikkerhedspolitik til at bryde sammen[18]. Uhensigtsmæssig brugeradfærd er således en gennemgående trussel. Sikring mod denne trussel sker på traditionel vis, nemlig gennem træning af brugere og udvikling af systemer med god brugbarhed.

6.1 Analyse af id-i-alting

Id-i-alting-cases omfatter primært kommunikation af en sekvens af bits (id-kode), som identificerer en enhed, såsom en mobiltelefon eller et rfid-tag. Hvis denne enhed er tæt knyttet til en person (fx indopereret, eller en mobiltelefon, som man altid har på sig), vil id-koden også fungere som

[17] [Octave].

[18] Et godt eksempel er historien fra [Bardram] om hvorledes personale på et dansk hospital fandt det for besværligt med personligt login hver gang de skulle registrere data i it-systemet, og som konsekvens loggede en medarbejder ind på alle maskiner hver morgen, hvorefter alle frit havde adgang til systemet. Dette gør arbejdet meget lettere for personalet, men umuliggør meningsfyldt logning på baggrund af hver enkelt bruger, hvilket ellers er et krav på danske hospitaler [Sundhedsstyrelsen].

personlig identifikation[19]. Hvis enheden er løsere tilknyttet en person (fx i tilfældet med liftkort), er id-koden ikke nødvendigvis en personlig identifikation, men tjener til at identificere personen i en givet sammenhæng (her anvendelsen af skilifter).

Det overskyggende sikkerhedsproblem inden for denne type af pervasive computing har derfor rod i problemer relateret til identifikation. Det mest diskuterede sikkerhedsproblem i denne forbindelse har hidtil været relateret til privacy, idet det åbenlyst er et spørgsmål, hvorvidt man kan sikre at personlig information forbliver privat, samtidig med at brugen af disse enheder (se afsnit 4.1) bliver mere og mere udbredt. Andre relevante problemer er relateret til integritet og tilgængelighed.

6.1.1 Trusler mod fortrolighed i id-i-alting

I forbindelse med id-i-alting er truslerne mod fortrolighed alle forbundet med privacy. I den retlige analyse i bilag 2 er det lagt til grund, at den gældende lovgivning, når der ses bort fra at adgangen til samtykke kan udgøre en vis risiko, kan håndtere disse spørgsmål, idet der dog er behov for en regulering i forhold til overvågning af ikke-identificerbare personer. Uanset denne konstatering foreligger der fra et teknisk perspektiv en potentiel trussel mod privacy, og denne beskrives nærmere i det følgende.

Systemer, som benytter id-koder til at afbilde fysiske objekter ind i det virtuelle rum, kan fx fungere på følgende måde: hvert objekt får en id-kode, og der vedligeholdes en database med oversigt over hvilke objekter der har hvilke id-koder. Når en læser (med en bestemt geografisk placering) "ser" en id-kode, kan systemet på denne baggrund konkludere, at det objekt med den sete id-kode er i nærheden af læseren. Rfid fungerer på denne måde. Udover database med afbildningen fra id-koder til fysiske objekter er det naturligvis muligt for systemet at opbygge en database over registrerede observationer af en given id-kode.

Med udgangspunkt heri er der tre typer af trusler mod privacy: aflæsning af id-koder, misbrug af eksisterende databaser med registrerede id-koder og endeligt en kombination af de to førstnævnte.

Da id-koder oftest sendes trådløst, vil det være muligt ubemærket at opsnappe disse, idet en modtager ofte let kan skjules. Umiddelbart er denne trussel mere alvorlig jo større afstand id-koder kan opsnappes fra, idet angriberens muligheder hermed øges. Eksempelvis udsender en GSM-telefon i dag en id-kode, som kan aflæses på flere kilometers afstand, en bærbar computer som er sat op til trådløs kommunikation udsender en entydig adresse (når den opdager et trådløst netværk), som også kan opsnappes over stor afstand, mens et lille (passivt) rfid-tag ofte kræver, at læseren af id-koden er relativt tæt på tag'et (mindre end en meter). En angriber, som ønsker at opsnappe id-koden fra et rfid-tag skal altså umiddelbart være placeret tæt ved tag'et.

Andre aspekter end den fysiske teknologi er dog også relevante for, hvor stor afstand en id-kode kan læses fra. Tages igen rfid-tag som eksempel bemærkes, at visse protokoller[20] til læsning af koden fra et sådan tag virker på den måde, at læseren udsender et kendt præfix af koden, hvorefter tag'et afsender næste bit[21]. Denne proces gentages til hele koden er læst (denne metode gør det muligt at skelne koder fra mange tags, som samtidig reagerer på læseren). Helt konkret betyder

[19] Biometrisk identifikation, der blot består af en biometrisk karakteristik ved en person omdannet til en sekvens af bits, er et andet eksempel på personlig identifikation.
[20] Fx EPC – Electronic Product Code [EPC].
[21] Se [AutoID].

dette, at det vil være muligt at aflæse tag'ets identitetskode ud fra de signaler, som læseren sender. Senderen udsender normalt sine signaler med væsentligt større styrke end tag'et, og ikke sjældent kan disse læses på stor afstand (op til 100 m).

Overordnet er aflæsning af id-koder således muligt ud fra et rent teknisk perspektiv, men det kræver naturligvis, at en angriber er i besiddelse af en læser, som er i en vis nærhed af den enhed, der skal aflæses. Der kan her skelnes mellem angribere, som målrettet opsætter læsere for at registrere enheder i et givet område, og læsere der er opsat med et legitimt formål, og som læser og registrerer enheder, som ellers ikke er relevante for dette formål. Som eksempel på sidstnævnte kan nævnes access points til trådløse netværk, som registrerer hvilke pc'er, der bevæger sig gennem netværkets område, selvom disse pc'er ikke ønsker at bruge netværket, eller tilsvarende rfid-læsere i butikker, som aflæser tags på alle varer, inklusiv varer købt andre steder. Selvom man må forvente, at legitime læsere ikke umiddelbart bliver misbrugt, er det centralt for vurderingen af denne trussel, at de meget let kan blive misbrugt.

Evnen til at aflæse id-koden fra fx en mobiltelefon eller et rfid-tag fortæller som udgangspunkt *intet* om den enhed eller bruger, denne id-kode er knyttet til. Hertil kræves sædvanligvis adgang til den database, som knytter id-kode sammen med enhed og/eller bruger. Således giver ovenstående eksempler altså ikke informationer om hvad en bruger fx har købt i andre butikker, men det giver dog mulighed for eksempelvis at følge en vare, og dermed en (anonym) brugers færden i fx et storcenter.

Det bemærkes, at muligheden for overvågning ikke er ny eller speciel for pervasive computing. Det har også tidligere været muligt ved hjælp af fx videoovervågning, men med id-i-alting bliver det meget let at automatisere indsamlingen og behandlingen af disse oplysninger. Som det fremgår af ovenstående, er den øgede udbredelse af it-udstyr, som kommunikerer trådløst, samt det faktum at udstyret relativt let kan bringes til at udsende en entydig id-kode, med til at gøre det nemmere at spore bæreren af udstyret. I og med at id-koder allerede er givet på elektronisk form, og hver enkelt person får mere og mere udstyr indeholdende it, øges muligheden for at lave en præcis sporing af bæreren. En forudsætning for en sådan sporing er dog, at man aflæser og analysere id-koder. Der skal altså vedligeholdes databaser med id-koder og den kontekst, hvori de er aflæst.

Dette leder til næste trussel, som er misbrug af databaser, der indeholder id-koder som er personhenførbare, enten direkte eller indirekte via sammenkædning af informationer. Sådanne analyser er udbredte til fx at finde svindel med kreditkort og identificere forbrugsmønstre[22], og på samme måde er det let at forestille sig værdien af analyser af bl.a. forbrugsmønstre på baggrund af informationer fra brug af rfid i detailhandlen. I forbindelse med angreb på databaser er det vigtigt at forstå, at en angriber skal have adgang til databasen og derfor ofte vil være en insider. Truslen mod privacy i forbindelse med sporing kommer derfor i høj grad fra de organisationer, og deres ansatte, som kontrollerer disse databaser. Til sammenligning med den mere direkte og håndgribelige trussel om brud på anonymitet ved fx aflæsning af hvad en person på gaden har i sin indkøbspose er denne trussel mindre åbenbar, fordi den baseres på analyse af en mængde opsamlede data, hvor hver enkelt tilfælde af aflæsning kan virke uskyldig.

Den sidste trussel er kombinationen af aflæsning af id-koder og (mis)brug af databaser. Fx kan man kikke på anvendelsen af rfid-tags til tyverisikring. Købes en vare med et rfid-tag på i en butik, vil en

[22] Se fx [CreditCardFraud].

anden butik, som også benytter rfid, kunne aflæse hvad man har i tasken. Det nye her er altså at udover at kunne følge en given id-kode haves adgang til databasen, som knytter denne id-kode til mere interessante data. Afhængigt af hvilket datamateriale der er til rådighed, vil den anden butik have en ide om hvilke varer man kunne være interesseret i, måske hvem man er eller endda hvad man tidligere har købt i forskellige butikker. Angreb mod privacy af denne type vil generelt være mere komplekse end angreb som blot analyser en enkelt database, både fordi det kræver (online) adgang til de relevante databaser, og fordi angrebet formodentlig vil involvere flere organisationer, som enten skal arbejde sammen, eller også skal en organisation opnå uautoriseret adgang til en anden organisations database.

6.1.2 Trusler mod integritet i id-i-alting

Angreb mod integriteten af en identifikationsmekanisme vil ofte have karakter af forsøg på at lave en falsk identifikation. De nævnte scenarier giver en række motiver til at gøre dette. Her nævnes blot to:

- I eksemplet fra Mexico, hvor rfid-tags indopereres i forbindelse med adgangskontrol til fortrolige dokumenter, kan en person være interesseret i at udgive sig for en anden person for netop at opnå adgang til visse dokumenter.
- Hvis et rfid-tag benyttes til at identificere en vare i forbindelse med betaling for varen, kan en (uærlig) kunde (som har fysisk kontrol over tag'et) være interesseret i at varen bliver identificeret som en væsentlig billigere vare.

I alle scenarierne foregår identifikation ved transmission af en konstant id-kode. Som nævnt ovenfor i forbindelse med behandling af fortrolighed kan denne kode let opsnappes, hvorefter det er let at overtage denne identifikation. Hvis enheden bruges til at identificere en person, kan man nu udgive sig for at være vedkommende ("identify theft").

Så længe der er en (økonomisk) gevinst ved sådanne angreb, vil truslen være reel. Der findes talrige eksempler på dette, såsom den første generation af mobiltelefoner, hvor man ved hjælp af en simpel radiomodtager kunne opsnappe telefonens id og så kopiere denne til en anden telefon.

Det skal understreges, at langt fra alle former for identifikation er så usikre som de her beskrevne. Dette behandles nærmere i afsnit 6.1.5.

6.1.3 Trusler mod tilgængelighed i id-i-alting

Herudover kan tre typer trusler mod tilgængelighed identificeres. Dels trusler som har til formål at forhindre en enhed i at udsende sin id-kode, dels trusler som har til formål at hindre det system i at fungere, som modtager og anvender id-koder. Endeligt kan tilgængelighed hindres ved strømsvigt, dvs. at en enhed løber tør for batteri.

Førstnævnte vil være en yderst relevant trussel i indkøbsscenariet, idet en uærlig kunde kan tænkes at kunne undgå betaling for en vare ved et fuldt automatiseret kasseapparat[23], såfremt varens rfid-tag hindres i at udsende sin id-kode. Igen afhænger muligheden for dette af dels den anvendte kommunikationsteknologi, dels af de anvendte logiske protokoller. Rent praktisk kan et sådant angreb foregå ved at afskærme tag'et (varen), så det ikke kan svare på modtagerens signaler (fx ved at lægge varen i en pose foret med et passende skærmende materiale). I andre systemer opereres

[23] Hvis der ikke er tale om et fuld automatiseret kasseapparat, findes truslen naturligvis stadig, men situationen er da ikke anderledes end i butikker i dag.

med mulighed for at slå et tag fra (bl.a. for at begrænse truslen mod privacy). Dette skaber en risiko for, at en kunde kan slå tag'et fra inden varen er købt.

Trusler mod tilgængelighed af de systemer, som anvender id-koderne, vil ofte have karakter af denial-of-service-angreb, hvor modtager-systemet oversvømmes med flere koder, end det kan håndtere. Et sådan angreb kan naturligvis have store konsekvenser for eksempelvis forretninger, der baserer betaling på id-koder fra rfid-tags, eller virksomheder, hvis infrastruktur er baseret på trådløse netværk. Denne form for angreb er teknisk mere krævende end det førstnævnte, men Blocker-tag'et (se nedenfor) er et eksempel på teknologisk hjælpemiddel, der kan overstrømme en læser.

Begge disse typer trusler virker meget sandsynlige i forbindelse med detailhandlen, simpelthen fordi butikstyveri er et udbredt fænomen.

Den sidste type trussel mod tilgængelighed, det at løbe tør for batteri, kunne fx realiseres med et angreb som Stajano[24] kalder "sleep deprevation torture", som dybest set går ud på at sende signaler til en enhed som denne forventes at svare på, hvorved den med tiden vil løbe tør for batteri. I dagligdags applikationer synes denne form for angreb dog ikke særligt realistisk, på nær i det tilfælde som omhandler alarmer (fx til beskyttelse mod tyveri), hvor det åbenlyst kunne være i en tyvs interesse.

Trusler mod tilgængelighed er hardware- og softwarefejl, som også findes i id-i-alting, behandles i forbindelse med analysen af services-i-alting i afsnit 6.2.3 og 6.2.6.

6.1.4 Sikring af fortrolighed i id-i-alting

Ovenstående analyse af trusler mod fortrolighed – dvs. privacy – i forbindelse med id-i-alting arbejder med en række implicitte antagelser, fx at rfid er ensbetydende med entydig identifikation, og dermed at fx rfid-taggede varer i detailhandlen tildeles et unikt id, som følger varen gennem hele dens "liv", det vil specielt også sige efter at den har forladt butikken. Som tidligere nævnt er der ingen a priori grund til, at identifikationsløsninger fordrer systemer som bruger entydig identifikation. Dette gælder ikke bare rfid men også andre identifikationsteknologier som fx WiFi og mobiltelefoner. Vi vil diskutere dette nærmere nedenfor.

Et system til identifikation kan karakteriseres ved følgende 4 egenskaber:

- Brug af databaser – indeholder enheden en id-kode som via en database kobles med logisk information (som beskrevet i afsnit 6.1.1) eller haves den logiske information også på enheden (inkluderende hvis den eneste information er id-koden). Rfid som beskrevet her er af den første type.
- Entydig identifikation eller kontekstafhængig genkendelse – har enheden en fast entydig id-kode, eller kan den fx have flere forskellige id-koder til brug i forskellige sammenhænge.
- Autorisation til læsning af id-kode – skal en anden enhed, fx en rfid-læser, godkendes af enheden før enheden afgiver sin id-kode eller afgives id-koden til alle der beder om den.
- Brugerkontrol – er brugeren involveret i at afgøre hvem der får hvilke informationer fra enheden.

[24] [Stajano].

Rfid, fx EPC, benytter entydig identifikation, ingen autorisation og som udgangspunkt ingen kontrol. I denne situation findes der tekniske såvel som ikke-tekniske mekanismer til beskyttelse af privacy. Den retlige analyse i afsnit 5 angiver en række ikke-tekniske midler, som kan tages i brug. Disse inkluderer åbenhed, samtykke og klare definitioner af hvem der er dataansvarlig for fx en given database med id-koder. Der er tale om en retlig regulering med det formål at beskytte mod de i afsnit 6.1.1 beskrevne trusler. Sådanne ikke-tekniske løsninger baseres på retlig regulering i form af lovgivning og/eller frivillige aftaler. I bilag 3 gives et oplæg til netop sådan en frivillig aftale i form af et forslag til et kodeks for benyttelse af fx rfid-teknologien i detailhandlen.

Fastholdes de teknologiske antagelser, er den primære tekniske metode til sikring at de involverede databaser er forsvarligt beskyttede, hvilket understreger behovet for klarhed af den dataansvarlige, som det også nævnes i den retlige analyse i afsnit 5.

Der findes flere måder, hvorpå man giver brugeren kontrol over aflæsning af id-koder. Grundlæggende er det de i afsnit 6.1.3 beskrevne trusler mod tilgængelighed (det vil altså sige, at disse trusler i denne sammenhæng pudsigt nok kan anskues som sikringsmekanismer!). En mobiltelefon kan eksempelvis hindres i at udsende sin id-kode, hvis man slukker for den. Denne mulighed eksisterer ikke for rfid-tags, men for disse er fx Kill-mode[25] og Blocker-tags[26] foreslået. Generelt har disse løsninger den begrænsning, at de reducerer funktionaliteten, fx er en slukket mobiltelefon mindre anvendelig i forhold til den tænkte anvendelse.

Som det også er nævnt i afsnit 5, er kontrol over egne data – i en eller anden form – generelt ønskeligt. Dette kan enten være i form af kontrol over hvilke data en enhed afgiver i en given situation eller kontrol over allerede opsamlede data, fx kontrol over hvilke data en given forretning gemmer og/eller videregiver om en persons indløb.

I tilfælde, hvor fx rfid-tags benyttes til at mærke en vare, har butikken kontrollen over tag'et så længe varen ikke er solgt. Når først varen er solgt, kan køberen være interesseret i at slå rfid-tag'et fra, så andre fx ikke ved at læse tag'et kan se, hvilke varer, køberen har i indkøbsposen. Senere kunne køberen dog være interesseret i at slå tag'et til igen (fx hvis ens fryser via dette tag kan holde styr på indholdet i fryseren). Det afgørende her er altså, at køberen før køb af varen ikke må være i stand til at få kontrol over varens rfid-tag, men efter købet vil han være interesseret i at have den fulde kontrol. I forbindelse med rfid kunne man også forestille sig, at det efter køb af en vare bliver muligt for brugeren at opnå fuld kontrol over den id-kode, som enheden udsender. Specielt omfatter dette muligheden for selv at bestemme id-kode, dvs. fx muligheden for at give en enhed en ny id-kode for derved at fjerne muligheden for at samkøre data om en persons private enheder med fx data fra de forretninger, som sælger enhederne[27]. Dette kan principielt gøres med enheder med lille it-kapacitet, men dette er ikke muligt med almindelige rfid-tags, og som nævnt ovenfor kræves metoder til håndtering og overdragelse af kontrollen over enheden[28].

Betragtes enheder, som har større it-kapacitet, fx mere avancerede rfid-tags, smart cards (og dermed mobiltelefoner) mv., vil det være muligt at sikre, at enheder kun afleverer deres id til andre enheder,

[25] Kill-mode tillader, at et rfid tag kan slukkes ved at sende en bestemt "kill-kode" til tag'et. Når først dette er gjort, kan tag'et ikke genoplives.
[26] Et Blocker-tag (se [Blocker]) udsender mange forskellige id-koder på en gang og forvirrer derved rfid-læseren, så der blokeres for læsning af koden i andre tags.
[27] Se fx [Engberg].
[28] Anderson og Stajanos "Ressurecting Duckling" beskrevet i [Stajano] er et forslag til løsningen heraf.

som er godkendt på forhånd, fx vha. kryptografi. Dette forhindrer at fremmede systemer kan følge enheden, men forhindrer ikke tracking vha. autorisede enheder. Det skal her også bemærkes, at en række enheder og protokoller som fx BlueTooth og GSM som faktisk understøtter kryptografi alligevel fortæller deres id-kode til alle som beder om den. Anvendelsen af kryptografi er altså ikke i sig selv en garanti for at data som id-koder beskyttes.

Samlet er den primære metode til sikring af privacy ved brugen af global identifikation at regulere brugen af – herunder beskytte – databaser som indeholder id-koder og tilknyttet data, samt styre hvilke enheder der er autoriseret til at læse en id-kode. Derudover findes visse tiltag som teknisk forhindrer aflæsning, men fælles er at de umiddelbart virker besværlige for den almindelige bruger.

Som nævnt ovenfor er der ingen a priori grund til at bruge entydig identifikation. Dette kan undgås ved enten helt at gemme id-koden vha. kryptografi[29] som beskrevet nedenfor eller ved at bruge løsninger, hvor id-koderne skiftes ud (automatisk eller under brugerkontrol) undervejs i enheds livscyklus.

Der findes tekniske løsninger, som sikrer anonymitet, samtidig med at egenskaber som fx uafviselighed kan opretholdes. Fx findes løsninger til anonym håndtering af rettigheder, hvor anonymiteten kun er givet så længe man ikke forsøger at snyde, i hvilket fald brugerens identitet afsløres, således at han kan stilles til regnskab[30]. Anvendelse af sådanne teknikker kræver imidlertid, at den underliggende teknologi understøtter avancerede kryptografiske mekanismer, hvilket kan være en teknologisk udfordring. I øvrigt vil anonymitet i praktiske løsninger formodentligt også ofte blive fravalgt, fordi behovet for anonymiteten ikke står mål med prisen.

Den grundlæggende ide i denne form for sikring af privacy er at reducere værdien af id-koder gemt i databaser. Dette leder os til den mulighed, der eksisterer for at bruge løsninger, som ikke benytter en database, fx i visse netværksprotokoller, hvor en enhed blot meddeler en adresse (en id-kode) som bruges til at sende den svaret i den aktuelle kommunikation; et eksempel er MAC-koder, som er omtalt i forbindelse med WiFi. I denne sammenhæng skal det bemærkes, at blot fordi en database ikke er en del af infrastrukturen, betyder det ikke, at man ikke kan opbygge en database over aflæste id-koder og dermed haves stadig trusler mod sporing.

Der findes således flere gode ideer til hvorledes man kan sikre privacy på teknisk vis, og det er et område, som der forskes meget i. Fælles er at disse løsninger kræver mere; både af enhed og bruger pga. den øgede tekniske kompleksitet. På den anden side ændrer disse løsninger ikke ved den grundlæggende funktionalitet som tilbydes, dvs. de cases og scenarier der er beskrevne i afsnit 4.1 kan realiseres uden at brugen ændres væsentligt. I tilfældet med fx brugen af rfid i detailhandlen og lignende vil det dog kræve billige rfid-tags, som kan lave de krævede beregninger (ellers bliver disse løsninger for dyre), og det vil kræve, at løsningen designes således at den nemt kan bruges af den almindelige forbruger.

6.1.5 Sikring af integritet i id-i-alting

I denne forbindelse er det primære mål at opnå sikker identifikation af enheder. De beskrevne trusler i afsnit 6.1.2 er reelt alle en form for spoofing, fx i form af identity theft.

[29] En teknisk faldgrube er her, at den krypterede værdi som udsendes skal være forskellig fra gang til gang, ellers vil den krypterede id-kode for alle praktiske formål fungere som selve id-koden.
[30] Se fx [Chaum].

Tager vi igen udgangspunkt i rfid-teknologien så giver denne – i form af de billige og udbredte passive tags – meget dårlig sikkerhed. For mange af de beskrevne anvendelser kan man dog argumentere for, at sikkerheden alligevel er passende *til formålet*. Enten fordi sikkerhedskravene ikke er så høje (hvem kunne finde på at spoofe en liter mælk i køleskabet?), eller fordi rfid kan anvendes i sammenhæng med andre teknologier: i eksemplet med indopererede rfid-tags kunne man fx forestille sig en kombination med fysisk adgangskontrol, hvor besiddelsen af rfid-tag'et kun er et af flere identifikationselementer; efter aflæsning kunne id-koden benyttes til automatisk at hente et billede frem på en vagts skærm, hvorved værdien af at spoofe et tag reduceres til nær nul.

En lang række andre identifikationsteknologier som fx BlueTooth og WiFi beskyldes for at være usikre. I realiteten må de dog nok vurderes at være blandt de bedste bud på sikker identifikation i praksis. En udtalt styrke ved disse protokoller er, at de er standardiserede og udbredte, og det er netop derfor, at de er under kraftig beskydning. Dette er præcist styrken, under den centrale forudsætning at de identificerede svagheder i disse standarder til stadighed adresseres, fordi eventuelle svagheder så kan findes og rettes. Benyttes en ikke-standard-protokol vil der være en risiko for, at denne har svagheder som ikke kommer til offentlighedens kendskab. Et godt eksempel på dette er GSM, hvor der benyttes en proprietær protokol, som har vist sig at have adskillige væsentlige svagheder[31].

6.1.6 Sikring af tilgængelighed i id-i-alting

Tilgængelighed er som oftest det sværeste at sikre sig imod. Denial-of-service-angreb i form af fx jamming af en rfid-læser kan være svære at forhindre med udelukkende tekniske løsninger. En typisk løsning vil være at identificere et angreb, når det finder sted – og gerne hvorfra – og så stoppe angrebet derefter. Misbrug af de Blocker-tags (beskrevet ovenfor) af butikstyve illustrerer problemet. Som nævnt i afsnit 6.1.3 udsender Blocker-tags en række koder. Læseren kan dog nemt opdage dette, idet der også udsendes koder, som ikke relevante eller gyldige (fx koder for varer som ikke føres i butikken).

Sikring af batterilevetid er et centralt element i konstruktionen af enheder, og derfor må det antages, at de mest almindelige problemer er eller bliver imødegået per automatik. En interessant løsning er naturligvis passive rfid-tags, som slet ikke har batteri. Til gengæld kan sådanne enheder kun stille meget begrænset funktionalitet til rådighed.

6.2 Analyse af services-i-alting

6.2.1 Trusler mod fortrolighed i services-i-alting

De identificerede trusler mod fortrolighed i de tre services-i-alting-scenarier falder i to grupper: trusler mod privacy og trusler mod fortrolighed af data, som kommunikeres eller opbevares.

Ligesom i id-i-alting er identifikation af enheder et meget væsentligt element. Enheder skal ikke blot sende en id-kode til en læser, men skal fx også identificeres som hørende til en bestemt person og agere i forskellige netværk. Dette er tilfældet i ESN-scenariet, hvor servicepersonens enhed indgår i et netværk med en række enheder i den bygning, han servicerer. Dette giver anledning til en række privacy-relaterede trusler i forhold til overvågning af hvor han er hvornår. Det skal dog bemærkes, at der er tale om overvågning i forbindelse med udførelsen af et job, hvorfor der kan

[31] Beskrevet i [Anderson].

være grunde til at overvågningen faktisk er ønskelig. En anden situation hvor overvågning kan være ønskelig er i Healtcare for tomorrow-scenariet, hvor en diabetespatient overvåges, hvis bestemte betingelser er opfyldte – fx overvåges det hvorvidt hun, inden for 10 minutter efter at hendes blodsukker er blevet for lavt, har taget insulin fra køleskabet. Desuden har specielt healthcare-scenarierne den forskel, at den database som de følsomme overvågningsdata gemmes i ofte vil være placeret i patientens hjem. Derved reduceres risikoen for insiderangreb drastisk.

Samlet giver services-i-alting ligesom id-i-alting anledning til en række privacy-relaterede trusler. I visse af de tænkte anvendelser virker det dog, som om den reelle trussel er mindre, bl.a. i de tilfælde hvor den følsomme database så at sige er under den overvågedes egen kontrol.

Udover trusler relateret til privacy møder vi i services-i-alting et krav om beskyttelse af fortrolig information. Dette er specielt udpræget i forbindelse med "healthcare"-scenarier, hvor patienten typisk ikke er interesseret i at helbredsinformation kan læses af andre end de relevante læger og sygeplejersker. De udvalgte scenarier fokuserer på hjemmepleje, men problematikken er ikke mindre relevant på hospitaler og lignende (eksempelvis i forbindelse med elektroniske patientjournaler). For hospitaler findes specifikke sikkerhedskrav, som bl.a. angiver hvilke data der skal holdes fortrolige[32]. Disse regler stammer delvist fra mere generelle sikkerhedsregler for behandlingen af følsomme persondata[33]. Der er altså ikke alene en trussel mod fortrolighed af data som kommunikeres og opbevares i disse scenarier; i en række tilfælde er der udstukket regler som specifikt stiller krav om at denne trussel imødegås.

Truslerne mod fortrolighed i denne gruppe af scenarier omfatter således trusler mod privacy (som i id-i-alting), mod fortrolighed af data, der kommunikeres (internt i hjemmet og eksternt mellem gateway og et centralt system) samt mod fortrolighed af data i forbindelse med lagring og brug.

6.2.2 Trusler mod integritet i services-i-alting

Scenarierne peger på tre typer af trusler: modifikation af data i forbindelse med kommunikation, uautoriseret adgang og afvisning af indgåede aftaler.

Integritet af datakommunikation er essentiel i alle scenarierne inden for services-i-alting, og i forbindelse hermed er det som regel også vigtigt at være sikre på oprindelsen af data. Eksempelvis ønsker lægen at sikre sig, at helbredsinformationer kommer fra den rigtige patient, og at det faktisk er præcist de målte data som når frem fra sensor til læge. I modsat fald kan man forestille sig, at patienten fejlbehandles. Tilsvarende problemstillinger mødes i ESN-scenariet, hvor der downloades information om de bygninger, som skal vedligeholdes. Alvoren af disse trusler er stor, ikke nødvendigvis fordi chancen for at data faktisk modificeres er stor, men fordi konsekvenserne er uacceptable fx i form af fejlbehandling. Det skal her bemærkes, at truslen mod integritet af data enten kan være rettet mod kommunikationen fra sensor til gateway (herunder introduktion af falske sensorer) eller kommunikationen fra gateway til central.

I eu-Domain-scenarierne benyttes identifikation af en enhed (person, som besidder enheden) til at få adgang til information og bygninger (servicemanden kan få adgang til de bygninger, som skal vedligeholdes, og sygeplejersken kan få adgang til patienten, hvis der er indløbet alarmer). En trussel mod sikkerheden (integriteten) af identifikationsprotokollen vil altså kunne medføre

[32] Se [Sundhedsstyrelsen].
[33] Se [Datatilsynet].

uautoriseret fysisk adgang. Generelt benyttes identifikationen i disse scenarier også til at skaffe sig adgang til netværk, til information eller til bygninger, idet denne adgang er forbeholdt bestemte personer i de refererede scenarier. Der er således trusler om både fysisk og logisk uautoriseret adgang. Igen må denne trussel behandles meget alvorligt for at løsningerne bliver accepteret. Eksempelvis er det på den ene side vigtigt for patientens tryghed, at sygeplejersken kan komme ind, hvis det bliver nødvendigt, men på den anden side ønsker patienten naturligvis ikke, at systemet giver andre adgang.

Allerede i dag er uautoriseret logisk adgang til lukkede systemer et kendt problem. En populær teknik blandt indbrudstyve har været at benytte fjernbetjeninger til dyrt tv- og hifi-udstyr til at finde ud af hvorvidt et givent hus vil være "profitabelt" at bryde ind i. Indbrudstyven forsøger ved hjælp af sin egen fjernbetjening at afgøre, om der er "ønskede" apparater i hjemmet. Hvis apparaterne ikke er slukket ordentligt, vil de reagere på fjernbetjeningen (fx spille høj musik), og indbrudstyven kan således uden at komme ind i hjemmet afgøre om der er det udstyr han er ude efter.

Den sidste trusseltype er afvisning af indgåede aftaler, som fx ses i ESN-scenariet hvor der indgås aftaler med underleverandører. Almindeligvis ønskes det at sådanne aftaler er uafviselige, dvs. at servicemanden ikke skal kunne indgå bindende aftaler om en reservedel med to forskellige leverandører for at være sikker på at få reservedelen, for dernæst at løbe fra den aftale som leveres sidst. Sikkerhedsproblematikken relateret til dette er også central for scenarier af typen agenter-i-alting og vil blive diskuteret yderligere i den forbindelse.

6.2.3 Trusler mod tilgængelighed i services-i-alting

I alle tre scenarier er tilgængelighed essentiel for at systemerne kan bruges i praksis. Truslerne falder i tre grupper, hvoraf to vedrører fejl og to vedrører muligheden for at afvikle "fremmed" software, nemlig: hardwarefejl, softwarefejl og ondsindet software.

I "healthcare"-scenarierne er det naturligvis ikke acceptabelt, hvis en patient ikke kan behandles, fordi en enhed fejler, hvad enten dette skyldes en hardware- eller softwarefejl. Ligeledes, men måske mindre alvorligt (det drejer sig trods alt ikke om menneskeliv), forholder det sig i ESN-scenariet, hvor det er uacceptabelt, at en bygning er uden varme eller elektricitet i nogle dage, fordi systemet ikke virker ordentligt.

Problemet omkring fejlbehæftet software forværres af ønsket om at kunne downloade ny software til en enhed, enten automatisk eller manuelt (se både ESN- og EPCiR-scenarierne). Dette er allerede et kendt sikkerhedsproblem i forbindelse med applikationer, som hentes over internettet, og det øger naturligvis truslen mod tilgængelighed af de enheder, som anvendes i services-i-alting-scenarierne.

Muligheden for at installere ændret eller mere software åbner også vejen for at ondsindet software "ved egen kraft" – vira, orme osv. – kan trænge ind i systemerne. Dette er et af de mest udbredte problemer i "pc-verdenen", og trenden er netop at mange små enheder begynder at benytte operativsystemer efter samme grundideer som fx pc'er, og derfor er der ingen grund til at tro andet end at vira mv. også vil blive et stort problem inden for pervasive computing. Der er da også allerede rapporteret om de første vira på mobiltelefoner[34].

[34] Se [MobilVira].

6.2.4 Sikring af fortrolighed i services-i-alting

Sikring af privacy for services-i-alting byder ikke på noget nyt i forhold til id-i-alting som diskuteret ovenfor. Behovene for sikring kan variere afhængigt af hvor alvorlige man anser truslerne for at være, men de sikringsmekanismer som er til rådighed er principielt de samme.

Fortrolighed af opbevarede data sikres som udgangspunkt ved hjælp af kryptering, samt ved hjælp af adgangskontrol som styrer hvilke brugere har adgang til hvilke data. I forbindelse med adgangskontrol er identifikation af brugere, som nævnt i forbindelse med trusler mod integritet i afsnit 6.2.2 vigtig, idet overtagelse af andres identitet i en given situation kan give vedkommende uautoriseret adgang og derved kompromittere fortroligheden. Adgangskontrol omtales nærmere nedenfor under sikring af integritet (afsnit 6.2.5).

Adgangskontrol adresserer dog ikke det aspekt, som vedrører kommunikation af data over "åbne" netværk[35] eller blot placering af data på en enhed som er let tilgængelig, fx en PDA eller en bærbar pc. Her benyttes kryptografi til at sikre fortrolighed. I lukkede systemer, som er kendetegnende for services-i-alting, vil det ofte være muligt at sætte den kryptografiske infrastruktur, der tillader kommunikation af krypterede data, op i forbindelse med den aftaleindgåelse, som ligger til grund for det lukkede system. Det skal her understreges, at sikre løsninger bør hvile på anerkendte standarder for anvendelsen af kryptografi, som fx RSA og AES – herunder standarder for infrastrukturen.

Et åbent problem i forbindelse med pervasive computing er hvorvidt det faktum, at mange enheder har begrænset it-kapacitet, gør at traditionelle kryptografiske algoritmer ikke længere kan benyttes, simpelthen fordi de fx tager for lang tid eller bruger for megen hukommelse. Der findes dog eksempler på løsninger som bruger RSA til services-i-alting-lignende scenarier[36], og hvor dette ikke rækker, kunne man overveje at bruge andre kryptosystemer som er mere performance-"venlige", såsom public-key[37]-løsninger baseret på såkaldte elliptiske kurver (som allerede er standardiseret) i stedet for RSA som er det mest udbredte i dag. Endeligt skal det bemærkes, at brugen af gateways, dvs. løsninger hvor man har en central enhed med stor it-kapacitet, kan lette arbejdet, idet de kryptografiske algoritmer i visse tilfælde kan tilpasses således at de tungeste beregninger laves her.

Kommunikationen fra en lille enhed (fx en sensor i en bandage) til en gateway vil desuden i en række tilfælde formodentlig ikke kræve så høj grad af kryptografisk sikkerhed, såfremt denne kommunikation ikke kan aflyttes uden for hjemmet. Såfremt dette ikke kan sikres (afhængig af teknologien), kræves naturligvis yderligere sikkerhed, hvilket grundet beregningsmæssige begrænsninger i sensoren, kan blive en udfordring.

Fortrolighed af data skal således sikres på traditionel vis. Den primære udfordring, som fremgår her, er at få små enheder med begrænset it-kapacitet til at kryptere data. Løsningen på dette afhænger i sidste ende af en cost-benefit afvejning, idet sådanne enheder ofte er relativt dyre (i forhold til tilsvarende enheder, som ikke understøtter kryptografi). Derudover er der udfordringer i forbindelse med de for kryptografi nødvendige infrastrukturer til udveksling og håndtering af kryptografiske nøgler samt adgangskontrol, som omtalt nedenfor under sikring af integritet. Der er dog ingen

[35] Som for eksempel WiFi og andre former for trådløs kommunikation, men også kommunikation over internettet i bred forstand.
[36] Se [MicrosoftResearch].
[37] Public-key kryptografi er den form for kryptografi, som ligger bag digitale signaturer, og er den form for kryptografi som kræver mest it-kapacitet. RSA er den mest udbredte type public-key kryptografi.

principielle hindringer for anvendelsen af kryptografi til at sikre fortrolighed (eller integritet – se nedenfor) i forbindelse med services-i-alting.

6.2.5 Sikring af integritet i services-i-alting

Integriteten af data, som kommunikeres i forbindelse med disse scenarier, kan i de fleste tilfælde sikres med traditionelle teknikker. Dette gælder for eksempel data, som sendes fra en central gateway i en bygning til en central server (eller en anden gateway), idet de involverede enheder her vil have tilstrækkelig regnekraft til at understøtte standardiserede kryptografiske metoder. Derudover gør ovenstående bemærkninger om kryptografi på enheder med lille it-kapacitet sig naturligvis også gældende her.

Den anden centrale trussel mod integritet i disse scenarier retter sig mod adgangskontrol (fysisk adgang tilbygninger og logisk adgang til it-systemer og data). Sikringen af dette omfatter, som nævnt i afsnit 6.2.4, sikker identifikation af brugeren samt et sikkert system til autorisation af brugere, som ønsker adgang. Udover de tre traditionelle elementer: noget man ved (fx password), noget man har (fx et token med digital signatur) og noget man er (biometri), vil adgangskontrol i forbindelse med pervasive computing i visse tilfælde trække på et fjerde element, hvor man er – dvs. ens fysiske geografiske placering (dette skal oplagt også betragtes ud fra et privacy perspektiv, idet der implicit i sådanne løsninger er involveret sporing).

Den sidste type af trusler er rettet mod uafviselighed aftaler, dvs. at aftaler er bindende. Systemer, som sikrer uafviselighed, kan fx bestå af en digital signatur sammen med et sæt regler for brugen af den digitale signatur, dvs. hvorledes aftaler skal håndteres elektronisk for at være bindende. I de tilfælde, hvor aftalerne indgås af deltagere i et lukket netværk – hvilket er tilfældet i de tre services-i-alting-scenarier, vil regelsættet ofte være fastlagt i forbindelse med oprettelsen af netværket. I situationer, hvor aftaler ikke indgås inden for et lukket netværk, vil fastlæggelsen af et sådant regelsæt være mere besværligt, som vi skal se i afsnit 6.3.5. Endeligt skal det bemærkes, at digitale signaturer baserer sig på public-key kryptografi, hvorfor de ovenfor nævnte problemer omkring enhedernes begrænsede it-kapacitet også gør sig gældende her. Samlet virker det dog ikke urealistisk at få både kryptografi og aftaler på plads i forbindelse med services-i-alting-scenarierne, fordi der er tale om lukkede systemer, hvor der ofte er en central enhed med større it-kapacitet til rådighed.

6.2.6 Sikring af tilgængelighed i services-i-alting

De beskrevne trusler mod tilgængeligheden kan umiddelbart adresseres med to mekanismer: sikkerhed for at hardware og software er korrekt, fx gennem certificering, og brugen af sikre operativsystemer.

Det vil formodentligt altid være tilfældet, at brugen af pervasive computing vil presse teknikken til det yderste, hvorfor det til stadighed vil være rimeligt at forestille sig anvendelsen af enheder med specialiseret software. Disse enheder bør – afhængigt af anvendelsen – være certificeret på en eller anden vis, så brugeren kan have en vis sikkerhed for korrekt opførsel. Det forventes at sådan certificering kan finde sted på baggrund af eksisterende metoder som fx the Common Criteria[38].

En sådan certificering kan dog hurtigt blive værdiløs, hvis det er muligt at ændre (dele af) den software, som afvikles på enheden. Til dette formål findes der efterhånden flere “sikre”

[38] [CommonCriteria].

operativsystemer, som afvikler fremmede programmer i stærkt kontrollerede omgivelser og benytter fx digital signatur til at sikre oprindelsen af programmerne. Dette vil reducere risikoen for de enheder, som har it-kapacitet nok til at anvende sådanne operativsystemer. I visse tilfælde kan det være nødvendigt at begrænse muligheden for installation af fremmede programmer for at eliminere denne trussel.

6.3 Analyse af agenter-i-alting

Værdier og trusler i disse scenarier er overordnet set dækket af analyserne af id- og services-i-alting. I relation til de løsninger, som kan anvendes i disse scenarier, rejser der sig nu en række nye problemer som følge af det endnu større antal enheder, åbenheden af systemerne og brugen af intelligente agenter som autonomt udfører handlinger på vegne af deres "ejere".

I scenariet Maria – road warrior beskrives det, hvorledes Marias armbånd automatisk identificerer hende i forbindelse med hvad der kan sammenlignes med gammeldags paskontrol. Sikkerheden af denne autentifikation beror implicit på, at armbåndet (og det system som armbåndet taler med) er overbevist om, at det faktisk er Maria som besidder armbåndet (brugerautentifikation), og at Maria *ønsker* (kontrol) at identificeres af systemet (i det konkrete tilfælde synes dette åbenbart, men generelt er det ikke nødvendigvis tilfældet).

6.3.1 Trusler mod fortrolighed i agenter-i-alting

Den øgede mængde af interaktion mellem agenter vil i sig selv give anledning til en række trusler mod fortrolighed af personlige data, og kontrollen med dette vil i høj grad påhvile agenterne. Dette omfatter lagring, kommunikation og behandling af disse data i agenten. Baseret på agenter-i-alting scenarierne kan det forventes, at disse agenter vil kontrollere, herunder behandle og kommunikere, en stor mængde personlig data (såsom medicinsk data), hvorfor sikring af dette ville blive vigtig for brugerens accept af sådanne systemer.

Med hensyn til privacy har vi nu at gøre med anvendelser, hvor brugerne benytter enheder som afgiver id-koder til "fremmede" systemer. En umiddelbar vurdering er, at dette øger risikoen ved registrering af disse id-koder i databaser, bl.a. fordi der ikke nødvendigvis vil være en entydig retlig regulering heraf på tværs af landegrænser.

6.3.2 Trusler mod integritet i agenter-i-alting

Udover tidligere nævnte trusler retter de primære problemer relateret til integritet sig mod uafviselighed og en form for uautoriseret adgang. Sidstnævnte er måske ikke så meget en trussel som et problem, der skyldes behovet for interaktion med fremmede agenter, enheder og brugere.

I scenarierne indgås en række aftaler fx i forbindelse med kørelejlighed og køb af varer. Disse er bindende – dvs. uafviselige – i den forstand, at de efterfølgende giver anledning til betaling. Såfremt disse aftaler alligevel ikke kan bruges til at inddrage skyldige betalinger, vil anvendelsen i disse scenarier falde til jorden. Dette er relateret til det allerede eksisterende problem vedr. den retlige gyldighed af digitale signaturer. Det bemærkes, at der her er den yderligere udfordring, at hvor en digital signatur i dag typisk genereres på baggrund af brugerens eksplicitte accept (fx i browser eller email-program) vil en agent i disse scenarier på baggrund af sin konfiguration mere eller mindre selvstændigt kunne lave en sådan på vegne af sin ejer.

Som det fremgår af ovenstående beskrivelse, involverer agenter-i-alting konstant identifikation og typisk overfor "fremmede" enheder, dvs. enheder man dybest set ikke ved om man kan stole på. Det

er allerede i dag et stort problem for forældres tryghed ved deres børns brug af internettet, at det er det muligt for fremmede at kontakte børnene elektronisk. Hvis børn udstyres med agenter, der er opsøgende i samme grad som i eksemplet med Carmen, hvor hendes agent selv sørger for at finde kørelejlighed, er der en stor risiko for "uautoriseret adgang", dvs. at den fremmede enhed får adgang til flere informationer, fx navn og adresse, end vi ønsker. For at imødegå den hermed følgende utryghed er det vigtigt, at agenter kan konfigureres og kontrolleres, så ikke blot børn, men alle kun er i kontakt med agenter tilhørende personer, som man ønsker at have kontakt med. Dette kan dog synes i modstrid med ideerne bag agenter-i-alting, hvor vi netop ønsker at interagere – elektronisk – med fremmede eller deres agenter. Problemet er dybest set hvordan og hvor meget vi kan stole på personer, enheder og agenter, vi måske aldrig har mødt før.

6.3.3 Trusler mod tilgængelighed i agenter-i-alting

Truslerne mod tilgængelighed er uændrede i forhold til id- og services-i-alting. Den store forskel er, at teknologien forestilles udbredt i meget større skala. Derfor vil det enkelte individs daglige liv formodentlig også blive langt mere afhængig af teknologien, og problemer med tilgængelighed kan få større konsekvenser.

6.3.4 Sikring af fortrolighed i agenter-i-alting

Som nævnt ovenfor bringer disse scenarier intet væsentligt nyt på banen. Det skal dog bemærkes, at fx personlige agenter kan antages at have tilstrækkeligt regnekraft til at kryptere data med traditionelle, stærke krypteringsmetoder, fordi den kapacitet som kræves for at kunne afvikle en sofistikeret agent vil være langt større end hvad der kræves af kryptografi. Det er derfor muligt at sikre personlig data med brug af avancerede kryptografiske metoder.

Ligeledes kan det også forventes at være muligt at implementere gode identifikationsprotokoller (i hvert fald på enheder som afvikler agenter), der ikke umiddelbart afslører ejerens identitet, men måske blot et pseudonym eller, mere generelt, at ejeren har de privilegier som kræves i en given situation (hvorvidt sådanne løsninger kan bruges, afhænger dog også af om en sådan anonym adgang overhovedet kan tillades). Givet den øgede risiko mod netop privacy, som beskrevet ovenfor, virker det fornuftigt, at der kunne gøres en ekstra teknisk indsats.

6.3.5 Sikring af integritet i agenter-i-alting

Som nævnt i afsnit 6.3.2 omfatter sikring af integritet understøttelse af uafviselige aftaler samt kontrol over hvilke fremmede agenter, man ønsker at "indlede et forhold til".

Ønsker man at benytte de mest udbredte kryptografiske infrastrukturer til håndtering af uafviselige aftaler, kræver disse scenarier internationalt samarbejde, fx en international digital signatur. Dette har været på manges ønskeliste i de sidste 10-15 år, men er endnu langt fra en realitet, og det er et spørgsmål, om en sådan global infrastruktur kan etableres. For at understøtte de angivne scenarier skal alle agenter certificeres. Hertil skal tilføjes certifikater til andre (relevante) enheder på global plan, hvor certifikater og de tilhørende kryptografiske teknikker ønskes anvendt. Udstedelse af certifikater, som anvendes helt transparent af diverse enheder, sker allerede i dag i forbindelse med produktion af chips til disse enheder (eksempelvis betalingskort og chips til pc'er med indbyggede nøgler). Dette er således teknisk muligt, men skal op i en større skala for at understøtte disse scenarier. Udover det rent praktiske med at udstede certifikater må der som et minimumskrav benyttes bedre løsninger til revokering af certifikater – spærrelister som de bruges i dag er ikke anvendelige, fordi de simpelthen bliver for store. Generelt må man sige, at teknologien til dette i store træk eksisterer i dag, men den er slet ikke implementeret i tilstrækkelig grad.

Selvom fx digitale signatur-løsninger skalerer, findes der stadig problemer. Ideen ved et digital signatur-system er, at man tillægger tillid til udsagn om, hvem der ejer en given kryptografisk nøgle på baggrund af, at en CA "siger god" for denne binding mellem individ/enhed og nøgle[39]. Det springende punkt er her, at man via sin tillid til CA tillægger CA's udsagn, dvs. certifikater, tillid. Spørgsmålet er hvorvidt en almindelig dansk bruger uden større it-indsigt vil have tillid til fx en national japansk CA eller måske en CA drevet af en privat person (fx til certificering af personens egne enheder)?

Derudover er der en yderligere komplikation, som præcist vedrører problemet omkring tillid eller uautoriseret adgang. Som nævnt tidligere består adgangskontrol af identifikation og autorisation. Under antagelsen af at en fremmed enhed er sikkert identificeret, hvilke privilegier skal vi da tilskrive den? Dvs. selvom vi med sikkerhed har fastslået en enheds, agents eller persons identitet, stoler vi så på vedkommende? Ønsker vi fx at indgå aftaler som involverer penge? Generelt er tillid i litteraturen omtalt som et af de fundamentale forskningsproblemer inden for sikkerhed og pervasive computing, og der foregår en række forskningsaktiviteter på dette område bl.a. SECURE-projektet[40] med dansk deltagelse.

6.3.6 Sikring af tilgængelighed i agenter-i-alting

Her er intet nyt at tilføje i forhold til analyserne af id- og services-i-alting.

6.4 Oversigt over mulige tekniske sikkerhedsproblemer

Sammenfattende har ovenstående analyse anvist en række potentielle sikkerhedsproblemer relateret til brugen af pervasive computing. På mange områder adskiller disse sig ikke væsentligt sig fra kendte problemstillinger vedrørende brugen af it. Den store forskel fra dagens it-løsninger ligger dels i anvendelsen af enheder med meget begrænset regnekraft, dels i den forventede store udbredelse.

Nedenstående tabel giver en oversigt over de trusler, som er blevet identificeret i foregående afsnit. Det bemærkes, at trusler i id-i-alting-scenarierne også findes i services-i-alting, ligesom trusler i disse scenarier også findes i agenter-i-alting. I nedenstående tabel er kun angivet den første type af scenarie, hvor disse trusler er beskrevet ovenfor.
Nedenstående tabel skal naturligvis ikke forstås således, at trusler beskrevet ved fx services-i-alting-scenarier ikke kan forekomme i id-i-alting, men den afspejler en overordnet tendens i mulige trusler mod pervasive computing.

Udfald	**Beskrivelse**	**Type af scenarie**
Kompromittering af fortrolighed	Sporing eller identifikation af person i forbindelse med registrering af id-kode	Id-i-alting
	Misbrug af database indeholdende registrerede id-koder	Id-i-alting

[39] Den danske offentlige digitale signatur, [DigitalSignatur], er et godt eksempel på en sådan infrastruktur, og der findes en række udbredte infrastrukturer og anerkendte kryptografiske standarder, som måske kan anvendes direkte. TDC har rollen som CA i den danske digitale signatur.
[40] Se [Secure].

	Kompromittering af data anvendt i systemet (fx personlige data)	Services-i-alting
Kompromittering af integritet	Forfalskning af id-kode (overtagelse af identitet)	Id-i-alting
	Uautoriseret adgang (fysisk eller logisk)	Services-i-alting
	Modifikation af data anvendt i systemet (fx personlige data)	Services-i-alting
	Bindende aftaler i *lukket* system	Services-i-alting
	Bindende aftaler i *åbent* system	Agenter-i-alting
	Tillid til fremmede agenter (og deres ejere)	Agenter-i-alting
Kompromittering af tilgængelighed	Strømsvigt	Id-i-alting
	Forhindre enhed i at udsende id-kode	Id-i-alting
	Denial-of-service angreb mod læser	Id-i-alting
	HW-fejl	Services-i-alting
	SW-fejl	Services-i-alting
	Installation (download) af usikkert sw	Services-i-alting
	Virusangreb mod enheder	Services-i-alting

7 Diskussion og anbefalinger

Baseret på ovenstående identifikation af trusler og mulige løsninger diskuteres i dette afsnit de mest væsentlige it-sikkerhedsmæssige udfordringer. Vi vil opdele diskussion efter et tidsperspektiv, da en række problemer har forskellig karakter på kort hhv. lang sigt. Dette skyldes både at forventninger til og den konkrete viden om den anvendte teknologi er meget forskellig, samt at en række løsninger som ikke er realiserbare på kort sigt kan være det på længere sigt.

7.1 Kortsigtet perspektiv

Baseret på den retlige analyse samt analysen af id-i-alting samt services-i-alting vurderes de væsentlige kortsigtede problemer at være:

- Privacy
- Den praktiske anvendelse af mekanismer som sikrer traditionel fortrolighed
- Brugbarhed

I analysen er også omtalt problemer i forbindelse med integritet, primært i form af sikker identifikation, og tilgængelighed. Nedenfor i afsnit 7.1.4 diskuteres hvorfor disse problemer anses for mindre væsentlige.

7.1.1 Privacy

Både den tekniske og den retlige analyse peger på privacy som et problem i forbindelse med pervasive computing. Hovedkonklusionen på dette område er, at udfordringen består i at sikre, at pervasive computing realiseres på en måde som sikrer privatlivets fred. Anvendelser af fx rfid er ud fra en teknisk anskuelse sårbare (se afsnit 6.1), men persondataloven kan håndtere disse sårbarheder, givet at den praktiske udfyldning af loven løbende opdateres (se afsnit 5).

De problemstillinger, som vedrører privacy, altså anonymitet og sporing, er ikke nye for pervasive computing. Det nye er derimod skalaen og dermed formodentlig også den økonomiske gevinst ved at udføre sådanne handlinger. Samtidig kan frygten hos forbrugeren virke hæmmende for udbredelsen af pervasive computing og derved potentielt reducere en stor samfundsmæssig gevinst. Det mest aktuelle eksempel på disse problemer er anvendelsen af rfid, specielt i detailhandlen, hvor den af forbrugeren opfattede risiko er stor. Hvor stor den reelle risiko for fremtidige brud på privatlivets fred er, vil i vist omgang afhænge af, at der fastsættes klare retlige regler, da truslen for et retlig og evt. økonomisk efterspil kan fungere som modvægt til de motiver, der nu måtte være for sådanne brud. Det skal dog bemærkes, at risikoen for opdagelse kan være lille, i hvilket tilfælde den samlede risiko for straf naturligvis mindskes tilsvarende.

Udover fastsættelse af regler kan privacy-problematikken også adresseres fra et teknisk perspektiv, ved at benytte løsninger som i mindre grad – eller slet ikke – muliggør fx sporing (se afsnit 6.1.4). I tilfældet med rfid vil dette dog kræve helt nye løsninger baseret på rfid-tags med øget funktionalitet, som derved også må forventes at være dyrere. På kort sigt er det bedste bud på en løsning derfor at basere sig på solide, forståelige og bredt accepterede regler og aftaler til at styre brugen af pervasive computing. Et konkret initiativ på denne front kunne være definitionen af en branchekodeks for anvendelsen af rfid i detailhandlen.

Det anbefales, at der udformes en branchekodeks for brugen af rfid i detailhandlen.

Et oplæg til en sådan kodeks er givet i bilag 3.

Hvorvidt sådanne regler i praksis er nok til at skabe den fornødne tryghed hos den almindelige bruger er uvist, og derfor bør forskellige tekniske løsningsmuligheders praktiske relevans løbende overvejes. Spørgsmålet er dog hvorvidt kendte tekniske løsninger på kort sigt finder kommerciel anvendelse, og derfor bør det overvejes at iværksætte initiativer, som kan fremme anvendelsen af løsninger som teknisk fjerner eller reducerer truslen mod privacy. Mere herom i afsnit 7.1.5.

Det understreges at truslen mod privacy ikke er begrænset til brugen af rfid i detailhandlen. De gælder inden for andre sektorer som fx sundhedssektoren[41], og ligeledes for andre teknologier som mobiltelefoner og gammeldags kreditkort. Brugen af rfid i detailhandlen er dog speciel, fordi den skala hvori teknologien anvendes er meget større end hidtil set.

Bemærk at sporing ikke nødvendigvis er et onde. I nogle anvendelser, fx på en række arbejdspladser, kan det meget vel vise sig at personalet gerne benytter fx location tracking, idet det letter deres arbejde, ligesom tracking af patienter kan føre til hurtigere hjælp. Den samme teknologi giver således anledning til forskellige trusler og risici ved forskellige anvendelser.

7.1.2 Fortrolighed

Et andet relateret problem er, jf. afsnit 6.2.1 og 6.1.4, fortroligheden af følsomme persondata. Ifølge Datatilsynet[42] skal følsomme persondata, fx helbredsdata, som transmitteres over et åbent net eller på et flytbart medie (fx en PDA eller en laptop) være stærkt krypterede[43]. Dette krav er også eksplicit i sundhedsstyrelsens it-sikkerhedspolitik for sygehuse[44]. Det er dog formodentlig ikke altid udbredt praksis at følge disse regler, bl.a. fordi det ofte besværliggør adgangen til data.

Når enheder med meget få beregningsressourcer, som fx en trådløs blodtryksmåler, begynder at transmittere følsomme persondata i form af måledata, så skal disse som udgangspunkt også behandles på samme måde. Her er problemet ikke nødvendigvis manglen på vilje til at følge reglerne, som det blotte faktum at enheden måske ikke er i stand til at udføre stærk kryptering (dette er dog ofte et spørgsmål om økonomi og ikke teknik, jf. afsnit 6.2.4). Et andet problem kan være at standardopsætningen ikke benytter det nødvendige sikkerhedsniveau. BlueTooth[45] sikrer fx fortrolighed ved hjælp af en nøgle på mellem 8 og 128 bit – her skal altså vælges den maksimale sikkerhed før følsomme persondata må transmitteres, hvilket også kræver at enhederne faktisk understøtter denne nøglestørrelse.

Der er således spænding mellem reglerne for fortrolig kommunikation af følsomme personhenførbare data og praksis for dette, både hvad angår brugen og hvad angår det teknisk mulige. Af bilag 2 fremgår det, at valg af teknologi ikke påvirker de retlige krav til sikkerhed, men er det realistisk at kræve, at følsomme personhenførbare data som transmitteres trådløst fra en

---

41 Se fx [Anderson].
42 Se [Datatilsynet].
43 Datatilsynet skriver i [StærkKryptering] at dette betyder mindst 128-bit nøgler for symmetrisk kryptering.
44 Se [Sundhedsstyrelsen].
45 BlueTooth-enheder er begyndt at blive godkendt i USA (af FDA) til brug i sundhedssektoren [FdaApproval]

meget lille enhed med kort rækkevidde skal være stærkt krypterede? For at undgå misforståelser omkring hvor og hvornår der stilles krav om brug af stærk kryptering på enheder med lille it-kapacitet, bør disse krav klargøres.

Det anbefales at skabe klarhed omkring behovet for stærk kryptering af følsomme persondata i forbindelse med anvendelsen af pervasive computing.

Som det fremgår ovenfor er denne anbefaling specielt relevant for trådløs kommunikation fra enheder med kort rækkevidde.

7.1.3 Brugbarhed

Det sidste problem er brugbarhed. Den centrale pointe her er, at hvis ikke brugerne anvender systemet som tiltænkt, så er der stor risiko for at hele it-sikkerhedspolitikken falder sammen som et korthus.

Afsnit 7.1.1 nævner problemet med brugbare metoder til kontrol af enheder, som udsender id-koder, men efterhånden som flere og flere daglige gøremål efterhånden bliver elektronificeret ved udbredelsen af pervasive computing, øges vigtigheden af, at bruger og system "forstår" hinanden. Dette betyder, at it-sikkerhedsrelaterede mekanismer som fx brugerautentifikation og håndtering af certifikater i en række anvendelser skal gøres bedre.

Det er ikke oplagt hvordan dette problem bedst kan håndteres, men det står klart at forståelsen mellem system og bruger kan bedres ved at brugerne dygtiggøres. Her tænkes ikke bare på at deres it-færdigheder i traditionel forstand forbedres, men på at den almindelige brugers operationelle forståelse af it-sikkerhedsrelaterede problemer, som fx det at vælge et fornuftigt password og det at man ikke fortæller sit password til fremmede, øges.

7.1.4 Mindre problemer

Ud fra vores analyse ovenfor kan det synes påfaldende, at specielt to problemer ignoreres her:

- Sikker identifikation, dvs. trusler mod integritet
- Tilgængelighed, herunder vira mv.

Sikker identifikation kan, hvis man skal måle størrelsen af problemerne ud fra medieomtale, synes at være et væsentligt it-sikkerhedsproblem i forbindelse med pervasive computing. En række udbredte protokoller som fx WiFi og BlueTooth har fået tilsyneladende drøje hug, men til mange praktiske formål giver disse protokoller en rimelig sikkerhed. Dette skyldes bl.a. at disse protokoller som oftest forbedres, når svagheder identificeres. Netop dette er et vægtigt argument for at benytte disse protokoller til sikker identifikation.

Et andet argument er, at sikker identifikation i mange situationer vil være en forudsætning for den kommercielle udbredelse af pervasive computing løsninger, specielt i forbindelse med services-i-alting, og derfor er det rimeligt at tro, at sikker identifikation automatisk sættes højt på listen når disse systemer udvikles.

I øvrigt viser erfaringen, at problemer relateret til identifikation af brugere ofte skyldes andet end angreb på de kryptografiske protokoller. Eksempelvis har mange fået uautoriseret adgang til it-systemer ved at lokke password ud af brugere (også kaldet "social engineering"), og mange banker

verden over står i dag over for sikkerhedsproblemer grundet “phishing”, hvor man lokker bankkunden til et vellignende men falsk site, og her får lokket kodeord eller lignende ud af kunden. Disse problemer er vigtige, men betragtes her som en del af brugbarhedsproblematikken (se ovenfor).

Det er et anerkendt princip inden for it-sikkerhed, at man bør benytte gennemafprøvede sikkerhedsmetoder (det vil fx sige anerkendte kryptografiske algoritmer og protokoller). Dette gælder ikke bare til sikker identifikation, men også til at sikre integritet i bredere forstand og naturligvis til at sikre fortrolighed.

Det anbefales, at der benyttes anerkendte protokoller til sikker kommunikation.
Der kunne fra officiel side vedligeholdes en liste over anbefalede sikkerhedsmekanismer til pervasive computing.

De identificerede trusler mod tilgængelighed, fx vira, batterilevetid og forhindring af et rfid-tag i at udsende sin id-kode, vurderes også som mindre væsentlige i forhold til denne rapport. Grunden hertil er den simple, at problemerne ikke er særegne for pervasive computing, og de skal formodentlig løses med standardteknikker kendt fra fx pc-verdenen. Vira muliggøres eksempelvis - i forbindelse med pervasive computing - i høj grad af at små enheder begynder at benytte samme typer af operativsystemer som pc'er, og derfor synes det også oplagt at der kan benyttes de samme metoder til sikring. Ligeledes for skærmning af rfid-tags, fx brugt til tyverisikring, hvor den bedste løsning synes at være, at man holder øje med at dette ikke sker; det er principielt ikke anderledes end almindeligt butikstyveri.

7.1.5 Generel anbefaling

Ser vi bort fra de retlige mekanismer beskrevet ovenfor, har gode pervasive computing-løsninger ud fra et sikkerhedsperspektiv en række ønskelige tekniske egenskaber:

- Beskyttelse af privacy, herunder minimal eller ingen registrering af personhenførbare data
- Brug af standard sikkerhedsmekanismer
- Eventuel understøttelse af krav om anvendelse af stærk kryptografi
- God brugbarhed

En anbefaling, som er blevet overvejet, vedrører en sikkerhedsdeklaration for enheder og systemer inden for pervasive computing. En sådan deklaration kunne fx angive hvilke mekanismer der benyttes til sikker identifikation, iagttagen af evt. regler om beskyttelse af følsomme og persondata og oplysninger relateret til privacy (fx hvilke data et system registrerer eller i hvilket omfang en enhed “frivilligt” afgiver id-koder). Umiddelbart synes det dog svært at kvantificere dette på en god måde (fx kan der være stor uenighed om hvorvidt en given protokol faktisk giver sikker identifikation).

Et helt andet perspektiv på hvorledes disse ønskelige egenskaber kan formidles er ved at vise deres værd i praksis. Som løftestang for anvendelsen af pervasive computing-teknologier, som fx rfid, kunne det være interessant med en national indsats for at demonstrere, at disse egenskaber kan realiseres i en kommerciel løsning, herunder specielt at de umiddelbare sårbarheder som er

identificeret i afsnit 6.1 kan imødegås med tekniske virkemidler. Et sådant rfid-projekt kunne fokusere på et område inden for detailhandlen eller lignende offentlige områder, fx biblioteker[46].

Det anbefales at igangsætte et projekt, som demonstrerer anvendelsen af rfid inden for detailhandlen eller lignende område, på en måde så privatlivets fred er sikret med tekniske virkemidler.

Et første skridt i et sådant projekt bør være en nærmere definition af de ønskelige sikkerhedsmæssige krav[47] og konkrete ideer til deres realisering[48]. Herunder er det naturligvis vigtigt med en økonomisk vurdering for at sikre at projektet er relevant.

7.2 Langsigtet perspektiv

I et langsigtet perspektiv vurderes de væsentlige nye problemer at være:

- Integritet, specifikt
  - Indgåelse af uafviselige aftaler
  - Tillid
- Privacy
- Brugbarhed

7.2.1 Indgåelse af uafviselige aftaler

Når agenter indgår aftaler, som skal være uafviselige, rejser der sig en række praktiske problemer. Allerede i forhold til den "almindelige" danske digitale signatur er der uklarheder omkring den juridiske gyldighed. Det er oplagt, at problematikken kun forværres af at agenter nu skal kunne indgå aftaler på vegne af brugere. På den anden side er Danmark blandt de førende nationer inden for anvendelsen af digital signatur, og det synes derfor oplagt at undersøge problemet nærmere.

Det anbefales at undersøge i hvilket omfang det retligt er muligt at lade agenter indgå gyldige aftaler på vegne af deres ejer.

Det kan virke urealistisk at agenter overhovedet skulle kunne gøre dette, men det er et centralt element i agenter-i-alting. Det virker derfor rimeligt at få afstemt forestillingerne om fremtidens anvendelse af pervasive computing med de krav, som juraen stiller til teknologien, hvis den skal anvendes i praksis.

En mulig konklusion er at brugeren altid skal involveres i den endelige aftaleindgåelse, men en sådan konklusion stiller spørgsmålstegn ved værdien af agenter – i hvert fald som de er beskrevet i agenter-i-alting.

[46] Faktisk afventer Biblioteksstyrelsen at anbefale brugen af rfid, bl.a. pga. privacy-bekymringer [Biblioteksstyrelsen].
[47] Disse krav kunne inkludere, at en bogs tag fx kun kan aflæses af bibliotek og låner, men ikke af andre lånere eller andre rfid-systemer; mere vidtgående skulle biblioteket måske ikke engang kunne aflæse udlånte bøger, så længe de ikke er returneret, selv når de fysisk er på biblioteket. Derudover skal brugerne naturligvis kunne scanne bøgerne hjemme selv.
[48] Det kan forventes, at der bliver behov for mere sofistikerede rfid-tags, som kan udføre visse beregninger.

7.2.2 Tillid

Som tidligere nævnt vil det næppe være realistisk at forvente én global infrastruktur til digitale signaturer eller lignende. Det kan dog forventes, at en række regionale infrastrukturer bliver etableret, og det kan også forventes, at nogle af disse kan kobles sammen. Dette vil i stor udstrækning være tilstrækkeligt til at avancerede kryptografiske teknikker kan sikre kommunikationen mellem forskellige enheder – herunder indgåelse af bindende aftaler.. Etableringen af en sådan infrastruktur vil dog ikke løse det "menneskelige aspekt af problemet": hvorledes man etablerer tillid mellem personer, enheder og agenter som ikke kender hinanden på forhånd. Som nævnt i afsnit 6.3.5 er dette et område der forskes meget indenfor, men endnu er der ikke fundet nogen gylden løsning.

7.2.3 Privacy

I forhold til den kortsigtede diskussion er der her to ting at tilføje. På lang sigt kan det selvsagt forventes, at pervasive computing bliver mere udbredt end på kort sigt, hvilket i sig selv kan give anledning til en eskalering af problemerne. Omvendt kan det også forventes, at teknologien er mere udviklet: der er fx så småt rfid-tags på vej som kan lave kryptografi, og på lang sigt er det generelt forventeligt, at selv meget små enheder vil kunne udføre beregninger som kan medvirke til at sikre privacy. Dette vil måske gøre det lettere at realisere nogle af de allerede kendte tekniske løsninger (se afsnit 6.1.4).

Som allerede nævnt bør det løbende overvejes hvilke tekniske løsninger til sikring af privacy, der er praktisk anvendelige. Anvendelsen af mere teknisk orienterede løsninger til sikring af privacy vil altid være en afvejning mellem forskellige forhold, bl.a. hvad teknologien kan og hvad den koster. En sådan forståelse kunne fx sikres ved, at der blev udpeget en ekspertgruppe med det ansvar at følge udviklingen inden for tekniske metoder til sikring af privacy.

Det anbefales, at der nedsættes en ekspertgruppe til at følge udviklingen inden for tekniske metoder til sikring af privacy.

En første opgave for denne ekspertgruppe kunne være at medvirke til fastlæggelse af kravene til det i afsnit 7.1.5 beskrevne projekt.

Det påpeges, at blot fordi tekniske løsninger til sikring af privacy eksisterer, vil de ikke nødvendigvis blive anvendt, medmindre de parter som investerer i løsningen kan se en forretningsmæssig fordel i den[49] - eller der lovgives. Det kan således ikke afvises, at det vil være nødvendigt med offentlige tiltag for at skubbe disse løsninger i gang, fx i form af projekter som det beskrevet i afsnit 7.1.5.

7.2.4 Brugbarhed

I forlængelse af den kortsigtede diskussion kan det tilføjes, at det på lang sigt formodentlig er både mere realistisk og mere nødvendigt at gøre noget ved brugbarhedsproblematikken, pga. den større udbredelse.

[49] Der findes således adskillige systemer til anonym betaling, men disse har aldrig slået an.

Som nævnt ovenfor kan brugbarheden forbedres ved at brugerens forståelse for systemet øges. Det modsatte perspektiv er naturligvis, at systemets forståelse for brugeren øges, dvs. at systemet konstrueres så det passer naturligt i den tænkte anvendelse[50]. Dette er en udfordring ift. en række tekniske løsninger, bl.a. løsninger som er tiltænkt at give brugeren øget kontrol over fx id-koden på et rfid-tag. En lang række af sådanne løsninger lider af den svaghed, at de typisk pålægger brugeren en byrde i form af nøglehåndtering, idet de baserer sig på forskellige former for kryptografi. Det er ofte således, at teknisk smarte løsninger kræver teknisk "smarte" brugere, og når teknologien er allemandseje vil dette ikke være tilfældet.

Udvikling af sikkerhedsløsninger med god brugbarhed kan udover viden om brugbarhed baseres på viden om sofistikeret teknisk sikkerhed (fx kryptografi). Danmark har stærke traditioner både inden for teknisk sikkerhed og inden for udvikling af it med god brugbarhed. Det virker som en oplagt mulighed at forsøge at kombinere disse forskningsområder for at adressere nogen af de her nævnte problemer.

Det anbefales at satse på dansk forskning og udvikling som integrerer brugbarhed og teknisk sikkerhed.

[50] Jakob Nielsen argumenterer for denne tilgang frem for uddannelse af brugere [Nielsen].

8 Bilag

Til rapporten knytter sig følgende bilag.

- Bilag 1: Referencer
- Bilag 2: Detaljeret retlig analyse
- Bilag 3: Forslag til branchekodeks
- Bilag 4: Scenarier

Bilagene findes på Rådet for it-sikkerheds hjemmeside www.rfits.dk

Udarbejdelse af rapporten

Denne rapport er udarbejdet af Alexandra Instituttets Center for it-sikkerhed i samarbejde med Peter Blume, professor dr. jur., Københavns Universitet.

For Alexandra Instituttets Center for it-sikkerhed har følgende deltaget i projektgruppen:

- Michael Østergaard Pedersen, ph.d.-studerende ved Aarhus Universitet
- Jakob Illeborg Pagter, adjunkt ved Aarhus Universitet og projektleder ved Alexandra Instituttets Center for it-sikkerhed, samt
- Torben Pryds Pedersen, udviklingschef, Cryptomathic A/S