# Resultatkontrakt

## Basale IKT Infrastrukturer – the Internet og things

14. december 2009

## 1.1 Basale IKT infrastrukturer – the Internet of things

| Skema til beskrivelser af forsknings- og udviklingsaktiviteter | | | |
|---|---|---|---|
| **Aktivitetsområde (navn):** | **Towards the Internet of Things** | **Aktivitetsområde nr.:** | 1 |
| **Sammenfatning** | Denne aktivitet sigter mod at opbygge viden og udvikle værktøjer, som stiller det danske erhvervsliv i stand til bedre at udnytte den gryende trend indenfor IKT infrastruktur der betegnes "Internet of Things" (IoT). Forenkelt kan dette beskrives som at (næsten) alle apparater kommer på internettet.<br>Et væsentligt element henimod realisering af denne vision er den ligeledes forholdsvis nye trend Cloud Computing (CC), som forventes at slå igennem som en af de primære modeller for levering af it-tjenester inden for få år.<br>Vi vil i denne aktivitet have to overordnede foci:<br>Dels helt basale mekanismer, der indgår i den teknologiske realisering fa IoT og CC, herunder CC platforme, offline tilgang, kommunikationsteknologier og –protokoller, samt nye metodikker, algoritmer og patterns for udvikling af løsninger til IoT.<br>Og dels en række sikkerhedsmæssige problemstillinger, som IoT og CC giver anledning til, herunder tilgængelighed, integritet og fortrolighed, og løsninger herfor herunder perimeterløs sikkerhed, secure multiparty computation, secure mashups, og obfuskering.<br>Aktiviteterne vil resultere i nye forskningserkendelser, samt en række nye forskningsbaserede serviceydelser til det danske erhvervsliv, specielt SMV'er.<br>Resultaterne af aktiviteten vil blive formidlet bredt igennem Alexandra Instituttets store SMV kontaktnet, vores forskellige netværk, via nettet, fagpressen og konferencetidsskrifter. Formidlingsaktiviteterne vil bl.a. inkludere etablering af interessegrupper af bl.a. SMV'er, workshops, foredrag, pressemeddelelser, samt både popuplærvidenskabelige og akademiske artikler. | | |
| **Formål og målgruppe** | Formålet med denne aktivitet er at udvikle viden og værktøjer som kan hjælpe danske virksomheders forretningsmæssig udnyttelse af "Internet of Things" (IoT). Dette retter sig både imod virksomheder som er leverandører af IoT-infrastruktur (fx softwareleverandører) og virksomheder der bygger og bruger løsninger baseret på IoT, og teknologier såsom RFID, trådløse sensor systemer, indlejrede systemer, robotter etc.<br>Udvalget af emnerne dækker centrale dele af de IKT emner, der beskrives på www.bedreinnovation.dk, specielt den under: Fremtidens IKT infrastrukturer – the Internet of things.<br>Resultatet af aktiviteten være udbygning af eksisterende viden og udvikling af nye softwareværktøjer med afsæt i Alexandra Instituttets spidskompetencer samt hjemtagning og opbygning af ny viden på områder hvor der ikke pt. er de nødvendige kompetencer i Danmark.<br>"The Internet of Things" (IoT) er et samlende begreb for det fænomen at ordinære objekter (things) som biler, kaffemaskiner og meget andet udstyres med små (og større) computere som er på internettet. Denne udvikling muliggør en lang række af nye innovative løsninger med både erhvervs- og samfundsmæssig nytte[1]. Eksempelvis indenfor området pervasive healthcare hvor der er gode | | |

[1] IoT har også stor politisk bevågenhed i EU. Se f.eks. Internet of Things - An action plan for Europe - http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

| | |
|---|---|
| | muligheder for danske virksomheder til at udvikle innovative løsninger, såvel som store samfundmæssige potentialer.<br>IoT er som begreb nært beslægtet med "Pervasive Computing" PC (eller it-i-alting), men IoT tænkes her som et endnu bredere begreb som særligt inkluderer den infrastruktur som er nødvendig for at gøre mange PC-løsninger kommercielt relevante; en kaffemaskine som er "på nettet" skal tilgås via en tjeneste, og denne tjeneste udbydes typisk via nettet. I denne aktivitet vil der i denne sammenhæng være særligt fokus på den relativt nye trend "Cloud Computing" (CC). CC forventes at slå igennem som en af de primære modeller for levering af it-tjenester inden for få år. Grunden hertil er den enkle at stordriftsfordele muliggør betydelige besparelser på driftsudgifterne[2]. Dette betyder fx at en lille ny virksomhed ikke længere behøver investere i egen hardware, men i stedet kan leje sig ind og derved kun skulle betale for de ressourcer som faktisk bruges (dette er en central fordel ved CC – man betaler kun for de beregningsressourcer man faktisk bruger). Følgelig vil opstarten af en virksomhed ikke længere kræve store initielle investeringer i infrastruktur og CC har dermed potentialet til at accellerere udviklingen imod IoT. Særligt vil CC gøre det muligt for langt flere SMV'er at levere konkurrencedygtige ydelser i en IoT-verden fordi omkostninger og risiko forbundet med udrulning af en ny løsning kan reduceres kraftigt igennem anvendelsen af CC.<br>Denne aktivitet er således ikke bare baseret på at udvikle "kaffemaskiner som er på nettet", men på en holistisk tilgang hvor vi *også* vi fokusere den infrastruktur som er nødvendig.<br>Det store samfunds- og erhvervsmæssige potentiale knyttet til IoT og CC risikerer dog ikke at blive fuldt udnyttet. Dette skyldes at disse løfter om nye forretningsmuligheder og reducerede omkostninger trues af en række problemer, og løsninger på disse problemer er kritiske for at gevinsterne kan høstes. Det er en række af disse udfordringer som denne aktivitet overordnet har fokus på:<br>• Softwarearkitektur og algoritmer for IoT<br>• Sikkerhed i IoT<br>Samlet kan disse problemstillinger adresseres ved en målrettet indsats imod at gentænke, revidere og nyudvikle de grundlæggende IKT-infrastrukturer som danner fundamentet for IoT og herunder CC.<br>Alexandra Instituttet har i denne aktivitet specifikt fokus imod SMV'er og offenlige organisationer inden for følgende områder hvor vi allerede har et stærkt eksisterende erhvervssamarbejde:<br>• Healthcare-løsninger<br>• Home Automation<br>• Industriel IT<br>• Webtjenester<br>• Finanssektoren<br>Indenfor disse forskellige områder vil der blive studeret konkrete cases. Disse cases hjælper med at fokusere arbejdet samtidigt med at de giver et godt afsæt for kommercialiseringen af aktivitetens resultater.<br><br>Dette projekt vil bibringe konkrete teknologisk effekter som følger:<br>• Ny viden – overblik over centrale software og sikkerhedsproblemstillinger relateret til IoT. Dette vil være en kombination af aktiv videnetablering (de projekter Alexandra Instituttet selv er med i) og "passiv" videnetablering (dvs. studier af international state-of-the-art). |

[2] Armbrust et al.: *Above the Clouds*; UC Berkeley 2009; http://radlab.cs.berkeley.edu. Heri dokumenteres fx en effektiviseringsgrad på en *faktor* mellem 5 og 7 ved at skifte fra mellemstore til store datacentre (som er fundamentet for Cloud Computing).

| | |
|---|---|
| | Denne viden vil udmunde i teknologiske serviceydelser i form af rådgivning omkring anvendelse af IoT med fokus på danske virksomheders behov og hvordan disse behov kan adresseres.<br>• Nye værktøjer og demonstratorer– softwareværktøjer og demonstratorer bygget ved hjælp af disse, som med afsæt i Alexandra Instituttets spidskompetencer adresserer specifikke problemer og som går ud over hvad der er national og international state-of-the-art.<br>Disse resultater vil i sig selv udgøre eller igennem produktmodning danne basis for teknologiske serviceydelser som ellers ikke er kommercielt tilgængelige nationalt såvel som internationalt.<br>• Vidensprednning – udbredelse af kendskab til de mange forretningsmuligheder knyttet til IoT, med afsæt i den i projektet etablerede viden og de udviklede værktøjer, men også mere generel oplysning ifht. hvilke typer af løsninger IoT muliggør. |
| **Aktivitetsplanens indhold** | Denne aktivitet har som nævnt fokus på essentielle infrastrukturelle udfordringer i udviklingen imod IoT. Meget groft er disse udfordringer delt op i softwarearkitekturer og –algoritmer samt sikkerhed for IoT. Her gennemgås det faglige indhold af denne aktivitet delt op efter disse to emner, hvorefter aktivitetens udbytte opsummeres og holdes op imod resultatkontraktkravene.<br><br>**Sikkerhed for IOT:** Som beskrevet ovenfor under ”formål og målgruppe” er tillid til it-sikkerheden i mange tilfælde essentielt for at realisere de kommercielle potentialer i IoT. Overordnet handler it-sikkerhed om at sikre tre fundamentale egenskaber ved it-systemer:<br>• Tilgængelighed – at vi har adgang til data når vi ønsker det, fx at vi kan læse vores mail når vi ønsker det.<br>• Integritet – at data er i den forventede tilstand, fx at indholdet af vores mail er uændret ifht. afsendelsestidspunktet.<br>• Fortrolighed – at data ikke er set af uvedkommende, fx at indholdet af en mail med forretningshemmeligheder ikke kan ses af konkurrenter.<br>Den traditionelle tilgang til it-sikkerhed er baseret på at sikre disse egenskaber via det såkaldte *perimeterparadigme*. Den basale ide er at bygge et fysisk og logisk hegn uden om en virksomhed, dennes it-komponenter og data; den såkaldte *perimeter*. Traditionelle komponenter i dette hegn (perimeteren) er fx firewalls og anti-virus. Med dette hegn på plads kan verden anskues i en forsimplet sort/hvid-optik: brugere, enheder og data indenfor perimeteren er ”gode” og dem uden for perimeteren er ”dårlige/onde”. Dette paradigme har været særdeles succesfuldt og danner fundamentet for stort set hele it-sikkerhedsbranchen.<br>Det grundlæggende sikkerhedsproblem ved IoT er at det underminerer perimeterparadigmet og skaber behov for ”perimeterløs” sikkerhed[3]. Mindst tre forskellige teknologiske trends relateret til IoT dokumenterer dette problem:<br>• Pervasive Computing – i pervasive computing er data på enheder som er *overalt* og taler med hinanden på dynamisk vis. Selv forsøg på at ”hegne” simple mobile enheder som laptops ind i ejerorganisationens infrastruktur er problematiske.<br>• Cloud Computing – den grundlæggende ide i CC er at data overdrages til tredjeparter. Dermed er det tredjepartens perimeter og ikke ens egen man skal stole på.<br>• Mutual Computing – både på forbruger- og virksomhedsniveau vil IoT i stort omfang blive knyttet til tjenester hvor personer og organisationer udveksler data. |

[3] Denne udvikling er præcist fundamentet for ”The Jericho Forum” (www.jerichoforum.org), som har en lang række store internationale virksomheder som medlem.

| | |
|---|---|
| | Den grundlæggende hypotese for at konstruere vellykket sikkerhed for IoT er at denne sikkerhed skal baseres på et nyt paradigme *perimeterløs sikkerhed* . Dette vil kunne medvirke til at levere kosteffektiv sikkerhed under hensyntagen til at perimeteren ikke længere findes.<br>På dette overordnede strategiske niveau vil denne aktivitet i første omgang hjemtage, producere og opsamle viden om: 1) fundamentale sikkerhedsproblemer som står i vejen for den forretningsmæssige udnyttelse af IoT, 2) strategier for perimeterløse sikkerhedsløsninger baseret på eksisterende teknologi og baseret på nye sikkerhedsteknologier (særligt de nedenfor nævnte) og 3) dokumentation af forretningsmæssige potentialer som er ubenyttede som følge af sikkerhedsproblemer i relation til IoT. Konkret vil dette munde ud i etablering af en gruppe (et Perimeterfree Security Team – PST) som besidder denne viden og kan levere rådgivningsydelser baseret herpå.<br><br>Aktiviteten vil på det værktøjsorienterede niveau have fokus på at etablere viden om og producere infrastrukturkomponenter som vurderes at have særlig betydning for perimeterløs sikkerhed og som samtidigt udnytter Alexandra Instituttets styrkeposition indenfor sikkerhed for IoT og anvendt kryptografi. Det drejer sig specifikt om<br>• Secure Multiparty Computation (SMC)<br>• Secure Mashups<br>• Obfuskering<br><br>Et grundlæggende problem forbundet med IoT såvel som CC er at man ofte er i den situation at man betror sine data til en fremmed enhed. Det kan være en lokal mobil enhed som har mere processeringskraft eller en fjern server som gemmer ens data eller udfører komplekse beregninger på disse. Dette kan være et stort problem såfremt omtalte data er følsomme (enten forretningsmæssigt eller personligt), hvorfor man ønsker at holde dem fortrolige og derfor skal stole på den fremmede enhed. En løsning er naturligvis ikke at overlade data til andre, men det betyder ofte at den ønskede effekt ikke opnås. SMC er en teknologi som tillader at man kan anvende del-og-hersk paradigmet på denne type problemer: data krypteres og deles imellem *flere* enheder og disse enheder kan så arbejde sammen om at gennemføre den ønskede beregninger uden at nogen af dem nogensinde får adgang til de fortrolige data. Anvendes SMC i en mere simpel form, kan det også anvendes til at konstruere redundans og derigennem sikre tilgængeligheden af gemte data uden at kompromittere fortrolighed og integritet – en kombination af egenskaber som det ellers kan være svært at opnå.<br>Den grundlæggende hypotese er at SMC kan medvirke til at løse centrale problemer relateret til IoT, nemlig håndtering af både fortrolighed, integritet og i et vist omfang tilgængelighed når data overdrages til tredjeparter. Specifikt vil der i projektet bliver arbejdet på at videreudvikle open-source frameworket viff, samt bygge konkrete applikationer baseret på dette. Dette arbejde vil ske i naturlig forlængelse af aktiviteter i Alexandra Instituttets nuværende resultatkontrakt. De konkrete mål og de relaterede cases er specificeret nedenfor under milepæle. |

[4] https://www.borger.dk/Lovgivning/Hoeringsportalen/Sider/Fakta.aspx?hpid=2146000664

[5] Alexandra Instituttet arbejder ikke indenfor selve hardwarelaget af kommunikations teknologierne, her henvises til en anden GTS: Delta.

[6] En international konkurrent er SAP Research, men deres løsninger er pt. teknisk underlegne.

[7] Forsknings- og Innovationschef for it-sikkerhed, Jakob I. Pagter, er dansk repræsentat i IFIP TC11, den tekniske kommitte under den FN-anerkendte forsknings- og udviklings organ IFIP (www.ifiptc11.org) og medlem af ”The Cloud Security Alliance” (/www.cloudsecurityalliance.org).

[8] http://rwi.future-internet.eu

Secure Mashups relaterer til fænomenet mashups (fra Wikipedia: *"a mashup is a web page or application that combines data or functionality from two or more external sources to create a new service"*). Muligheden for at kombinere forskellige eksisterende tjenester og komponenter er en central drivkraft, men sikkerheden halter fordi mashups ofte kombinerer data med forskellig sikkerhedsstatus og placerer dem på – for organisationen der ejer data – uforudsete steder..
Den grundlæggende hypotese for secure mashups er, at det er muligt at konstruere en komponent som på enkel vis forbedrer fortrolighed og integritet af mashups ved automatisk at beskytte data som overdrages til tredjeparts tjenester og komponenter. For mashup-udvikleren vil dette blot være endnu en tjeneste der skal bruges, men for dataejeren giver det værdifuld kontrol over data.

Obfuskering er det sidste specifikke sikkerhedsværktøj som der vil være fokus på i denne aktivitet. Dette er ikke en teknologi som Alexandra Instituttet i øjeblikket besidder specifikke kompetencer indenfor, men obfuskering forventes at blive en central teknologi indenfor IoT og er nært relateret til vores kompetencer indenfor anvendt kryptografi. En vigtig problemstilling indenfor perimeterløs sikkerhed er hvordan man beskytter data på pervasive og mobile enheder. Eftersom vi ikke kan antage enheden som værende indenfor en perimeter (og dermed beskyttet af anti-virus), må vi derfor acceptere at den kan være .kompromitteret. Et grundlæggende problem ved det gamle perimeterparadigme er, at man alligevel ikke kan garantere at en enhed ikke er 100% fri for virus på grund af den hastighed hvorved nye sårbarheder opdages. Den perimeterløse tilgang er altså således at antage at enheder er kompromitterede, men hvordan beskytter vi så kritiske data der befinder sig på enheden?
Hypotesen er at obfuskering i en lang række tilfælde kan være en central del af svaret i bestræbelserne på at sikre integriteten af en enhed. Obfuskering muliggør at vi kan etablere et "helle" på enheden, en lille software-"ø" som for alle praktiske formål ikke er inficeret (men resten af enheden kan være det). Herudfra har man så et fundament hvorpå man kan bygge den nødvendige sikkerhed.

**Software-arkitektur, -infrastruktur og algoritmer for IoT og CC**
IoT og CC giver en række udfordringer for software arkitekter og programmører hvis disse nye muligheder skal udnyttes optimalt. En række problemer er kendte fra traditionel *distribueret computing*, mens andre udfordringer opstår med de nye anvendelser af teknologierne. Ved distribueret computing forstår vi her en beregning i et forbundet net at computere hvor der potentielt er stor latency (forsinkelse) mellem knuderne i netværket, ligesom der er en reel risiko for at man ikke får svar tilbage på en udsendt forespørgsel. Vi betragter her ikke *parallel computing*, der er karakteriseret ved at en række beregnings enheder er koblet tæt sammen (ofte direkte på print kort), og hvor latency kun er et lille problem, og decideret manglende svar ikke vil forekomme med mindre der er er hardware svigt. Parallel computing adresseres i ansøgningen vedrørende Massive Datamængder.

I sikkerhedsafsnittet ovenfor er det beskrevet at *tilgængelighed i skyen* er et væsentligt sikkerhedsaspekt ved CC. De ovenfor beskrevne aktiviteter omkring sikring af tilgængelighed forudsætter en række basale mekanismer til *offline access*. Der er en række tiltag i gang for dette, f.eks. indeholder Google Gears (http://gears.google.com) mekanismer der muliggør delvis offline access til visse Google Docs.

- Men *teknologierne hertil er stadig gryende*, og vi vil som en del af denne aktivitet fokusere på at erhverve og udbygge den nyeste viden om disse

problemer og herigennem klæde det danske erhvervsliv på til bedre at kunne udnytte IoT og CC.

Generelt betyder overgangen fra traditionelle Desktop baserede løsninger til CC baserede løsninger et paradigmeskift for mange software arkitekter og programmører. En række *patterns* og nye begreber såsom service Oriented Architecture (SOA), REST, Software-as-a-service (SaaS), Security-as-a-service, Hardware-as-a-Service (HaaS), Rich Internet Applications og Virtualisering er blandt mulighederne når der skal designes nye software systemer til IoT og CC.

- I samarbejde med bl.a. forskergrupper på Århus Universitet, Datalogisk Institut og private firmaer som de på Katrinebjerg placerede frontløbere indenfor virtualisering VMware vil Alexandra Instituttet iværksætte nye F&I projekter til videnhjemtagning og forskning indenfor disse nye metodikker og teknologier til realisering og udnyttelse af IoT og CC. Udover konkrete forskningsresultater forventes det at der kan genereres en række teknologiske services for danske virksomheder, services der kan hjælpe disse med at udnytte disse nye muligheder.

Udover en række nye begreber og patterns så opstår en række nye *platforme* omkring IoT og CC. Med platforme menes her både hardware og software platforme. Eksempler er Goggles Android arkitektur for mobiltelefoner – denne definerer et operativ system for mobile enheder med – ifølge Google – speciel support for CC, og har samtidig ført til en helt ny hardware portefølge fra f.eks. HTC, der var den første mobil-producent på markedet med en mobiltelefon designet specifikt til Android. Tilsvarende ses en helt særegen hardware-portefølge branded af Apple Computer med deres proprietære iPhone hardware og tilhørende software arkitektur. Microsoft har lanceret Windows Azure som deres bud på et Cloud Computing Operating System.

- Som en forudsætning for vores andre CC aktiviteter ser vi en nødvendighed af at få opbygget en erfaringsbase med disse nye CC platforme, herunder at hjemtage viden om state-of-the-art og at forske i hvorledes man kan bygge bro mellem disse i udgangspunktet ikke-integrerede platforme.

I alle distribuerede og/eller internet forbundne systemer anvendes en række forskelligartede *kommunikationsteknologier og protokoller*, for både trådet og trådløs transmission. I takt med at CC ideen bliver mere og mere udbredt vil de forskellige pervasive systemer komme til at indgå i brugerens personlige sky, f.eks. vil hjemmets IT infrastruktur til kontrol af energi, klima, og underholdning blive en del af skyen for brugeren, ligesom en række telemedicinske løsninger vil kunne komme til at udgøre dele af skyen for patienter udenfor hospitalets vægge. I dag findes en lang række trådede og trådløse standarder for pervasive apparater spændende fra standard ethernet baseret IP (IPv4 & IPv6) over de forskellige telefoni standarder (tale og data), WiFi, 802.15.4 baserede protokoller (f.eks. ZigBee og 6lowpan), BlueTooth, Z-wave, uPnP, og IO-Homecontrol. Inden for healthcare er der nye forslag til standardiseret kobling af healthcare devices, f.eks. IEEE/ISO 11073 på lavt niveau, og HL7 og OpenEHR på højere niveau. Et tiltagende problem for den IP baserede kommunikation er at den udbredte IPv4 standard er ved at løbe tør for adresser. Man har defineret IPv6 standarden til afløsning for IPv4, men det tager tid at få denne indført. I regi af denne resultatkontrakt vil der blive forsket, videnhjemtaget og formidlet omkring IPv6, til støtte omkring IT & Telestyrelsens igangværende strategi og handlingsplan for IPv6[4].
Et stort problem for brugen af de ressourcer som kommunikerer vha disse mekanismer er den store forskelligartethed i disse kommunikationsteknologier og -protokoller, og integration imellem disse er derfor bydende nødvendigt for at

| | |
|---|---|
| | få disse ressourcer til at indgå naturligt i skyen.<br>En række igangværende projekter (Homeport, Dit Hus mfl.) arbejder med tiltag i den retning. Et forholdsvist nyt initiativ - 6lowpan "*IPv6 over Low power Wireless Personal Area Networks*" - sigter mod at internet-enable alle sådanne devices ved at benytte en ny protokol i stedet for de mange forskellige nævnt ovenfor. Inden for Pervasive Healthcare kan nævnes det igangværende Caretech projekt Akutflow (med Cetrea A/S).<br>I denne aktivitet vil vi dels sikre opbygning og vedligehold af state-of-the-art og forskningsbaseret viden indenfor dette hastigt voksende område, dels vil vi gennem specifikke cases arbejde for at udbrede anvendelsen og integrationen af disse teknologier i dansk erhvervsliv og sundhedsvæsen:<br>• Videnopbygning omkring state-of-the-art og aktuel forskning indenfor protokoller, kommunikationsmekanismer og lignende på applikations laget[5]<br>• Mulige F&I projekter i forlængelse af ISIS Katrinebjerg projektet Homeport og fortsætterprojektet Dit Hus. Her vil interessegruppen Hjem Til Fremtiden i Infinit netværket kunne spille en aktiv rolle,, og evt. afvikle forprojekter før egentlige F&I projekter i resultatkontrakt regi.<br>• Potentielt et F&I projekt omkring 6lowpan. Et EU projekter under ansøgning (FP7, call5) kunne kandidere hertil: *Smart Santander* – integration af information om en bys transport systemer, luft kvalitet, turist attraktioner, etc.<br>• Caretech projektet Net4care. Net4Care er en vision om en sammenhængende og landsdækkende infrastruktur til fremtidens netværksbaserede sundhedsvæsen. Det er en teknisk og organisatorisk infrastruktur der binder hjem, arbejde og sundhedsleverandør sammen. Der er tilsagn fra Flex-Control A/S om deltagelse i dette projekt. Flex-Controls producerer i dag intelligente onlinesystemer til fjernovervågning og -styring i virksomheder og i private huse.<br>• Potentielle F&I projekter omkring kommunikationsaspekter indenfor intelligente tekstiler/bandager, specielt med anvendelse indenfor healthcare. Interessegruppen for Intelligente Tekstiler i Infinit netværket vil spille en aktiv idegenererings- og matchmakingrolle her, og evt. afvikle forprojekter før egentlige F&I projekter i resultatkontrakt regi. Her forventes synergi med Caretech projektet MIKAT (Mobil og Instrumentel Kognitiv Adfærds-Terapi), hvor brug af biosensorer og feedback igenem bl.a. påklædning skal benyttes til monitorering og styring af angsttilfælde.<br>Spredningen af den indsamlede og producerede viden, vil bl.a. benytte Infinit interessegrupperne nævnt ovenfor, samt SundhedITnet som formidlingskanaler.<br><br>**Ny viden og teknologi opbygget**<br>Projektet vil opbygge ny viden og teknologi baseret på ideen om perimeterløs sikkerhed. Dette drejer sig både om viden i bred forstand, samt mere snævre tekniske softwareværktøjer indenfor fx SMC. Indenfor arkitektur, infrastruktur og algoritmer vil der blive hjemtaget, og videreforsket i bl.a. emnerne offline caching – google gears mm.,arkitektur patterns for CC og IoT, platforme for CC og IoT samt IoT og CC protokoller, specifikt IPv6, 6lowpan, ISO 11073<br><br>**Forbedringer af Teknologisk Service**<br>Ifht. perimeterløs sikkerhed er dette ikke en tilgang til it-sikkerhed som er repræsenteret hos danske udbydere af it-sikkerhedsydelser. Eksempelvis er der ingen danske medlemmer af The Jericho Forum (omtalt andetsteds). Alexandra Instituttets Center for it-sikkerhed har i nogen tid interesseret sig for dette emne, men har ikke haft ressourcerne til at udvikle målrettede teknologiske serviceydelser. Igennem definitionen af PST samt de konkrete værktøjer vil både Alexandra Instituttets egne ydelser og niveauet for Teknologisk Service indenfor |

| | |
|---|---|
| | it-sikkerhed blive udbygget i betydelig grad. Det skal her også nævnes at Alexandra Instituttet er verdens førende indenfor SMC-teknologien[6].<br>Alexandra Instituttet vil igennem de her foreslåede aktiviteter supplere DELTA vedrørende rådgivning på applikationslaget om IoT og CC kommunikations protokoller.<br>Ydermere er der ifølge vores erfaring ikke nogen virksomheder med samlet rådgivning omkring platforme, arkitektur patterns og komponenter for IoT og CC i Danmark. Alexandra vil opbygge et SoftWare Architecture Team (SWAT) som kan rådgive omkring dette.<br>Endelig er der ikke nogen virksomheder med samlet rådgivning omkring perimeterløs sikkerhed for IoT. Alexandra vil opbygge et Perimeterlessfree Security Team – PST. Grundlaget for denne ydelse er under udvikling i den eksisterende resultatkontrakt.<br><br>Ifht. det private rådgivermarked indenfor de beskrevne faglige områder er visionen at de her beskrevne services vil positionere Alexandra Instituttet som "rådgivers rådgiver". Visionen er videre at de private rådgivere så kan bringe disse services videre ud i markedet.<br><br>**Tidhorisont på markedsmodning**<br>De teknologiske serviceydelser som bliver resultatet af dette projekt vil være markedsmodne over et tidsinterval som går fra 1 til 5 år. Softwareløsninger baseret på SMC vil kunne sælges allerede efter år. Rådgivningsorientede ydelser som SWAT og PST forventes kommercielt operationellet i løbet af år 2. De øvrige softwareværktøjer forventes markedsmodne efter 3-5 år.<br><br>**Forventede samarbejdspartnere**<br>• <<slettet<br><br>**International videnhjemtagning**<br>Ifht. it-sikkerhed er Alexandra Instituttet allerede repræsenteret i flere internationale fora[7] og planlægger yderligere at melde sig ind i "The Jericho Forum". Derudover vil dette projekts deltagere deltage i internationale konferencer; både for at præsentere projektets arbejde, men også på andre konferencer for at hjemtage ny viden. Sluttelig vil der blive søgt oprettet strategiske partnerskaber med internationale partnere. I øjeblikket er det planen at gå i dialog med Fraunhofer og SAP Research.<br>Omkring generel infrastruktur og aloritmer påtænkes benyttet en række internationale partnere, herunder Ericsson, IPSOAlliance, IETF, VMware, Future Internet Assembly on Real World Internet[8], Gridmanager, partnere fra internationale forskningsprojekter, såsom PalCom og Hydra, store danske virksomheder med internationale kontakter, såson Skov A/S, Danfoss, COWI samt internationale kontakter Alexandra har kontakt med igennem nære samarbejder med andre videninstitutioner. |
| **Koordinering og samspil med andre F&I-aktiviteter** | Følgende projekter påtænkes medfinansieret:<br>• CACE – Computer Aided Cryptographic Engineering. EU/FP7-projekt med fokus på at gøre det let for "almindelige" softwareudviklere at anvende kryptografi. Dette projekt understøtter direkte udviklingen af værktøjer hvor kryptografi indgår i løsningen.<br>• COBE – Confidential Benchmarking. Projektansøgning indsendt til Forskningsrådet for Teknologi og Produktion. Dette projekt studerer brugen af Secure Multiparty Computation til at realisere sikre benchmarkingsystemer og er således direkte relateret til et af delmålene i denne aktivitet.<br>• JOIN – EBST finansieret projekt. Online innovations community, hosted på |

| | |
|---|---|
| | Amazon eller Google og implementeret vha CC teknologier. Samarbejde med Innovationsnetværk for Livsstil Bolig og Beklædning, Cuusoo (Japan), Crossroad Innovation.<br>• Sikkerhedsplaster. iKRAFT finansieret projekt (under ansøgning). Trådløs monitorering af handicappede i svømmehal. Samarbejde med DELTA, Active Institute, Egmont Højskolen<br>• Net4Care. Beskrevet ovenfor. Samarbejde med Flex-Controls m.fl.<br>• @aGlance. iKRAFT ansøgning med sigte på at udbyde CC services til understøttelse af planlægning, afvikling og oplevelse af, samt evaluering af større events på geografisk spredte områder. Samarbejde med Danmarks Smukkeste festival, Sydøstjyllands Politi, Brand&Redning Skanderborg, Århus Universitet<br>• Et EU projekt indenfor IoT, 6lowpan eller CC generelt (evt. Smart Santander)<br>Denne aktivitet vil desuden samarbejde uformelt med, men ikke medfinansiere, følgende:<br>• Innovationsnetværket Infinit. En række vidanspredningaktiviteter indenfor denne resultatkontrakt vil i praksis blive udbudt igennem Infinit, der således vil benyttes som formidlingskanal. Specifikt påtænkes et tæt samarbejde med interessegrupperne Intelligente Bygninger og Intelligente Tekstiler.<br>• Det højteknologiske netværk SundhedsITnet. På samme måde som for Infinit vil en række vidanspredningsaktiviteter i regi af denne resultatkontrakt indenfor anvendelsesområdet pervasive healthcare blive udbudt igennem SundhedsITnet, der således også vil fungere som formidlingskanal. |
| **Formidlings- og spredningseffekt:** | Generelt vil aktivitetsområdet benytte de formidlings- og spredningsmekanismer som Alexandra Instituttet råder over.<br>• Landsdækkende kontakt til SMV'ere gennem instituttets vidanspredningsinfrastruktur, som dels består af afdelinger i Århus, København, Herning og Sorø, dels består af en række formaliserede samarbejder med erhvervscentre rundt omkring i landet. Herigennem opbygges interessentgrupper og gennemføres idégenereringsworkshops med udvalgte virksomheder.<br>• Formidling af viden igennem instituttets mange netværk, blandt andet medlemsnetværk, vores højteknologiske netværk og vores innovationsnetværk.<br>• Internetbaseret formidling via alexandra.dk.<br>• Publicering i dels populærvidenskabelige skrifter samt til forskningskonferencer og i internationale forskningstidskrifter.<br>• Formidling via fagpressen (fx Ingeniøren, ComputerWorld, version2.dk) igennem pressemeddelelser og øvrigt kommunikationsarbejde.<br>Som beskrevet ovenfor ("tidsmæssig horisont for markedsmodning"), vil en mindre del af de udviklede services kunne sælges relativt hurtigt, men størstedelen forventes at kunne sælges i den sidste del af eller efter resultatkontraktperioden. En del af den samlede vidanspredningssaktivitet for området vil være en overordnet analyse, inkl. en løbende evaluering af brugernes ønsker og krav, hvilket periodisk vil danne grundlag for feedback til området om brugernes krav og ønsker med henblik på at informere og evt. udvikle indsatsen.<br>Kvalitative mål for vidanspredning i regi af denne aktivitet:<br>• Kommunikationsstrategi for området baseret på målgruppe- og markedsforståelse. Strategien vil omfatte videnoverførende aktiviteter, der er tilpasset målgrupperne og den form for påvirkning, som området søger med sin kommunikation. De nedenstående kvalitative mål for vidanspredning inddrages og tilpasses i kommunikationsstrategien. Løbende udvikling af planer for nyttiggørelse af områdets resultater og delresultater i samspil med områdets interessenter på baggrund af analyse og evalueringer. |

| | |
|---|---|
| | • Minimum 2 artikler pr år på internationalt anerkendte forskningskonferencer.<br>• Mindst 2 brugerworkshops pr. år med fokus på ønsker og krav til aktiviteten.<br>• Mindst 1 vidensprednings arrangement pr. år . I relevant omfang i samarbejde med Infinit interessegrupperne Intelligente Bygninger og Intelligente Tekstiler, samt SundhedsITnet<br>• Vidensprednings i udstillinger/messer for danske SMV'er såsom eSkills week 2010<br>• Etablering af SWAT og PST.<br>• I år 3 forventes en kommerciel omsætning på: 0,7 millioner kr. |
| **Centrale kompetencer involveret i F&I-projektet** | • F&I chef, Softwareinfrastrukturer, Peter Andersen<br>• F&I chef, IT-sikkerhed, Jakob I. Pagter<br>• F&I chef, Forretningsforståelse, Camilla Kølsen<br>• F&I ingeniør, Jerker Hammarberg<br>• Projektleder, Svend Thielsen<br>• Projektleder, Hans Christian Damgaard<br>• F&I specialist, Mirko Presser<br>• F&I specialist, Thomas Jakobsen<br>• F&I specialist, Janus Dam Nielsen |
| **Milepæle år 1** | **F&I-indikatorer**<br>• Første version af State-of-the-art beskrivelser baseret på international videnhjemtagning og litteraturstudier af:<br>o Online/offline teknologier<br>o IPv6 & 6lowpan<br>o Homecontrol- og healthcare kommunikationsprotokoller<br>o Virtualisering<br>o CC og IoT arkitektur og platforme<br>o Sikkerhed for IoT generelt<br>o Secure Mashups<br>• Forskningsaktivitet<br>o Publicering af mindst 1 videnskabelig artikel vedrørende sikkerhed for IoT<br>o Publicering af mindst 1 videnskabelig artikel vedrørende software og algoritmer for IoT.<br>o Opstart af Net4Care projekt.<br>o Opstart af synergiaktiviteter med JOIN, Sikkerhedsplaster, og @aGlance.<br>o Opstart at mindst 1 yderligere F&I projekt, evt. om IPv6 & 6lowpan.<br>o Opstart af COBE-projektet.<br>• Demonstratorer<br>o @aGlance-demonstrator på festival<br>o Private Information Retreavel in Healthcare (PIR)<br>o Distribueret Lagring<br>**Målgruppeservice**<br>• Kommunikationsstrategi<br>• Mindst 2 brugerworkshops med faglige oplæg fra aktiviteten og deltagelse af minimum 10-15 virksomheder.<br>• Mindst 1 vidensprednings arrangement i Infinit interessegrupperne Intelligente Bygninger og Intelligente Tekstiler, samt i SundhedsITnet; hvert arrangement inkluderer faglige oplæg om denne aktivitet og der er deltagelse af minimum 20-30 virksomheder.<br>• Mindst 2 præsentationer ved eksternt arrangerede vidensprednings arrangementer såsom erhvervsklubber, konferencer, virksomhedsarrangementer, o.a.<br>• Mindst 2 pressemeddelelser til fagpressen.<br>• Opstart at SWAT og PST initielt med intern projekter som målgruppe |

| | |
|---|---|
| **Milepæle år 2** | **F&I-indikatorer**<br>• Udbygning State-of-the-art beskrivelser baseret på international videnhjemtagning og litteraturstudier af:<br>o Online/offline teknologier<br>o IPv6 & 6lowpan<br>o Homecontrol- og healthcare kommunikationsprotokoller<br>o Virtualisering<br>o CC og IoT arkitektur og platforme<br>o Sikkerhed for IoT generelt<br>o Obfuskering<br>• Forskningsaktivitet<br>o Publicering af mindst 1 videnskabelig artikel vedrørende sikkerhed for IoT<br>o Publicering af mindst 1 videnskabelig artikel vedrørende software og algoritmer for IoT.<br>o Net4Care model for organisatorisk og teknisk infrastruktur etableret samt pilotprojekter igangsat<br>o Bidrag til infrastruktur for JOIN, Sikkerhedsplaster, og @aGlance<br>o Opstart af min. 1 nyt forskningsprojekt om sikkerhed for IoT<br>o Opstart at mindst 1 yderligere F&I projekt, evt. omhandlende intelligente bygninger eller intelligente tekstiler<br>• Demonstratorer<br>o Benchmarking<br>o Secure Mashups<br>o Udbygget @aGlance-demonstrator<br><br>**Målgruppeservice**<br>• Mindst 2 brugerworkshops med faglige oplæg fra aktiviteten og deltagelse af minimum 10-15 virksomheder.<br>• Mindst 1 videnspredningsarrangement; hvert arrangement inkluderer faglige oplæg om denne aktivitet og der er deltagelse af minimum 20-30 virksomheder.<br>• Mindst 4 præsentationer ved eksternt arrangerede videnspredningarrangementer såsom erhvervsklubber, konferencer, virksomhedsarrangementer, o.a.<br>• Deltagelse på mindst en relevant udstilling/konference (hvis fokus inkluderer SMV'er) med faglig præsentation af aktiviteten. Disse udstillinger/konferencer udvælges som en del af kommunikationsstrategien, men kunne fx være IT-sikkerhed (Dansk ITs årlige konference om it-sikkerhed) eller JAOO.<br>• Mindst 2 pressemeddelelser til fagpressen.<br>• SWAT og PST etableret og udbudt til eksterne kunder |
| **Milepæle år 3** | **F&I-indikatorer**<br>• Udbygget State-of-the-art beskrivelser baseret på international udvikling indenfor:<br>o Online/offline teknologier<br>o IPv6 & 6lowpan<br>o Integration af Homecontrol- og healthcare kommunikationsprotokoller<br>o Virtualisering<br>o CC og IoT arkitektur og platforme<br>o Sikkerhed for IoT generelt<br>• Forskningsaktivitet<br>o Modnet Net4Care infrastruktur<br>o Net4Care demonstrator udviklet<br>o Bidrag til demonstratorer for JOIN, Sikkerhedsplaster, og @aGlance |

| | |
|---|---|
| | ○ Publicering af mindst 1 videnskabelig artikel vedrørende sikkerhed for IoT<br>○ Opstart af min. 1 nyt forskningsprojekt om sikkerhed for IoT<br>○ Opstart at mindst 1 yderligere F&I projekt<br>• Demonstratorer<br>○ Distribueret billedbehandling PoC<br>○ Obfuskering PoC<br>○ @aGlance baserede kommercielt tilgængelige teknologiske services.<br>**Målgruppeservice**<br>• Mindst 2 brugerworkshops med faglige oplæg fra aktiviteten og deltagelse af minimum 10-15 virksomheder.<br>• Mindst 1 vidensprednings arrangement; hvert arrangement inkluderer faglige oplæg om denne aktivitet og der er deltagelse af minimum 20-30 virksomheder.<br>• Mindst 4 præsentationer ved eksternt arrangerede vidensprednings arrangementer såsom erhvervsklubber, konferencer, virksomhedsarrangementer, o.a.<br>• Deltagelse på mindst en relevant udstilling/konference (hvis fokus inkluderer SMV'er) med faglig præsentation af aktiviteten. Disse udstillinger/konferencer udvælges som en del af kommunikationsstrategien, men kunne fx være IT-sikkerhed (Dansk ITs årlige konference om it-sikkerhed) eller JAOO.<br>• Mindst 2 pressemeddelelser til fagpressen.<br>• SWAT benyttet af mindst 3 eksterne kunder<br>• PST benyttet af mindst 3 eksterne kunder |