Aktivitet	Forskning og udvikling		
Aktivitetsplan (titel):	Sikkerheds- og privacyværktøjer	**Aktivitetsplan nr.:**	4
Resumé	Denne aktivitetsplan har fokus på at udvikle viden og værktøjer, som gør det muligt for danske virksomheder at drive og styrke deres forretning, på trods af de store udfordringer de står overfor inden for it-sikkerhed og privacy. Aktiviteten tager afsæt i Alexandra Instituttets stærke kompetencer inden for it-sikkerhed, suppleret med specialiseret viden fra DELTA og DBI omkring hhv. hardware og brugeradfærd i relation til it-sikkerhed. Et vigtigt element i aktiviteten er, at de konkrete delemner, som bliver belyst, udvælges med input fra en interessentgruppe med et bredt udsnit af repræsentanter.		
1) Målgruppe og behov	It-sikkerhed og privacy bliver vigtigere og vigtigere i det moderne it-baserede samfund. Der er mange eksempler på utilstrækkelig sikkerhed (f.eks. meget omtalte sårbarheder som heartbleed[1], stuxnet[2] og cryptolocker[3]). Samtidig er der en række politiske tiltag, som understreger, hvordan it-sikkerhed kommer højere og højere op på den samfundsmæssige dagsorden: 1) EU barsler med en ny persondataforordning[4]; 2) Danmark har lanceret en national strategi for cybersikkerhed[5]; 3) der er et meget eksplicit fokus på it-sikkerhed og privacy i vækstplanen for digitalisering[6]. Denne udvikling understøttes af internationale undersøgelser, som spår om en stadig vækst i markedet for it-sikkerhed, f.eks. Markets and Markets, som vurderer, at der vil være en stigning på knap 10% pr. år fra 2015 til 2020 til en samlet værdi af over 1 billiard DKK om året[7]. Dette er en stor udfordring for danske virksomheder, fordi det kræver ændrede processer, nye værktøjer og specialistkompetencer. Det er en særlig udfordring for SMV'er, da de udsættes for samme sikkerheds- og privacykrav som store virksomheder, men uden at de har mulighed for at kunne opbygge egen specialistkompetence eller kvalificeret kunne vælge de rette processer og værktøjer. Potentialet kan grundlæggende tilskrives to parallelle udviklinger: 1) Megatrends som cloud, mobile, big data, internet-of-things (IoT) og bring-your-own-device. Det betyder, at sikkerhedsløsninger i meget højere grad må fokusere på at beskytte data, uafhængigt af hvor de er (inden for vs. uden for perimeteren), og hvad de skal bruges til. For at opnå dette, skal der typisk benyttes tekniske virkemidler som f.eks. kryptografi, og sikkerheden skal være *designet* ind i løsningen fra starten - dette kaldes populært sagt Security- og Privacy-by-Design (SPbD). 2) regulative krav fra både EU og nationalt (se ovenfor) stiller øgede krav til virksomhedernes sikkerhed, og f.eks. det aktuelle udkast til EUs kommende persondataforordning nævner eksplicit *Privacy-by-Default* som et paradigme, fremtidige løsninger *skal* efterleve. Tilsvarende ligger		

[1] https://da.wikipedia.org/wiki/Heartbleed-bug
[2] https://en.wikipedia.org/wiki/Stuxnet
[3] https://en.wikipedia.org/wiki/CryptoLocker
[4] http://ec.europa.eu/justice/data-protection/
[5] http://www.fmn.dk/nyheder/Pages/Regeringen-styrker-cyber-og-informationssikkerheden.aspx
[6] http://www.evm.dk/aftaler-og-udspil/15-02-26-aftale-om-vaekstplan-for-digitalisering
[7] http://www.marketsandmarkets.com/PressReleases/cyber-security.asp

	der i Erhvervs- og Vækstministeriets vækstplan for digitalisering i Danmark oplæg til, hvordan danske virksomheder kan gennemgå et såkaldt sikkerhedstjek. Problemet eksisterer både for *brugervirksomheder*, som har brug for at vælge de rigtige løsninger for at leve op til kunders og myndigheders krav, understøttet af kommentarer på bedreinnovation.dk fra f.eks. DI/ITEK, CFIR og IDA. Ligeledes for *leverandørvirksomheder*, som ønsker at lave innovative it-løsninger i lyset af f.eks. overholdelse af persondataforordning, cookiedirektiv m.v., understøttet af kommentarer fra virksomheder som Grundfos, Eurisco og KMD. For begge typer er evnen til både at designe og implementere den *rigtige* sikkerhedsmæssige løsning af stor forretningsmæssig betydning. De udviklede kompetencer og serviceydelser vil være relevante for en stor del af alle danske virksomheder, ikke mindst SMV'er, på tværs af forskellige brancher. Dette inkluderer f.eks. internethandel (FDIH har mere end 2000 medlemmer), produktionsvirksomheder som ønsker at digitalisere deres produktionssystemer (i alt skønnes der at være ca. 15.000 produktionsvirksomheder i Danmark), og leverandører af it-services, samt leverandører af it-baserede services (som f.eks. regnskabssystemer). Identifikationen af målgrupperne og deres behov tager afsæt i de generelle politiske, samfunds- og forretningsmæssige trends beskrevet ovenfor, og som bekræftes af de mange kommentarer på bedreinnovation.dk.
2) Den nye teknologiske serviceydelse	Historisk har it-sikkerhed været bygget op omkring det såkaldte perimeterparadigme med fokus på tilgange som antivirus, firewalls, adgangskontrol og ikke mindst organisatoriske sikkerhedstiltag. I en moderne it-verden hvor megatrends som cloud, mobile, BYOD, IoT og big data sætter dagsordenen for it-anvendelsen, er dette paradigme ikke længere tilstrækkeligt, og it-sikkerhedsløsninger må i meget højere grad fokusere på at beskytte data, uafhængigt af hvor de er (inden for vs. uden for perimeteren), og hvad de skal bruges til. Et stærkt virkemiddel til at realisere it-sikkerhed og privacy er kryptografi, da kryptering af data giver matematiske garantier for den realiserede sikkerhed (noget traditionel perimetersikkerhed kun i helt særlige tilfælde kan opnå). Dette dokumenteres blandt af det nuværende udkast til den kommende persondataforordning, hvor det er gjort eksplicit, at forebyggende tekniske tiltag som kryptering kan reducere bødestraf og administrative omkostninger i tilfælde af, at data falder i de forkerte hænder. Korrekt anvendt praktisk kryptografi muliggør en lang række forretningsmæssigt attraktive it-løsninger på en måde, som er *både* sikkerhedsmæssigt forsvarlig *og* kosteffektiv. Vi kan med andre ord høste større digitaliseringsgevinster, fordi vi kan få *bedre* og *billigere* sikkerhed ved at gå nye veje. De fundamentale kompetencer inden for kryptografi og it-sikkerhed eksisterer i dag i Alexandra Instituttet, men de beskrevne behov i markedet nødvendiggør en videreudvikling og vedligeholdelse af disse. Desuden er der behov for at gøre dem tilgængelige i en form, som er brugbar for den store gruppe af potentielle aftagere. Derudover suppleres disse kompetencer med viden om hardware og adfærd fra hhv. DELTA og DBI. Samlet giver dette "hold" os mulighed for at arbejde med it-sikkerhed og privacy ud fra en holistisk tankegang, hvor alle væsentlige elementer betragtes: det drejer sig om selve den tekniske løsning, de

	hardwaremæssige sikkerhedsantagelser, som danner fundament for teknikken, brugerne og deres adfærd, og endelig den fysiske sikring af virksomheders it-løsninger. Dette gør sig gældende for de løsninger, som udvikles i dette projekt og for de produkter som er på markedet, og de produkter danske virksomheder udvikler. Målet med denne aktivitet er at opbygge kompetencer og ydelser, som kan understøtte dette. I det følgende gives et overblik over de kompetencer og ydelser, der vil være i fokus. Yderligere detaljer fremgår nedenfor under "Aktiviteter". <u>Kompetencer (konsulentydelser):</u> • Analyse og kortlægning af cybersikkerhedsstandarder på verdensplan med særligt fokus på det standardiseringsarbejde som pågår. • Identifikation af branchers udfordringer med produktsikkerhed, og hvorvidt dette influerer på markedsadgang. • Brugeradfærd (analyse af brugeradfærd; beskyttelse mod social engineering angreb, e.g. phishing-forsøg; test og evaluering af it-løsninger ift. adfærd). • Kryptografi (herunder traditionel kryptografi; PETs som f.eks. U-prove og IdentityMixer; Multiparty Computation; Block chain-teknologi – stammer fra bitcoin, men har stort potentiale inden for mange andre områder, hvor der er behov for dokumentation af transaktioner). • Identitetssystemer (f.eks. OpenID Connect og UMA). • Risikoanalysemetoder som f.eks. OCTAVE. • Domæneviden om sikkerhed og privacy ift. megatrends som IoT, Big Data, cloud, mobile og bring-your-own-device (BYOD). <u>Produktscreening</u> – eksempler på hvad det kunne omfatte: • Sikker mail – hvilke produkter i markedet lever op til danske SMV'ers krav til sikker email. • Sikker fildeling – hvilke produkter i markedet lever op til danske SMV'ers krav til sikker fildeling (gør eksempelvis Dropbox?). • Udvikling af rådgivningsydelse i form af assessments af sikkerhed for devices og elektronikprodukter. • Produkter/ydelser omkring sikker brugeradfærd. <u>Metoder (konsulentydelser):</u> • Produktscreening. • Analyseframeworks relateret til megatrends. • Screening og opbygning af framework for standarder inden for cybersikkerhed i fysiske produkter – devices. <u>Løsninger (produkter)</u> – eksempler på hvad det kunne omfatte: • Brugervenlig installation af smart grid-komponenter. • Løsninger baseret på Multiparty Computation (MPC) til f.eks. sikker benchmarking på tværs af virksomheder. Sidst på året starter et projekt (hvor vi er med) under Industriens Fonds Big Data-satsning med dette som fokus. Vi forventer god synergi med dette projekt og vil se på, hvordan vi kan bygge videre på resultaterne derfra og fra andre MPC-projekter. Ovenstående lister er ikke fuldstændige, da vi igennem inddragelse af interessentgruppen vil udpege de konkrete produkter og løsninger, som der vil komme fokus på. Den fundamentale grund til at markedet ikke selv kan udvikle de her beskrevne ydelser er, at specielt kryptografi er en meget specialiseret

	kompetence, som er dyr at udvikle og vedligeholde. Grundlæggende findes der i Danmark allerede virksomheder, som arbejder med kryptografi. Det er både mindre virksomheder som Cryptomathic og store internationale spillere som IBM, der har placeret deres Crypto Competence Center for EMEA i København. De eksisterende spillere i markedet har dog i høj grad fokus på eksisterende og konsoliderede markeder som f.eks. den finansielle sektor. Der er også (ganske få) virksomheder, som arbejder med rådgivning om f.eks. Privacy-by-Design, Open Business Innovation og Peercraft (se bedreinnovation.dk). Disse virksomheder er potentielle aftagere af særligt de kompetencer, der udvikles i denne aktivitet, i en klassisk "rådgivers rådgiver"-model, idet disse virksomheder typisk ikke selv har eller kan opbygge den dybe tekniske viden, som er fundamentet for denne aktivitet. Der er – med vores nuværende viden – ikke aktører, som leverer den type ydelser, der er beskrevet i denne aktivitet. Ift. screening m.v. af produkter har denne aktivitet også den fordel, at den er forankret hos en uvildig spiller på markedet. I forhold til assessment af device-sikkerhed er der ikke identificeret uvildige aktører, som varetager dette på dansk grund. Dertil kommer, at manglende standarder på området gør rådgivning omkring dette vanskeligt på nuværende tidspunkt. Gennem aktiviteten er det målet at opbygge dybere viden om og præge internationale standarder på området, så private aktører på sigt kan få en referenceramme at udvikle services indenfor. DBI har historik for at tænke sikkerhed ind i brugerrelaterede løsninger. Dette gør sig ligeledes gældende ved it-løsninger, hvor vi analyserer brugernes adfærd for derved at identificere, om der er mulige, utilsigtede sikkerhedsbrister.. Aktivitetens forskellige ydelser har forskellig tidshorisont for markedsmæssig udbredelse: • Kompetencer – løbende • Screenings og guides – år 1-3 i aktiviteten • Metoder – år 2-3 i aktiviteten • Innovative anvendelser af eksisterende teknologier – år 3 i aktivitet • Nye løsninger – 1-3 år efter denne aktivitets gennemførelse
3) Aktiviteter	Grundlæggende er denne aktivitet meget teknisk, hvilket giver en stor risiko ift. at sikre den nødvendige markeds- og samfundsmæssige relevans. Indsatsen vil derfor udføres i et tæt samarbejde mellem de tekniske sikkerhedsspecialister og Alexandra Instituttets eksperter inden for kravsafdækning og evaluering. Vi vil blandt andet arbejde ud fra spørgsmål som: Er der begrænsninger knyttet til de eksisterende forretningsprocesser, der hæmmer sikkerhed eller privacy? Skal der laves ændringer i forretningsmodellen for at opnå tilfredsstillende sikkerhed eller privacy? Det grundlæggende "flow" for de forskellige ydelser og kompetencer er derfor som følger: 1. Afdækning af behov. 2. Udvikling af kompetencer/ydelser – her vil i høj grad være tale om dybt teknisk arbejde med fokus på f.eks. kryptografi 3. Afprøvning og demonstration 4. Information og vidensprednin I alle faser vil vi i størst muligt omfang trække på den interessentgruppe,

	som foreslås etableret ifm. projektet. Igennem samarbejdet med interessentgruppen vil der ske en afstemning af arbejdsdelingen mellem GTS-aktørerne og de private leverandører og rådgivere inden for aktiviteten og de planlagte ydelsers område. Det konkrete arbejde er organiseret i fem arbejdspakker. Både Alexandra Instituttet, Delta og DBI bidrager forholdsmæssigt til hver af disse. AP1 – Kompetencer: Denne arbejdspakke har fokus på at videreudvikle de nødvendige kompetencer i Alexandra Instituttet samt hos DELTA og DBI. Arbejdet vil være drevet af det behov, som identificeres i de øvrige arbejdspakker og vil bestå i desktop research inden for state-of-the-art, deltagelse i konferencer, skrivning af videnskabelige artikler og i relevant omfang certificeringer. Tematisk forventer vi, at fokus vil være på de emner, som er beskrevet ovenfor. Der vil hvert år blive udarbejdet white papers, som dokumenterer den erhvervede viden. Vi forventer igennem denne arbejdspakke at oparbejde viden, som er central i de øvrige arbejdspakker, og som kan føre til konsulentydelser i klassisk ”rådgivers rådgiver”-forstand. AP2 – Metoder: Denne arbejdspakke har fokus på at udvikle metoder. Disse metoder tjener to formål: 1) som et værktøj i AP3 og 2) som en ydelse som kan leveres til virksomheder, der har behov for at få gennemført en sikkerhedsanalyse. Der findes i dag forskellige metoder til at gennemføre sikkerhedsanalyse. Vi har gode erfaringer med OCTAVE udviklet af det amerikanske CERT i samarbejde med Carnegie-Mellon University.Ift. en række af de behov, som falder indenfor denne aktivitet, er OCTAVE dog for omfangsrig. Vores plan er at udnytte ”fællestræk” i de systemer, vi analyserer. Analyseres f.eks. systemer til sikker email, er vores hypotese, at vi på baggrund af en grundig analyse kan lave en letvægstmetode, som gør det let at gennemføre efterfølgende analyser. Tilsvarende forventer vi at kunne lave metoder tilpasset f.eks. IoT og Big Data, hvor en række af de grundlæggende udfordringer knyttet til disse trends kan ”genbruges”. Deltagelse i lovgivnings- og standardiseringsarbejde, hvorved der skabes viden om implementérbare sikkerhedslovgivninger (DELTA). Formidle, påvirke og nationalt samarbejde omkring åbne standarder for sikkerhed i forhold til kommende nationale, NATO- og EU-direktiver (DELTA). Gennemgang og analyse af brugernes adfærd med f.eks. systemer til sikker e-mailkommunikation vil kunne skabe grundlæggende metoder, der kan bruges til at rådgive SMV'er om deres ansattes brugeradfærd, og hvordan de sikrer sig, at deres it-politik overholdes i skiftende brugsmiljøer, f.eks. når en medarbejder arbejder hjemme. Derudover vil udvikling af nye standarder for sikkerhedspolitikker kunne sikre, at data håndteres hensigtsmæssigt, samtidig med at den fysiske sikring af væsentlige it-funktioner, som f.eks. serverrum, er optimeret. Vi forventer således at kunne udvikle ydelser, hvor vi meget kosteffektivt kan hjælpe danske virksomheder med at gennemføre forsvarlige sikkerhedsanalyser. AP3 – Produktscreening: Denne arbejdspakke har fokus på at evaluere forskellige moderne sikkerhedsprodukter af relevans for SMV’er. Det kunne f.eks. være løsninger til krypteret e-mail eller sikker fildeling. Vi

	forventer at gennemføre 10 screenings i løbet af projektet, som alle vil følge denne skabelon: 1. Udvælgelse af produktkategori i samarbejde med interessentgruppen. 2. Etablering af baseline sikkerhedskrav for produkter – kræver igen input fra interessentgruppe. 3. Identifikation af konkrete produkter i kategorien. 4. Evaluering af udvalgte produkter. 5. Publikation af resultatet. Vi forventer herigennem at opbygge betydelig erfaring med at screene it-produkter og -løsninger ud fra et sikkerhedsperspektiv. Disse produktscreeninger kan i sig selv føre til en ydelse og vil ligeledes gøre det muligt for danske virksomheder at få evalueret deres produkt eller bestille evaluering af bestemte produkter eller nye produkttyper. Det vi vil lave kan forstås som en letvægtsudgave af Common Criteria (ISO 15408), som ikke er praktisk anvendeligt for denne type virksomheder[8]. <u>AP4 – Innovative løsninger</u>: På baggrund af vores aktiviteter i AP2+3 samt dialog med vores interessentnetværk forventer vi at kunne identificere "gaps", hvor der er behov for nye sikkerhedsløsninger. Her gives to eksempler på, hvad dette kunne være: 1. Brugervenlig konfiguration af SmartGrid-komponenter. Abstrakt set er det "let" at lave en sikker SmartGrid-infrastruktur. Dette problem er fx studeret i CHPCOM-projektet. Udfordringen er dog at SmartGrid-komponenter behandles af installatører og brugere som ikke har de store sikkerhedsforudsætninger, og det er derfor kritisk at brug og konfiguration er så brugervenligt som muligt. 2. Sikker samkøring af fortrolige data. Indenfor en række felter er der kendte begrænsning omkring samkøring af fortrolige data. Dette "gap" kan helt eller delvist adresseres vha teknikker fra Multiparty Computation. Vi forventer at kunne udvikle 1-2 ydelser i form af nye løsninger pr. år gennem dette arbejde. <u>AP5 – Videnspredning og forretningsudvikling</u> I denne arbejdspakke arbejdes der med videnspredning som beskrevet i afsnit 5). Derudover vil der væres fokus på forretningsudviklingsaktiviteter for de ydelser, som kommer ud af de øvrige arbejdspakker. Planen er her at inddrage forretningsudviklingsspecialister for at opnå de bedste resultater. I relation til de beskrevne aktiviteter og ydelser finder vi en række risici, som skal mitigeres: • Den endelige udformning af den kommende persondataforordning er endnu ikke kendt. For de fleste danske virksomheder vil det dog være for sent at reagere om 3 år, da lovgivningen her vil være trådt i kraft[9]. Derfor handler det om at have en fleksibel tilgang, som vi mener denne aktivitet har.

[8] Ifølge IT- og Telestyrelsen vejledning (http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/vejledninger/Pages/CommonCriteria.aspx) koster en evaluering typisk flere millioner DKK.

[9] http://www.bechbruun.com/da/Videncenter/Nyheder/2015/Juni/Et+skridt+taettere+paa+den+nye+persondataforordning

	• Opbakning fra tonegivende interessenter såsom Digitaliseringsstyrelsen, Erhvervsstyrelsen, brancheorganisationer m.v. Som det fremgår nedenfor har GTS-institutterne bag denne aktivitet et stærkt netværk inden for it-sikkerhed som inkluderer disse interessenter, og de vil blive inddraget i aktiviteten. • Der er en risiko for, at danske eller internationale aktører vil udbyde lignende services i aktivitetsplanens løbetid. I tilfælde af at dette sker, vil parterne interagere med de respektive virksomheder og tilpasse aktiviteten.
4) Vidensamarbejde og -hjemtagning	Alexandra Instituttet har allerede et nært samarbejde med Aarhus Universitet inden for it-sikkerhed. Det er forventningen, at denne aktivitet kan bruges som løftestang til at styrke samarbejdet med andre danske universiteters aktiviteter inden for it-sikkerhed (bl.a. DTU og ITU). Desuden er det planen at samarbejde med nationale spillere inden for it-sikkerhed (ikke mindst ifm. videnspredning), f.eks. Rådet for Digital Sikkerhed (hvor Alexandra Instituttet er repræsenteret i bestyrelsen) og DI/ITEK (hvor Alexandra Instituttet er repræsenteret i DIs it-sikkerhedsudvalg). Internationalt er det planen at hjemtage viden gennem deltagelse i konferencer og at samarbejde med internationale partnere gennem EU-projekter. Aktuelt er der samarbejde indenfor it-sikkerhed med bl.a. Bristol University, Cybernetica, Fraunhofer og SAP Research.Projekter i samarbejde med Goethe Universität Frankfurt og IBM Research Zürich er i støbeskeen. Ift. forskningsprojekter vil denne aktivitet bygge på viden etableret i en række afsluttede nationale og internationale forskningsprojekter, bl.a. ABC4Trust, COBE og CHPCOM samt tidligere resultatkontraktaktiviteter som ”Identitet på nettet i et globalt perspektiv” (2013-2015). Denne aktivitet vil have synergieffekter med flere eksisterende projekter, bla. PRACTICE (EU-projekt med fokus på Multiparty Computation), og BDbS (et projekt under Industriens Fonds Big Data-satsning) og CFEM. Vi ønsker at medfinansiere PRACTICE og CFEM med denne aktivitet. Derudover er der flere nye projekter i støbeskeen, blandt andet Emergent Identity System (Innovationsfonden), Privacy-enhanced Interoperable NEtwork of TRust E-sErvices (H2020) og Big Dandi (Inno+), som vi forventer vil have synergi med denne aktivitet. Såfremt disse ansøgninger går igennem, har vi ønske om at benytte denne aktivitet som medfinansiering. Ift. forskningsprojekter er det også planen at deltage i nye ansøgninger med afsæt i denne aktivitet. Endelig vil aktiviteten være i dialog med både Digitaliserings- og Erhvervsstyrelsen, både for at give input og for at sikre, at denne aktivitet er i tråd med deres tiltag.
5) Inddragelse og videnspredning	Vi vil etablere en interessentgruppe med deltagelse af danske virksomheder og organisationer, hvor vi vil tilstræbe at få deltagelse fra brugervirksomheder, leverandører, offentlige og private organisationer. Her vil vi invitere interesseorganisationer som DI/ITEK, Rådet for Digital Sikkerhed, Forbrugerrådet, FDIH (Foreningen for Dansk Internet Handel) m.fl. til at deltage i interessentgruppen. Interessentgruppen vil blive inddraget i den strategiske styring af projektet og vil f.eks. kunne få indflydelse på, hvilke produkttyper, der laves screening af, eller hvilker domæner, der fokuseres på ift. samkøring af data. (Dette er beskrevet ovenfor i afsnit 3). Ud over interessentgruppen vil vi bidrage med indlæg på større nationale konferencer, ligesom vi vil bidrage til aktiviteter afviklet af de relevante

	innovationsnetværk (IFFI, CenSec, InfinIT, Service Platform). Vi vil udarbejde vejledninger (evt. i samarbejde med partnere som DI/ITEK, Rådet for Digital Sikkerhed, m.fl.) og levere indhold til artikler i fagpressen (f.eks. version2.dk). De konkrete mål fremgår af milepælene. Det er svært at sætte præcist tal på målgruppen, da den grundlæggende består af alle danske virksomheder, som bruger it-løsninger eller systemer – ikke mindst SMV'er. Det er klart, at der vil ske en fokusering gennem projektet qua de produkter og løsninger, der bliver udvalgt, men det vil naturligvis blive tilstræbt at gå efter de emner der har størst effekt.
6) Sammenhæng med institutstrategi	Alexandra Instituttet har i en årrække haft it-sikkerhed og privacy som fokusområde, hvilket fremgår som et af de faglige "ben" i den seneste strategi. Aktiviteten spiller derfor en væsentlig rolle i Alexandra Instituttets fremtidige kommercielle forretning. Alexandra Instituttets Security Lab er nationalt førende ift. løsninger baseret på avanceret forskningsbaseret kryptografi og er ligeledes på højde med international forskning på området[10]. Security Lab fungerer desuden regelmæssigt som rådgiver for Digitaliseringsstyrelsen inden for dette domæne. DELTA har i mange år beskæftiget sig med produktsikkerhed. I takt med at devices bliver forbundet til nettet eller i systemer, efterspørger DELTAs kunder i høj grad services omkring cybersikkerhed af deres produkt. Aktiviteten ligger derfor i naturlig forlængelse af DELTAs services og er et vigtigt led i DELTAs fremtidige strategi. Det er en del af DBI's strategi at udvikle metoder og ydelser, som er til gavn for SMV'er. Den nye viden vil på sigt muliggøre en ydelse til SMV'er, hvor DBI vil kunne gennemgå og analysere medarbejderes brugeradfærd og dermed optimere virksomheden til at kunne imødegå it-sikkerhedsmæssige udfordringer med deres eksisterende og/eller nye systemer og løsninger. DBI har desuden 15 års erfaring med at sikre virksomheder, og det giver således god mening for DBI at være med i et sikkerhedsprojekt.
7) Milepæle år 1	<u>Vidensamarbejde, -hjemtagning- og kompetenceopbygning</u> • 4 publikationer om året (efter år 3: 8 Alexandra, 2 DBI, 2 Delta). Kan være whitepaper[11], forskningsartikel. Kan også være bidrag til vejledninger fra f.eks. DI/ITEK eller Rådet for Digital Sikkerhed. [AP1] • Deltagelse i mindst 2-4 internationale konferencer. [AP1] • Deltagelse i mindst 2 forskningsansøgninger. [AP1] <u>Udvikling af teknologisk service</u> • År 1 fokus på metode til screenings [AP2] • 2 screenings [AP3] • 1 udviklet løsning [AP4] <u>Inddragelse og vidensprednin</u>g • 2-3 møder med deltagere fra interessentgruppen (inkl. møder til fagligt arbejde i WP2+3+4). [AP5] Der opnås herunder en afklaring af de involverede GTS-institutters rolle ift. private rådgivere og leverandører mhp. at optimere synergi og komplementaritet og undgå

[10] Labchef Jakob Pagter har f.eks. været invited speaker hos både ISACA Nordic's årlige konference i Stockholm i 2013 og på Real World Crypto 2014 i New York (den førende konference inden for anvendt moderne kryptografi)
[11] Er som udgangspunkt interne/fortrolige og har sigte på den interne forankring af viden.

	konkurrenceforvridning. Den opnåede fælles forståelse sammenfattes skriftligt. • 20 medlemmer i interessentgruppe. [AP5] • Præsentation på mindst 1 national konference. [AP5] • 2 artikler distribueres til fagpressen. [AP5] • En offentlig workshop/konference. Fokus valgt i samarbejde med interessentgruppe. Kan afvikles i samarbejde med anerkendt partner (f.eks. Dansk IT). [AP5] <u>Andet</u> • Udvikling af forretningsmodel (Business Model Canvas) for mindst 1 potentiel ydelse. [AP5]
Milepæle år 2	<u>Vidensamarbejde, -hjemtagning- og kompetenceopbygning</u> • 4 publikationer om året (efter år 3: 8 Alexandra, 2 DBI, 2 Delta). Kan være whitepaper[12], forskningsartikel. Kan også være bidrag til vejledninger fra f.eks. DI/ITEK eller Rådet for Digital Sikkerhed. [AP1] • Deltagelse i mindst 2-4 internationale konferencer. [AP1] • Deltagelse i mindst 2 forskningsansøgninger. [AP1] <u>Udvikling af teknologisk service</u> • Metode til udvalgt domæne [AP2] • 4 screenings [AP3] • 2 udviklede løsninger [AP4] <u>Inddragelse og vidensprednin</u><u>g</u> • Kvartalsvis møde med deltagere fra interessentnetværk (inkl. møder til fagligt arbejde i AP2+3+4). [AP5] Herunder drøftes fælles forståelse af arbejdsdeling mellem aktørerne, jf. år 1. • 30 medlemmer i interessentgruppe. [AP5] • Præsentation på mindst 2 nationale konferencer. [AP5] • 3 artikler distribueres til fagpressen. [AP5] • En offentlig workshop/konference. Fokus valgt i samarbejde med interessentgruppe. Kan afvikles i samarbejde med anerkendt partner (f.eks. Dansk IT). [AP5] <u>Andet</u> Udvikling af forretningsmodel (Business Model Canvas) for mindst 3 potentielle ydelser. [AP5]
Milepæle år 3	<u>Vidensamarbejde, -hjemtagning- og kompetenceopbygning</u> • 4 publikationer om året (efter år 3: 8 Alexandra, 2 DBI, 2 Delta). Kan være whitepaper[13], forskningsartikel. Kan også være bidrag til vejledninger fra f.eks. DI/ITEK eller Rådet for Digital Sikkerhed. [AP1] • Deltagelse i mindst 2-4 internationale konferencer. [AP1] • Deltagelse i mindst 2 forskningsansøgninger. [AP1] <u>Udvikling af teknologisk service</u> • Metode til udvalgt domæne [AP2] • 4 screenings [AP3] • 1 udviklet løsning [AP4]

[12] Er som udgangspunkt interne/fortrolige og har sigte på den interne forankring af viden.
[13] Er som udgangspunkt interne/fortrolige og har sigte på den interne forankring af viden.

	<u>Inddragelse og videnspredning</u> • Kvartalsvis møde med deltagere fra interessentnetværk (inkl. møder til fagligt arbejde i WP2+3+4). [AP5] Herunder drøftes fælles forståelse af arbejdsdeling mellem aktørerne, jf. år 1. • 40 medlemmer i interessentgruppe. [AP5] • Præsentation på mindst 2 nationale konferencer. [AP5] • 3 artikler distribueres til fagpressen. [AP5] • En offentlig workshop/konference. Fokus valgt i samarbejde med interessentgruppe. Kan afvikles i samarbejde med anerkendt partner (f.eks. Dansk IT). [AP5] <u>Andet</u> Udvikling af forretningsmodel (Business Model Canvas) for mindst 4 potentielle ydelser. [AP5]
Titel ved præsentation på BedreInnovation.dk	Sikkerhed- og Privacy-by-Design