Standarder, test og certificering

A. INDLEDENDE OPLYSNINGER	
Aktivitetsområde	Indsatsområdet Digital sikkerhed, tillid og dataetik
Institut	Alexandra Instituttet (Lead) og FORCE Technology
Titel *Dækker indholdet af aktiviteterne*	Standarder, test og certificering
Nummerering *Af beskrivelsen*	2
Version	1
Periode *Forventet start og slut*	1/1 2021-31/12 2021
Kontaktperson	Kristian Krämer

B. ÆNDRINGER
Angiv her, hvis en planlagt aktivitet er ændret i forhold til den forudgående version af beskrivelsen.

C. BESKRIVELSE	
1. Mål *Hvorfor?* Hvad er målet for aktiviteterne? Hvordan bidrager de til det overordnede mål for aktivitetsområdet?	Denne aktivitet vil fortsætte og udvide Alexandra Instituttets og FORCE Technology's involvering i certificering indenfor, og standardisering af, nye avancerede digitale teknologier, og bidrage til de overordnede mål omkring dette i indsatsområdet. Standarder kan hjælpe virksomheder med at navigere i de forskellige sikkerhedsniveauer, specifikationer af systemers adfærd og fremtidig regulering omkring ansvarlig og tillidsskabende AI. Dette giver dem redskaber til at placere sig selv og deres produkter på korrekte niveauer – noget, vi ved fra virksomhederne (især SMV'erne), kan være en stor udfordring. Desuden er standarder en måde for virksomheder at kommunikere deres produkters egenskaber med deres kunder, hvilket er vigtigt, da vi begynder at se flere og flere krav fra kunder om, at produkter skal leve op til visse standarder. Konkret vil dette aktivitetsområde bidrage til indsatsområdet overordnede mål med en eller flere virksomhedscases og et eller flere nye samarbejder med vidensinstitutioner fx gennem F&I ansøgninger. Det vil desuden udbygge og udvikle digitale test- og certificeringsfaciliteter indenfor cybersikkerhed med fokus på sikkerhed produkter og systemer, og stille dette til rådighed som en teknologisk service.
2. Indhold *Hvad* skal der ske? Hvilke(n) konkret(e) aktiviteter udføres?	Standardiseringsarbejde – Arbejde i standardiseringsudvalg i Dansk Standard, i EU-regi (f.eks. CEN/CELEC) og internationalt (f.eks. ISO) og viden-hjemtagning fra internationale standarder (f.eks. NIST). Bidrag og overvågning af standarder og fremtidig certificering inden for NLP, kunstig intelligens, cybersikkerhed i IoT og OT på produkt- og systemniveau, cybersikkerhed generelt og avanceret kryptografi. Etablering af aktivt samarbejde med Mærkningsordningen for It-sikkerhed og Ansvarlig Dataanvendelse Certificering - Vi forventer at kunne certificere efter ETSI EN 303 645 "Cyber Security for Consumer Internet of Things: Baseline Requirements" baseret på ETSI EN 103

	701 efter det første år. Vi vil fra start desuden arbejde på at kunne certificere efter standarder inden for IEC 62443. Certificering vil ske i samarbejde mellem de to GTS-institutter. Alexandra Instituttet vil i forbindelse med disse aktiviteter arbejde på at blive Akkrediteret Test Lab indenfor cybersikkerhed, dette arbejde vil Alexandra Instituttet påbegynde i denne periode. Udvikling og afprøvning af teknologiske services indenfor disse aktiviteter vil blandt andet ske gennem et eller flere case forløb med virksomheder.
3. Aktører *Hvem* udfører aktiviteterne? Hvilken afdeling af instituttet? Evt. hvilke eksterne parter er med (videninstitutioner, virksomheder, erhvervsorganisationer, myndigheder, klyngeorganisationer eller andre).	Direkte involverede GTS Institutter: • Alexandra Instituttet A/S: Security Lab, People Technology and Business Lab og Artificial Intelligence and Data Analysis Lab. Alexandra tilføjer faglig viden omkring cybersikkerhed og kunstig intelligens og projektledelse. • FORCE Technology Product Compliance, der tilføjer viden om standarder og certificeringer. • Samarbejde gennem Nordic IoT Center. Eksterne parter: • Dansk Standard • Mærkningsordningen for It-sikkerhed og Ansvarlig Dataanvendelse • Erhvervsstyrelsen /CFCS – i forbindelse med EU's cybersikkerhedsforordning. Erhvervsstyrelsen/CFCS repræsenterer DK i forbindelse med cybersikkerhedsforordningen, vi vil derfor forsøge at samarbejde med dem omkring udbredelse af viden om denne. • Erhvervsorganisationerne DI og DE
4. Sammenhæng med andre projekter (evt.) Indgår aktiviteten i andre eksternt finansierede projekter?	Denne aktivitet har sammenhæng med disse RK-indsatsområder: Digitale teknologier til datadrevet, bæredygtig vækst (Alexandra Instituttet) IoT-drevet forretningsdesign (FORCE Technology og Alexandra Instituttet Eksternt finansierede projekter: • CIDI: Cyber secure IoT in Danish Industry (Industriens Fond). Projektets formål er at støtte danske IoT producenter med cybersikkerheden i produkterne bla. gennem brug af standarder. • Sb3D: Security by Design in Digital Denmark (Industriens Fond). Projektets formal er at øge brugen af Security by Design i IT-løsninger. • Nyt projekt - Der vil i dette projekt være afsat midler til en mulig ansøgning indenfor området.
5. Følgegruppe Har følgegruppen forholdt sig til aktiviteten? I så fald hvordan? Hvis ikke, hvornår forventes følgegruppen at blive præsenteret for aktiviteten? (Det sidste bør kun gælde under opstarten af indsatsområdet).	Samarbejdet med følgegruppen i denne aktivitet sker gennem aktiviteten *Demonstration af anvendelighed og værdiskabelse ift. indsatsområdet Digital sikkerhed, tillid og dataetik,* hvor risikostyring omkring potentiel konkurrence også vil blive håndteret. Denne aktivitet leverer desuden dyb fagligt og relevant indhold og oplæg til teknologisk services, som følgegruppen efterfølgende forholder sig til. Følgegruppen vil formentligt blive differentieret i forhold til faglig interesse fx opdelt mellem cybersikkerhed og kunstig intelligens.
6. Formidling af resultater (evt). Hvordan/hvor kan interesserede virksomheder og andre få viden om resultaterne af aktiviteterne? (Anføres/tilføjes hvis det ikke allerede fremgår af beskrivelsen ovenfor, f.eks. ved links til konferencer, hjemmeside, publikationer etc.).	Hovedparten af formidlingen i denne aktivitet sker gennem aktiviteten *Demonstration af anvendelighed og værdiskabelse ift. indsatsområdet Digital sikkerhed, tillid og dataetik,* hvor denne aktivitet leverer fagligt indhold. En del af formidlingen vil dog ske direkte gennem standardiseringsarbejdet. OPDATERING: Væsentlige aktiviteter og resultater opnået i 2021: • Case omkring IoT sikkerhed efter ETSI EN 303 645 og ETSI TS 103 701

	• Udgivelse af specifikation i samarbejde med Dansk Standard: DS/PAS 2600:2021, Cybersikkerhed i produkter (IoT) • Input til kommende specifikation omkring virksomheders resiliens i samarbejde med bl.a. Danske Standard og DBI. • Opdateret rapport omkring Lightweight Cryptography inkl. standardisering af dette • Opdateret rapport omkring Post-quantum Cryptography inkl. standardisering af dette. • Udbygning af test of certificeringsfaciliteter omkring: ETSI EN 303 645, ETSI TS 103 701 og IEC 62443