Standarder og kritiske systemer

A. INDLEDENDE OPLYSNINGER	
Aktivitetsområde	Indsatsområdet Digital sikkerhed, tillid og dataetik
Institut	Alexandra Instituttet (Lead) og FORCE Technology
Titel *Dækker indholdet af aktiviteterne*	Standarder og kritiske systemer
Nummerering *Af beskrivelsen*	2
Version	1
Periode *Forventet start og slut*	1/1-2022-31/12-2022
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 Alexandra Instituttets og FORCE Technology's involvering i certificering, og standardisering af, nye avancerede digitale teknologier for øget cybersikkerhed Når virksomheder begynder at arbejde mere seriøst med sikkerhed, bliver forskellige standarder ofte involveret. Dette gøres for både at sikre at det implementerede sikkerhedsniveau ligger på niveau med best practice og for at kunne dokumentere sikkerhedsniveauet for eksterne interessenter. Særligt i forbindelse med kritiske systemer er grundig dokumentation ofte en nødvendighed, da virksomheden selv, eller dens kunder, ofte er omfattet af regulering såsom NIS-direktivet (og/eller opdateringen NIS2) Konkret vil aktivitetsområdet have et fokus på hvordan virksomheder kan anvende standarder i praksis, hvorved de kan dokumentere deres implementerede sikkerhed. Dette vil opnås gennem virksomhedscases, hvor virksomheder bl.a. hjælpes med at udvikle den nødvendige dokumentation således forskellige, almene sikkerhedsfunktioner kan valideres ud fra en dertil udviklet testplan. De resulterende værktøjer, processer og erfaringer vil være grundlaget for aktivitetens videnspredning.
2. Indhold *Hvad* skal der ske? Hvilke(n) konkret(e) aktiviteter udføres?	Fortsat standardiseringsarbejde – Arbejde i standardiseringsudvalg i Dansk Standard, i EU-regi (f.eks. CEN/CELEC) og internationalt (f.eks. ISO), gennem S-441 udvalget, både som bidrag til og overvågning af relevant standarder. For at hjælpe virksomheder med at komme i gang med arbejdet omkring validering af deres sikkerhedsfunktioner vil der blive udviklet en række eksempler på fremgangsmåder og dokumentationsformer for hvordan dette kan opnås. Her er der fokus på hvordan men kommer fra kravspecifikation til en testet, valideret og dokumenteret funktion.

	Indgåelse af nyt samarbejde med EnergiCERT og/eller en anden aktør indenfor kritisk infrastruktur, eksempelvis sundhedsdatastyrelsens DCIS eller andre DCIS'er. Formålet med disse samarbejder er at identificere konkrete udfordringer for virksomhederne indenfor kritisk infrastruktur. Samarbejdet forventes at have et overlap med sporet "Sikker brug af følsomme data", idet opsamling af data til beskyttelse af (kritiske) systemer i sig selv kan indebære en risiko, der kan mitigeres ved brug af teknikker beskrevet i "Sikker brug af følsomme data" sporet. Fortsatte virksomhedscases omkring ETSI EN 303 645 test efter ETSI EN 103 701. Ønske om yderligere 1-3 cases, før en egentlig service for "verifikation efter standard" er moden. Processen dokumenteres med henblik på en DANAK-akkreditering. Ligeledes udbygges samarbejdet med D-mærket, således processer og dokumentation kan genbruges hvor muligt.
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, Human Insights Lab, Artificial Intelligence and Data Analysis Lab, samt det tværgående team Research & Innovation. • FORCE Technology Product Compliance. • Samarbejde gennem Nordic IoT Center. Eksterne samarbejdspartnere: • Dansk Standard • Innovationsnetværkene MADE, CenSec og DigitalLead • D-Mærket • Erhvervsstyrelsen /CFCS – i forbindelse med EU's cybersikkerhedsforordning. • EnergiCERT • Erhvervsorganisationerne DI og DE • Universiteter, vi har allerede samarbejder med: AAU, DTU, ITU og AU
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 formål er at øge brugen af Security by Design i digitale produkter og løsninger. • SIOT: Secure Internet of Things – Risk analysis in design and operation (Innovationsfonden DIREC) projektets formal er værktøjer til risikoanalyser indenfor cybersikkerhed. • Crucial: Projektets formål bl.a. opdagelse af kompromitterede systemer indenfor kritisk infrastruktur, primært vand og el. • 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).	I den forgående periode har vi været i løbende dialog med både virksomheder, rådgivere, offentlige organisationer og universiteter gennem indsatsens netværks- og følgegrupper. Her har vi bredt identificeret markedsmæssige udfordringer og problemområder, som i dag ikke bliver dækket af teknologiske services. I den kommende aktivitetsperiode vil vi etablere 3 mindre følgegrupper (én for hver aktivitetsbeskrivelse), der vil være mere agile i forhold til den løbende dialog omkring markedssituationen og indsatsområdets aktiviteter.

	I denne aktivitet etableres en specifik følgegruppe med fokus på standarder og kristiske systemer. Følgegruppen sammensættes af aktører på tværs af private virksomheder, offentlige organisationer og vidensinstitutioner, der kan bidrage positivt ind i samtlige aktiviteter. Konkurrencesituationen vil desuden vendes løbende på møder med følgegruppen, så det sikres at der ikke udvikles komponenter og services der er konkurrenceforvridende. Aktivitetsbeskrivelsen er sendt i "e-mail/telefonisk høring" i følgegruppen, forinden den er uploadet på Bedreinnovation.dk. Hen over perioden præsenteres følgegruppen for fremdrift på aktiviteten på følgegruppemøderne og i den løbende ad hoc dialog.
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 resultater og erfaringer i denne aktivitet vil blive formidlet gennem aktiviteten *Demonstration af anvendelighed og værdiskabelse* ift. indsatsområdet *Digital sikkerhed, tillid og dataetik,* i form af videnskabelige artikler, white papers, blog posts og oplæg på konferencer eller webinarer hvortil denne aktivitet leverer fagligt indhold. En del af formidlingen vil dog ske direkte gennem standardiseringsarbejdet. De udviklede ydelser vil også stilles til rådighed for markedet gennem den digitale TDU. OPDATERING: Væsentlige aktiviteter og resultater opnået i 2022: • 1 nyt forskningsprojekt ved Industriens Fond: CyPro omkring sikring af IoT • Kompetenceopbygning omkring radioudstyrsdirektivet (RED) og CyberResilience Act (CRA) • Input til lovforslaget CRA • Afvikling af caseforløb omkring ETSI 303 645 og 103 701 • Udvikling af guides omkring risikostyring (med DS), samt risiko og trusselsmodellering