

Sammenlignende oversigt

Tilgangen i nuværende L93 vs. frivillige tilvalgsløsninger til etablering af trustworthy ansvarlig sikkerhed uden overvågning baseret på en udbygning af MitID med Trustworthy PKI, biometriske borgerkort og CitizenKey

Hensyn	Nuværende Tele/MitID	MitID udbygget med Trustworthy PKI / CitizenKey
Princip	Sikkerhed baseret på overvågning via infrastrukturen Fokus på at varetage og prioritere sekundære hensyn	Trustworthy forebyggende sikkerhed uden overvågning. Fokus på at sikre borgeren, borgernes selvbestemmelse og retssikkerhed først og dernæst sekundære hensyn
Identitetssikkerhed	Lav/middel - Man kan ikke være sikker på hvem der bruger et kommunikationsmiddel. - MitID kan ikke lave NSIS Høj til f.eks. Betroede ansatte - Borgerne har ikke egenkontrol over nøgler.	Altid Høj - Altid stærk integritet - Alle transaktioner er NSIS Høj - Borgerne får via et Borgerkort (biometrisk chipkort) egenkontrol over nøgler, dvs. identitetstyveri forebygges
CyberSecurity	Lav/middel - Når man stripper borgernes og devices sikkerhed for at kunne overvåge dem, skaber man optimale strukturer for cyberangreb. - Overvågning kan gribe ind og skabe modangreb - Men Overvågning sikrer ingen og er i sig selv et angreb.	Høj - Man kan ikke angribe nogen eller noget, man ikke kan genkende eller sigte efter. - Trustworthy strukturer betyder at selv enkeltstående succesfulde angreb ikke kan eskalere. Små fejl bliver ikke til store nedbrud eller smitter. - Usikrede systemer og devices kan ”pakkes ind” med et <aktivt totalforsvar uden overvågning> indtil systemer eller Devices opgraderes.
Forebygge BigTech / Overvågningskapitalisme	Lav - Kravet om identifikation af devices stripper borgernes sikkerhed mod opsamling og misbrug af persondata - Overvågning underminerer markedsdannelsen	Høj - Trustworthy PKI muliggør datadeling uden borgeren reduceres til produktet - Løser Schrems II problemet / ingen persondata i udenlandske cloud

Ansvarlighed	Lav • Kriminelle stjæler andres identitet for at omgå overvågningen • Der er ingen 1:1 kobling mellem device og bruger	Høj • Uanset kommunikationsform, så vil Biometriske Borgerkort være låst til brugeren på tværs af devices • Mulighed for nuancerede krav som tilpasses situationen
Politiets adgang til efterforskning af alvorlig kriminalitet	Lav / middel • De kriminelle kan omgå overvågningen. • Borgerne kan ikke beskytte sig mod identitetstyveri, fordi nøglekontrollen ligger centralt	Høj • Kriminelle vil ikke bruge CitizenKey fordi personen altid kan gøres ansvarlig for handlingen. • Dommeren kan ”plukke” transaktioner begået af den samme person ud af høstakken af handlinger. • Nøgler kan ikke overføres, dvs.
Forebyggelse af kriminalitet	Lav • Kriminelle har let adgang og ved hvordan man omgå sikkerheden. • Borgerne og systemer har svært ved at beskytte sig	Høj • Kriminelle kan ikke få adgang til nøgler til at få adgang uden at inkriminere sig selv. • Nuancerede krav til sikkerhed som tilpasses til situationen – større sårbarhed → større krav. • Transaktionen styrer sikkerhed, f.eks. kan man forebygge moms/skattesvindler fordi betalingen indbygget skaber et moms/skatte-ansvar • Borgere og systemer sikres by design
Omkostninger	Dyr og bureaukratisk • Overvågning kræver omfattende ekstraressourcer som både belaster statskassen og teleselskaberne • Logningsdata er sensitive og skal beskyttes mod sekundær misbrug	Billig og fri • Trustworthy logning udnytter at digitalisering alligevel registrerer data i transaktionen • Trustworthy sikre data er frie og kan deles og genbruges uden begrænsninger ligesom de kan lagres uden særlige krav til sikkerhed eller begrænsninger • Markedsfinansieret via effektivisering uden driftstilskud fra statskassen

Retssikkerhed	Dårlig • Overvågning skaber mistillid, fordi overvågning underminerer sikkerheden både i forhold til kommercielle, bureaukratiske og andre strukturer. • Databaser med persondata er vanskelige at sikre og nemme at misbruge uden sporbarhed. • Strukturen er fastlåst i en negativ spiral • Ifølge GDPR skal persondata slettes hurtigst muligt.	Stærkt og sikret by design • Ingen overvågning • Dansk jurisdiktion og lovgivning kan indbygges – selv i forhold til cloud, blockchain og cyberspace • Klare regler og mulighed for at nye bedre tilpassede versioner kan fungere parallelt med gamle strukturer. • Trustworthy sikkerhed fint sameksistere med de nuværende Overvågningsstrukturer • Kontrollen over borgernes data forbliver indenfor jurisdiktionen • Indenfor jurisdiktionen forbliver kontrollen hos borgeren indtil dommeren eventuelt åbner • Når data ikke skabes som identificerede persondata kan data eksistere så længe de kan skabe værdi for nogen, f.eks. forskning
Teleselskabers mulighed for at konkurrere	Stærkt begrænset med unfair konkurrencebetingelser i forhold til BigTech. • Nuværende telelovgivning baseret på telestandarder med indbygget overvågning lægger stærke begrænsninger og store omkostninger på teleselskaber. • Over-the-top teleselskaber løber med gevinsterne, fordi teleselskaberne fodrer identificerede borgere til BigTech, f.eks. cookie, Skype og Google. • Forbrugerne pålignes store ekstraomkostninger	Indbygget fair konkurrence • Når hver transaktion er isoleret, stilles konkurrencen lige og bedste løsning til prisen vinder. • Teleselskaber kan konkurrere på lige fod med over-the-top

Andre forhold	• Grundlæggende uforeneligt med menneskerettigheder / EU lovgivning • Fastlåser i stive strukturer og standarder med dårlig understøttelse af innovation, opgradering og konkurrence på ny eller anderledes funktionalitet • Dårlig dataetik	• Kan etableres indenfor gældende lovgivning (f.eks. eIDAS, GDPR) og standarder (f.eks. ETSI PKI) • Understøtter credential-baseret identitet såsom eIDAS 2.0 / EU Digital Wallet / SSI under overvejelse i EU Kommissionen og igangværende interoperabilitet mellem Tyskland og Spanien • Understøtter gradvis opbygning og modning • Understøtter semantisk interoperabilitet og sameksistens mellem flere standarder på samme tid, dvs. så man indfører mulighed for evolutionær udvikling i digitale strukturer • Tømmer gradvis legitime transaktioner fra den nuværende <grå kasse> over i pre-validerede <hvide rum>, så stadigt flere ressourcer kan fokusere på de tilbageværende transaktioner i den <grå kasse> • Kræver bedre koordinering og nye supportstrukturer (Citizen First) • Dataetik indbygget via design
---------------	--	---