FOI
Totalförsvarets forskningsinstitut

Vid korrespondens åberopa
FOI beteckning

Datum
2024-01-22

Nr FOI-2023-1892

Finansdepartementet
Regeringskansliet
103 33 Stockholm

Er referens
fi.remissvar@regeringskansliet.se
fi.ofa.dof.remisser@regeringskansliet.se

Vår handläggare
Daniel Eidenskog

Remissvar gällande SOU 2023:61 En säker och tillgänglig statlig e-legitimation

Sammanfattning av FOI:s synpunkter

Totalförsvarets forskningsinstitut (FOI) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på betänkandet. Remissvaret utgår huvudsakligen från två perspektiv: totalförsvar och informations-/cybersäkerhet.

FOI tillstyrker förslaget som lämnas i betänkandet. Dock anser FOI att utredningen har underskattat den komplexitet och därmed de kostnader som de säkerhets-relaterade aspekterna för systemet innebär. Därtill finns ytterligare ett antal synpunkter och kommentarer på förslaget som FOI anser behöver hanteras för att en statlig e-legitimation ska kunna fullgöra sitt syfte på ett tillförlitligt och säkert sätt.

Det är bra att det införs en statlig e-legitimation på högsta tillitsnivå. Exempelvis har staten ett viktigt ansvar i att motverka digitalt utanförskap. I dagens digitala samhälle blir tillgången till en e-legitimation alltmer avgörande för stora delar av befolkningens vardag samtidigt som det finns befolkningsgrupper som inte kan få tillgång till någon av de befintliga kommersiellt tillgängliga e-legitimationerna. En statlig e-legitimation kan också utgöra en signifikant faktor för ett det digitaliserade samhället ska fortsätta fungera i händelse av exempelvis krig.

FOI anser att informations- och cybersäkerhetsfrågorna inte har omhändertagits tillräckligt väl i betänkandet. En statlig e-legitimation på högsta tillitsnivå med de sociotekniska system som krävs för denna kommer att vara utsatt för en omfattande hotbild samtidigt som konsekvenserna av angrepp kan bli mycket stora. Dessutom är målbilden att systemet även ska fungera under svåra påfrestningar, höjd beredskap

Postadress
FOI
164 90 STOCKHOLM

Besöksadress
Gullfossgatan 6, Kista
Leveransadress
Gullfossgatan 12, Kista

Telefon
08-55 50 30 00

Fax

registrator@foi.se
Orgnr: 202100-5182
www.foi.se

och krig. Säkerhetsaspekterna behöver därmed tas på mycket stort allvar och säkerhetsarbetet måste ges de förutsättningar som krävs.

Övergripande kommentarer

Nedan följer de övergripande kommentarer som FOI har på betänkandet. Dessa kommentarer berör innehåll som är spritt på flera ställen i betänkandet och kan därmed inte hänföras till ett enskilt avsnitt.

Totalförsvaret

Utredningen har kommit fram till att den statliga e-legitimationen ska fungera även under svåra påfrestningar, höjd beredskap och krig, vilket ger stor påverkan på kravbilden avseende exempelvis robusthet och säkerhet i systemet. Vilken kravbild som systemet måste uppfylla beror på vilka typer av situationer som systemet ska klara av. Det är därför av stor vikt att berörda myndigheter tidigt tar fram en analys av de situationer som systemet ska hantera, exempelvis utifrån olika scenarier. Detta ger underlag för att kunna fastställa en gemensam målbild avseende aspekter såsom informations- och cybersäkerhet, redundans, underleverantörer, försörjnings-beredskap samt personalsäkerhet.

Kommersiella aktörer inom IT-området kan normalt sett inte förväntas bygga system som ska fungera i en krigssituation då det oftast är alltför kostnadsdrivande för att vara kommersiellt gångbart. En säker och robust statlig e-legitimation kan därmed vara en signifikant faktor i att det digitala samhället kan fortsätta att fungera även i krig. Dock förutsätter det att en tillräckligt stor andel av befolkningen har en sådan e-legitimation. Staten bör därför eftersträva att så stor andel av befolkningen som möjligt har en statlig e-legitimation, exempelvis genom att framtida nationella id-kort även inkluderar e-legitimation.

Målsättningen att den statliga e-legitimationen ska fungera även i krig kan medföra att samhällskritiska system hos förlitande parter utformas utifrån att e-legitimationen i princip alltid är tillgänglig. Denna typ av beroende från de förlitande systemen kan ge risker för att förlitande system i praktiken blir oanvändbara om den statliga e-legitimationen inte klarar av att uppfylla sina säkerhetsmål. Utifrån detta perspektiv är det således viktigt att den statliga e-legitimationen håller hög tillgänglighet. Det är också viktigt att de förlitande systemen har en reservplan för att kunna hantera situationer där e-legitimationen inte är tillgänglig även under längre perioder.

Utredningsdirektiven tar upp kostnadseffektivitet som ett mål för utredningen. Beroende på tolkning av ordet kostnadseffektivitet kan detta stå i konflikt med totalförsvarsperspektivet och att den statliga e-legitimationen ska fungera även i krig. Det är viktigt att systemet redan från början ges de ekonomiska förutsättningar som krävs för att nå den säkerhetsnivå som behövs för att uppnå säkerhets- och tillförlitlighetsmålen.

Informations- och cybersäkerhet

En sådan statlig e-legitimation som föreslås i betänkandet utgör ett mycket komplext socioteknisk system som dessutom har många olika externa beroenden och hög exponering mot andra system och yttre aktörer. Hotbilden mot ett sådant system måste antas vara mycket hög, där såväl främmande makt som kriminella har intressen av att angripa systemet. Systemet är dessutom av central betydelse för tilltron till svenska legitimationer och därmed tilltron till de identiteter som verifieras genom systemet. Brister i systemet för den statliga e-legitimationen kan även påverka andra e-legitimationer som givits ut genom id-växling från en statlig e-legitimation. Konsekvenserna av ett angrepp kan således bli mycket omfattande och kostsamma. Systemet måste därför hålla en mycket hög säkerhetsnivå och bör utformas och förvaltas i samverkan med relevanta expertmyndigheter för att minimera samhällsrisker, cybersäkerhetsrisker och risker för brott (såsom bedrägerier). Relevanta myndigheter att ta med i samarbetet är bland annat Polismyndigheten, Säkerhetspolisen, Försvarsmakten, FRA, MSB och FOI. Ett tydligt exempel där expertmyndigheterna bör vara delaktiga är valet av kryptoalgoritmer och kryptografiska lösningar som bör göras i nära samråd med Militära underrättelse- och säkerhetstjänsten (MUST) vid Försvarsmakten för att nå en lämplig utformning som även är framtidssäker (t.ex. avseende kvantdatorer).

Betänkandet är otydligt i frågor som berör hur informations- och cybersäkerheten ska säkerställas för systemet som helhet. Betänkandets fokus i dessa frågor tycks vara på bärarkorten, men bäraren utgör bara en liten del av helheten som även inkluderar centrala tjänster, databaser, mobilappar samt andra funktioner och tjänster som samtliga måste hålla adekvat säkerhetsnivå. Vissa delar av systemet kommer sannolikt att omfattas av krav på säkerhetsskydd. Vissa delar av systemet, såsom utfärdarens privata nycklar (eller motsvarande), måste skyddas synnerligen väl.

Betänkandet nämner ledningssystem för informationssäkerhet enligt ISO 27001 som en möjlig väg att uppnå bättre styrning av informations- och cybersäkerhetsarbetet samt ökad tillit och förtroende för utfärdaren. FOI vill poängtera att det finns ett stort glapp mellan den processorienterade säkerhet som nås med standarder såsom ISO 27001 och den faktiska säkerhet som krävs för att skydda system med den hotbild som kan antas mot det aktuella systemet. Även mer tekniskt orienterade säkerhetsstandarder såsom ISO 15408 (Common Criteria) har svårt att ge den nivå av säkerhet som krävs i praktiken för komplexa system med hög hotbild.

FOI anser att de utgiftsbedömningar som tas upp i betänkandets avsnitt 9.5 inte tar höjd för de säkerhetskrav som indikeras av utredningen. Mer om detta återfinns nedan under rubriken *Avsnitt 9.5, Förslaget om ansvar för utfärdande av en statlig e-legitimation*.

Ansvarsfördelning

FOI anser att det är bra att ansvaret för grundidentifiering läggs hos de som är mest erfarna och kunniga inom detta område samt redan har det som sin dagliga syssla. Genom att lägga detta ansvar hos Polisen och Utlandsmyndigheterna/UD uppnås en likvärdig säkerhetsnivå i grundidentifieringen som för nationella id-kort och pass. Samtidigt innebär det att hanteringen av den statliga e-legitimationen delas på flera myndigheter vilket kan leda till oklarheter i ansvarsfördelningen mellan de olika myndigheterna. Ett exempel är fördelningen av såväl ansvar som befogenheter för respektive organisation vid en säkerhetsincident, där oklarheter kan göra att viktiga åtgärder faller mellan stolarna eller att brådskande åtgärder försenas.

I utredningens förslag ligger förvaltningsansvaret för systemet hos Digg. FOI har anledning att ifrågasätta om Digg i sin nuvarande skepnad har förmåga att förvalta ett så pass komplext och säkerhetskritiskt system som en statlig e-legitimation. Samtidigt är det inte nödvändigtvis Digg som sköter driften av systemet. Om någon annan sköter driften uppstår ytterligare gränsytor där ansvarsfördelningen kan bli oklar. Att systemet ska fungera även vid höjd beredskap och krig ställer mycket stora krav på driftorganisationen och på samarbetet mellan förvaltning och drift. Kravställning av säkerhet är generellt sett svårt vilket innebär att gränsytan mellan de olika organisationerna blir kritisk, speciellt i de fall där kommersiella aktörer upphandlas för att hantera funktioner i systemet. En viktig notering är att upphandling till lägsta pris sällan premierar leverantörer som prioriterar säkerheten. Fördelning av ansvar, befogenheter och beredskap utgör viktiga avtalsfrågor som måste utredas.

Motverka kriminalitet

Målsättningen att den statliga e-legitimationen ska utformas, utfärdas och fungera på sätt som motverkar bedrägeribrott är viktig för att säkerställa medborgarnas tilltro till den statliga e-legitimationen. FOI anser att även fingeravtryck och därtill hörande biometri bör lagras i utfärdarens databas samt kunna användas vid sökningar i samband med utfärdande av identitetshandlingar. Syftet med detta är att kunna kontrollera identiteten i samband med utfärdande av nya identitetshandlingar där fingeravtryck ger en säkrare och mer distinkt kontroll som exempelvis kan motverka utfärdande av identitetshandlingar för flera identiteter till en fysisk person. Tillåten användning av lagrade fingeravtryck bör i stället begränsas genom lag till endast detta ändamål. Sådan lagring och behandling anser FOI vara motiverad och bör rimligtvis vara förenligt med EU-lagstiftning då den återfinns i motsvarande lagstiftning i exempelvis Finland.[1]

[1] Finlands Lag om identitetskort (25.8.2016/663), 9 a §

Kommentarer per avsnitt

FOI:s resterande synpunkter presenteras nedan och följer betänkandets disposition.

Kapitel 1. Författningsförslag

27 §: Försvarsmyndigheterna bör få egen rådighet över vilka tjänster de använder för att kunna möta de speciella säkerhetsbehov som finns inom försvarsområdet. FOI föreslår att ett undantag införs i likhet med undantaget i förordning 2023:709, 3 §, som träder i kraft 2025-01-01. Där undantas Inspektionen för strategiska produkter, Regeringskansliet, Säkerhetspolisen och myndigheter som hör till Försvarsdepartementet från kravet på att använda tjänster för identifiering som tillhandahålls inom auktorisationssystemet för tjänster för elektronisk identifiering och för digital post.

Avsnitt 7.2.2, Den statliga e-legitimationen ska tillhandahållas på ett kontaktlöst kort

FOI håller med om bedömningen att ett kontaktlöst kort är den lämpligaste bäraren för en e-legitimation på högsta tillitsnivå. FOI håller även med utredningen om att det snarast möjligt även ska vara möjligt att ge ut den statliga e-legitimationen på ett fysiskt identitetskort och då lämpligtvis det nationella id-kortet. Detta bör underlätta spridningen av den såväl den statliga e-legitimationen som det nationella id-kortet bland befolkningen vilket i sin tur förbättrar befolkningens beredskap i händelse av krig (se rubrik *Totalförsvaret*).

Avsnitt 7.2.4, Den statliga e-legitimationen ska utformas för att tillåta anpassningar och innehålla personlig prägel

Ordvalet ”personlig prägel” är olyckligt då det är en väletablerad fras som betyder något annat än vad som avses i betänkandet. Lämpligare ordval vore ”fysiska kännetecken” eller ”prägling”.

Avsnitt 7.2.5, Säker utformning av den statliga e-legitimationen

Den refererade NISU-utredningen presenterades 2015, det vill säga innan mycket av den pågående utvecklingen inom post-kvantkrypto. Resultaten från utredningen kan därmed åtminstone delvis anses som föråldrade. Val av kryptoalgoritmer och utformning av kryptologiska funktionskedjor är mycket svårt utan expertkunskaper. FOI anser därför att val av kryptoalgoritmer och utformning av kryptologiska lösningar för den statliga e-legitimationen måste göras i samråd med Försvarsmakten/MUST. Den kryptologiska utformningen kan bli delvis dimensionerande för den tekniska lösningen, varför samråd bör sökas redan tidigt i processen.

Avsnitt 7.2.6, Den statliga e-legitimationen ska innehålla vissa biometriska uppgifter om innehavaren

Utredningens förslag att lagen ska ta höjd för eventuell framtida biometrisk identifiering är bra. Lagstiftning bör inte utformas utifrån dagens tekniska begränsningar, utan på ett teknikneutralt sätt utifrån de ändamål och de ramar som lagen ska tillåta.

Avsnitt 7.6.3, Myndigheten för digital förvaltning ska ansvara för att utfärda den statliga e-legitimationen

FOI håller med utredningen om att det är problematiskt att Digg tilldelas tillsynsansvar inom e-legitimationsområdet samtidigt som de är såväl utfärdare av den statliga e-legitimation som förvaltningsansvariga för olika system inom e-legitimationsområdet. Den organisatoriska lösningen som gjorts hos FMV utgår från en betydligt mer begränsad problembild, där det handlar om två relativt små organisationsenheter i en stor organisation. I fallet med e-legitimationerna anser FOI att tillsynsansvaret bör ligga hos en annan myndighet än Digg för att säkerställa oberoende. Tillsynsfrågan bör dessutom utvidgas till att även omfatta mer konkreta delar, såsom systematiskt säkerhetsarbete för det sociotekniska systemet samt säkerheten hos de tekniska implementationer som används för e-legitimationer.

Avsnitt 7.9, Finansiering av den statliga e-legitimationen

När en gemensam bärare för såväl nationellt id-kort som statlig e-legitimation finns tillgänglig bör avgiften för ett kort med båda funktionerna läggas på samma nivå som avgiften för en enskild identitetshandling. Syftet med detta är att undanröja hinder som gör att medborgarna avstår från att skaffa båda identitetshandlingarna när de har behov av någon av dem. Motivet för detta är totalförsvarsperspektivet som tas upp ovan under rubrik *Totalförsvaret*.

Avsnitt 9.5, Förslaget om ansvar för utfärdande av en statlig e-legitimation

FOI ställer sig helt frågande till rimligheten hos de kostnadsuppskattningar som gjorts av Digg avseende förvaltning av systemet för utfärdande av e-legitimationer. Förvaltningskostnaderna uppgår enligt bedömningen till 25,5–30 miljoner kronor per år. Av denna summa avser 4,5–6 miljoner arbete inom informations- och cybersäkerhet, inklusive säkerhetsmässig förvaltning och vidareutveckling, incidenthantering, samverkan, omvärldsbevakning inkl. 24/7-beredskap samt säkerhetsprövning av personal. FOI:s erfarenhet från åtskilliga uppdrag är att säkerhetsaspekterna kräver betydligt större insats för att ge verkan, speciellt i komplexa system som är utsatta för en hög hotbild och där angrepp kan leda till allvarliga konsekvenser. Även den kostnadspost för säkerhetsgranskning och penetrationstester som utredningen tillfört i sin egen beräkning bedömer FOI som otillräcklig för ett system av denna typ.

Utredningen pekar på att delar av systemet mycket väl kan komma att omfattas av säkerhetsskyddslagen, vilket är en bild som FOI delar. Att ha ett system med externa anslutningar som omfattas av säkerhetsskyddskrav måste anses som mycket kostnadsdrivande.

I avsnitt 7.4.4 i betänkandet framgår att ”tillhandahållandet behöver kunna ske under normala förhållanden, svåra påfrestningar, höjd beredskap och krig”. Att systemet ska kunna fungera även under höjd beredskap och krig utgör kostnadsdrivande krav. FOI ställer sig frågande till om detta är omhändertaget i kostnadsberäkningarna som delvis framstår som optimistiska även för en lösning som bara är tänkt att fungera under normala förhållanden.

Utöver ovanstående kommentarer finns det flera andra frågetecken i kostnadsuppskattningarna. Utredningen pekar exempelvis på värdet av certifieringar och att förvaltningsorganisationen bör sträva efter exempelvis ISO 27001-certifiering, vilket också tillför kostnader i verksamheten som inte uppenbarligen tagits upp i beräkningarna. Det tycks även saknas poster i kostnadsuppskattningen för kontinuerlig vidareutveckling av systemet ur de funktionella och användarmässiga perspektiven.

Detta remissvar har beslutats av generaldirektör Jens Mattsson efter föredragning av förste forskare Daniel Eidenskog. I den slutliga handläggningen har även jurist Kaj Calissendorff och särskild rådgivare Mikael Wiklund deltagit.

…….

Jens Mattsson

……..

Daniel Eidenskog

FOI
Totalförsvarets forskningsinstitut

Datum
2024-01-22

Nr FOI-2023-1892

Sändlista

Finansdepartementet (fi.remissvar@regeringskansliet.se och fi.ofa.dof.remisser@regeringskansliet.se)

För kännedom

Försvarsdepartementet

Internt FOI

Registrator

GD-sekreterare

Särskild rådgivare

Chefsjurist

AC