Remissyttrande
2019-08-29 Dnr: Ju2019/01281/L4

Justitiedepartementet
103 33 STOCKHOLM

Remissyttrande över Betänkande av 2017 års ID-kortsutredning – Ett säkert statligt ID-kort, med e-legitimation

Sammanfattning
Verisec AB har sedan 2002 varit verksamt inom området digitala identiteter. Företaget lanserade 2017 e-legitimationen Freja eID+ som i januari 2018 som första mobila e-legitimation i Sverige fick E-legitimationsnämndens (numera DIGG – Myndigheten för digital förvaltning) godkännande för kvalitetsmärket Svensk e-legitimation. I vårt yttrande kommer vi fokusera på de delar som handlar om e-legitimation.

Våra synpunkter på utredningen kan sammanfattas nedan och utvecklas i den följande texten:

- Tillitsnivån bör baseras på eIDAS och inte på det svenska tillitsramverket
- Kräv användning av den statliga ID-handlingen på fler områden än vad som föreslagits
- Tillåt access till ID-kortets biometriska data vid utfärdande av kvalitetsmärkt Svensk e-legitimation
- Gör det till lagkrav att myndigheter, regioner och kommuner använder e-legitimationer med det statliga kvalitetsmärket Svensk e-legitimation
- Bygg ID-växlingen på NFC-chip samt tillgång till biometriska data på kortet
- Ta bort den föreslagna åldersgränsen och låt vårdnadshavare bestämma
- Möjliggör kvalificerade elektroniska underskrifter med den statliga e-legitimationen
- Klargör i lagstiftningen att en kvalitetsmärkt Svensk e-legitimation är likställd det statliga ID-kortet och pass vid legitimering i fysiska sammanhang
- Undvik begreppsförvirring och använd begreppet kvalitetsmärkt Svensk e-legitimation

5.3 Tillitsnivåer

Vi förordar att den statliga e-legitimationen utformas för att motsvara eIDAS nivå hög och att man i tillämpningen av tillitsnivå alltså inte utgår från den föreslagna nivå 4. Utredningen diskuterar även detta alternativ i punkten 12.8. Det råder inte någon konsensus inom EU länderna att det finns en direkt motsvarighet mellan de tillitsnivåer som används i Sverige och eIDAS-nivåerna och utredningen pekar själv på de skillnader som föreligger. Tillämpning en av parallella tillitsnivåer skapar problem och när det nu finns ett Europeiskt regelverk inom eIDAS, som är mycket tydligt, torde det vara en stor fördel att utgå från detta regelverk istället för det svenska tillitsramverket.

Bakgrunden till detta är att man från det offentliga har urvattnat det svenska tillitsramverket. E-legitimationer som inte har genomgått en statlig granskning – och därmed inte enligt någon officiell standard kan sägas vara godkänd för tillitsnivå 3 – har genom en lång rad undantag och genom praxis ändå fått statusen såsom godkänd på tillitsnivå 3. Utredningen konstaterar ju detta själv på sidan 137: ”BankID är inte granskad av Myndigheten för digital förvaltning men anses enligt uppgift på myndighetens webbsida motsvara tillitsnivå 3 enligt tillitsramverket.”

Genom att luta sig mot eIDAS undviker man att trovärdigheten kring tillitsnivån ifrågasätts, såväl i Sverige som inom EU.

8.6.3 Områden som inte har krav på statlig fysisk identitetshandling

Huvudsyftet med den statliga ID-handlingen är att minska och motverka bedrägerier. Det vore då rimligt att – när väl en så här omfattande förändring görs – att kraven på en säker ID-handling gäller i alla de sammanhang där bedrägeri möjliggörs genom osäkra ID-handlingar. Paketutlämning är ett av flera exempel, som utredningen föreslår fortsatt skall kunna fortgå med osäkra ID-handlingar. Det antas att näringslivet på eget initiativ skall ställa krav på säkrare ID-handlingar. Givet att det sedan 2005, då det nationella ID-kortet infördes, fortfarande är det osäkra körkortet som är den mest använda ID-handlingen i Sverige finns inget som talar att en självreglering plötsligt skulle komma till stånd.

För att få ett verkligt genomslag för den nya statliga ID-handlingen bör det införas krav på att den används i betydligt fler sammanhang än utredningen föreslår. Utredningen är också otydlig i denna del. I punkt 8.5.2 klargörs att körkort inte längre skall betraktas som en ID-handling, vilket är bra, men huruvida körkortet fortsatt skulle kunna vara en ID-handling i den oreglerade del som näringslivet själv skall sätta riktlinjer kring framgår inte.

11.6.3 Kontroll av biometriska uppgifter i andra sammanhang

Att addera biometriska data på ett chip på ID-handlingen höjer säkerhetsnivån exponentiellt mycket. Det förutsätter dock att det går att matcha dessa data mot individen. Det enda sammanhang som detta föreslås vara tillåtet är vid uthämtning av ID-handlingen samt vid in och utresa från landet.

Vi menar att det vid utfärdande av en e-legitimation baserat på det statliga ID-kortet och dess tillhörande e-legitimation skall vara tillåtet för en e-legitimationsutfärdare som är godkänd för det statliga kvalitetsmärket Svensk e-legitimation, att ta del av den biometriska datan för ett säkrare utfärdande.

Utan att möjliggöra en biometrisk kontroll vid en sådan ID-växling lämnas en mycket sårbar länk i kedjan. Utredningen talar om att det skall ske med kortläsare i någon form, men i ett sådant fall räcker det med att en förövare tillfälligtvis får tillgång till ett statligt ID-kort, kommer över PIN-koden och därefter kan växla till en e-legitimation som öppnar alla dörrar i den digitala världen. En sådan bristfällig ID-växling skulle göra det mycket enklare för bedragare att utfärda falska e-legitimationer än vad fallet är idag. Möjlighet för en godkänd e-legitimationsutfärdare att få använda biometrin på ID-kortet borde därför vara en självklarhet vid tillfället för utfärdandet.

Trots utredarens förslag om att begränsa tillgången till den biometriska datan, föreslår man själv på sidan 363 att exempelvis den ansiktsbild som finns på chipet kan visas på en handlares skärm då en individ legitimerar sig med det statliga ID-kortet. Detta är en mycket bra idé som höjer säkerheten och adderar värde till den statliga ID-handlingen. Men utredarens idé står i märklig kontrast till vad man själv föreslår i stycke 11.6.3.

12.3 En statlig e-legitimation

Vi tycker att det är ett bra förslag med en statlig e-legitimation som kan växlas över till en annan e-legitimation. Vi vill dock framhålla att bevekelsegrunderna som anges numera är obsoleta. Det finns

nu ett alternativ till BankID, som fyller kraven för eIDAS, som inte kräver att användaren är kund i en specifik bank och som är godkänd enligt kraven för det statliga kvalitetsmärket Svensk e-legitimation.

Vi delar dock farhågorna kring att det finns en dominerande aktör. Utmaningen det offentliga Sverige har är just nu inte fler e-legitimationer, det är att myndigheter, regioner och kommuner erbjuder medborgarna alla de alternativ som finns. Med mindre än att man från lagstiftarens håll kräver att offentliga e-tjänster kräver identifiering med e-leg som har det statliga kvalitetsmärket Svensk e-legitimation kommer de praktiska problemen med en dominerande aktör att kvarstå under överskådlig tid. Utredaren spekulerar på sidan 345 om att ”Vi utgår från att myndigheterna i samarbete med den utfärdande myndigheten ser till att möjliggöra en sådan identifiering” och konstaterar att någon lagreglerad skyldighet inte krävs. Önskar lagstiftaren bryta det de facto-monopol som finns bör man revidera denna ståndpunkt.

Vi menar också att den ID-växling som föreslås, från den statliga e-legitimationen till en annan e-legitimation, endast skall vara tillåten för utfärdare som är godkända för kvalitetsmärket Svensk e-legitimation.

Ansvarsförhållandena vid en ID-växling berörs inte i utredningen. Det klargörs att den statliga myndighet som utfärdar den statliga e-legitimationen har det juridiska ansvaret både gentemot innehavaren och de förlitande aktörerna. Det måste klargöras hur ansvarsfrågan hanteras efter det att en ID-växling har skett.

Man kan skönja att utredaren har en viss insikt om de praktiska problem som följer med en ID-växling från ett kort till en annan e-legitimation. Ett av skälen som anges, varför en statlig e-legitimation behövs, är att om en individ tappar sin mobiltelefon så skall hen kunna växla över till sin statliga e-legitimation. Det torde dock vara lättare att skaffa en ny mobiltelefon än att få tag på en kortläsare i en sådan situation. All erfarenhet visar att e-legitimationer som bygger på kort och kortläsare inte får något större genomslag. Så var det i Sverige innan de mobila e-legitimationerna slog igenom och så är det fortfarande i exempelvis Tyskland.

Vi förespråkar, som utredaren också verkar vara inne på, att satsa på kortläsning via NFC vilket gör att mobiltelefonen kan användas som kortläsare. I kombination med PIN-kod och möjlighet att läsa ut den biometriska datan från ID-kortet skapas förutsättningar för att säkert växla den statliga e-legitimationen till en annan kvalitetsmärkt Svensk e-legitimation.

12.7 Personer som kan få en statlig e-legitimation

De skäl som anförs att medborgare under 13 år inte skall kunna få en statlig e-legitimation är inte relevanta i ett större perspektiv. Idag introduceras unga människor i den digitala världen redan från tidig skolålder. Användandet av e-legitimationer ökar i snart sagt varje område i samhället, inte minst inom skolan där digitala prov snart kommer vara en verklighet. Mycket talar för att det mesta av digitaliseringen kommer att bygga på att användaren har en e-legitimation och att då sätta den ”digitala myndighetsåldern” till 13 år vore ett stort misstag. Det bör inte finnas någon åldersgräns utan vara upp till varje vårdnadshavare att bestämma.

12.9 Elektronisk underskrift

I första delen av utredningen argumenteras för att den statliga e-legitimationen skall motsvara eIDAS på nivå hög, så att svenskar har en möjlighet att komma åt alla tjänster i EU, på alla tillitsnivåer. Detta

är rimligt. Lika rimligt vore då att tillse att den statliga e-legitimationen kan användas för kvalificerade elektroniska underskrifter inom eIDAS.

Utredaren grundar sin slutsats att förespråka avancerade underskrifter på att denna nivå är vad som är vanligast i Sverige. Det skall dock påtalas att eIDAS främsta syfte handlar om gränsöverskridande identifiering och signering. Och inom EU är det främst kvalificerade underskrifter som gäller, vilket utredaren också konstaterar. Därför är det också självklart att den statliga e-legitimationen skall kunna användas för kvalificerade elektroniska underskrifter.

13.4 Förslag som leder till bättre kontroll av ID-handlingar
Utredaren konstaterar att det är mycket säkrare att legitimera sig med en e-legitimation i ett fysiskt sammanhang, än med en fysisk ID-handling. Detta genom att kontrollen sker elektroniskt och att bördan för kontrollen lyfts från människa till maskin.

Genom att individer legitimerar sig med en e-legitimation i ett fysiskt sammanhang uppnår man alla de förslag som läggs fram kring bättre kontroll av ID-handlingar.

Vi föreslår att det i lagstiftningen klargörs att elektronisk identifiering i fysiska sammanhang med en godkänd Svensk e-legitimation är likställd med legitimering med det statliga ID-kortet eller pass.

16.4 Förslaget till lag om ändring i lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism.

I paragrafen används begreppet ”en statlig e-legitimation”. Vi föreslår att skrivelsen ändras till ”En statligt kvalitetsmärkt e-legitimation”. DIGG – Myndigheten för digital förvaltning gör stora ansträngningar för att få acceptans för den statliga kvalitetsmärkningen och för att inte underminera detta bör staten och lagstiftningen vara konsekvent i begreppsanvändningen.

Stockholm den 30 augusti 2019, för Verisec AB

Johan Henrikson,
VD Verisec AB
Mobil: +46 733 45 89 02
E-post: johan.henrikson@verisec.com