Finansdepartementet

Yttrande angående En säker och tillgänglig statlig e-legitimation

SOU 2023:16

Dnr: C 2023-1733

1.1. Sammanfattande kommentarer

Chalmers har tagit del av betänkandet och instämmer att det är en viktig uppgift att utveckla en säker och tillgänglig statlig e-legitimation. Vi är ense om att det är viktigt att både höja säkerhetsnivån på e-legitimation och samtidigt minska beroendet av de privata aktörerna. Detta i enlighet med målen i eIDAS förordningen. Det är även viktigt att den statliga e-legitimationen är tillgänglig för så många som möjligt.

Samtidigt saknar vi en djupare analys av andra europeiska länders erfarenheter av statlig e-legitimation med värdefulla slutsatser att dra nytta av. Vi önskar att det framgår tydligare från rapporten om vad den avsedda användningen av e-legitimation innebär, då vi redan idag har både fysiska och elektroniska legitimationer som används flitigt i samhället. För att säkerställa en bred användning av e-legitimation är det viktigt att överväga dess användningsområden och incitament. Så länge befolkningen kan autentisera sig med kommersiella appar är det otydligt vad som skulle motivera dem att byta till e-legitimation. Det är avgörande att identifiera de incitament som skulle uppmuntra befolkningen att övergå till e-legitimation, speciellt om Skatteverket och andra offentliga institutioner fortsätter att acceptera BankID och Freja+ som autentiseringsmetod. Detta är särskilt relevant om e-legitimation kräver extra hårdvara.

1.2. Kommentarer på specifika kapitel i betänkandet

Sektion 5

Vi saknar en djupare analys av andra europeiska länders erfarenheter av statlig e-legitimation där det finns framgångsrik och värdefull erfarenhet att dra nytta av. Till exempel nämns det att e-legitimation i Nederländerna är gratis, kan användas i telefoner, kräver ingen speciell hårdvara medan den samtidigt kan nå hög tillitsnivå eftersom den kan kommunicera genom telefonens NFC-läsare med nederländska körkort och nationellt id-kort. Det verkar som att den nederländska lösningen har några fler fördelar jämfört med de alternativ som föreslås i utredningen där man behöver betala 400 kr för ett separat kort vilket inte går att använda för legitimering på Internet. Även andra länder såsom Spanien och Estland har fördelaktiga lösningar som utredningen skulle kunna analysera och ta nytta av.

Sektion 6

Vi önskar att det framgår tydligare från rapporten vad den avsedda användningen för e-legitimation är, då vi redan idag har både fysiska och elektroniska legitimationer som flitigt används i samhället. För att säkerställa en bred användning av e-legitimation är det viktigt att överväga dess användningsområden och incitament. Så länge befolkningen kan autentisera sig med kommersiella appar är det otydligt vad som skulle motivera dem att byta till e-legitimation. Det är avgörande att

identifiera de incitament som skulle uppmuntra befolkningen att övergå till e-legitimation, speciellt om Skatteverket och andra offentliga institutioner fortsätter att acceptera BankID och Freja+ som autentiseringsmetod. Detta är särskilt relevant om e-legitimation kräver extra hårdvara.

Sektion 7.2.2

Att inkludera ett chip för högre nivå av autentisering tillsammans med kontaktlösa kort kan öka användbarheten. Det är dock viktigt att ta hänsyn till attacker mot distansavgränsande protokoll och problem som uppstår med opålitlig strömförsörjning till smartkortet vid verifiering. Kontaktlös autentisering kan fortfarande accepteras, men inte på den högsta säkerhetsnivån om den inte kan kombineras med andra metoder som pinkod eller ansiktsigenkänning.

Sektion 7.2.4

Vi är överens om att kortet bör ha en personlig prägel och kan dessutom inkludera punktskrift med viss personlig information. Detta är fördelaktigt både för tillgänglighet, då det gör kortet tillgängligt för en bredare grupp människor (synskadade), och gör det svårare att förfalska det fysiska kortet.

Sektion 7.2.5

Att använda “två olika krypteringsalgoritmer samtidigt” kan öka e-legitimationens säkerhet men bara i enstaka fall. Första problem är att “krypteringsalgoritm” kan tolkas som en chiffersvit, en grupp av kryptografisk primitiver, där förändring av ett av primitiverna skulle resultera i en annan “algoritm”. Detta kan vara en svaghet då problem kan uppstå i både implementationen eller primitiven som är gemensam för båda sviterna. Dessutom, skulle liknande algoritmer användas, till exempel SHA-384 och SHA-512, finns det en stor risk att framtida sårbarheter i en av algoritmer även påverkar den andra.

Därför skulle vi rekommendera att i stället kräva åtminstone två olika chiffersviter som inte delar kryptografiska primitiver eller använder kryptografiska primitiv som är baserade på samma grundläggande koncept. Ett exempel skulle vara att använda SHA-512 som kondensat i en svit och SHA-3 i den andra.
Vi anser också att rekommendationen borde breddas för att undvika andra risker. Bland annat, så borde en av chiffersviterna vara designad att motstå kvantdatorer, valet av svit vid användning borde förstärkas så att nedgradering till en svagare svit blir omöjlig. Olika hemliga nycklar bör också användas för varje svit och för de olika användningsområdena på kortet, exempelvis autentisering och underskrift. Det kan också vara relevant att säkerställa att användaren har möjlighet att använda olika personliga koder på de olika användningsområdena. Detta så att användaren inte kan luras att göra en annan operation än den avsedda.

Vi håller också med om att “det behöver därtill finnas en leveransförmåga även under perioder av svåra påfrestningar, kris och ytterst krig”. Vi anser däremot att detta kan bara garanteras om e-legitimationen kan användas i ett decentraliserat läge där det endast krävs kontakt med systemet som ska autentisera användaren. För detta kan olika åtgärder tas, som till exempel att publicera listor av återkallade krypteringsnycklar samt att begränsa dessa nycklars giltighetsperiod så att listan kan begränsas.

Sektion 7.3

Det är otydligt om designen tillåter autentisering med det fysiska e-legitimationskortet via tredjepartsappar på mobiltelefoner och surfplattor. Vi har följande kommentarer på de tre olika sätten kvalificerade elektroniska underskrifter kan skapas. För scenario 1, där identifiering görs i en kommersiell tjänst, blir det problematiskt att säkra försörjningskedjan. Scenario 2, där e-legitimationen kan skapa underskrifter, är ett scenario där det inte finns liknande nackdelar. I scenario 3, där en fristående tjänst används, krävs extra interaktion över Internet för att verifiera att certifikat inte har återkallats. Detta strider mot behovet om att systemet ska fungera utan Internetåtkomst.

Sektion 7.4.3

Vi håller med om att legitimationen borde kunna användas av hela samhället, för att vara framgångsrik. Detta kräver också att samhället kan använda e-legitimationen för sina system, oberoende av vilken tillverkare de valt. Därför rekommenderar vi att teknisk dokumentation för mjukvaran som interagerar med kortet blir fritt och tillgänglig. Dokumentationen bör finnas på både svenska och engelska. Mjukvaran, bortsett från den som körs i kortet, bör publiceras med en fri licens. Ett bra exempel på hur detta kan ske är Estlands Open-eID (https://github.com/open-eid).

Sektion 7.7

För att motverka kända säkerhetsbrister kan det vara bra att låta medborgare förnya sina kort tidigare än utgångsdatumet om de önskar det. Det finns dock brister i hanteringen av namn- och könsändringar. Dessutom är det viktigt att klargöra om återkallelse kommer att ske med hjälp av en svartlista med certifikat.

Sektion 7.11

I dokumentet diskuteras sekretess vid lagring och åtkomst, men det verkar inte finnas någon information om integritetsvänlig tillhandahållande av information (dvs. att påvisa vissa attribut utan att avslöja dem helt, till exempel att en person är över 18 utan att visa hela födelsedatumet). Ett sådant tillhandahållande kan tekniskt sett uppnås genom kryptografiska tekniker som gruppsignaturer eller attributbaserade uppgifter (eng. Attribute Based Credentials). Faktum är att sådana idéer redan övervägs i andra länder, till exempel i Spanien (se https://cadenaser.com/nacional/2024/01/16/verificacion-de-edad-sin-nombres-ni-apellidos-asi-se-impedira-que-los-menores-vean-porno-cadena-ser/), eller experiment i Frankrike (se https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process för anonymt åldersbevis med gruppsignaturer) och i Nederländerna (se https://www.yivi.app/en/for-me/yivi-providers för integritetsskyddande röstning i Amsterdam med hjälp av ABC).

Sektion 7.11.5

Eftersom förslaget beaktar algoritmisk ansiktsigenkänning (se sektion 7.11.5), undrar vi om en proportionalitetsprövning har utförts och fått ett positivt resultat. I dokumentet står det ingenting om särskilda åtgärder för lagring, bearbetning och åtkomst till databasen som lagrar dessa uppgifter, även om det erkänns att det "motiverar reglering". Möjligtvis skulle tillgången till denna databas kunna kräva beslut från domstol? Vi pekar på riskerna för "funktionskrypning" (dvs. gradvis utvidgning av funktioner) i samband med denna praxis, och varnar för den falska positiva paradox (se https://hal.science/hal-01157921/document samt https://en.wikipedia.org/wiki/Base_rate_fallacy#False_positive_paradox) som kan uppstå till följd av den.

Vi förstår att någon typ av databas behövs för att kunna tillhandahålla en e-legitimationstjänst, vi anser dock att informationen i 14§ av förordningens förslag samt i sektion 7.11.5 är mer än vad som behövs. Vi instämmer med att informationen i första, tredje och fjärde styckena kan behövas för att kunna spärra legitimationer samt för att kunna kontakta personen ifall problem uppstår med sin legitimation. Informationen i sjunde, åttonde och nionde styckena kan vara viktigt för både utfärdande och processen för återkallelse. Uppgifterna i andra stycket "kopia av den ansiktsbild som tagits vid ansökan och biometriska uppgifter som tagits fram ur ansiktsbilderna" kan behövas för att kunna säkerställa att en person bara har en legitimation. Dock tror vi att detta kan förarga integritetsaktivister. Enligt vår tolkning så finns det ingen orsak att behålla "aktiveringskod" eller "kondensat av innehavarens personliga kod" i databasen då denna information borde verifieras av kortet själv. Dessutom skulle den typen information behövas spåras.

Slutligen, vi är oroade över användningen av bilderna samt den biometriska informationen. Denna information bör, i så lång utsträckning som möjligt, verifieras av kortet själv och inte sparas i en databas. Skulle det sparas i en databas borde åtgärder tas för att säkerställa att informationen endast kan användas för de ändamål som planerats. Ett register bör också etableras innehållande vem, när och varför databasen konsulterades. Detta så att användningen kan kontrolleras av oberoende part vid överträdelse.

Göteborg 2024-01-30

I tjänsten,
Francisco Blas Izquierdo Riera, handläggare
francisco.izquierdo@chalmers.se
031 772 11 56

I tjänsten,
Benjamin Lundblad, handläggare
beneri@chalmers.se
0760 313371

I tjänsten,
Victor Morel, handläggare
morelv@chalmers.se
073 940 84 38

I tjänsten,
Elena Pagnin, handläggare
elenap@chalmers.se
031 772 50 82

I tjänsten
Andrei Sabelfeld, handläggare
andrei@chalmers.se
031 772 10 18