

Remissvar av promemorian Ett statligt identitetskort, Ju2026/01595

Sammanfattning

Chalmers tekniska högskola (Chalmers) har tagit del av förslagen i promemorian "Ett statligt identitetskort". Chalmers begränsar sitt remissvar till frågor som rör informationssäkerhet i pass- och identitetskortsverksamheten. I övrigt har Chalmers inte några synpunkter på de lämnade förslagen.

Chalmers förhåller sig positivt till värnandet av medborgares informationssäkerhet och integritet genom att begränsa tillgången till integritetskänslig data. Chalmers tillstyrker i synnerhet förslagen i avsnitt 9.13.3 om att fingeravtryck och biometriska uppgifter som tas fram ur fingeravtryck ska förstöras omedelbart efter utfärdandet av pass och/eller identitetskort och att integritetskänslig data som sparas i pass- och identitetskortsverksamheten allmänhet beläggs med sökförbud (avsnitt 9.10).

Vi rekommenderar att vissa begrepp och begreppsanvändningen bör förtydligas. Förfarandet för att ansöka om e-legitimation genom bud öppnar för en möjlig väg för bedrägerier, och vi föreslår ett sätt att begränsa denna risk. Därutöver rekommenderar vi att privata aktörers användning av e-legitimationen, i synnerhet för att kontrollera biometriska uppgifter, bör föregås av ett explicit, informerat samtycke från användaren. Vi anser att tydligare möjligheter för granskning av användningen av automatiserad ansiktsjämförelse bör övervägas. Slutligen belyser vi att vissa tolkningar av regeln för direktåtkomst vid giltighetskontroller kan strida mot EU:s förordning om elektronisk identifiering. Vi utvecklar dessa rekommendationer i nästa avsnitt.

Detaljerade kommentarer

Om begreppsanvändningen inom elektronisk identifiering

Promemorian behandlar tre typer av elektronisk identifiering: (i) e-legitimationen på det statliga identitetskortet, (ii) EU:s digitala identitetsplånbok (EUDI wallet), och (iii) den fristående e-legitimationen som regleras i lagen om statlig e-legitimation och elektronisk identifiering (2026:1358). Vi vill understryka vikten av att tydligt särskilja dessa tre typer av elektronisk identifiering, exempelvis genom att utveckla begreppsapparaten i promemorian till att innefatta (i) e-legitimation på kort, (ii) identitetsplånbok och (iii) fristående e-legitimation.

Om skiljandet mellan lag och teknisk specifikation

Det framgår tydligt av promemorian att lagtext och tekniska specifikationer (som regleras på lägre nivå) behöver skiljas åt. Promemorian behandlar detta medvetet och understryker vikten av att separera dessa aspekter. I promemorian behandlas den tekniska implementationen, vilket vi anser är en rimlig standpunkt, eftersom tekniska specifikationer kan behöva förändras i takt med teknikutvecklingen och säkerhetskrav. Vi anser att lagen samtidigt bör fastställa omfång för, och definiera, underliggande säkerhets- och integritetskrav. Vi väntar oss att specifikationer av mer teknisk karaktär, exempelvis referensarkitekturer, kommer tillgängliggöras i sinom tid och lämnar gärna synpunkter på dessa.

Ansökningar om statlig e-legitimation genom bud i förhållande till eIDAS (avsnitt 6.3)

Chalmers tillstyrker målet att tillgängliggöra den statliga e-legitimationen för personer som inte kan inställa sig personligen för en ansökan om e-legitimation på grund av sjukdom eller funktionshinder. Vi delar bilden att skälen till ett sådant tillgängliggörande blir starkare i takt med samhällets digitalisering. Däremot anser vi att resonemanget i avsnitt 6.3 (s. 95-96) inte är tillfredsställande ur ett säkerhetsperspektiv i förhållande till eIDAS (EU 910/2014) och EU:s förordning 2015/1502 om tillitsnivåer för elektronisk identifiering.

Möjligheten att ansöka genom bud skapas i 3 kap. 2 § andra stycket i förslaget till lag om statligt identitetskort, genom att tillåta budförfarande för ansökningar om identitetskort utan resefunktion. Genom 5 kap. 1 § andra stycket öppnas även möjligheten för budförfarande i ansökningar om e-legitimation.

Bedömningen i avsnitt 6.3 skiljer sig från motsvarande bedömning i *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61) med motiveringen att den föreslagna e-legitimationen kommer utfärdas genom samma ansökningsprocess som identitetskortet. Å andra sidan innebär också en gemensam process att både den fysiska identitetshandlingen och e-legitimationen delar svagheter. Vi anser att motiveringen inte visar att identitetshandlingarna uppnår tillitsnivå hög i förordningens (2015/1502) bemärkelse. En bedömning mot EU:s förordning om tillitsnivåer för elektronisk identifiering (2015/1502) verkar saknas både i promemorian och den tidigare utredningen *Ett säkert statligt ID-kort - med e-legitimation* (SOU 2019:14), där ansökningar genom bud för e-legitimation först lyftes.

Förordningen (2015/1502) ställer upp två krav som vi anser inte avhandlats i promemorian. För det första behöver den utfärdande myndigheten jämföra en fysisk egenskap hos den sökande mot en tillförlitlig källa (Bilaga, avsnitt 2.1.2). För det andra behöver aktiveringsprocessen kontrollera att medlet för elektronisk identifiering endast levererats till ägaren.

I promemorian gäller följande:

- En välliknande ansiktsbild ges in snarare än att det tas under ansökningsförfarandet, enligt 3 kap. 4 § i förslaget till lag om statligt identitetskort. Samtidigt ges inga fingeravtryck in.
- Budet och ett vittne ska intyga att ansiktsbilden föreställer sökanden enligt 3 kap. 4 § i förslaget till förordning om statligt identitetskort.
- Sökningen med hjälp av den ingivna ansiktsbilden som tillåts i avsnitt 9.10.1 i promemorian (s. 147) jämför således en bild i registret med en ingiven bild, vilket inte kan likställas med en direkt jämförelse med en person som inställt sig fysiskt.
- Identitetskortet kan lämnas ut till budet vid personlig inställelse enligt 4 kap. 1 § andra stycket i lagförslaget.
- Aktiveringsprocessen lämnas som en fråga för Polismyndigheten utan vidare kommentar i promemorian.

Vår tolkning är dessutom att budförfarandet inte beskriver "samma förfaranden som används på nationell nivå i medlemsstaten av den enhet som ansvarar för registreringen för att erhålla sådant erkänt fotografiskt [...] identifieringsbevis" som accepteras enligt punkt 2, avsnitt 2.1.2 i bilagan till förordningen 2015/1502. Det beskrivna budförfarandet framstår därför som ett undantag till förfarandena enligt förordningen 2015/1502 och inte en beskrivning av en sådant förfarande. Budförfarandet framstår som genomförbart endast eftersom det faller utanför EU:s förordning 2025/1208 om säkrare identitetskort för unionsmedborgare. Förordningen 2025/1208 kräver att biometriska uppgifter inhämtas av bemyndigad personal.

I ljuset av detta framstår budförfarandet som en möjlig väg för bedrägerier. Till exempel skulle budet och vittnet i samförstånd kunna ge in en bild på en person som är lik den sökande eller en digitalt skapad eller behandlad bild och på det sättet erhålla en e-legitimation knuten till en potentiellt utsatt person. E-legitimationen skulle sedan kunna användas för att skapa kvalificerade digitala underskrifter (enl. 5 kap. 1 § andra stycket i förslaget till förordning) och utgöra grunden för aktiveringsprocessen för EU:s digitala identitetsplånbok (EUDI wallet) (enl. avsnitt 3.9 i promemorian).

Vi föreslår därför att lagen bör kräva att en e-legitimation endast kan utfärdas och aktiveras när kraven för tillitsnivå hög enligt EU:s förordning 2015/1502 uppnås. Till exempel skulle ett identitetskort som utfärdats genom bud kunna innehålla en inaktiv e-legitimation som endast aktiveras när utfärdande myndighet kan kontrollera sökanden direkt, antingen fysiskt hos sökanden eller via direktlänk med den sökande och jämföra mot den ingivna ansiktsbilden.

Rätten att meddela föreskrifter: Samtycke och villkor för användning (avsnitt 9.5.2)

Promemorian behandlar att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om villkor för användningen av den statliga e-legitimationen. Promemorian tar upp att sådana villkor kan avse offentliga och privata aktörers användning av e-legitimationen i sina nättjänster, såsom kontrollen av biometriska uppgifter i samband med identifiering.

I detta sammanhang vill vi belysa möjligheten att kräva informerat samtycke till sådana aktörers användning av e-legitimationen. Promemorian fastslår att EU:s identitetskortsförordning kräver innehavarens samtycke innan privata aktörer får åtkomst till ansiktetsbilden på e-legitimationen. I promemorian anses detta krav vara uppfyllt eftersom den enskilde initierar kontrollen av biometriska uppgifter. Vi anser dock att ett explicit krav på informerat samtycke, exempelvis i form av en explicit medgivande, bör finnas i lag eller förordning vid privata aktörers användning av e-legitimationen. Ett sådant krav ställs inte från dataskyddsförordningens håll.

Den tyska identitetskortslagen "Personalausweisgesetz" (PAuswG) är ett gott exempel i denna fråga:

- Enligt § 18(4) PAuswG kan personuppgifter endast överföras efter att nättjänsten kan uppvisa ett giltigt auktoriseringsintyg och identitetskorthavaren matar in en PIN-kod. Innan PIN-koden matas in måste vissa uppgifter från auktoriseringsintyg visas för identitetskorthavaren, och identitetskorthavaren kan välja att utesluta vissa personuppgifter från överföringen.
- § 27 PAuswG kräver också att identitetskorthavaren vidtar rimliga åtgärder för att hålla PIN-koden hemlig och för att säkerställa, genom tekniska och organisatoriska medel, att e-legitimationen endast används i en miljö som kan räknas som säker enligt teknikens ståndpunkt. Det är ett krav på en slutanvändare som icke-expert sannolikt inte kan uppnå. För att kunna ta ett informerat beslut behöver därför slutanvändaren delges vem som söker tillgång till personuppgifterna, vilka personuppgifter som eftersöks och ändamålet med personuppgiftsbehandlingen.

Säkerhet och tillgång till personuppgifter (avsnitt 9.7, 9.8.1)

Promemorian föreslår att ett sammanhållet pass- och identitetskortsregister bör hållas (s. 129). Promemorian framhåller samtidigt att det inte är "lämpligt att reglera exakt vilka konkreta säkerhetsåtgärder som bör vidtas" i pass- och identitetskortsverksamheten (s. 128). Vi vill understryka att säkerheten kring själva pass- och identitetskortsregistret är viktig och bör övervägas noggrant, möjligen inom ramen för promemorian. Ett sammanhållet register, som dessutom har flera möjliga åtkomstvägar enligt promemorian, utgör ett konkret och tydligt mål för illvilliga aktörer.

Användning av modern teknik för sökningar (avsnitt 9.9.3)

Promemorian fastställer (s. 142) att ansiktetsbilder ska få sparas och att passmyndigheterna och Utrikesdepartementet ska få söka bland dessa med hjälp av "modern teknik". Begreppet modern teknik definieras inte ytterligare, och det framgår inte av promemorian om det ställs särskilda krav på sådan

teknik för att den ska betraktas som modern. Vi anser att detta borde förtydligas. Bör exempelvis sökfunktionen ställa krav på integritet, säkerhet eller granskningsbarhet med stöd av modern teknik?

Granskningsbarhet av sökningar för att utreda vissa allvarliga brott (avsnitt 9.10.2)

Promemorian föreslår att det ska vara tillåtet, efter beslut av åklagare, att använda automatiserad ansiktsjämförelse i pass- och identitetskortsregistret vid förundersökningar om vissa allvarliga brott. Promemorian föreslår däremot inget sätt att kontrollera eller granska att användningen av automatiserad ansiktsjämförelse (eller annan personuppgiftsbehandling) sker ändamålsenligt och endast för ändamålen som anges i promemorian. Användningen av automatiserad ansiktsjämförelse i förundersökningssyfte ska dokumenteras i ett förundersökningsprotokoll, vilket erbjuder ett visst mått av granskningsbarhet av användningen. Vi anser att starkare granskningsbarhet bör övervägas i form av manipulationssäker loggning av sökningar och motsvarande beslut av åklagare, och att dessa loggar kan granskas av relevanta myndigheter vid behov.

Därutöver vill vi belysa risken för en intressekonflikt mellan allmänhetens intresse för att skydda sin integritet och förundersökningens intresse att utreda brott. Om den beslutande åklagaren också är förundersökningsledare finns risken att beslut om sökningar tas oftare än när det är absolut nödvändigt. Vi anser promemorian bör överväga en tillgänglig juridisk mekanism för att allmänheten ska kunna granska sådana jämförelser.

Direktåtkomst för giltighetskontroller (avsnitt 9.11.2)

Den föreslagna pass- och identitetskortsdatalagen tillåter utlämning av uppgifter gällande ett pass eller statligt identitetskorts giltighet genom direktåtkomst, oavsett vem mottagaren är (s. 155). Promemorian framhåller att implementationen av sådan direktåtkomst är en tillämpningsfråga (s. 158). Det framgår dock att sådana kontroller kommer göras mot Polismyndighetens register (s. 178). Det framkommer i promemorian att Polismyndigheten också kan komma att behandla uppgifter om vilka förlitande parter en person har identifierat sig mot (s. 116). Det fastställs i promemorian att personuppgiftsbehandlingen inom ramen för pass- och identitetskortsverksamheten kan anses innefatta kartläggning av enskildas personliga förhållanden (s. 109).

I ljuset av detta anser vi att reglerna kring direktåtkomst för giltighetskontroller bör förtydligas, eftersom vissa tolkningar av reglerna kan komma att strida mot integritetsskyddet som den europeiska digitala identitetslagstiftningen bygger på. Om varje giltighetskontroll innebär en förfrågan till utfärdande myndighet kan den utfärdande myndigheten få kännedom om vilka tjänster identitetskorthavaren använder och med vilken frekvens dessa används. Vi anser att det är möjligt att ett sådant förfarande strider mot EU:s förordning om elektronisk identifiering (910/2014, ändrad i 2024/1183) och de krav som föreskrivs för en digital identitetsplånbok. I synnerhet kan förfarandet strida mot Artikel 5a(16)(a) i förordningen, som fastställer att identitetsplånboken inte ska "tillåta tillhandahållare av elektroniska attributsintyg eller någon annan part att, efter utfärdandet av attributsintyget, erhålla data som gör det möjligt att spåra, länka, korrelera transaktioner eller användarbeteende eller på annat sätt få kännedom om transaktioner eller användarbeteende".

Vi anser att samma principer bör gälla för den statliga e-legitimationen, som kommer utgöra grunden för aktivering av identitetsplånboken. Vår rekommendation är att begränsa direktåtkomst för giltighetskontroll till att endast kontrollera om e-legitimationen är återkallad eller utgången. Det finns integritetsskyddande lösningar för att uppnå sådana kontroller. exempelvis publika återkallelselistor, kortlivade elektroniska attributsintyg, eller tjänstespecifika återkallelseintyg. Det sistnämnda används i den tyska e-legitimationen. Autentiseringsloggar bör också gallras regelbundet.

Detta yttrande har tagits fram av universitetslektor Elena Pagnin, tekniklektor Francisco Blas Izquierdo Riera, postdoktor Shai Levin och doktoranderna Emil Babayev och Hanna Ek.

Göteborg 2026-10-22

I tjänsten,

Elena Pagnin
Universitetslektor
Institutionen för data- och informationsteknik
Chalmers tekniska högskola