Finansdepartementet

103 33 Stockholm

Delbetänkande En säker och tillgänglig statlig e-legitimation

(SOU 2023:61)

(Fi2023/02704)

Sammanfattning

Försäkringskassan bedriver en verksamhet som i praktiken är beroende av att allmänheten kan identifiera sig elektroniskt. Samtidigt finns det i samhället ett inte obetydligt digitalt utanförskap parallellt med en växande identitetsbaserad brottslighet med stora konsekvenser på välfärdssystemet.

Givet de utmaningar som samhället står inför välkomnar Försäkringskassan införandet av statlig e-legitimation på högsta tillitsnivå. Försäkringskassan hänvisar samtidigt till det särskilda yttrande som myndighetens expert har lämnat.

I samband med införandet av den statliga e-legitimationen önskar Försäkringskassan peka på behovet av en sammanhållen hantering av såväl fysiska som digitala identiteter och verifiering av dessa. Mer konkret behövs en åtstramning avseende antalet godkända identitetshandlingar och utfärdare därav, ett robust och enhetligt system för grundidentifiering samt metoder för verifiering baserat på biometri.

Försäkringskassan bedömer att utredning eller fördjupad analys behövs inom följande områden.

- Id-växling
- Bärare av den statliga e-legitimationen och förslag om en statlig e-legitimation på olika tillitsnivå
- Till vilka den statliga e-legitimationen ska göras tillgänglig med fokus på ålder
- Säkerhetskrav
- Grundidentifiering
- Myndigheten för digital förvaltnings (Digg) roll som utfärdare av den statliga e-legitimationen
- Kostnadsaspekter
- Författningsförslag

6 Varför behövs en statlig e-legitimation?

6.4 Bättre förutsättningar för id-växling

Försäkringskassan instämmer i att en statlig e-legitimation kan erbjuda utökade möjligheter till id-växling vilket i sin tur kan bidra till ökad konkurrens på e-legitimationsområdet. Även om utfärdande av en statlig e-legitimation ska föregås av ett system med grundidentifiering genom fysisk inställelse och insamlande och verifiering

av biometriska uppgifter finns det fortfarande risker med ett id-växlingsförfarande. Dessa risker måste identifieras och hanteras. I annat fall kan den organiserade brottsligheten få ett nytt brottsverktyg.

Om ID-växling ska tillåtas måste man hantera riskerna genom exempelvis krav på att id-växling ska ske genom användande av biometri på fysiska platser med hjälp av maskinell avläsning.

7 Utredningens överväganden och förslag

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

Försäkringskassan ställer sig bakom utredningens bedömning att den statliga e-legitimationen så snart som möjligt ska finnas även på ett statligt utfärdat identitetskort. En viktig parameter i bekämpandet av den identitetsrelaterade brottsligheten bör vara en sammanhållen statlig identitetsförvaltning med så få ansvariga utfärdare som möjligt. Därtill behövs en begränsning i antalet godkända typer av fysiska identitetshandlingar. Utöver de säkerhetsvinster som kommer av att koncentrera och harmonisera processerna med identitetsförvaltning till någon eller några få myndigheter blir systemet även tydligare och mer överskådligt ur den enskildes perspektiv. Försäkringskassan ser därför positivt på utredningens bedömning att det finns ett behov av att en och samma myndighet ansvarar för att utföra grundidentifieringen inför utfärdande av såväl de fysiska identitetshandlingar som tillhandahålls av staten som en statlig e-legitimation. I ljuset av detta anser Försäkringskassan att den statliga e-legitimationen ska förläggas till det nationella identitetskortet.

Försäkringskassan förutspår att efterfrågan av en e-legitimation förlagd på ytterligare ett kort, som inte fyller någon annan funktion än att vara bärare av den statliga e-legitimationen och för vilket en ansökningsavgift ska tas ut, kommer vara låg. Detta särskilt med beaktande av redan befintliga e-legitimationer. Det nationella identitetskortet betraktas som en värdehandling. För den enskilde medborgaren torde det ha ett bra symbolvärde i motsats till ett kontaktlöst kort. För det nationella identitetskortet finns dessutom ett etablerat utgivningsförfarande med säkra och välfungerande rutiner, vilket det finns klara fördelar att dra nytta av beträffande den statliga e-legitimationen. För att tillgodose behovet för de som inte kan erhålla ett nationellt identitetskort föreslår Försäkringskassan ett system med en statlig e-legitimation på olika tillitsnivå med olika bärare i relation till bakomliggande grundidentifiering. Det nationella identitetskortet blir därmed bärare av e-legitimation på högsta tillitsnivå för de med svenskt personnummer.

För de med samordningsnummer föreslås ett annat kort som bärare av e-legitimationen med olika tillitsnivåer baserat på genomförd identitetskontroll.

Genom att basera den statliga e-legitimationen på vad du som medborgare har rätt att göra istället för att diskvalificera de som inte når upp till nödvändiga krav för tillitsnivå hög skapar man bättre förutsättningar för digital inkludering.

7.4.2 Till vilka och på vilket sätt ska den statliga e-legitimationen tillhandahållas?

Utredningen föreslår att den statliga e-legitimationen ska göras tillgänglig för personer som innevarande kalenderår är eller ska fylla nio år. Utredningen konstaterar att risker hänförliga till användandet av e-legitimationen kan motverkas av förlitande parter som i varje tjänst avgör om minderåriga ska ha tillgång till tjänsten eller om vissa ålderskategorier ska sakna tillgång.

Enligt Försäkringskassan ska en statlig e-legitimation på högsta nivå inte vara tillgänglig för barn enligt vad som föreslås. Detta särskilt med beaktande av de risker för missbruk och oegentligheter som det kan medföra. En effekt av utredningens förslag kan bli att en övervägande andel förlitande parter av säkerhetsskäl stänger ute barn från att använda tjänsterna, om inte barn redan är exkluderade från sådana tjänster på grund av bristande rättshandlingsförmåga. Istället för att lägga ansvaret på förlitande parter anser Försäkringskassan att ovan föreslagna system med olika tillitsnivå ska tillämpas även i fråga om ålder varvid tillitsnivå hög ska vara förbehållen personer över 18 år och lägre nivåer förbehållna yngre personer.

7.4.4 Säkerhetsbehov vid tillhandahållande av den statliga e-legitimationen

Försäkringskassan delar utredningens bedömning avseende säkerhetsbehov och att en certifiering enligt ISO/IEC-standard är nödvändig. Infrastrukturen och tjänsterna kring den statliga e-legitimationen behöver vara robusta och klara av att stå emot cyberangrepp, distributed denial-of-service (DDoS), hackingattacker, skadlig kod med mera. I detta ligger bland annat att driften av infrastrukturen ska handhas av staten och inte privata aktörer.

7.5 Grundidentifiering

Försäkringskassan ser positivt på förslaget med en grundidentifiering som inbegriper personlig inställelse för att ta ansiktsbild, fingeravtryck och göra erforderliga jämförelser med sökandens identitetshandling samt att bäraren föreslås innehålla ett lagringsmedium för biometriska uppgifter. En säker identitetsförvaltning omfattar emellertid inte bara en struktur för grundidentifiering. Det måste även finnas förutsättningar för korrekt verifiering i användningsskedet. Försäkringskassan anser därför att det är nödvändigt att möjliggöra användning av biometriska uppgifter i samband med verifiering.

I fråga om samordningsnummer kvarstår den problematik som kommer av att det i Sverige i dagsläget saknas en fysisk identitetshandling som kopplar samman en individ med dennes unika samordningsnummer vilket är en brist i säkerhetshänseende som inte kan bortses ifrån. Även om det inte ligger inom ramarna för utredningens uppdrag så som det formulerats, är det enligt Försäkringskassan en fråga som måste hanteras i det fortsatta arbetet med att ta fram en statlig e-legitimation. I sammanhanget hänvisas även till ovan förslag om en statlig e-legitimation på olika tillitsnivå.

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

I anslutning till det säkerhetsgrundade granskningsansvar som åligger Digg noterar Försäkringskassan en problematik avseende opartiskhet. För det fall Digg ska ikläda sig rollen som såväl granskare av utfärdaren av den statliga e-legitimationen som utfärdare av densamma uppkommer oundvikligen en rollkonflikt. Utifrån ett förtroendeperspektiv behöver frågan utredas vidare. I det hänseendet önskar Försäkringskassan att man låter den identitetskontrollerande myndigheten även ansvara för utfärdandeprocessen istället för ett uppdelat myndighetsansvar. En sådan lösning bidrar till den enhetliga identitetsförvaltning i samhället som Försäkringskassan efterfrågar. Det bidrar också till bättre förutsättningar för opartisk granskning, en mer samlad personuppgiftshantering och troligtvis säkerhetsvinster.

9 Konsekvenser

9.5.1 Finansiering för utfärdande

Det framgår av förslaget att de årliga kostnaderna för utfärdandet av den statliga e-legitimationen i huvudsak ska finansieras via anslag. Försäkringskassan anser att det behövs ett förtydligande av hur detta förhåller sig till det beslutade

auktorisationssystemet och den där avsedda intäktsmodellen. I nuvarande valfrihetssystem tillämpas den transaktionsbaserade modellen med så kallade tickkostnader. För det fall samma modell ska användas för den statliga e-legitimationen inom ramen för auktorisationssystemet behövs en redogörelse för hur de intäkterna förhåller sig till planerad anslagsfinansiering.

9.7.1 Förslaget om kravet att vissa e-legitimationer ska godtas för identifiering i digitala tjänster

Utredningen konstaterar att de kostnader som kan uppstå till följd av förslaget ska finansieras inom den ordinarie verksamheten. Man bedömer vidare att de kostnader som redovisats och uppskattats i promemorian *Auktorisationssystem för elektronisk identifiering och för digital post* kan användas som utgångspunkt för det nu aktuella förslaget avseende en statlig e-legitimation. Försäkringskassan bedömer att nyssnämnda kostnader är för lågt beräknade och räknar med betydande omställnings- och anpassningskostnader. Endast en anslutning till identitetsfederationen Sweden Connect och åtgärder för att kunna läsa dess metadata kommer att kräva omfattande ombyggnationer avseende befintliga elektroniska tjänster inom myndigheten. I avsaknad av närmare kostnadsberäkningar i betänkandet kan Försäkringskassan inte i detalj redovisa och budgetera för kommande kostnader i anledning av förslaget.

1 Författningsförslag

Ansökan om samt utfärdande av den statliga e-legitimationen är i enlighet med presenterat förslag uppdelat på två myndigheter. Förfarandet nödvändiggör behandling av en rad olika personuppgifter, vissa av dem känsliga. Så som utredningens förslag ser ut i nuläget kommer den utfärdande myndigheten att hantera uppgifter och handlingar i olika system, där en databas över medel för elektronisk identifiering regleras särskilt i ett antal paragrafer. Det är till viss del oklart vilka uppgifter som hanteras utanför databasen och således behandlas på ett annat sätt hos den utfärdande myndigheten. Därtill finns det aspekter avseende den informationshantering som faller inom ramen för den identitetskontrollerande myndighetens verksamhet som behöver förtydligas. I samband med det uppkommer även frågor om sekretess. I nyssnämnda hänseenden krävs viss översyn avseende presenterade författningsförslag. Närmare detaljer följer nedan med uppdelning i berörda författningsförslag. Synpunkter av mer redaktionell karaktär föreslås även avseende förslag till lag om elektronisk identifiering.

1.1 Förslag till lag om elektronisk identifiering

16, 20 och 21 §§

I 20 § regleras ändamålet med personuppgiftsbehandlingen hos såväl den utfärdande som den identitetskontrollerande myndigheten. Vid en jämförelse mellan punkt 1 och 2 i första stycket i paragrafen kan man ana att uppgifter hanteras vid sidan av den föreslagna databasen och att det således finns ett särskilt system för att hantera ansökan och andra åtgärder av mer administrativ karaktär, det vill säga ett slags ärendehanteringssystem. Det vore för tydlighets skull lämpligt att införa en skrivelse som visar att det finns, eller förutsätts finnas, ett sådant system.

Ett alternativt till ett förtydligande enligt ovan kan vara en omskrivning i 16 § så att det därigenom framgår att databasen inte ska användas för handläggningsändamål. Det kan göras genom ett tillägg av ordet ”endast” enligt följande ”…*föra en databas som endast innehåller en samling uppgifter om statliga medel för*…”.

I fråga om 16 § kan även övervägas om formuleringen ”har utfärdat” bör bytas mot ”utfärdar”, detta med hänsyn till att uppgifter löpnade förs in i databasen.

Behandling av känsliga personuppgifter regleras i 21 §. I andra stycket 1 omnämns endast databasen. Denna skrivelse synes exkludera den personuppgiftbehandling som kan ske i den utfärdande myndighetens ärendehanteringssystem och i den identitetskontrollerande myndighetens för ändamålet framtagna system, vilket – om det inte är avsikten – bör ses över.

23 och 24 §§
I 23 § regleras tillgång till personuppgifter inom ramen för såväl den utfärdande som den identitetskontrollerande myndighetens verksamhet. Det kan övervägas om bestämmelsen bör kompletteras med en skrivelse om att åtkomst till personuppgifter ska kontrolleras och följas upp regelbundet. Det finns förvisso en föreskriftsrätt avseende personuppgiftstillgång i 24 §. Ur ett tydlighetsperspektiv kan det emellertid finnas fördelar med att frågor om kontroll och uppföljning behandlas direkt i aktuell lag. I 24 § 2 ges möjlighet till ytterligare föreskrifter avseende säkerhetsåtgärder. Krav på sådana säkerhetsåtgärder framgår dock redan av ett antal artiklar i EU:s dataskyddsförordning[1]. För det fall 23 § kompletteras enligt ovan förslag och i ljuset av befintlig reglering kan det övervägas om 24 § ska anses behövlig.

Synpunkter av redaktionell karaktär
Det bör övervägas en kursiv rubrik ovanför 15 § med följande lydelse: *Förhållandet till annan reglering.*

Om nuvarande 16-18 §§ placeras efter 20 § får man en bättre koncentration av de lagrum som avser personuppgiftsbehandling, vilket gör det lättare att överblicka regleringen.

Rubriken till 20 § lyder ”*Ändamål*”. I förtydligande syfte bör en rubrik som lyder ”*Ändamål för behandling av personuppgifter*” övervägas.

Rubriken till 22 § lyder ”*Integritetshöjande och säkerhetshöjande åtgärder*”. För att förtydliga vad paragrafen faktiskt avhandlar bör en annan rubrik övervägas, förslagsvis ”*Sökbegränsningar*”. Jämför 17 § lagen (2015:899) om identitetskort för folkbokförda i Sverige.

Bestämmelsen i 25 §, som rör rätten att göra invändning, bör flyttas upp i lagrumsordningen och komma närmast efter 15 §. Denna rockad faller sig logisk med hänsyn till att de båda lagrummen rör tillämplighet av EU:s dataskyddsförordning. Vidare bör rubriken till 25 § ändras till ”*Begränsning av rätten att göra invändningar*” vilket ger en mer rättvis bild av vad paragrafen handlar om.

1.3 Förslag till förordning om elektronisk identifiering

I 16 § regleras frågor om gallring. Enligt Försäkringskassan bör bestämmelsen ta sikte på samtliga uppgifter och handlingar som den utfärdande myndigheten hanterar, inte bara de som återfinns i databasen. Vidare uppkommer frågan hur denna bestämmelse förhåller sig till 18 § 2 förslag till lag om elektronisk identifiering, där längsta tid för behandling av personuppgifter i databasen omnämns i fråga om möjlighet att meddela föreskrifter. Bestämmelser om gallring och bestämmelser om längsta tid för personuppgiftsbehandling fyller inte samma funktion och är inte helt utbytbara[2].

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). Se exempelvis kapitel IV avsnitt 2 i förordningen.
[2] Prop. 2023/24:29 s. 79 f

1.4 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

6 §
Enligt den föreslagna lydelsen ska sekretess gälla för ”Myndigheten för digital förvaltnings databas över statliga medel för elektronisk identifiering”. Enligt förslaget är således sekretessen begränsad till att avse endast den databas som den utfärdande myndigheten är ansvarig för. Fingeravtrycken, eller de biometriska uppgifter som tas fram ur dessa, får emellertid inte sparas i databasen utan ska endast lagras tillfälligt i vad som får förstås vara den utfärdande myndighetens ärendehanteringssystem. Förslaget enligt 6 § kommer således inte omfatta uppgifter i ärendehanteringssystemet under den tillfälliga lagringstiden. Därmed är det enligt Försäkringskassans mening tveksamt om man tillmötesgår kraven i artikel 9 i EU:s dataskyddsförordning. Artikelns punkt 2 g) utgör grund för mycket av den behandling av känsliga personuppgifter som utförs av myndigheter och föreskriver undantag från det förbud avseende personuppgiftsbehandling som framgår av artikelns punkt 1. Således är bland annat behandling av biometriska uppgifter i identifikationssyfte tillåten om nationell rätt innehåller bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Med nu föreslagen skrivelse kan det ifrågasättas om nationell rätt lever upp till förordningens krav.

Vidare noteras att nu föreslagen utformning av 6 § endast tar i beaktande sekretess för uppgifter hos den utfärdande myndigheten som har registrerats i dess databas. Den informationshantering som sker hos den identitetskontrollerande myndigheten omfattas inte av föreslagen skrivelse. Försäkringskassan önskar att man redogör för hur skyddet ser ut avseende uppgifter hos den identitetskontrollerande myndigheten.

Försäkringskassan har inte några synpunkter på förslagen i övrigt.

Beslut i detta ärende har fattats av generaldirektör Nils Öberg i närvaro av rättschef Marie Axelsson, IT-direktör Peter Haglind och rättslig expert Charlotte Törnblom Karlberg, den senare som föredragande.

Nils Öberg

Charlotte Törnblom Karlberg