MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Yttrande

Diarienummer: 2023–4554

Klassificerings-ID: 3.5.2

Datum: 2024-01-30

Finansdepartementet

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

En säker och tillgänglig statlig e-legitimation (SOU 2023:61)

(dnr Fi2023/02704)

Myndigheten för digital förvaltning (Digg), som har i uppdrag att samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig, lämnar följande synpunkter.

Sammanfattning

Digg tillstyrker i huvudsak utredningens förslag men lämnar vissa synpunkter.

- Samtliga uppgifter om innehavaren, utöver den nyckel som används för att koppla ihop den fysiska bäraren med innehavaren, ska lagras i det register som Digg ska föra, och inte i den fysiska bäraren. Detta minskar kostnaden för utfärdandet av korten, underlättar för ändring och spärr av korten och förhöjer säkerheten i korten.
- Digg anser att ansiktsbild och dess biometriska uppgifter ska lagras i det register som Digg för, inte i den fysiska bäraren. Digg anser dock att fingeravtryck och dess biometriska uppgifter inte alls ska lagras i den statliga e-legitimationen eftersom det saknas sätt att använda dessa för autentisering på distans.
- Digg anser att det kan finnas behov av reglering av förlitande parters användning av biometriska uppgifter för autentisering. Det är inte klart om det bemyndigande som Digg ges att meddela föreskrifter om verkställigheten av förslaget till förordning om elektronisk identifiering omfattar ett bemyndigande att föreskriva om användning av biometriska uppgifter för autentisering.
- Den fysiska bäraren bör inte certifieras som en anordning för att skapa kvalificerade elektroniska underskrifter, eftersom det utgör en onödigt kostsam funktionalitet för kortet. Istället bör Digg ges i uppdrag att ta fram en statlig tjänst som kan användas för att framställa sådana kvalificerade elektroniska underskrifter.
- Digg anser att personkretsen för den statliga e-legitimationen även bör omfatta personer med samordningsnummer som har gjort sin identitet sannolik. Risker med samordningsnummer

uppstår inte vid utgivning utan vid användning, riskerna behöver därmed hanteras av förlitande parter. Det saknas också samband mellan en e-legitimations tillitsnivå och ett samordningsnummers identitetsnivå.

- Digg lämnar ett antal synpunkter på regleringen av behandling av personuppgifter.
- Digg bör ges ett bemyndigande att meddela föreskrifter om behandling av personuppgifter i de fall då Digg är personuppgiftsansvarig i förhållande till de identitetskontrollerande myndigheterna.

Generella synpunkter

Digg välkomnar utredningens förslag om den statliga e-legitimationen och att utredningens förslag i stort linjerar med de förslag som Digg la i myndighetens rapport *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas.* [1]

Digg delar uppfattningen att den statliga e-legitimationen på sikt bör kombineras med ett fysiskt id-kort. Förutsättningarna för detta bör lämpligen utredas i en statlig utredning, som också tar om hand utestående frågor om användning av biometriska uppgifter för autentisering.

Digg vill också påtala att Digg, i samma rapport, lyfte ett antal förslag på ytterligare åtgärder för att minska det digitala utanförskapet, bland annat att en utredning bör tillsättas som föreslår sätt att hantera de restriktioner ett förvaltarskap medför med avseende på e-legitimationer.

7.2 Utformning av den statliga e-legitimationen

7.2.3 Den statliga e-legitimationen ska innehålla namn och identitetsbeteckning

Digg vill förtydliga att det är centralt för den tekniska lösningen att den fysiska bäraren är fri från personuppgifter, annat än det kryptografiska nyckelpar som används för att koppla ihop den fysiska bäraren med innehavaren i Diggs register, samt eventuellt serienummer. När det i författning anges att ”den statliga e-legitimationen ska innehålla” bör detta enligt Digg därför inte förstås som att det är den fysiska bäraren som avses.

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

Digg delar utredningens bedömning att en personlig prägel bör kunna användas i syfte att särskilja den statliga e-legitimationens fysiska bärare från andra kort. Den statliga e-legitimationen syftar bland annat till att minska det digitala utanförskapet och det är därför viktigt med ett särskilt fokus

[1] *Dnr. I2022/01335.*

på tillgänglighetsfrågor. Hänsyn behöver dock också tas till möjligheten till en robust försörjningskedja och en tillförlitlig leveransförmåga även i tider då det råder störningar i logistik och kommunikation. Digg bedömer att leveransförmågan riskerar att påverkas negativt om det ställs krav på att kortet redan i tillverkningssteget förses med en sådan personlig prägel. Digg anser istället att baksidan av kortet förses med en skrivbar yta som innehavaren kan använda för att märka kortet med ett personligt kännetecken. I de fall det finns behov av taktila kännetecken bör dessa påföras i efterhand, exempelvis i form av ett klistermärke.

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

Digg tillstyrker att ansiktsbild och dess biometriska uppgifter ska lagras i den statliga e-legitimationen, men anser att de ska lagras i det register som Digg för och inte i den fysiska bäraren. Digg avstyrker dock att fingeravtryck och dess biometriska uppgifter alls ska lagras i den statliga e-legitimationen.

Enligt Diggs uppfattning bör Digg ges förutsättningar vid den föreslagna lagen och förordningens införande att lagra ansiktsbilder och dess biometriska data i det register som Digg ska föra, så som utredningen också föreslår. Ansiktsbilden och dess biometriska uppgifter kan då användas vid utgivning av den statliga e-legitimationen, och ansiktsbilden (men inte dess biometriska uppgifter) kan tillhandahållas till förlitande part vid autentisering, samt användas vid utgivning av en europeisk digital identitetsplånbok. Det behöver emellertid säkerställas att det finns rättsliga förutsättningar för Digg att lämna ut ansiktsbilder för autentisering till förlitande parter, med tanke på att utredningen föreslår sekretess för uppgifter i registret som innehåller ett omvänt skaderekvisit vad gäller fotografisk bild (jfr. utredningens förslag till förordning om ändring i offentlighets- och sekretessförordningen [2009:641]).

Diggs synpunkter om lagring av ansiktsbild

Digg anser att säkerheten för ansiktsbilden ökar och kostnaderna minskar om ansiktsbilden tillhandahålls från registret, istället för på den fysiska bäraren. Digg bedömer dessutom att lagring av ansiktsbild på den fysiska bäraren inte är förenlig med den tekniska lösning som utredningen föreslår, då lösningen innebär att personuppgifter framförallt av säkerhetsskäl inte lagras i bäraren. Dessa skäl beskrivs i Diggs rapport *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas.* [2]

För att ansiktsbilder ska kunna lagras i bäraren på ett säkert sätt måste de även skyddas mot obehörig avläsning och spridning. Det komplicerar utformningen av bäraren på ett högst väsentligt sätt, och potentiellt även användningen av den. Digg bedömer därutöver att kostnaderna för att ta fram e-legitimationen skulle öka om ansiktsbild ska lagras på den fysiska bäraren. Det kommer också

[2] *Bilaga 1 – Teknisk beskrivning av de föreslagna funktionerna (I2022/01335).*

att förlänga införandetiden, eftersom detta innebär nya typer av kortfunktioner som inte tidigare utvecklats och det därför saknas standarder och specifikationer för detta.

Diggs synpunkter om användning av fingeravtryck och dess biometriska uppgifter för autentisering

Det finns idag inga sätt att använda fingeravtryck och dess biometriska uppgifter för autentisering på distans. Sådan autentisering kräver att det fingeravtryck som lämnas för att jämföras med det lagrade fingeravtrycket lämnas med användning av betrodd utrustning för att läsa av fingeravtrycket, och kräver också att det går att verifiera att det faktiskt är en levande person som lämnar fingeravtrycket. Digg ser därför mycket stora utmaningar med att möjliggöra autentisering på distans med användning av fingeravtryck, eftersom tekniken saknas idag och det framstår inte som realistiskt att den kommer finnas tillgänglig inom överskådlig framtid.

7.3 Den statliga e-legitimationen bör kunna användas för att skapa kvalificerade elektroniska underskrifter

Digg instämmer i bedömningen av att den statliga e-legitimationen bör kunna användas för att skapa kvalificerade elektroniska underskrifter men avstyrker en av de lösningar som utredningen föreslår. Digg anser att utredningens förslag att den statliga e-legitimationen ska utgöra en anordning för att kunna skapa kvalificerade elektroniska underskrifter, utgör en onödigt kostsam funktionalitet för kortet. Skälet som utredningen anför för detta är bland annat att det vore billigare att använda ett kort med anordning för att skapa kvalificerade underskrifter än att skapa en statlig tjänst för att skapa kvalificerade elektroniska underskrifter. Digg anser dock att kostnaden för att skapa en sådan tjänst skulle understiga kostnaden av att använda ett certifierat kort. Digg förordar därför att myndigheten på sikt ges i uppdrag att ta fram en sådan statlig tjänst, snarare än att varje kort ska certifieras.

7.4 Tillhandahållande av den statliga e-legitimationen

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

Digg tillstyrker att den statliga e-legitimationen ska tillhandahållas till personer med samordningsnummer, men anser att personkretsen även bör omfatta personer som har gjort sin identitet sannolik. Digg har förståelse för behovet av att adressera problem med bedrägerier där personers samordningsnummer exploateras som brottsverktyg, men saknar ett resonemang kring den säkerhetsrisk som utredningen har bedömt finns med den statliga e-legitimationen om den även

skulle utfärdas till personer med samordningsnummer med sannolik identitetsnivå. Digg vill därför göra ett antal förtydliganden avseende utredningens förslag.

Tillitsramverket för Svensk e-legitimation vilar på några grundpelare i den svenska samhällsstrukturen, varav de två viktigaste är den svenska folkbokföringen och de id-handlingar som idag allmänt erkänns som fullgoda. Svenska e-legitimationer kan därför sägas ärva egenskaperna från tidigare led, och om folkbokföringsdatabasen innehåller felaktiga uppgifter, eller om en id-handling ges ut på felaktiga grunder, kan motsvarande felaktigheter återspeglas i utgivningen av e-legitimationer. Digg anser därför att det är av största vikt att lösa rätt frågor i rätt led, och att de myndigheter som ansvarar för tilldelning av identitetsbeteckningar respektive fysiska id-handlingar ges tillräckliga förutsättningar för att säkerställa att dessa överensstämmer med verkliga förhållanden.

Diggs förtydligande avseende hantering av risker

Innehavet av en e-legitimation medför i sig inte några rättigheter. Riskerna med samordningsnummer uppstår därför inte vid *utfärdandet* av en e-legitimation, utan vid *användandet* av e-legitimationen. Och likt utredningens resonemang avseende utgivning till minderåriga behöver även dessa risker motverkas av förlitande parter, genom att i ärendehandläggningen själva bedöma vad en person med samordningsnummer med en viss identitetsnivå ska kunna utföra och vilka eventuella tillkommande kontroller som bör göras för att hantera risker med olika former av bedrägerier. Förlitande parter behöver hämta in och kontrollera uppgift om ett samordningsnummers identitetsnivå från folkbokföringen, då det identitetsintyg som förmedlas vid en e-legitimering inte innehåller denna uppgift.

Riskerna minskas därmed inte genom att begränsa utgivningen av den statliga e-legitimationen till den styrkta identitetsnivån, utan genom att öka kunskapen hos förlitande parter kring samordningsnummer och vikten av att tillgodogöra sig den information som finns om dessa identitetsbeteckningar. Den statliga e-legitimationen bör därtill möjliggöra de digitala interaktioner som förlitande parter bedömer vara nödvändiga och lämpliga.

Diggs förtydligande avseende tillitsnivåer

Det finns inget samband mellan en e-legitimations *tillitsnivå* och vilka rutiner som tillämpats vid tilldelningen av ett samordningsnummer på en viss *identitetsnivå*. En Svensk e-legitimation får ges ut till personer med samordningsnummer som har styrkt sin identitet eller gjort identiteten sannolik, oavsett tillitsnivå. På motsvarande sätt innehåller eIDAS-förordningen inga krav på hur medlemsländerna ska hantera sina respektive befolkningsregister. Det är således, till skillnad från vad utredningen anför i avsnitt 9.9, fullt möjligt att med erforderlig säkerhet ge ut e-legitimationer baserat på samordningsnummer med sannolik identitetsnivå även på tillitsnivå 4 och den motsvarande tillitsnivån Hög för gränsöverskridande användning. Att den statliga e-legitimationen föreslås ges ut på den högsta tillitsnivån utgör därför i sig inget hinder mot att tillåta personer med samordningsnummer med sannolik identitetsnivå att ansöka om en statlig e-legitimation, och efter en identitetskontroll även kunna tilldelas en sådan, förutsatt att övriga krav är uppfyllda.

Diggs förslag om en samordnad identitetskontroll

Digg vill också påtala att konsekvensen av utredningens förslag blir att det för en person med samordningsnummer med sannolik identitetsnivå skulle krävas två personliga besök, till två separata myndigheter, för i grunden samma ärende: ett första besök till Skatteverket för att styrka sin identitet i syfte att få uppgift om styrkt identitet registrerad, därefter till den identitetskontrollerande myndigheten för att återigen styrka sin identitet, på väsentligen samma sätt, för att skaffa en statlig e-legitimation. Det kan därför finnas skäl att överväga en samordnad identitetskontroll för att underlätta för den sökande.

7.6 Ansvar för grundidentifiering och utfärdande

7.6.2 Få myndigheter bedöms ha de förutsättningar som krävs

Digg delar utredningens bedömning om att Polismyndigheten är den myndighet som är bäst lämpad för att utföra grundidentifiering i samband med utfärdande av en statlig e-legitimation.

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

Digg tillstyrker utredningens förslag och anser att myndigheten är lämpad för att ansvara för utfärdandet av den statliga e-legitimationen. Digg avser att vidta åtgärder för att säkerställa att de rollkonflikter som beskrivs av utredningen inte kommer att innebära några negativa konsekvenser i fråga om bland annat förtroende eller konkurrens (jfr. också avsnitt 7.10.4 i betänkandet).

7.7 Giltighetstid och återkallelse

7.7.2 Återkallelse och spärr av e-legitimationen

Digg avstyrker utredningens förslag om att den statliga e-legitimationen ska spärras automatiskt när dess giltighetstid har gått ut. En e-legitimations giltighetstid kontrolleras alltid vid autentisering, e-legitimationen blir därmed obrukbar när dess giltighetstid har passerat utan att ett särskilt spärrförfarande behöver ske. Att, som utredningen föreslår, också spärra e-legitimationen kommer enligt Diggs bedömning leda till onödig lagring av spärrinformation.

Digg anser att det är otydligt vad som faktiskt avses med återkallelse av e-legitimationen. Enligt Diggs uppfattning är det fullt tillräckligt att reglera spärr av e-legitimationen, eftersom den fysiska bäraren inte ska återlämnas när e-legitimationen har spärrats eller blir ogiltig.

Digg vill också upprepa vikten av att identitetsuppgifter endast sparas i registret, inte i bäraren (se 7.2.3). Det gör det möjligt att vid exempelvis namnbyte ändra uppgift i registret istället för att spärra

e-legitimationen. Därmed besparas användaren ett nytt ansökningsförfarande och en ny ansökningsavgift.

Mot bakgrund av Diggs resonemang om samordningsnummer (se 7.4.2) anser Digg även att ett samordningsnummer som ändrar identitetsnivå från styrkt till sannolikt inte bör leda till att den statliga e-legitimationen spärras. På motsvarande sätt kan det övervägas om en vilandeförklaring av ett samordningsnummer nödvändigtvis måste leda till att e-legitimationen spärras. Förlitande parter måste som angett likväl göra kontroller mot folkbokföringsdatabasen för att erhålla nödvändiga uppgifter om bland annat identitetsnivå. Som anges i 3 kap. 3 § lagen (2022:1697) om samordningsnummer kan Skatteverket förnya ett vilandeförklarat samordningsnummer. En spärr av den statliga e-legitimationen är dock oåterkallelig. Därför kan det övervägas om det finns andra lämpligare sätt att begränsa riskerna för att vilandeförklarade samordningsnummer missbrukas.

7.8 Användningen av den statliga e-legitimationen

Särskild reglering och rättspraxis i fråga om användning av e-legitimationer för betalningstransaktioner och ingående av kreditavtal

Digg anser att det är otydligt huruvida utredningen anser att betaltjänstlagens bestämmelser avseende obehöriga transaktioner är tillämpliga för de e-legitimationer – däribland den statliga e-legitimationen – som inte utfärdats av en betaltjänstleverantör. Digg ser därför att det finns behov av ett förtydligande i den fortsatta beredningen.

Behov av författningsreglering vid användning av den statliga e-legitimationen

Digg delar utredningens bedömning att det finns behov av författningsreglering av användning av den statliga e-legitimationen. Digg vill dock påtala att det inte är tydligt om det bemyndigande som ges enligt 27 § förslaget till lag om elektronisk identifiering faktiskt är delegerat till Digg i den tillhörande förordningen. Det synes inte ha varit avsikten med utredningens förslag att det bemyndigande som omfattar verkställighet av förordningen (9 § tredje stycket föreslagen förordning om elektronisk identifiering) ska omfatta villkor för när och hur den statliga e-legitimationen ska användas. Detta innebär i sådana fall att det saknas sådan reglering av när och hur den statliga e-legitimationen ska användas som utredningen anser behövs, och det saknas också bemyndigande för Digg att föreskriva om detsamma. Digg efterfrågar därför förtydligande i denna del.

7.9 Finansiering av den statliga e-legitimationen

Digg anser att priset för den statliga e-legitimationen är högt och att det kan medföra att färre skaffar e-legitimationen. Digg anser inte att det är kostnaden för kortet i sig som medför att kortet uppfattas som en värdehandling, och detta bör inte ensamt motivera priset för kortet. Det finns andra värdehandlingar som inger denna känsla hos användaren, exempelvis körkort, utan att vara förknippade med en hög kostnad. Det kan därför vara skäl att fråga sig om det är priset som avgör den upplevda känslan av en värdehandling, eller om det är vad som finns på själva kortet och vad användaren upplever att andra kan göra med kortet som är avgörande.

7.11 Behandling av personuppgifter

Digg lämnar synpunkter på utredningens förslag om regleringen av behandlingen av personuppgifter.

Digg anser att den föreslagna regleringen av ändamålen i lagen om elektronisk identifiering snarare är en redogörelse för vilka uppgifter som Digg i egenskap av utfärdande myndighet har än ändamålsbestämmelser. I syfte att renodla författningar som avser behandling av personuppgifter anser Digg att materiella bestämmelser som utgångspunkt bör regleras separat från bestämmelser om behandling av personuppgifter, förslagsvis under en egen rubrik i den föreslagna lagen.

Sådan materiell reglering bör ta sikte på Diggs ansvar som utfärdande myndighet att utfärda statligt medel för elektronisk identifiering (jfr. 4 § den föreslagna lagen), att föra register med en samling av uppgifter om statliga medel för elektronisk identifiering som myndigheten har utfärdat (jfr. 16 § den föreslagna lagen) samt att möjliggöra en säker användning av statliga medel för elektronisk identifiering (jfr. 20 § första stycket tredje punkten i den föreslagna lagen).

I den föreslagna lagen saknas en bestämmelse om myndighetens ansvar att möjliggöra en säker användning av statliga medel för elektronisk identifiering. Detta regleras i utredningens förslag enbart som ett ändamål med behandling av personuppgifter. Digg anser att det bör läggas till som en av myndighetens uppgifter i den materiella regleringen.

7.11.2 Personuppgiftsansvariga myndigheter

Digg anser att den utfärdande myndigheten bör bemyndigas med en rätt att meddela sådana föreskrifter om personuppgiftsbiträdens hantering av personuppgifter som avses i artikel 28.3 i EU:s dataskyddsförordning. En sådan rätt att meddela föreskrifter skulle väsentligt underlätta den hantering av personuppgiftsbiträdesavtal som annars måste ingås med var och en av de identitetskontrollerande myndigheterna.

7.11.4 Ändamålen med personuppgiftsbehandlingen ska framgå av lagen

Digg avstyrker att det ska finnas en uttömmande reglering av för vilka ändamål som Digg får behandla personuppgifter. Digg anser att ändamålet med behandling av personuppgifter istället bör formuleras brett och kopplas till myndighetens uppgifter i den materiella regleringen om den statliga e-legitimationen (se avsnitt 7.11).

Digg anser att de sekundära ändamålen som är föreslagna att föras in i lagen är obehövliga eftersom de enbart är av upplysande karaktär. Vad gäller uppgiftsutlämnande till Polismyndigheten bedömer Digg att utlämnande kan ske med stöd av 6 kap. 5 § offentlighets- och sekretesslagen (2009:400) och att ett sådant utlämnande är förenligt med de ursprungliga ändamålen för vilka personuppgifter behandlas (se HFD 2021 ref. 10). Av samma skäl behövs det inte någon förtydligande reglering om att personuppgifter får behandlas om det är nödvändigt för att fullgöra ett uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning.

Slutligen anser Digg att som huvudregel bör hänvisning till finalitetsprincipen enbart göras när finalitetsprincipen inte ska gälla.

7.11.5 Lagen ska innehålla bestämmelser om databasen över statliga e-legitimationer

Digg avstyrker användning av begreppet databas i förslagen till lag och förordning om elektronisk identifiering. Begreppet databas håller på att utmönstras ur svensk lagstiftning[3] och är inte teknikneutralt. Digg förordar att begreppet register används istället.

7.12 Sekretess

Digg tillstyrker utredningens förslag om sekretess för uppgifter men anser att begreppet register bör använda istället för begreppet databas.

7.13 Krav om att godta identifiering med vissa e-legitimationer

Digg ser positivt på utredningens förslag om att fler aktörer ska använda de tjänster för elektronisk identifiering som tillhandahålls genom auktorisationssystem. Digg anser att en av de mest centrala åtgärderna på e-legitimationsområdet är att alla digitala tjänster ska acceptera alla e-legitimationer med tillräcklig tillitsnivå, och att lagstiftning är ett nödvändigt steg för att åstadkomma detta. Digg vill dock påtala att kommuners och regioners anslutningsgrad till de tidigare valfrihetssystemen varit förhållandevis låg. Det kan därför finnas anledning att närmare utreda orsakerna till detta, samt om

[3] Se till exempel prop. 2014/15:63 Åklagardatalag, s. 79 f.

ett obligatorium är tillräckligt för att öka anslutningsgraden eller om det krävs ytterligare åtgärder, exempelvis sanktionsmöjligheter för den tillhandahållande myndigheten eller ökat stöd till aktörerna ifråga. Digg vill också påtala att statliga myndigheters skyldighet att ansluta till auktorisationssystem idag regleras av 3 § förordning (2023:798) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Detta yttrande har beslutats av generaldirektör Anna Eriksson. I den slutliga handläggningen har också juristerna Mathea Franzén och Erika Lidén, informationssäkerhetsspecialist Anders Nordlander, specialisterna Maria Engström, Emma Grefberg och Magnus Hoflin, enhetschef Lotta Hämäläinen, säkerhetschef/säkerhetsskyddschef Johan Gellerstedt, avdelningschef tillika ställföreträdande generaldirektör Chanett Edlund samt rättschef Linn Kempe deltagit. Föredragande har varit specialist Krista Arplund.

Anna Eriksson