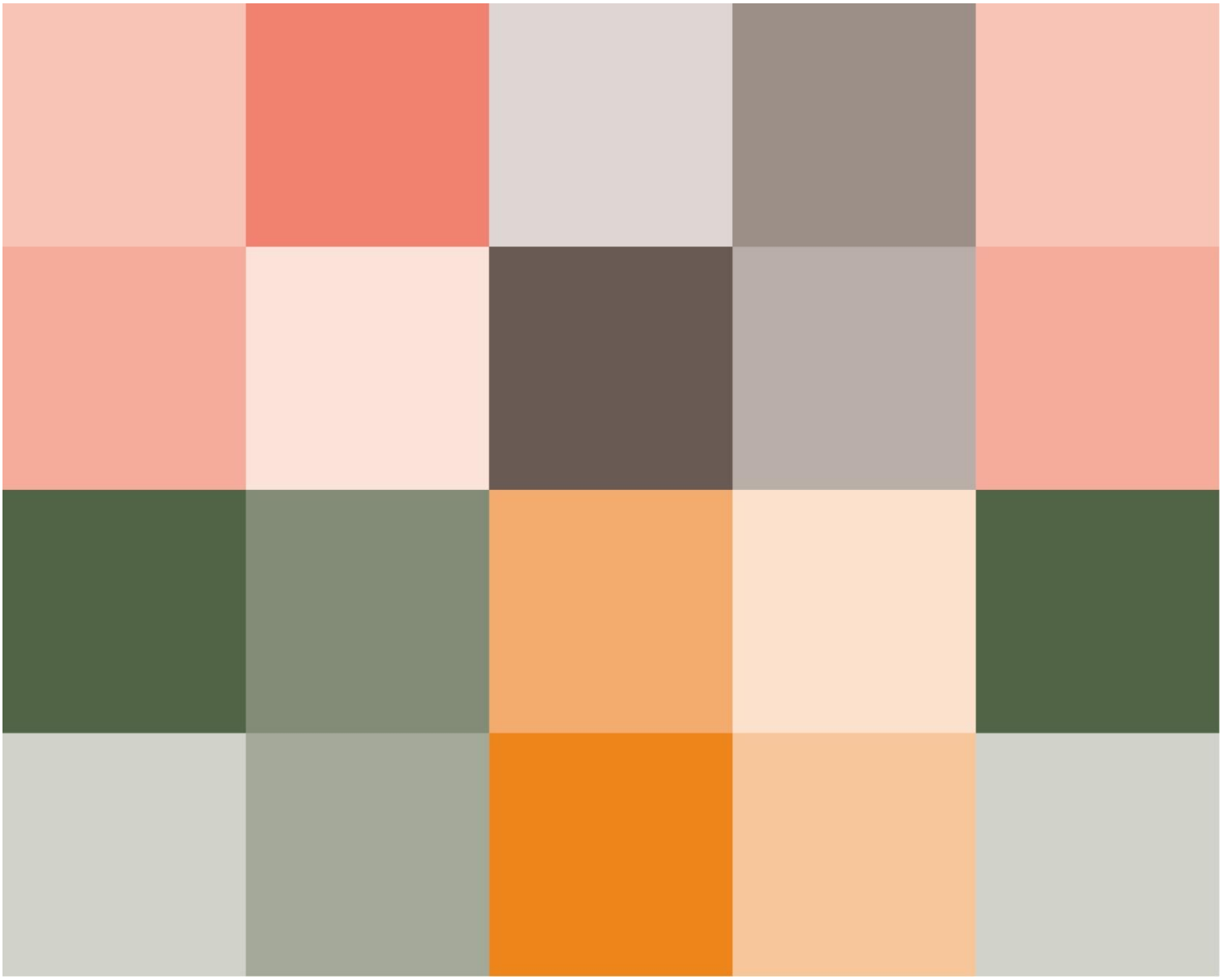

En säker och tillgänglig statlig e-legitimation

Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas (I2022/01335)

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Myndigheten för digital förvaltning, Digg, lämnar här förslag till framtagande och drift av en statlig e-legitimation utifrån regeringsuppdraget att analysera möjligheterna för och lämna förslag om framtagandet och driften av en statlig e-legitimation. I uppdraget har även ingått att föreslå en utformning som innebär att så många som möjligt kan använda e-legitimationen och hur den informations- och cybersäkerhet som krävs ska säkerställas. I den här slutrapporten från regeringsuppdraget redogör Digg också för rättsliga frågor, kostnader, finansiering och tidplan.

Digitaliseringen genomsyrar alla delar av vårt samhälle och Sverige har, ur ett internationellt perspektiv, en mycket hög användning av e-legitimationer. Det finns cirka 6000 tjänster som ställer krav på inloggning med e-legitimation. E-legitimationer är en samhällskritisk infrastruktur som måste fungera dygnet runt, årets alla dagar.

Men alla är inte med. I den så kallade fjärde industriella revolutionen befinner sig uppskattningsvis en miljon människor i Sverige i ett digitalt utanförskap genom att de saknar en e-legitimation. Det finns en mängd olika anledningar till att det är så, såväl strukturella som individuella, vilket kräver olika former av åtgärder. Det behövs en statlig e-legitimation, men det behövs också åtgärder för att få ihop helheten i e-legitimationssystemet, bland annat när det gäller hantering av den ökande brottsligheten. Utvecklingen av en statlig e-legitimation behöver påbörjas och säkerhetsfrågorna måste sättas i fokus. Det digitala utanförskapet måste minska och offentliga aktörer måste erbjuda alla godkända e-legitimationer för inloggning i sina digitala tjänster.

Diggs förslag är att den statliga e-legitimationen utfärdas på ett kontaktlöst aktivt kort. Kortet lämnas ut av en identitetskontrollerande myndighet efter kontroll av giltig id-handling. Den statliga e-legitimationen ska ges ut på den högsta tillitsnivån enligt EU:s regelverk. Digg föreslår också att den statliga e-legitimationen ska kunna ges ut till personer som har tilldelats ett samordningsnummer och kan styrka sin identitet. Vidare bedömer Digg att användarna kommer att efterfråga mobila lösningar på smarttelefoner.

Inom EU pågår utveckling av en europeisk digital identitetsplånbok där det kommer krävas en e-legitimation på den högsta tillitsnivån. Digg föreslår att den statliga e-legitimationen ska kunna användas för att få tillgång till den europeiska digitala identitetsplånboken och att Digg får i uppdrag att påbörja utveckling av e-legitimationen för att möta EU:s tidplan. I ett sådant uppdrag bör det också ingå att ytterligare undersöka hur den statliga e-legitimationen även kan tillhandahållas via de nationella id-korten.

Sverige valde tidigt en försörjningsmodell som bygger på att marknaden tillhandahåller lösningar för e-legitimering. Valet har tjänat digitaliseringen väl och Digg bedömer att

modellen bör bibehållas. Den statliga e-legitimationen föreslås vara ett komplement till de lösningar som marknaden erbjuder och erbjudas på samma villkor. Digg föreslår att den statliga e-legitimationen erbjuds offentliga aktörer via valfrihetssystem och att privata aktörer får tillgång till identifieringstjänsten för att sedan kunna utfärda identitetsintyg till digitala tjänster.

Genom att staten utfärdar digitala id-handlingar på samma sätt som fysiska id-handlingar utfärdas skapas nya möjligheter för utveckling och innovation samtidigt som själva utgivningsprocessen av den statliga e-legitimationen uppfyller kraven för den högsta tillitsnivån.

Men det räcker inte med att det finns en statlig e-legitimation. Den måste också gå att använda. Digg återkommer därför i rapporten till ett tidigare lämnat förslag om att myndigheter, kommuner och regioner måste acceptera alla godkända e-legitimationer. Detta kräver ny reglering och Digg välkomnar i rapporten att regeringen nyligen tillsatt en utredning som ska analysera frågan.

I konsekvensanalysen bedömer Digg att de sammanlagda kostnaderna för utveckling och uppbyggnad av verksamheten hos Digg uppgår till 80–100 miljoner kronor. De årliga kostnaderna för Digg bedöms därefter till cirka 70 miljoner kronor och årliga kostnader för de identitetskontrollerande myndigheterna bedöms till cirka 30 miljoner kronor. Baserat på utgivningsvolymerna kommer det över tid vara nödvändigt att se över beräkningarna. Digg bedömer utvecklingstiden till 24 månader, när nödvändiga beslut fattats av regering och riksdag.

Innehåll

Bilagor

1 Inledning

1.1 Om uppdraget

Myndigheten för digital förvaltning, Digg, fick den 16 juni 2022 ett regeringsuppdrag att analysera möjligheterna för och lämna förslag om framtagandet och driften av en statlig e-legitimation (I2022/01335).

Denna slutredovisning av uppdraget redogör för resultatet av de analyser som har genomförts. I enlighet med uppdraget redogörs för

- kostnader för att ta fram en statlig e-legitimation,
- de löpande kostnaderna för förvaltning och vidareutveckling samt för utfärdande av e-legitimationen,
- hur lång tid som krävs för att ta fram och kunna börja utfärda en statlig e-legitimation,
- hur utformning bör göras för att så många som möjligt ska kunna använda e-legitimationen,
- vilka personuppgifter som behöver behandlas för att kunna ansvara för den statliga e-legitimationen,
- vilket tekniskt stöd som behövs, hur cyber- och informationssäkerhet ska säkerställas,
- vilka funktioner som behövs för att e-legitimationen ska kunna användas i förhållande till förlitande parter,
- rollfördelningen mellan Digg, Polismyndigheten och utlandsmyndigheterna,
- rollkonflikter inom Digg eller andra myndigheter,
- finansieringsförslag för identifierade kostnader,
- uttag av avgifter,
- huruvida den statliga e-legitimationen ska finnas i flera format,
- beaktande av den pågående förhandlingen av revidering av eIDAS-förordningen[1],
- övervägande om en statligt utfärdad digital plånbok ska utgöra den statliga e-legitimationen, samt
- konsekvenser av de förslag som lämnas.

[1] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

1.2 Bakgrund

Sedan början av 2000-talet har offentlig förvaltning upphandlat elektronisk identifiering från privata leverantörer, delvis eftersom bankerna tidigt varit framgångsrika med att identifiera sina kunder elektroniskt. Avsikten med att gå upphandlingsvägen var att täcka in de e-legitimationer som användare kunde skaffa och samtidigt driva på innovativ utveckling, där man ansåg att privat sektor var mest lämpad. På grund av ändringar i lagstiftningen om offentlig upphandling 2008 var det då inte längre möjligt att upphandla flera leverantörer för samma typ av tjänster[2]. E-delegationen föreslog i sitt första delbetänkande införande av valfrihetssystem för elektronisk identifiering, där användarens val av e-legitimation skulle styra vilken leverantör som skulle få betalt[3]. E-delegationen bedömde att detta skulle främja mångfald genom att göra det möjligt för nya leverantörer att tillhandahålla tjänster på lika villkor. I en följande utredning lades grunden till en ny myndighet för samordning av den offentliga sektorns försörjning av e-legitimationer[4]. E-legitimationsnämnden startades den 1 januari 2011 och inrättade ett valfrihetssystem som gjorde det möjligt att använda tjänster från olika leverantörer utan att varje offentlig myndighet behövde teckna nya avtal eller genomföra nya tekniska integrationer för varje leverantör. För att möta olika behov inrättades ytterligare valfrihetssystem. När Digg bildades den 1 september 2018 övergick ansvaret för valfrihetssystemen från E-legitimationsnämnden till Digg och nämnden lades ned. Frågan om valfrihetssystem har åter aktualiserats i ett förslag som är under beredning i Regeringskansliet om att valfrihetssystem enligt lag om valfrihetssystem i fråga om tjänster för elektronisk identifiering ska ersättas av auktorisationssystem för sådana tjänster[5].

Styrningen av e-legitimationsområdet har varit föremål för ytterligare utredningar de senaste åren. I december 2017 överlämnade Utredningen om effektiv styrning av nationella digitala tjänster sitt slutbetänkande[6] till regeringen. Slutbetänkandet innehöll ett stort antal förslag till åtgärder för effektiv styrning och är under beredning i Regeringskansliet. Några förslag gällande e-legitimationer har dock tagits vidare. I detta sammanhang är 2017 års ID-kortsutredning relevant med förslagen att en statlig e-legitimation på högsta tillitsnivå ska utfärdas av staten, att den statliga e-legitimationen ska finnas på det statliga identitetskortet och att Polismyndigheten ska utfärda den statliga e-legitimationen[7]. Digg konstaterar att regeringen i och med aktuellt regeringsuppdrag

[2] SOU 2010:104. Utredningen om bildande av en e-legitimationsnämnd. *E-legitimationsnämnden och Svensk e-legitimation: slutbetänkande.*

[3] SOU 2009:86. E-delegationen. *Strategi för myndigheternas arbete med e-förvaltning: delbetänkande.*

[4] SOU 2010:104.

[5] Regeringskansliet. *Auktorisationssystem för elektronisk identifiering och digital post: promemoria.* 21 december 2020.

[6] SOU 2017:114. Utredningen om effektiv styrning av nationella digitala tjänster. *reboot – omstart för den digitala förvaltningen: slutbetänkande.*

[7] SOU 2019:14. 2017 års ID-kortsutredning. *Ett säkert statligt id-kort – med e-legitimation: slutbetänkande.*

valt att inte följa förslaget från 2017 års ID-kortsutredning avseende Polismyndighetens roll utan istället uppdragit åt Digg att utreda ansvaret för en statlig e-legitimation i alla delar förutom själva grundidentifieringen.

1.3 Metod

Digg delade in uppgifterna i regeringsuppdraget i de tre arbetspaketen Teknik, säkerhet och digital inkludering, Rättsliga frågor och Kostnader och finansiering, vilket också återspeglas i slutrapportens struktur.

Ansvaret för den statliga e-legitimationen innebär nya arbetsuppgifter för Digg som idag inte omfattas av myndighetens instruktion och inte heller har annat stöd i rättsordningen. Den statliga e-legitimationen kommer därför att behöva regleras genom ny författning. Digg inkommer av den anledningen med förslag på hur en författning för den statliga e-legitimationen kan utformas, se bilaga 4.

Digg har i uppdragets genomförande samarbetat med Polismyndigheten i frågor kopplade till utgivningsprocessen. Polismyndigheten har bistått med kompetens inom flera centrala områden, särskilt teknik, säkerhet, juridik och kostnadsanalys. Den 21 december 2022 inkom Polismyndigheten med promemorian i bilaga 2. Av promemorian framgår att det inom myndigheten pågår ett arbete med att renodla verksamheten, i syfte att ge Polismyndigheten möjlighet att fokusera på kärnverksamheten, det vill säga att minska brottsligheten och öka tryggheten. Polismyndigheten anför i promemorian att nya uppgifter, såsom grundidentifiering vid utfärdande av en statlig e-legitimation, inte bör påföras myndigheten. Anledningen till detta ställningstagande uppges vara att uppgifterna inte har polisiär relevans eller direkt kräver polisiär befogenhet, utan kan påföras annan huvudman. Digg har beaktat detta ställningstagande i föreliggande rapport, vilket fått konsekvensen att analyser gällande verksamheten vid passexpeditionerna inte varit möjliga att slutföra. I bilaga 3 kommenterar Digg de bedömningar Polismyndigheten anför i sin promemoria gällande den föreslagna tekniska lösningen för en statlig e-legitimation.

Försäkringskassan har bistått Digg med erfarenheter från den e-tjänstelegitimation (EFOS[8]) som Försäkringskassan tillhandahåller till tjugo statliga myndigheter. Erfarenheterna från Försäkringskassan har främst innefattat digital inkludering och kostnadsanalys kopplat till drift och förvaltning av en e-legitimation på den högsta tillitsnivån. Utrikesdepartementet har bistått Digg i frågor rörande utlandsmyndig-

[8] E-identitet för offentlig sektor

heternas roll i utgivningsprocessen. Myndigheten för samhällsskydd och beredskap (MSB) har bistått Digg i frågor rörande informations- och cybersäkerhet.

1.4 Avgränsningar

I arbetet med regeringsuppdraget har avgränsningar mot relaterade frågor löpande gjorts. Av hänsyn till den begränsade tid som stått till förfogande för att arbeta med en så pass omfattande uppgift som ett förslag till utformning av en statlig e-legitimation utgör, har det varit nödvändigt att avgränsa frågor kopplade till myndigheter som inte omfattas av aktuellt regeringsuppdrag. Det är fallet exempelvis när det gäller roller och uppgifter som Skatteverket och Statens servicecenter skulle kunna inneha.

Frågor som identifierats i uppdraget och som kräver ytterligare fördjupning alternativt bör utförs av någon annan än Digg återges i rapportens avslutande kapitel 9.

2 Sverige behöver en statlig e-legitimation

Sverige är ett av ett fåtal länder inom EU som inte har en statlig e-legitimation. Frågan har diskuterats under många år och utretts i flera omgångar. Utredningarna har samstämmigt slagit fast att Sverige behöver en statlig e-legitimation. Det nu förändrade säkerhetspolitiska läget, ett växande digitalt utanförskap och nya krav från EU gör frågan om en statlig e-legitimation mer aktuell än någonsin.

Digg välkomnar att regeringen tillsatt en ny utredning som fått i uppdrag att lämna förslag på hur en kostnadseffektiv statlig e-legitimation på högsta tillitsnivå kan utformas och tillhandahållas av Digg[9]. Detta understryker ytterligare frågans aktualitet.

2.1 En samhällskritisk infrastruktur

Säkerhetsläget i Sveriges närområde har på mycket kort tid allvarligt försämrats[10]. Hoten är komplexa, och en stor del av dessa riktar sig mot cyberdomänen. Samtidigt som den digitala utvecklingen har tjänat Sverige väl, följer med den också nya sårbarheter. Incidenter och angrepp mot våra digitala system har allt mer riktat uppmärksamheten mot cybersäkerhet och samhällets sårbarhet. Säpo konstaterar i sin årsbok 2021[11] att gapet mellan Sveriges förmåga att skydda sig mot ett cyberangrepp och motståndarens kapacitet består, vilket utgör en allvarlig sårbarhet.

Regering och riksdag har slagit fast att e-legitimationer är en samhällskritisk infrastruktur[12] [13]. Sådan infrastruktur måste fungera dygnet runt, årets alla dagar. I dagsläget är vi helt beroende av privata företags leveranser av e-legitimationer och det stora beroendet av en enskild leverantör gör samhället sårbart. Genom de cyberangrepp som riktats mot centrala funktioner de senaste åren har vi fått en försmak på hur det är när tekniken inte fungerar. Sverige är ett av ett fåtal länder i EU där det allmänna inte råder över den samhällskritiska digitala infrastruktur som e-legitimationer utgör. Digg är av meningen att det behövs en förändring.

Behovet av en statlig e-legitimation har påtalats av bland annat statliga myndigheter, Sveriges Kommuner och Regioner (SKR) och en rad intresseorganisationer sedan minst ett decennium utifrån perspektivet att det saknas en statligt utfärdad e-legitimation på den

[9] Dir. 2022:142. *Säker och tillgänglig digital identitet.*
[10] Försvarets radioanstalt. *Medarbetare i demokratins tjänst.* Årsrapport 2021.
[11] Säkerhetspolisen. *Säkerhetspolisen 2021.*
[12] Näringsdepartementet. *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi.* N2017/03643/D.
[13] Betänkande 2021/22:TU6. *Digitaliserings- och postfrågor.*

högsta tillitsnivån. Digg har i rapporter[14] [15] till regeringen det senaste året lyft fram behovet och ett av Diggs främsta argument är robusthetsperspektivet, att en statlig e-legitimation skulle kunna utgöra ett alternativ när andra lösningar inte är tillgängliga.

Digitaliseringsrådet, som inrättades av regeringen i syfte att bidra till bättre samordning och ett effektivt genomförande av regeringens strategiska arbete med digitalisering, påtalade behovet av en statlig e-legitimation. Rådet, som var verksamt 2017–2021, föreslog i en rapport till regeringen att det måste bli enklare att skaffa en e-legitimation utan att ge avkall på säkerheten[16]. De föreslog i samma rapport också att Digg skulle ges i uppdrag att öka den digitala tillgängligheten vid utformningen av e-legitimationslösningar med syfte att skapa förtroende och göra det möjligt för alla invånare att bli användare.

Riksbanken och Finansinspektionen är ytterligare exempel på myndigheter som har uttryckt likartade synpunkter. Riksbanken skrev följande i sitt remissvar på slutbetänkandet från 2017 års ID-kortsutredning[17]:

Enligt vad utredningen angett har många personer i Sverige redan en e-legitimation. Riksbanken delar utredningens betänkligheter mot att endast en privat aktör ges en så dominerande ställning på den svenska marknaden för e-legitimationer. Att endast privata aktörer utfärdar e-legitimation medför att staten inte kontrollerar villkoren för e-legitimationerna. Staten har därmed också begränsade möjligheter till insyn i och påverkan av e-legitimationens närmare utformning. Utredningen har visat att det finns behov av alternativa lösningar för e-legitimation utifrån flera perspektiv, särskilt när det gäller säkerhet, robusthet och tillgänglighet. I dag finns det inte något reellt alternativ att använda sig av om de privat utfärdade e-legitimationerna av någon anledning inte skulle fungera. Riksbanken håller därför med utredningen om att det även ur kontinuitets- och beredskapsperspektiv finns behov av en säker lösning som kan användas om de privata e-legitimationerna upphör att fungera.

Finansinspektionen gjorde i en rapport till regeringen i maj 2022 bedömningen att ett cyberangrepp som slår ut BankID kan få allvarliga konsekvenser för flera delar av det svenska samhället och att det därför finns skäl för samhället att ställa krav på att vissa samhällsviktiga tjänster ska acceptera flera olika e-legitimationer[18]. Finansinspektionen konstaterade också i rapporten att det finns starka skäl att fortsätta arbetet med att ta fram en statlig e-legitimation.

---

[14] Myndigheten för digital förvaltning. *Digital plånbok*. 2022.
[15] Myndigheten för digital förvaltning. *Utveckling av det svenska e-legitimationssystemet.* 2021.
[16] Digitaliseringsrådet. *En lägesbild av digital trygghet.* 2018.
[17] Riksbanken. *Remissvar om betänkandet Ett säkert statligt id-kort med e-legitimation (SOU 2019:14).* Dnr 2019-00588.
[18] Finansinspektionen. *Förstärkt digital motståndskraft hos företag i den finansiella sektorn.* 2022.

I en debattartikel i Dagens Nyheter i november 2022[19] skrev regeringens särskilda utredare för Betalningsutredningen[20] att det är en statlig kärnuppgift att hålla reda på sina medborgare och att ge ut en statlig e-legitimation. Utredaren argumenterade i debattartikeln utförligt för sitt förslag och anförde att det i en osäker värld ställs nya krav på säkerhet i hela vårt samhälle och för samhällskritisk infrastruktur som vi är beroende av, vilket kräver möjlighet till säker digital identifikation.

Flera utredningar och myndigheter pekar alltså på att det är dags att tänka om och att staten bör ta ett större ansvar för e-legitimationer. Även Statskontoret pekar på just digitalisering som ett skäl till att ompröva det statliga åtagandet. I en perspektivrapport diskuterade Statskontoret att det behövs omprövning av det statliga åtagandet för att hushålla med de offentliga resurserna och att se till att staten gör rätt saker[21]. Statskontoret menade att ofta kommer omprövning till stånd till följd av någon form av kris, stora omvärldsförändringar eller genom ett starkt politiskt tryck, men att det finns också skäl för mer regelbunden omprövning av statens åtaganden för att staten ska kunna möta de behov och utmaningar den står inför, exempelvis vad gäller demografi, digitalisering och klimatomställningar. Statskontoret såg behov av att dels diskutera vad staten ska finansiera, och dels att se över hur staten är organiserad för att förvaltningen ska fungera väl. Digg menar att när det gäller samhällskritisk infrastruktur i form av e-legitimationer är tiden mogen för en omprövning av det statliga åtagandet.

2.2 Alla är inte med

Vi befinner oss i en digital strukturomvandling som är så pass omfattande att den brukar kallas den fjärde industriella revolutionen. Sverige har många gånger klarat av stora förändringar genom breda insatser, organisering och långsiktigt ansvar. Digitaliseringen har förändrat samhället och transformeringen väntas fortsatt medföra stora förändringar på arbetsmarknaden, i samhället och i ekonomin. Det innebär rimligen också konsekvenser för jämlikheten.

Regeringens digitaliseringsstrategi har som övergripande mål att vi ska bli bäst i världen på att använda digitaliseringens möjligheter. Det betyder att vi måste bli bäst i världen på att bjuda in alla att delta i den digitala samhällsutvecklingen. Den offentliga förvaltningen finns till för sina målgrupper och ska anpassas efter deras behov.

Hur många människor står utanför eller upplever att de inte är delaktiga i det digitala samhället? Det är en fråga som uppmärksammas allt mer. Statistik från Statistiska central-

[19] Dagens Nyheter, DN Debatt. *Sverige måste införa en statlig e-legitimation.* 16 november 2022.
[20] Dir. 2020:133. *Statens roll på betalningsmarknaden.*
[21] Statskontoret. *Perspektiv på omprövning.* 2021.

byrån (SCB)[22] och Internetstiftelsen[23] visar att majoriteten i befolkningen upplever sig vara delaktiga samtidigt som cirka en miljon människor uppger att de aldrig använt internet eller definieras som sällananvändare. Digitaliseringsrådet konstaterade i en rapport att utmaningen att göra den digitala servicen mera tillgänglig är tydlig, men frågan om hur inkludering kan ske är komplex. Det finns inga enkla svar eller enkla lösningar. Snarare behöver samhället bli bra på att lösa svåra utmaningar genom att samlas kring en gemensam riktning. Det behövs välfungerande ekosystem som innebär att olika aktörer bidrar med sin del och kunskap till en större helhet[24].

Det svenska e-legitimationssystemet fungerar i stort relativt väl och Sverige är ett av länderna i världen med störst användning av e-legitimationer. I en internationell jämförelse befinner sig Sverige idag i yttersta framkant vad beträffar utbredning, genomslag och användning av e-legitimering och den samhällsservice som erbjuds via internet. Men det finns utmaningar när det gäller det digitala utanförskapet. Många grupper – bland annat äldre, personer med funktionsnedsättning och personer utan svenskt personnummer – har svårigheter att kontakta myndigheter via digitala kanaler. En statlig e-legitimation blir då en viktig möjliggörare i samhällets digitalisering genom att fler grupper i samhället kan erbjudas en digital identitet. På samma gång behövs också andra åtgärder för att minska det digitala utanförskapet, och det behövs mer kunskap om hur sambandet mellan olika faktorer ser ut och på så sätt utgör hinder för inkludering[25].

2.3 Säker grundidentifiering

I Sverige har utfärdande av id-handlingar aldrig varit en ren myndighetsuppgift. Historiskt tog dåvarande Postverket och bankerna huvudsakligen på sig uppgiften att förse invånarna med traditionella id-handlingar, eftersom de hade intresse av att deras kunder skulle inneha sådana handlingar. Sedan 2005 har det nationella id-kortet utfärdats av Polismyndigheten och sedan 2009 är det även möjligt för invånare som är folkbokförda i Sverige, men inte är svenska medborgare, att få en id-handling via Skatteverket.

Sedan dess har det blivit allt svårare att identifiera invånare på ett säkert sätt. Den breda flora av traditionella id-handlingar som används innebär betydande utmaningar även för utbildad personal att på ett säkert sätt kontrollera en persons identitet. Teknik för att skapa välliknande förfalskade id-handlingar har dessutom blivit alltmer tillgänglig. Som en åtgärd att motverka den identitetsrelaterade brottsligheten föreslog 2017 års ID-

[22] Statistiska centralbyrån. *Befolkningens it-användning 2022.*
[23] Internetstiftelsen. *Svenskarna och internet 2022.*
[24] Digitaliseringsrådet. *Delaktighet i en digital tid – fördjupningsrapport med förslag.* 2019.
[25] Ibid.

kortsutredning att endast en myndighet bör ha det huvudsakliga ansvaret för utfärdande av statliga fysiska id-handlingar[26].

Digitaliseringen har lett till allt färre personliga möten mellan såväl myndigheter som banker och den enskilde. Allt sedan Posten i början av 2000-talet avvecklade de traditionella postkontoren, har svårigheten att identifiera en person på distans tilltagit samtidigt som behovet av säker identifiering ökat. Tidigare kunde rekommenderade brev användas för att upprätta en distansrelation, men denna funktion har genom postmarknadens avreglering fått en ändrad hantering och innebär inte längre en sådan distansverifiering som kan läggas till grund för utgivning av e-legitimation.

I pandemins spår har det blivit uppenbart att det finns ett behov av en säker metod för grundidentifiering vid utfärdande av e-legitimation. En identitetskontrollerande myndighet[27] har de verktyg och det kunnande som krävs för en tillförlitlig grundidentifiering vid utfärdande av e-legitimation. Genom att en statlig e-legitimation ges ut vid personligt besök hos en identitetskontrollerande myndighet skapas möjligheter för samhällets olika aktörer att säkert och obehindrat identifiera fysiska personer elektroniskt på distans. Detta möjliggör för såväl befintliga som nya utfärdare av e-legitimationer att ge ut e-legitimationer på samtliga tillitsnivåer med en statlig e-legitimation som grund, utan att behöva övervinna det betydande hinder som det innebär att upprätta fysisk representation. På så vis kan innovationskraften i näringslivet tas tillvara, samtidigt som den statliga e-legitimationen också kan användas som en fristående lösning för de som önskar. Digg bedömer att detta kan leda till större valfrihet och ökad tillgänglighet för olika e-legitimationslösningar, samtidigt som sårbarheten i samhället minskar.

2.4 Alla e-legitimationer ska kunna användas…

Den statliga e-legitimationen måste även gå att använda, det räcker inte med att den bara finns. För att åstadkomma detta måste offentlig förvaltning (myndigheter, kommuner och regioner) acceptera alla e-legitimationer som Digg har granskat och godkänt. Idag får varje offentlig aktör själv bestämma vilka e-legitimationer som kan användas vid inloggning i de digitala tjänsterna. Digg har i en tidigare rapport till regeringen gjort bedömningen att en av de mest centrala åtgärderna på e-legitimationsområdet är att alla digitala tjänster ska acceptera alla e-legitimationer med tillräcklig tillitsnivå. Detta kräver lagstiftning[28].

[26] SOU 2019:14.
[27] Begreppet förklaras i författningsförslagen i bilaga 4
[28] Myndigheten för digital förvaltning. *Utveckling av det svenska e-legitimationssystemet.* 2021.

Diggs bedömning är att den tidigare föreslagna åtgärden att införa ett obligatorium i allra högsta grad är fortsatt angelägen och relevant. När en statlig e-legitimation införs krävs att den också kan användas för att uppfylla samhällets krav på säkerhet, tillgänglighet och robusthet i en säkerhetspolitiskt orolig tid. Digg anser att den statliga e-legitimationen ska finnas med som en del i det ekosystem som byggts upp under lång tid. Den statliga e-legitimationen ska utgöra ett komplement och en möjlighet att växla över till andras lösningar, inte en konkurrent eller ersättare. Vad som däremot är helt centralt är att den statliga e-legitimationen erbjuds tillsammans med samtliga godkända e-legitimationer i alla digitala tjänster i den offentliga förvaltningen.

Det är alltså inte bara statliga myndigheter som bör omfattas av ett sådant obligatorium. För att så många som möjligt ska kunna identifiera sig digitalt måste även regioner och kommuner godta alla e-legitimationer som Digg har godkänt. Denna uppfattning delas av SKR som dessutom vill se ett obligatorium för privata aktörer. I en debattartikel från den 8 december 2022 i Dagens Samhälle[29] konstaterade SKR:s digitaliseringschef att vissa grupper av individer idag ställs helt utanför systemet när de saknar möjlighet att skaffa en e-legitimation. SKR argumenterade att när fler och fler offentliga tjänster erbjuds digitalt leder detta till ett utanförskap för individen och till att alla verksamheter måste ha manuella processer för att ärendehantering. SKR vill därför se en lagreglering som innebär att alla av staten godkända e-legitimationer måste accepteras av alla offentliga och privata aktörer som kräver e-legitimation för identifiering.

Dagens Nyheter ställde på sin ledarsida den 3 januari 2023 frågan om e-legitimation blir ett nytt statligt it-haveri[30]. Ledarskribenten såg en risk i att den statliga e-legitimationen skulle bli ett nytt, stort it-projekt som sedermera havererar, i likhet med polisens Pust eller Stockholms Skolplattform. Skälet till denna risk uppgavs bland annat vara att det i direktiven till regeringens nya utredning inte fanns med något om öppen källkod, öppna standarder, eller att titta på existerande lösningar. Digg menar att den nu föreslagna statliga e-legitimationen är just en sådan beprövad lösning som bygger på öppna standarder som kan förväntas leda till kort införandetid och god hushållning med det allmännas resurser. Ytterligare detaljer kring den tekniska utformningen finns i avsnitt 4.1 samt i bilaga 1.

2.5 …även utanför Sverige

Enligt regeringsuppdraget ska Digg ta den pågående förhandlingen av förslagen om revideringar av eIDAS-förordningen i beaktande och säkerställa att analysen går i linje

[29] https://www.dagenssamhalle.se/opinion/debatt/staten-maste-ta-ansvar-for-en-e-legitimation-for-alla/ (Hämtad 2023-01-02)

[30] Dagens Nyheter, ledarsidan. *Blir e-legitimation ett nytt statligt it-haveri?* 3 januari 2023.

med dessa förslag och utvecklingen av den digitala plånboken. Vidare ska Digg enligt regeringsuppdraget överväga om en statligt utfärdad digital plånbok också ska utgöra den statliga e-legitimationen eller om det behövs både plånbok och e-legitimation. Förslaget om en europeisk digital identitetsplånbok kommer från EU-kommissionen och lanserades i samband med att förslaget till reviderad eIDAS-förordning presenterades den 3 juni 2021. Den reviderade förordningen ska komplettera den nuvarande lagstiftningen och infrastrukturen för gränsöverskridande e-legitimering.

Digg kan konstatera att i skrivande stund är eIDAS-förordningen fortfarande föremål för förhandling inom EU. Medlemsländerna enades om ett kompromissförslag i december 2022[31]. Under det svenska ordförandeskapet i EU:s ministerråd första halvåret 2023 kommer kompromissförslaget förhandlas med Europaparlamentet för att så småningom antas som EU-förordning. Översiktligt kan konstateras att som en del i den föreslagna revideringen av eIDAS-förordningen ingår ett förslag om en digital europeisk identitetsplånbok. En sådan plånbok ska enligt EU-kommissionens förslag erbjudas medborgare och företag, och genom en koppling till den nationella digitala identiteten bära bevis på andra personliga attribut, till exempel körkortsbehörighet, utbildningsbevis och bankkonton[32]. I förhandlingen har Digg en central roll i de delar av eIDAS-förordningen som rör elektronisk identifiering, inklusive plånboken. Digg har därmed löpande kunnat säkerställa att förslaget som lämnas i aktuellt regeringsuppdrag går i linje med kommande reglering och utvecklingen av en digital europeisk identitetsplånbok.

Diggs bedömning är att det behövs både en fristående statlig e-legitimation och en digital identitetsplånbok. Den digitala identitetsplånboken kommer att utformas på ett sätt som innebär att den bärs inuti innehavarens smarttelefon. Identitetsplånbokens många och komplexa funktioner kan förväntas ställa högre krav på kunskap och medvetenhet vid användningen än vad dagens e-legitimationslösningar gör. Samtidigt kommer de tekniska kraven på smarttelefonens funktioner öka. Den föreslagna digitala europeiska identitetsplånboken kan inte antas bli mer tillgänglig än vad dagens lösningar är, och utan en kompletterande statlig e-legitimation skulle förslaget i eIDAS-förordningen innebära att stora grupper fortfarande riskerar ett digitalt utanförskap. Digg bedömer också att det måste finnas ett effektivt sätt att skaffa en sådan identitetsplånbok. Det är inte acceptabelt att tvingas besöka en identitetskontrollerande myndighet varje gång en person skaffar en ny telefon, eller installerar om sin telefon. Den fristående statliga e-legitimationen behövs därför även för att kunna skaffa en identitetsplånbok på distans.

[31] https://www.consilium.europa.eu/sv/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/ (Hämtad 2023-01-02)
[32] https://www.digg.se/ledning-och-samordning/europeisk-digital-identitet (Hämtad 2023-01-02)

3 Analyser och överväganden kring val av teknisk lösning

I arbetet med hur en statlig e-legitimation bör utformas har analyser och överväganden gjorts kring såväl lämplig teknik som en effektiv utgivningsprocess. Digg har övervägt och analyserat potentiella lösningar för e-legitimationens utformning utifrån grundförutsättningarna att den statliga e-legitimationen ska:

- vara en robust lösning som fungerar om de privata alternativen blivit otillgängliga, det vill säga även i orostider med höjd beredskap och ytterst även i krig
- vara kostnadseffektiv och ha kort införandetid
- vara tillgänglig för så många som möjligt, både att skaffa och att använda
- uppfylla säkerhetskraven för den högsta tillitsnivån i eIDAS-förordningen och Tillitsramverket för Svensk e-legitimation
- utfärdas efter att grundidentifiering genomförts vid ett personligt besök hos en identitetskontrollerande myndighet
- gå i linje med utvecklingen av den europeiska digitala identitetsplånboken
- utformas för att så långt som möjligt förebygga och förhindra bedrägerier
- utformas i enlighet med gällande rättsliga förutsättningar

Samtliga förutsättningar påverkar vilka tekniska lösningar som kan komma ifråga och hur utgivningsprocessen bör utformas. I det följande redogörs översiktligt för hur dessa förutsättningar påverkat utformningen av Diggs förslag. En mer utförlig teknisk beskrivning finns i bilaga 1.

3.1 E-legitimering i Sverige

Sveriges framgångsrika digitalisering med hjälp av säker elektronisk identifiering står sig väl i en internationell jämförelse. Den breda användningen innebär ett ökat beroende i samhället till en specifik tjänst. Även om det finns alternativ, till exempel Freja eID+, så har Sverige en sårbarhet i beroendet till BankID, vilket i sin tur leder till att sårbarheterna och riskerna med tillhandahållandet också ökar. Störningar och avbrott kan relativt snabbt antas få stora negativa konsekvenser för flera delar av det svenska samhället. Det finns därmed anledning att reflektera över dessa beroenden och sårbarheter och planera för att exceptionella händelser kan inträffa och ha en beredskap för detta.

BankID är den mest använda e-legitimationen i Sverige och gör det möjligt att inom alla samhällssektorer både identifiera sig och skriva under handlingar elektroniskt. Under

2021 användes BankID i omkring 6000 olika digitala tjänster hela 6 miljarder gånger. Det är i genomsnitt drygt 17 miljoner transaktioner per dygn, eller nästan 200 transaktioner per sekund utslaget över tiden. Transaktionsvolymen när användningen är som mest intensiv kan dock antas vara flera gånger högre än genomsnittsvolymen.

Störningar i BankID-tjänsten till följd av till exempel driftproblem och överbelastnings-angrepp har förekommit, och har i varierande grad lett till otillgänglighet i upp till ett par timmar. Om BankID får ett avbrott i tjänsten slutar e-legitimering att fungera för en väsentlig del av samhället, vilket kan leda till svårigheter för såväl enskilda som samhället i stort. Konsekvenserna av ett avbrott i BankID-tjänsten skulle också kunna eskalera relativt snabbt, exempelvis skulle ett längre bortfall av BankID-tjänsten få allvarliga konsekvenser för betalströmmarna. Även om det finns alternativa e-legitimationslösningar på marknaden så skulle även den offentliga förvaltningen påverkas av ett avbrott i BankID-tjänsten. Digg bedömer att det inte är otänkbart att viss samhällsservice helt enkelt upphör om digitala system för ärendehandläggning slutar fungera.

3.2 Informations- och cybersäkerhet

E-legitimationer utgör en samhällskritisk infrastruktur som måste fungera även i höjd beredskap och ytterst även i krig. Från ett kontinuitets- och beredskapsperspektiv finns det därför behov av en säker lösning som kan användas som komplement till de e-legitimationslösningarna marknaden tillhandahåller.

Ökad digitalisering leder till ökade sårbarheter, och varje aspekt av samhället är idag exponerat för risker för avbrott i informationssystem, informationsstöld eller manipulation. I rapporten Cyberhot mot Sverige[33] konstateras att utvecklingen av cybersäkerhet tar för lång tid i förhållande till den ständigt tilltagande digitaliseringen av samhället. Samtidigt som angrepp från cyberkriminella har blivit vanligare bedöms de allvarligaste cyberhoten mot Sverige nu komma från andra stater.

System för elektronisk identifiering kan genom dess betydelse för säkerheten i andra system komma att bli måltavla för olika former av cyberangrepp. Störningar i e-legitimationssystemen kan snabbt få kännbara effekter för samhället; näringsliv, banker, offentlig sektor och inte minst för enskilda, även i en i övrigt normal situation. Digg fokuserar i kommande avsnitt på informations- och cybersäkerhetsfrågorna. Det handlar om digital säkerhet för att förebygga och hantera oönskade händelser med störningar av tillgänglighet, integritet och sekretess för olika delar av e-legitimationssystemet.

[33] RISE. *Cyberhot mot Sverige - En sammanfattning för ledare och beslutsfattare*. 2022.

3.2.1 Aktörer i e-legitimeringsprocessen

En e-legitimering äger rum när en e-legitimation används för att styrka en individs identitet vid inloggning i en digital tjänst. Förfarandet kräver ett bakomliggande samarbete av flera olika aktörer och system. Aktörerna är i huvudsak:

- **Användaren** som har en e-legitimation för att legitimera sig elektroniskt mot en digital tjänst.
- **E-legitimationsutfärdaren** som förser användaren med en e-legitimation och som ansvarar för de stödfunktioner som krävs för att ge ut, verifiera och spärra e-legitimationer.
- **Utställare av identitetsintyg** som genomför en elektronisk identifiering av användaren och därefter ställer ut ett identitetsintyg i överenskommet tekniskt format.
- **Förlitande aktör** som i rollen av tillhandahållare av en digital tjänst är den som förlitar sig på det identitetsintyg som ställs ut, och med detta som grund bereder användaren tillträde till tjänsten.

Varje aktör i ekosystemet, och varje relation mellan dessa aktörer, för med sig potentiella sårbarheter som genom oväntade händelser, misstag eller avsiktligt handlande av illvillig aktör kan leda till en säkerhetsincident.

3.2.2 Sårbarheter

I en inledande analys har tre grundläggande typer av sårbarheter identifierats, som var och en har potential att påverka informations- och cybersäkerheten i systemet för e-legitimationer.

- **Tekniska sårbarheter** – sårbarheter som beror på brister i teknik, arkitektur, ursprunglig design eller implementering.
- **Sårbarheter hos berörda aktörer** – sårbarheter som kan bero på brister i programvara, felkonfigurationer, bristande åtkomstkontroller, social manipulation eller angrepp mot leveranskedjan.
- **Sårbarheter på grund av beroenden** – sårbarheter som uppstår i relationen mellan berörda aktörer, deras funktioner och system, genom att det skapas beroenden som kan vara svåra att identifiera.

Sårbarheter av dessa olika typer måste identifieras och kategoriseras vid återkommande nulägesanalyser genomförda utifrån ett helhetsperspektiv. Det är inte tillräckligt att aktörerna var och en för sig analyserar situationen utifrån sitt eget perspektiv (användaren här undantagen). En öppenhet och samverkan mellan de ingående aktörerna

krävs för att kunna övervinna dessa typer av säkerhetshot. Syftet med sådan samverkan är att förstärka aktörernas förmågor att lösa sina respektive uppdrag bland annat genom gemensamma analyser och övergripande lägesbilder kring hot och sårbarheter, sprida information mellan ingående aktörer och omvärlden samt att koordinera arbetet vid allvarliga incidenter och cyberangrepp.

3.2.2.1 Det behövs flera lager av skydd

E-legitimationssystem måste omgärdas av flera lager av skydd så att en och samma sårbarhet inte riskerar att få katastrofal påverkan på säkerheten. Det finns exempel som visar att det hos varje inblandad aktör måste finnas en beredskap för och förmåga att hantera exceptionella händelser på ett ändamålsenligt sätt för att kunna upprätthålla säkerheten och tilliten till systemet. Ett exempel på detta är vad som skedde 2017 i och med den sårbarhet som uppdagades i vissa aktiva kort och som sedermera kom att kallas ROCA[34]. Estland drabbades hårt, men även Spanien och Slovakien tvingades till åtgärder.

Estland har sedan 2001 en e-legitimation på id-kort som den metod som krävs för att elektroniskt kunna få tillgång till offentliga tjänster. Varje estniskt id-kort är försett med chip som används för att invånaren ska kunna identifiera sig och skriva under handlingar elektroniskt. Detta chip hade genomgått såväl granskningar och certifieringsförfaranden för att så långt som möjligt minska riskerna att chipen skulle vara behäftade med sårbarheter, då en eventuell sårbarhet skulle kunna få mycket långtgående konsekvenser. Trots detta uppmärksammades de estniska myndigheterna sensommaren 2017 på att det fanns en allvarlig kryptografisk sårbarhet i de chip som användes i id-korten. Ett algoritmiskt fel hade påträffats i den mjukvara som användes för att framställa de kryptografiska nycklarna, vilket innebar att alla nycklar som genererades av chip-leverantörens programbibliotek påverkades. I Estland berördes samtliga då giltiga id-kort (cirka 800 000) som utfärdats sedan hösten 2014. Det visade sig att varje privat nyckel genom kryptoanalys kunde beräknas utgående från den publika nyckeln, vilket i så fall skulle leda till en total kompromettering av säkerheten i e-legitimationssystemet och göra det möjligt för en utomstående aktör att stjäla en individs digitala identitet och skriva under handlingar i dennes namn. Alla certifikat behövde därför spärras och nya nycklar genereras. På grund av det omfattande arbete och de stora kostnader det skulle medföra att utfärda nya kort till samtliga invånare valde den estniska myndigheten för informationssystem, RIA, en strategi som innebar att låta innehavarna på egen hand, med befintliga kort, genomföra nyckelbyte på distans genom ett självserviceförfarande.

[34] https://en.wikipedia.org/wiki/ROCA_vulnerability

I Spanien däremot, där man förlitade sig på samma typ av chip i de nationella id-korten, spärrades och återkallades 17 miljoner kort. Konsekvenserna i Spanien blev dock mer begränsade, då id-korten inte användes för elektronisk identifiering i någon större utsträckning.

3.2.3 Skyddsvärda tillgångar

Vid en analys av informations- och cybersäkerhetsrisker är det tillgångar som är själva målen för skyddet. Riskanalysen syftar således också till att dokumentera det som är skyddsvärt, inte bara att identifiera och analysera hot och sårbarheter. För att underlätta denna diskussion kan man göra skillnad mellan primära och sekundära tillgångar.

3.2.3.1 Primära tillgångar

Primära tillgångar utgörs av de grundläggande värden och som kräver skydd. Till exempel

- förtroende och anseende
- finansiella resurser
- känslig information (innefattande känsliga personuppgifter)
- verksamhetsprocesser och -aktiviteter
- människors liv och hälsa.

De primära tillgångarna i ett e-legitimationssystem kan sägas vara de förlitande aktörernas och användarnas intressen, deras förtroende till systemet och de investeringar samhället gjort i systemet. I de förlitande aktörernas intressen ligger skyddet av deras verksamheter och finansiella tillgångar. Ytterst behöver också människors liv och hälsa beaktas, genom de beroenden som uppstår till e-legitimationssystemet och anslutna digitala tjänster. Det är således oerhört stora skyddsvärden som är beroende av ett nationellt e-legitimationssystem.

3.2.3.2 Sekundära tillgångar

Sekundära tillgångar är sådant som måste skyddas för att i sin tur möjliggöra skyddet av de primära tillgångarna. Sekundära tillgångar inkluderar till exempel

- organisation, personal och kunnande
- driftanläggningar och andra utrymmen
- tekniska system
- innehavarnas medel för elektronisk identifiering (aktiva kort, personlig kod, stödprogramvara, osv.)

- tillfälliga känsliga uppgifter (identitetsintyg, sessionsnycklar, engångskoder, mm.).

De sekundära tillgångarna i e-legitimationssystemet kan sägas i huvudsak bestå av de tjänster som utfärdare av e-legitimation och utställare av identitetsintyg producerar.

I den arkitektur som Digg föreslår finns ett par ytterst känsliga tekniska system på vilka säkerheten vilar, i synnerhet identifieringstjänsten och funktionerna för utställande av identitetsintyg. Det finns även ett stort beroende till leverantören av de kontaktlösa aktiva korten samt de processer och rutiner som omgärdar utfärdandet. Tillitsramverket för Svensk e-legitimation ställer i dessa delar långtgående krav som måste uppfyllas av aktörerna i e-legitimeringsprocessen. Genom att kraven i det svenska tillitsramverket uppfylls, uppfylls även motsvarande krav i eIDAS-förordningens genomförandeakt (EU) 2015/1502 om fastställande av tillitsnivåer i enlighet med eIDAS-förordningen[35].

3.2.4 Hotbildsanalys

Hot är oönskade händelser som riskerar att få negativa konsekvenser för tillgångarna. Riskanalyser måste genomföras för att identifiera vilka tillgångar som är skyddsvärda och analysera specifika faktorer, till exempel sårbarheter, genom vilka olika hot kan komma att påverka tillgångarna.

Det finns inget självklart eller allmänt vedertaget sätt att beskriva hot. De oönskade händelserna behöver dock beskrivas tillräckligt specifikt för att möjliggöra de nödvändiga bedömningarna, och för att på så sätt ge spårbarhet på vilka grunder bedömningen gjorts. Bedömningen underlättas av om det finns en förteckning över de säkerhetsegenskaper som systemet ska upprätthålla.

För att enklare förstå olika tänkbara scenarier väljs här en ansats att beskriva vissa hot (oönskade händelser) indelade utifrån tänkbara hotaktörer. En hotaktör kan vara en enskild individ, en grupp eller ett nätverk av människor, en organisation eller en främmande stat.

En underindelning bör även göras, som beskriver tillvägagångssättet för en hotaktör att sätta ett hot i verket. Ett sådant arbete ryms inte inom tidsramarna för regerings-uppdraget, utan är något som behöver omhändertas i ett nästa steg. Digg räknar i det följande upp några exempel på hotaktörer i ett e-legitimationssystem.

[35] Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställandet av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentet och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

- **En tjänsteleverantör som agerar svikligt.** En tjänsteleverantör som förleder användaren att bruka en viss tjänst vars egentliga syfte är att samla in och exploatera användarens information. Ett tillvägagångssätt kan vara att etablera en tjänst och locka användarna att bruka den för något som till ytan ser ut att vara ett legitimt syfte, till exempel att genomföra en analys av användarens privatekonomi, men det som egentligen sker när användaren identifierar sig är att denne i själva verket släpper in tjänsten i exempelvis sin internetbank, där tjänsten samlar in uppgifter om användaren som sammanställs och exploateras på något sätt. Sådan exploatering kan till exempel ske genom vidareförsäljning till andra aktörer som har ett intresse av uppgifterna.
- **En användare med bedrägliga avsikter**. Användaren kan själv försöka utnyttja systemet för egen vinning genom att först genomföra någon åtgärd, för att i nästa steg förneka åtgärden. Ett tillvägagångssätt kan vara att användaren tecknar ett lån, för att i nästa steg föra undan pengarna och därefter förneka åtgärden genom att hävda att den skett obehörigen av någon annan.
- **Insiders**. Någon som arbetar i en betrodd roll vid en verksamhet i förlitandekedjan (leverantör av identitetsintyg eller utfärdare av e-legitimation) och som är sårbar för yttre påtryckningar kan utnyttja sin position och agera illojalt. Ett tillvägagångssätt kan vara att skaffa en e-legitimation i någon annans namn, för att i nästa led överlåta (sälja) den eller själv försöka utnyttja den. Till exempel för ekonomisk vinning eller för att komma över information om offret.
- **Organiserad brottslighet**. Sådana aktörer kan försöka iscensätta storskaliga och systematiska bedrägerier. Hotaktören kan ha hög motivation, stor kompetens och omfattande resurser till sitt förfogande. Ett tillvägagångssätt kan vara att utnyttja sårbarheter i användarnas webbläsare, i syfte att fånga upp och missbruka utställda identitetsintyg, eventuellt i kombination med olika former av social manipulation i syfte att vilseleda användaren.
- **Främmande statsaktör**. En främmande statsaktör kan försöka störa e-legitimationssystemet i syfte att skada allmänhetens tilltro det och för att orsaka avbrott i förlitande digitala tjänster. Ett tillvägagångssätt kan vara att iscensätta storskaliga och långvariga överbelastningsangrepp mot sådana centrala resurser som är nödvändiga för att e-legitimationssystemet ska kunna fungera normalt.

Samtliga dessa hot kan komma att påverka de primära tillgångarna negativt. Som synes är hotbilderna av mycket varierande karaktär, och hoten måste analyseras utifrån en helhetsbild av hela förlitandekedjan. En korrekt och djuplodande hotbildsanalys är nödvändig att genomföra i nästa steg. Analysen är avgörande för att kunna etablera det skydd och den beredskap som krävs för att hantera hoten om de sätts i verket.

3.3 Nya brottsmönster

Den tekniska utformningen av en e-legitimation förhindrar inte, och kan inte förhindra, en användare att använda sin e-legitimation på ett sätt denne egentligen inte hade tänkt sig. Så länge användaren förmår använda sin e-legitimation kan den också missbrukas. Digg beskriver här vissa brottsförebyggande åtgärder som kan vidtas för att förhindra och försvåra för vissa typer av brottsmönster i samband med e-legitimering.

3.3.1 Säker start kan förebygga telefonbedrägerier

Digitaliseringen har möjliggjort nya brottsmönster där en gärningsperson med digital teknik kan begå bedrägerier från vilken plats som helst utan att brottsoffret och gärningspersonen möts fysiskt. Bedrägerier[36] bedrivs som regel i organiserad form i kriminella miljöer och har ökat kraftigt under 2000-talet[37]. Som viktiga faktorer bakom denna utveckling anges bland annat digitaliseringen, i vilken e-legitimationen utgör en viktig komponent. Samtidigt har kontanthanteringen under samma period minskat avsevärt. Under 2021 var brottsvinsterna från telefonbedrägerierna 339 miljoner kronor. Förra året noterades en markant ökning då brottsvinsterna beräknades uppgå till 386 miljoner kronor enbart för perioden januari till augusti 2022[38].

Så kallad vishing, telefonfiske, innebär att en bedragare lurar en person att använda sin e-legitimation på ett sätt som leder till ekonomisk vinning för gärningspersonen. En sårbarhet som har utnyttjats av bedragarna är att det varit möjligt för bedragaren att starta en identifieringsprocess och låta personen slutföra den för att på så sätt ge bedragaren tillträde till exempelvis personens internetbank. Det förekommer också att traditionella bankdosor utnyttjas i samma syfte. Dessa typer av bedrägerier drabbar särskilt vissa sårbara grupper, såsom funktionsnedsatta eller äldre personer, men i vissa fall också företag.

Som ett skydd mot detta förfarande har BankID infört så kallad *säker start.* Det innebär att den som ska identifiera sig måste läsa av en optisk kod från skärmen för att starta identifieringsprocessen. Detta förhindrar bedragaren att endast via telefon förleda offret, då det också krävs att en länk eller motsvarande förmedlas till personen, och personen måste därefter klicka på länken och läsa av den optiska koden. Det är i dagsläget valfritt att använda processen, men från och med den 1 maj 2024 kommer det bli tvingande att använda *säker start* för BankID för samtliga förlitande digitala tjänster. Dessa åtgärder

[36] Med bedrägerier avses bedrägeribrott enligt 9 kap. brottsbalken (BrB) samt brott enligt bidragsbrottslagen (2007:612). De sistnämnda omfattar även det som i vardagligt kallar för välfärdsbrott.
[37] Polismyndigheten. *De dödliga bedrägerierna, En rapport om bedrägeribrottslighet och skjutvapenvåldet.* 2022.
[38] Ibid.

försvårar tillvägagångssätten för att genomföra telefonbedrägerier och kräver att bedragaren förleder offret genom fler och mer komplicerade steg.

3.3.2 En korrekt folkbokföring kan försvåra för välfärdsbrottsligheten

När det gäller brottslighet som särskilt riktas mot välfärdssystemen förekommer det att oriktiga uppgifter om identiteter eller bosättning blir registrerade i folkbokförings-databasen för att därefter användas för att begå brott. Exempelvis används förfalskade eller manipulerade identitetshandlingar vid anmälan om folkbokföring och på så sätt skapas en falsk identitet som sedan kan användas i olika syften. Det förekommer också att personer har två eller fler identiteter vilket kan ge möjlighet att få flera parallella bidrag från välfärdssystemen. Identiteterna kan även utnyttjas som målvakter. Ett annat återkommande tillvägagångssätt är identiteter som felaktigt folkbokförts på postbox-adresser samt så kallade skenskrivningar där 20–30 personer blivit folkbokförda på en och samma adress utan att egentligen bo där.[39]

När det kommer till e-legitimationer kan folkbokföringens betydelse inte nog understrykas. Uppgifterna i folkbokföringen ligger även till grund för utgivning av e-legitimationer. Om en identitet har registrerats felaktigt i folkbokföringen riskerar en e-legitimation att utfärdas på dessa felaktiga grunder, under förutsättning att personen ifråga kunnat identifiera sig som den registrerade. Kontrollerna som vidtas vid Skatteverket och Migrationsverket har avgörande betydelse för riktigheten i dessa uppgifter.

Åtgärder som vidtas för att minska riskerna för felaktigheter i folkbokföringen får därför effekter även för e-legitimationssystemet. En viktig åtgärd som nyligen beslutats är att Skatteverket kommer ta över ansvaret för tilldelning av samordningsnummer. I samband med denna förändring införs också en nivåindelning för samordningsnummer. Nivån sätts utifrån vilken identitetskontroll som föregått tilldelningen. Bestämmelserna träder i kraft den 1 september 2023[40].

En annan åtgärd för att motverka brottsligheten på området är ett mer effektivt informationsutbyte mellan inblandade parter. I utredningen Stärkta åtgärder mot penningtvätt och finansiering av terrorism ges ett konkret exempel på informationsutbyte mellan kreditinstitut, i syfte att bekämpa bland annat målvaktsproblematiken[41].

---

[39] Nationella underrättelsecentret. *Identitetsrelaterad brottslighet.* 2015.
[40] Lag (2022:1697) om samordningsnummer
[41] SOU 2021:42. *Utredningen om stärkta åtgärder mot penningtvätt och finansiering av terrorism: slutbetänkande.*

Brottsligheten drivs av ekonomiska motiv och genom att försvåra att föra undan brottsvinsterna försvåras hela brottsupplägget.

3.3.3 Förstärkt säkerhet kan förhindra identitetsintrång

Idag är det lätt att få tillgång till uppgifter om någon annans identitet, familjeförhållanden och adress.[42] Även uppgifter om personers ekonomiska förhållanden finns relativt lättillgängliga. Många av dessa uppgifter är offentliga hos myndigheterna eller kan inhämtas på annat sätt, till exempel genom att personen själv delar med sig av informationen på sociala medier. Tillgängligheten av dessa uppgifter har lett till att det att har blivit lättare att utge sig för att vara någon annan och att använda någon annans identitet i olika sammanhang. Genom att bruka förfalskade eller manipulerade id-handlingar kan gärningspersonerna inleda eller ta över en bankrelation och på så sätt komma över en e-legitimation som kan användas för att begå brott i nästa led.

En annan form av så kallad olovlig identitetsanvändning kan ske genom att utnyttja sårbarheter i manuella rutiner kopplade till folkbokföringen, till exempel genom obehörig adressändring som sker på enkel pappersblankett som sänds till Skatteverket.

Kopplingen mellan denna typ av brottslighet och e-legitimationer är inte alldeles tydlig. Det förekommer att bristande säkerhet i traditionella id-handlingar möjliggör för en gärningsperson att skaffa en e-legitimation i någon annans namn. Sårbarheterna är därmed inte direkt kopplade till den hantering som omgärdar e-legitimationer, utan får ses som ett mer allmänt problem i samhället. Flera utredningar[43] [44] har pekat på behovet av att förstärka säkerheten i de traditionella id-handlingarna och att begränsa det antal varianter som allmänt erkänns.

3.3.4 Förfalsknings- eller sanningsbrott

I den fysiska tillvaron ses det som en självklarhet att en person inte får använda en annan persons id-handling eller att lämna ut sin id-handling för att någon annan ska kunna utge sig för att vara den som anges i legitimationen. Det gäller till exempel vid en minderårigs utnyttjande av någon annans id-kort för att köpa alkohol. I den elektroniska miljön gäller samma regler men det uppfattas inte som lika självklart att ett missbruk är straffbart.

Det finns ett antal förfalsknings- eller sanningsbrott, bland annan urkundsförfalskning, förnekande av underskrift, osann försäkran eller osant intygande.[45] Att hjälpa någon att utföra ett ärende elektroniskt genom att missbruka dennes e-legitimation kan alltså utgöra

[42] SOU 2017:37. Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden. *Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra: slutbetänkande.*

[43] SOU 2017:37.

[44] SOU 2019:14.

[45] 14 kap. 1 §, 15 kap. 3, 10. 11. 12 §§ BrB.

missbruk av urkund. Dessa brott utförs ofta som ett genomgångsled till ett bedrägeri eller till ett bidragsbrott.

3.3.5 Grundidentifiering som brottsförebyggande åtgärd

Digg bedömer att den tekniska utformningen av en statlig e-legitimation inte kan användas för att förhindra brotten som beskrivits i föregående avsnitt. Säker grundidentifiering är därför helt avgörande som brottsförebyggande åtgärd vid utfärdandet av e-legitimationen. Den identitetskontrollerande myndigheten måste ges de verktyg som står till buds för att genomföra en så säker identifiering som möjligt, till exempel genom åtkomst till bilder i passregistret och att effektivt kunna spärrkontrollera traditionella id-handlingar (framförallt körkort). Detta är förfaranden som privata aktörer kan ha svårt att genomföra vid grundidentifiering, bland annat på grund av begränsad tillgång till folkbokföringsuppgifter och begränsade möjligheter att genomföra det personliga mötet.

3.3.6 En säker användning som brottsförebyggande åtgärd

Ytterligare en åtgärd att förebygga brott via e-legitimation är att på ett tekniskt sätt erbjuda en så säker användning som är möjlig från praktiska utgångspunkter. Det handlar om att försvåra möjligheten att lura innehavare att använda sin e-legitimation på fel sätt genom att exempelvis säkerställa att den personliga koden anges på samma enhet som e-legitimationen befinner sig.

En annan metod är att i samband med en elektronisk identifiering tekniskt förmedla vissa riskindikatorer till förlitande aktör. Sådana riskindikatorer kan användas av förlitande aktör för att avgöra behovet av vidare kontroller i syfte att säkerställa att en viss åtgärd inte genomförs obehörigen. Riskindikatorerna framställs från tekniska parametrar som härrör från användningen. Digg bedömer att hur dessa bör utformas för att bli ett effektivt verktyg för förlitande parter, och de rättsliga förutsättningar som behövs för att kunna förmedla sådana uppgifter, behöver utredas vidare.

3.4 Det digitala utanförskapet

Enligt regeringsuppdraget ska Digg säkerställa att e-legitimationen utformas på ett sådant sätt att så många som möjligt kan skaffa och använda den. Detta kräver att stor vikt fästs vid att möta behoven från de användargrupper som idag inte kan eller vill skaffa en e-legitimation från någon av de privata utfärdarna, och som därför riskerar att hamna i ett digitalt utanförskap. I analysarbetet har framför allt fem övergripande grupper identifierats:

- Äldre personer, födda på 40-talet eller tidigare använder e-legitimation i väsentligt lägre utsträckning än yngre personer[46]
- Personer med funktionsnedsättning som ibland kan ha svårt att skaffa och använda e-legitimation
- Personer som av olika skäl inte använder smarttelefoner
- Personer som tillfälligt vistas i Sverige och därför endast har samordningsnummer samt personer som av olika anledningar, till exempel ekonomiska svårigheter, inte har en bankrelation och därmed inte kan skaffa BankID
- Personer som inte har en svensk fullgod id-handling

Gruppindelning gällande det digitala utanförskapet har här gjorts för att förenkla resonemang och analyser. Digg vill dock betona att det exempelvis finns stora variationer av såväl behov som digital kompetens inom grupperna och att enskilda individer kan tillhöra flera grupper samtidigt. Det digitala utanförskapet är i verkligheten mycket mer komplext och inte på något sätt så homogent som framställningen här kan ge en bild av.

Digg har i analysen utgått ifrån att för att möta dessa användargruppers behov bör utgivningen inte kräva att sökanden har egen teknisk utrustning, varken i form av egen dator eller smarttelefon. Diggs förslag till teknisk utformning av den statliga e-legitimationen har styrts av dessa förutsättningar och presenteras översiktligt i avsnitt 4.1. En fördjupad beskrivning återfinns i bilaga 1.

Vidare bör stegen i utgivningsprocessen – ansökan, grundidentifiering, tillhandahållande och aktivering – också innefatta ett minimum av interaktion på elektronisk väg och ta hänsyn till relevanta tillgänglighetsaspekter i varje steg. Diggs förslag till utformning av utgivningsprocessen presenteras i avsnitt 5.2.

3.5 Tillitsramverket för Svensk e-legitimation

Tillitsramverket för Svensk e-legitimation syftar till att etablera gemensamma krav för utfärdare av e-legitimationer. Kraven vilar på internationella standarder samt erkända och etablerade principer. Kraven är fördelade på olika skyddsklasser – tillitsnivåer – som svarar mot olika grader av teknisk och operationell säkerhet hos utfärdaren och olika grader av kontroll av att en person som tilldelas en e-legitimation verkligen är den hen utgett sig för att vara.

[46] Internetstiftelsen. *Svenskarna och internet 2022, tabellbilaga.* 2022.

Kraven formuleras enligt en allmänt vedertagen modell för elektronisk identifiering, där hanteringen av e-legitimationen delas in i tre olika faser;

- ansökan och fastställande av sökandens identitet
- utfärdande och tillhandahållande av e-legitimationshandling
- verifiering av e-legitimation och utställande av identitetsintyg.

I var och en av dessa faser krävs särskilda åtgärder för att upprätthålla den angivna skyddsnivån för hanteringen av e-legitimationer.

Tillitsnivåerna är definierade utifrån en konsekvensbaserad modell för riskbedömning. Valet av vilken tillitsnivå som ska krävas för en digital tjänst görs genom en avvägning utifrån sex olika riskområden och vilka negativa konsekvenser en felaktig legitimering skulle kunna föra med sig. Digg har publicerat en vägledning för förlitande aktörer, för att underlätta att välja rätt tillitsnivå för varje digital tjänst.

Tillitsramverket togs fram av dåvarande E-legitimationsnämnden och publicerades i en första version i slutet av 2013. Tillitsramverket förvaltas idag av Digg som en central komponent i det nationella e-legitimationssystemet. Utfärdare som granskats och godkänts av Digg gentemot tillitsramverkets bestämmelser på lägst tillitsnivå 3 får teckna licensavtal att nyttja Kvalitetsmärket Svensk e-legitimation i anslutning till de erbjudna tjänsterna. För leverantörer som vill ingå avtal om e-legitimering enligt Valfrihetssystem 2017 gäller samma krav.

Tillitsramverket har under lång tid förankrats med såväl utfärdare av e-legitimationer som förlitande aktörer, och det råder idag bred konsensus kring de regler som uttrycks där.

Sverige, genom dåvarande E-legitimationsnämnden, deltog i arbetet med utformningen av kommissionens genomförandeförordning[47] för fastställande av tillitsnivåer enligt artikel 8.3 i eIDAS-förordningen[48], där det svenska tillitsramverkets lades som förlaga till en stor del av bestämmelserna i denna genomförandeförordning. Olika medlemsländers seder och bruk krävde dock att flera regler generaliserades och gavs en annan utformning. Till exempel har andra länder inte alltid en samlad folkbokföring med en samordnad identitetsbeteckning likt den Sverige har. En annan aspekt är att utställande av

[47] Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

[48] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

identitetsintyg inte omfattas av reglerna, då detta ansågs vara avgränsat genom det så kallade interoperabilitetsramverket (som inte heller omfattar sådana bestämmelser).

Eftersom de EU-gemensamma reglerna är fastställda genom författning är de också svåra att ändra och utveckla, inte minst eftersom reglerna påverkar samtliga länders e-legitimationssystem som redan anmälts och konsekvenserna av vissa ändringar är därför svårbedömda. Svårigheterna att utveckla regelverket utgör även hinder för att möta såväl teknikutveckling som nya hotbilder.

Den höga abstraktionsnivån i vissa formuleringar har också lett till att reglernas innebörd tolkas på olika sätt av olika aktörer. Det har till exempel förekommit att ackrediterade organ för bedömning av överensstämmelse gjort bedömningar vid certifieringar som senare helt förkastats av medlemsländernas experter i samband med sakkunniggranskningar. Även inom samarbetsorganet gör olika experter olika bedömningar. Då samarbetsorganets uttalanden i dessa frågor antas genom konsensusbeslut innebär det att de mer restriktiva tolkningarna vanligen ges företräde, men utfallet beror också till viss del på vilka experter som deltar i de aktuella sakkunniggranskningarna.

Reglerna i genomförandeförordningen åtföljs av en vägledning som tagits fram av medlemsländerna inom samarbetsorganet. Denna vägledning har ingen formell status, men används i stort vid de sakkunniggranskningar som sker i samband med länders föranmälan av nationella e-legitimationssystem. I sakkunniggranskningarna förekommer det att även andra förfaranden än de som uttryckligen beskrivs i genomförandeförordningen och vägledningen godtas. Ett exempel är det aktiveringsförfarande som krävs för den högsta tillitsnivån, och vars huvudsyfte är att säkerställa en separation av arbetsuppgifter genom utgivningsprocessen. Här anges uttryckligen att tillhandahållandet ska innefatta ett aktiveringsförfarande. I denna fråga har dock även andra sätt som uppfyller syftet att uppnå separation av arbetsuppgifter godtagits i sakkunniggranskningarna.

Digg har deltagit aktivt i ett betydande antal sakkunniggranskningar av andra länders e-legitimationssystem, och har genom detta förvärvat stor erfarenhet av gällande praxis, och bedömer att det förslag till utformning av en statlig e-legitimation som lämnas i denna rapport faller väl inom ramarna för de regler som gäller för den högsta tillitsnivån, och att inga avsteg görs från genomförandeförordningens skrivningar.

Behovet av ett nationellt tillitsramverk har ifrågasatts men skälen bakom att etablera och vidmakthålla ett nationellt tillitsramverk är flera. Dels att säkerställa regelverkets relevans över tid och utifrån nationella förhållanden, dels för att klargöra förhållanden som kan vara svåra att tolka utifrån genomförandeförordningen och tillgänglig dokumentation från arbetet inom samarbetsorganet. Det möjliggör också för Digg att utveckla reglerna och vidta de åtgärder som krävs för att upprätthålla säkerheten och tilliten i det nationella

e-legitimationssystemet, så länge dessa åtgärder också är förenliga med eIDAS-förordningens bestämmelser och den praxis som arbetas fram successivt inom samarbetsorganet.

Det nationella tillitsramverket fungerar därmed idag som en precisering av de krav som ställs genom den något mer generaliserade regleringen som följer av eIDAS-förordningen. De svenska tillitsnivåerna 2, 3 och 4 svarar dock genomgående mot kraven för eIDAS tillitsnivåer låg, väsentlig och hög. Behovet att närmare precisera reglerna som följer av eIDAS-förordningen har också identifierats i andra länder där inte endast en statligt utfärdad e-legitimation förekommer. Förutom Sverige har numera till exempel Nederländerna, Frankrike och Danmark motsvarande nationella tillitsramverk.

4 Förslag till utformning

4.1 Ett kontaktlöst aktivt kort

Digg föreslår att den statliga e-legitimationen ges ut i formen av ett kontaktlöst aktivt kort.

Digg ser den statliga e-legitimationen som ett komplement till dagens lösningar. Enligt regeringsuppdraget ska e-legitimationen vara tillgänglig för så många som möjligt och Digg bedömer att ytterligare en mobil variant som kräver en smarttelefon inte skulle bli mer tillgänglig än de mobila lösningar som redan finns att tillgå. Kravet på större tillgänglighet skulle således inte uppfyllas. Digg föreslår därför en lösning baserad på ett fysiskt kort, vilket också för med sig robusthetshöjande aspekter när e-legitimationen inte är beroende av att var och en har en fungerande smarttelefon. Digg ser också den föreslagna lösningen som en instegslösning. Den statliga e-legitimationen kan utgöra ett sätt att skaffa andra e-legitimationer, genom så kallad id-växling.

Kontaktlösa aktiva kort utgör en beprövad teknik som använts under lång tid för just detta ändamål. De är också relativt billiga, från ett tjugotal kronor per styck i större volymer, och har lång livslängd. Korten kan läsas i såväl smarttelefoner och surfplattor som vanliga datorer. I anslutning till den föreslagna lösningen behöver Digg ta fram nödvändig programvara och handledningar för de olika typer av enheter som ska stödjas.

För att minimera utvecklingsarbetet föreslår Digg att en öppet standardiserad teknik för det aktiva kortet väljs. De egentligen enda förekommande heltäckande öppna specifikationerna för denna typ av kort är PIV[49]. Andra typer bygger vanligtvis i varierande grad på den internationella standarden ISO/IEC 7816-15[50]. Denna standard är dock endast ett ramverk, inom vilket variationsmöjligheterna är närmast oändliga. E-legitimationer med denna standard som utgångspunkt fungerar således på vitt skilda sätt, och är dessutom ofta leverantörsspecifika, vilket driver utvecklingskostnader, bidrar till leverantörsinlåsningar och minskar den tekniska interoperabiliteten.

Digg bedömer att genom att basera den statliga e-legitimationen på PIV-specifikationerna underlättas också upphandling och utveckling. Ett flertal leverantörer tillhandahåller redan idag kompletta certifierade produkter på den öppna marknaden med de funktioner

[49] Personal Identity Verification: https://csrc.nist.gov/Projects/piv/piv-standards-and-supporting-documentation (Hämtad 2023-01-02)
[50] ISO/IEC 7816-15:2016. *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application.* 2016.

som krävs. Leverantörerna erbjuder vanligen även logistiklösningar och tjänster för att skapa visst innehåll på korten.

Digg behöver, som tidigare nämnts, ta fram den programvara och sådan handledning som behövs för att kunna använda kortet tillsammans med smarttelefoner, surfplattor och datorer. Genom att bygga på PIV-specifikationerna finns ett stort utbud av program-bibliotek att tillgå och standardapplikationer som bygger på öppen källkod. Detta kortar ner utvecklingstider och minskar kostnaderna.

Den app för smarttelefoner som föreslås är endast ett hjälpmedel för att läsa kortet och innehåller alltså inte någon e-legitimation. Appen förmedlar endast kommunikationen mellan Diggs system och kortet. Kommunikationen sker krypterat. Detta innebär att personer som behöver hjälp med att utföra ett ärende digitalt kan låna en närståendes eller en väns telefon, och bruka den för att identifiera sig. Ingen känslig information behandlas eller bevaras i smarttelefonen. Diggs bedömning är att de allra flesta identifieringar kommer ske med stöd av appen, vilket kräver att den är säker, användarvänlig och tillgänglig. De tekniska kraven på smarttelefonen är i det här sammanhanget låga, och i princip samtliga smarttelefoner som finns i omlopp idag har den nödvändiga tekniken inbyggd.

I förslaget till teknisk utformning för en statlig e-legitimationen är en motsvarande mekanism som BankID:s *säker start* tvingande och Digg föreslår att det inte ska finnas någon annan metod för att starta identifieringsprocessen. En ytterligare skyddsåtgärd är att den personliga koden måste anges på samma enhet som kortet läses med. Det är alltså inte möjligt för en bedragare som kommit över en användares personliga kod att ange denna mot Diggs identifieringstjänst, och sedan lura användaren att endast läsa av sitt kort.

Vissa användargrupper kommer även ha behov av att använda kortet tillsammans med en vanlig dator, som då kan behöva kompletteras med en kortläsare. Denna programvara kan också behöva tas fram i olika versioner för att möta vissa användargruppers särskilda behov. Det är till exempel tänkbart att synskadade har behov av en programvara som fungerar på ett annat sätt än den som andra föredrar att använda.

Det kan också finnas behov av att stödja funktionen på olika plattformar, till exempel Linux, Microsoft Windows och Mac OS.

Digg bedömer att det är det lämpligt att låta publicera relevanta delar som öppen källkod, så att intressenter kan granska och förstå hur lösningen fungerar samt ta fram egna anpassade klientprogramvaror.

4.1.1 Andra lösningar som övervägts

Digg har i analysen övervägt andra tänkbara varianter av teknisk utformning av den statliga e-legitimationen, bland annat dosor för engångslösenord, FIDO2-enheter och befintliga id-handlingar. För- och nackdelar med dessa varianter sammanfattas nedan.

4.1.1.1 Dosor för engångslösenord

Olika typer av enheter för engångslösenord skulle kunna utgöra ett alternativ för en statlig e-legitimation. De har använts under lång tid inom banksektorn, och en stor del av befolkningen är vana användare. Dosor finns även i versioner för personer med olika former av funktionsnedsättning.

Dessa dosor saknar dock som regel de certifieringar som krävs för den högsta tillitsnivån. De är förhållandevis dyra och har begränsad livslängd på grund av att de måste innehålla ett batteri. Mängden elektroniska komponenter samt förekomsten av batteri torde även kräva att det inrättas ett kretslopp för återvinning av enheterna för att lindra den miljöpåverkan dessa annars kan antas få.

Ytterligare begränsningar utgörs av att dosornas säkerhetsfunktioner bygger på symmetrisk kryptografi, vilket innebär att utfärdaren måste hantera en stor mängd känsligt nyckelmaterial. Detta medför vissa risker och begränsningar i utformningen av säkerhetsarkitekturen. Sammantaget utgör dosorna visserligen ett tänkbart alternativ, men med flera betydande nackdelar.

4.1.1.2 FIDO2-enheter

FIDO2[51] är en relativt ny teknik på stark frammarsch, med det övergripande syftet att ersätta lösenord för identifiering av användare i tjänster på internet.

Tekniken bygger på öppna standarder som förvaltas av FIDO Alliance, som i sin tur stöttas av tongivande aktörer inom it-branschen, finansteknik och e-handel. FIDO2-specifikationerna omfattar även det mellanlager som krävs för kommunikation mellan webbläsare och medlet för identifiering. Den tekniska arkitekturen är dock utformad för många bilaterala relationer, och utifrån att de olika parter användaren interagerar med inte ska kunna länka samman identiteten mellan sig. Användningsfallen för en e-legitimation ser något annorlunda ut, även om det skulle vara möjligt att använda FIDO2-tekniken även på detta sätt.

[51] https://fidoalliance.org/fido2 (Hämtad 2023-01-02)

Avgörande för att inte gå vidare med FIDO2-enheter har varit att detta är en teknik med relativt avancerade enheter och ett förhållandevis högt pris. Dessutom utvecklas enheterna ständigt, och en och samma typ av enhet är i produktion endast under en begränsad tid vilket skulle leda till att flera olika typer av enheter (med delvis olika egenskaper) behöver kunna hanteras parallellt. Digg bedömer att även anmälan enligt eIDAS-förordningen skulle påverkas, då byte av enheter utgör en sådan ändring som måste anmälas och som kan kräva en förnyad sakkunniggranskning.

Risken för sårbarheter i enheterna är också större på grund av utvecklingstakten. Dessa enheter har vanligen inte de certifieringar som krävs för den högsta tillitsnivån, vilket också går att hänföra till utvecklingstakten.

På motsvarande sätt som för dosor för engångslösenord skulle det sannolikt bli nödvändigt att etablera ett kretslopp för återvinning av uttjänta enheter för att begränsa lösningens miljöpåverkan.

4.1.1.3 Befintliga id-handlingar

Digg har också övervägt att använda befintliga id-handlingar för den statliga e-legitimationen. Idag är det endast det nationella id-kortet och Skatteverkets id-kort som är försedda med sådant chip som skulle kunna bära en statlig e-legitimation.

Digg har valt att inte utreda Skatteverkets id-kort som ett alternativ. Digg tolkar det faktum att Skatteverket inte är en utpekad part i aktuellt regeringsuppdrag som att det inte är i denna riktning regeringen har avsett att utvecklingen av en statlig e-legitimation ska ske. Vidare får Skatteverkets id-kort inte ges ut till dem som endast tillfälligtvis vistas i landet och därför endast har samordningsnummer[52].

Det nationella id-kortet skulle kunna komma ifråga som bärare av en e-legitimation. Det nationella id-kortet kan dock endast skaffas av den som är svensk medborgare, och därmed utesluts viktiga målgrupper för den statliga e-legitimationen. Processen att skaffa ett nationellt id-kort är också förhållandevis lång och priset på 400 kronor kan verka avhållande.

Digg bedömer att det nationella id-kortet på sikt skulle kunna bli en kompletterande bärare av den statliga e-legitimationen, men det svarar alltså i nuläget inte upp mot grundförutsättningarna enligt Diggs analys.

[52] Lag (2015:899) om identitetskort för folkbokförda i Sverige

4.2 Tillitsnivå

Digg föreslår att den statliga e-legitimationen ska ges ut på den högsta tillitsnivån.

Flera utredningar har lämnat förslag om att Sverige ska ha en statlig e-legitimation på den högsta tillitsnivån[53] [54], dock utan att närmare precisera skälen. Lösningen som Digg föreslår uppfyller kraven på den högsta tillitsnivån, vilket förklaras ytterligare i det följande.

De e-legitimationslösningar som används idag når upp till den näst högsta tillitsnivån, huvudsakligen av två anledningar kopplade till utgivningsprocessen respektive innehavarens tekniska utrustning. Det är vanligt att BankID ges ut på distans, via innehavarens internetbank, vilket inte är förenligt med reglerna för den högsta tillitsnivån. Det finns också tillkommande tekniska krav på innehavarens mobila enheter som leder till att vissa grupper av användare utesluts från de tillhandahållna lösningarna. Detta avser dock i första hand användare av vissa enklare och äldre typer av enheter, och kan förvisso förväntas vara ett övergående problem.

De ökade krav som ställs genom eIDAS-förordningen samt behovet av en säker grundidentifiering talar för att en statlig e-legitimation bör ges ut enligt kraven på den högsta tillitsnivån enligt Tillitsramverket för Svensk e-legitimation. Det innebär att den statliga e-legitimationen ges ut på motsvarande sätt som traditionella id-handlingar samt lägger grunden för att den ska bli så gångbar som möjligt, såväl vid användning inom landet som i gränsöverskridande sammanhang.

För att den statliga e-legitimationen ska kunna ges ut och användas på den högsta tillitsnivån ställs vissa tekniska krav på e-legitimationshandlingens utformning. Det krävs att medlet för elektronisk identifiering har ett robust tekniskt manipulations- och kopieringsskydd, vilket i praktiken behöver styrkas genom certifiering utförd av oberoende part. För att ett införande ska kunna ske på ett kostnadseffektivt och snabbt sätt behöver den tekniska lösning som väljs redan ha efterfrågade certifieringar.

Det ska i sammanhanget noteras att varken det svenska tillitsramverket eller reglerna i kommissionens genomförandeförordning (EU) 2015/1502 kräver sådan certifiering. Det har dock i sakkunniggranskningar av andra medlemsländers e-legitimationssystem framträtt som praxis att det granskade medlemslandet antingen med stöd av egna

[53] SOU 2019:14
[54] SOU 2017:114

expertmyndigheter genomfört formell säkerhetsevaluering eller att man har kunnat lägga fram relevanta oberoende certifieringar.

Som exemplet från Estland i avsnitt 3.2.2.1 visar är sådana certifieringar inte någon garanti för att sårbarheter inte kan förekomma i den valda lösningen. Digg föreslår av bland annat denna anledning att den personliga koden registreras vid sidan om kortet och verifieras genom ett så kallat nollkunskapsbevis mot centrala system som Digg tillhandahåller. Det minskar det säkerhetsmässiga beroendet till kortet på så sätt att den personliga koden inte kan åsidosättas genom sårbarheter i kortets chip, så som skedde i Estland.

Genom att basera den föreslagna lösningen på PIV-specifikationerna kan ett flertal leverantörer redan idag erbjuda likvärdiga och i huvudsak interoperabla produkter som kan ersätta varandra. Detta ger möjlighet att skapa diversitet i försörjningskedjorna. Förslaget innebär också att beroendet till kortleverantörens verksamhet minimeras, och innefattar även krav på att mer än en kryptografisk algoritmuppsättning ska stödjas av den valda kortlösningen för identifiering och underskrift.

En annan implikation av att den statliga e-legitimationen ska leva upp till kraven för den högsta tillitsnivån är att utgivningsprocessen (ansökan, grundidentifiering, tillhandahållande och aktivering) måste delas upp i mer än ett steg. Detta följer av krav på separation av arbetsuppgifter i utgivningsprocessen. Det är alltså inte acceptabelt att en person vid utgivningsstället handlägger samtliga delar, någon del av processen behöver ske oberoende av handläggaren. I eIDAS-förordningens regelverk förutsätts det vara aktiveringssteget som ska säkerställa denna separation, något som i viss mån begränsar tillgängligheten för vissa grupper. Digg har valt att föreslå en lösning med ett sådant aktiveringsförfarande som uttryckligen föreskrivs i genomförandeförordningen[55].

I övrigt har kravställningen som den högsta tillitsnivån för med sig begränsade återverkningar på den föreslagna lösningen. Att identifiering ska ske vid personligt besök är redan en grundförutsättning i uppdraget till Digg, och är annars en av de övriga materiella skillnaderna mellan den högsta och den näst högsta tillitsnivån.

4.3 Åldersgräns

Digg föreslår att den statliga e-legitimationen får ges ut till den som är 13 år eller äldre. För att en minderårig ska kunna få en statlig e-legitimation krävs vårdnadshavares godkännande.

[55] Kommissionens genomförandeförordning (EU) 2015/1502, bilagans avsnitt 2.2.2 för nivån *hög*.

Det finns inte någon generell åldersgräns i tillämpliga regelverk eller författning för när e-legitimationer får ges ut. Det finns alltså inte några legala hinder mot att en e-legitimation ges ut till en minderårig person. Med minderårig avses här en person som är under 18 år.[56]

En utgångspunkt för bedömningen av vad som är en lämplig ålder för en e-legitimation är att det krävs att den minderåriga har nått behövlig förståndsmognad. Digg har övervägt en lösning där personal vid de identitetskontrollerande myndigheterna ska göra en individuell bedömning av den sökandes mognadsgrad. Digg har dock bedömt att det är mer ändamålsenligt med en generell åldersgräns som framgår direkt i förordning om statlig e-legitimation, se bilaga 4.

Id-kortsutredningen föreslog en 16-årsgräns utifrån att behovet av en legitimationshandling ansågs var kopplat till behovet av att kunna utöva sin rättshandlingsförmåga[57]. Behovet av att kunna identifiera sig elektroniskt är dock betydligt bredare och inte endast kopplat till förmåga att rättshandla.

Viss ledning i frågan om lämplig undre åldersgräns kan hämtas från lagen (2015:899) om id-kort för folkbokförda i Sverige. Dessa id-kort, som ges ut av Skatteverket, innehåller även en e-legitimation och får ges ut till den som är 13 år eller äldre. En åldersgräns på 13 år för den statliga e-legitimationen möter även det ökade behov som finns av att kunna legitimera sig, särskilt i elektroniska miljöer. Exempelvis vid kontakter med vården, tillgång till den egna journalen och hantering av receptärenden. En e-legitimation kan också antas bli mer och mer behövlig och användbar inom skolväsendet framgent.

Den som är minderårig kan inte själv ansöka om att få en e-legitimation, det kräver vårdnadshavares godkännande. För minderåriga som står under vårdnad av bägge föräldrarna är dessa vårdnadshavare och detta ska i princip alltid utövas gemensamt. Det innebär att i förekommande fall ska båda vårdnadshavarna lämna godkännande om att den minderåriga kan få en statlig e-legitimation, och att detta ska ske innan e-legitimationen kan ges ut. Digg föreslår därför att det i förordningen om statlig e-legitimation ska framgå att en statlig e-legitimation får utfärdas till den som är minderårig endast om barnets vårdnadshavare har lämnat skriftligt medgivande.

[56] 9 kap. 1 § föräldrabalken (1949:381)
[57] SOU 2007:100. Id-kortsutredningen. *Id-kort för folkbokförda i Sverige: slutbetänkande*.

4.4 Samordningsnummer

Digg föreslår att den statliga e-legitimationen får ges ut även till den som har tilldelats ett samordningsnummer och kan styrka sin identitet.

Ett samordningsnummer är en identitetsbeteckning för personer som inte är eller har varit folkbokförda i Sverige, men som ändå har behov av att ha kontakt med svenska myndigheter eller andra delar av samhället. Samordningsnummer tilldelas den som har anknytning till Sverige och har behov av ett samordningsnummer men inte uppfyller kraven för att bli folkbokförd. Det kan vara aktuellt för den som till exempel ska arbeta eller studera i Sverige kortare tid än ett år eller för den som äger en fastighet och därför kan behöva teckna avtal om el och sophämtning. Det behövs även ett samordningsnummer för att kunna öppna ett bankkonto. Vid ingången till förra året fanns knappt 360 000 aktiva samordningsnummer av detta slag registrerade i Skatteverkets folkbokföringsdatabas.

E-legitimationer ges idag inte ut till personer med samordningsnummer i någon relevant omfattning, till stor del på grund av att dessa personer vanligtvis saknar svensk fullgod id-handling. Detta leder till ett växande utanförskap för denna tämligen stora grupp av människor, där det blir allt svårare att få tillgång till grundläggande samhällstjänster. Utanförskapet medför i sin tur svåra problem att komma in i det svenska samhället.

De begränsningar i tillvaron som avsaknad av ett personnummer innebär för dem som vistas i Sverige har också granskats av EU-kommissionen i ett antal så kallade pilotärenden,[58] bland annat utifrån frågan om det föreligger hinder för den fria rörligheten enligt unionsrätten. Framställarna i dessa ärenden har i avsaknad av ett personnummer upplevt hinder för att få tillgång till relevanta tjänster i vardagslivet. EU-kommissionen har också konstaterat att problemen förblir olösta och avser att återkomma om vidare hantering av frågan.

Det har vidtagits åtgärder för att komma tillrätta med problematiken. Bland annat kan samordningsnummer numera begäras av den enskilde själv, där det tidigare krävdes att en myndighet begärde samordningsnumret för att det behövdes i den egna verksamheten. Vidare har ett förslag till stärkt system för samordningsnummer[59] nyligen antagits av riksdagen, och de huvudsakliga förändringarna träder i kraft den 1 september 2023. De nya reglerna innebär att samordningsnummer inrättas i tre nivåer beroende på vilken identitetskontroll som föregått tilldelningen. Den högsta nivån, kallad *styrkt identitet*,

[58] EUP[2016]8967, EUP[2018]9384 och EUP[2019]9455
[59] Prop. 2021:22/276

tilldelas den som har styrkt sin identitet vid personlig inställelse genom att framlämna ett giltigt pass, id-kort eller motsvarande annan id-handling. Den myndighet som utför identitetskontrollen ges också möjlighet att kontrollera biometriska uppgifter som finns lagrade i de id-handlingar som överlämnas vid kontrollen.

Huvuddelen av de idag tilldelade samordningsnumren kommer att inordnas i kategorin *sannolik identitet*, som anger att en begränsad identitetskontroll har föregått tilldelningen av samordningsnumret där personlig inställelse sällan har varit en del av identitetskontrollen, och där olika rutiner har tillämpats vid olika myndigheter. Identitetskontrollen som hittills gjorts i samband med tilldelning av samordningsnummer kan närmast jämföras med de regler som i fortsättningen gäller för tilldelning av samordningsnummer med uppgift om *sannolik identitet*.

Den process som föreskrivs för identitetskontrollen för den högsta nivån är likvärdig med det som Digg i avsnitt 5.2.3 föreslår ska tillämpas vid utgivning av den statliga e-legitimationen. Det vore därför rimligt att samordna sådan utgivning av den statliga e-legitimationen till personer med samordningsnummer, så att det sker av samma identitetskontrollerande myndighet och enligt samma rutiner som vid tilldelningen av samordningsnummer. Den som då enligt övergångsbestämmelserna erhåller det som kallas *sannolik identitet* kan således genom att skaffa en statlig e-legitimation i den processen styrka sin identitet, och på så sätt upphöja dessa uppgifter till den högsta nivån. På samma sätt vore det rimligt att den som besöker en identitetskontrollerande myndighet för att få ett samordningsnummer, samtidigt också erbjuds möjlighet att skaffa den statliga e-legitimationen.

Den statliga e-legitimationen kan alltså aldrig bli aktuell för en person vars identitet bedömts som *sannolik* i enlighet med de nya bestämmelserna som beskrivits ovan, eller i de fall där det råder osäkerhet om personens identitet.

4.5 Mobil lösning

Dagens e-legitimering domineras av mobila lösningar på smarttelefoner. Digg bedömer att detta kommer att efterfrågas av användarna även när det gäller den statliga e-legitimationen. Den pågående utvecklingen inom EU bör dock också beaktas när det gäller utveckling av en mobil lösning för den statliga e-legitimationen.

Den föreslagna europeiska digitala identitetsplånboken ska uppfylla kraven för den högsta tillitsnivån och de specifikationer som nu tas fram är främst inriktade på mobilbaserade lösningar[60]. Plånboken ska kunna fungera på ett smidigt sätt såväl vid elektronisk

[60] Det kan dock inte helt uteslutas att andra lösningar kan bli aktuella, till exempel för organisationer.

identifiering på distans som i det fysiska mötet. Detta ställer sådana krav på innehavarens utrustning att plånboken knappast kommer vara tillgänglig för så många som möjligt. Därtill återstår omfattande arbete med att ta fram tekniska specifikationer och utveckla de system som krävs i form av bakomliggande infrastruktur och den programvara som innehavaren ska ha i sin telefon.

Den statliga e-legitimationen som föreslås av Digg passar in i arbetet med den europeiska identitetsplånboken på så sätt att den kan användas för att skaffa den elektroniska identitetsplånboken. Det bör inte krävas ett förnyat besök till ett utgivningsställe varje gång en användare installerar om eller byter telefon.

Arbetet med den europeiska identitetsplånboken är dock omgärdat av vissa osäkerhetsfaktorer, inte minst med avseende på tidplanen. Det komplicerade utvecklingsarbete och de omfattande integrationer som krävs för att ge ut och använda identitetsplånboken kan förväntas ta lång tid. Beroende på hur detta arbete fortskrider kan det övervägas om Digg ska påbörja arbetet att ta fram en statlig mobil e-legitimationslösning innan den digitala identitetsplånboken finns tillgänglig.

4.6 Nya krav på Diggs säkerhetsarbete

Informations- och cybersäkerhet är ett omfattande arbete som kräver ett ansvarsfullt ledarskap, att arbetet bedrivs på ett systematiskt och strukturerat sätt samt att rätt och tillräckliga resurser görs tillgängliga för att bedriva arbetet. Att vara e-legitimationsutfärdare och möta de utmaningar som informations- och cybersäkerhetsfrågorna för med sig skulle innebära att nya krav ställs på Diggs verksamhet, inte minst på säkerhetsområdet. Digg skulle i en roll som utfärdare av den statliga e-legitimationen behöva vidareutveckla sin säkerhetskultur, alltså de gemensamma attityder, värderingar och uppfattningar som chefer och medarbetare har om förhållandet till säkerhet och arbetsmiljö. Det som kännetecknar god säkerhetskultur i en verksamhet är att ledningen, chefer och medarbetare prioriterar och hanterar säkerhetsfrågor på alla nivåer. Synen på informations- och cybersäkerhet måste vidgas från att kanske främst ha varit en it-relaterad fråga till att bli mer holistisk och omfatta hela utfärdarverksamheten.

Det dagliga arbetet på säkerhetsområdet för en statlig e-legitimation skulle innefatta kontinuerlig omvärldsbevakning, deltagande i olika samarbetsorgan på säkerhetsområdet, föra intressentdialoger, genomföra regelbundna riskanalyser, styra och införa risklindrande åtgärder, arbeta med intern kontroll och medverka i oberoende revisioner av verksamheten, säkerställa verksamhetens kontinuitet, säkerhetspröva personal som ska delta i verksamheten, hantera, utreda och rapportera inträffande incidenter, rapportera resultatet av säkerhetsarbetet till myndighetens ledning, och så vidare. Säkerhetsarbetet

kring den statliga e-legitimationen skulle fordra att Digg knyter till sig långsiktig strategisk och teknisk säkerhetskompetens då området ständigt kommer att vara under utveckling och utsättas för prövningar i form av förändrade hotbilder, nya risker och angreppsförsök.

För det fall den statliga e-legitimationen är en sådan verksamhet som är av betydelse för Sveriges säkerhet kan den komma att omfattas av säkerhetsskyddslagstiftningen (se även avsnitt 9.5.6). Ansvaret är i sådana fall långtgående. Det kommer sannolikt fordras att utfärdarverksamheten i viss mån avskiljs från Diggs övriga verksamhet för att begränsa säkerhetsskyddslagens räckvidd så att inte dess bestämmelser ska bli alltför betungande, se också avsnitt 7.2 om rollkonflikter.

5 Förslag till utgivningsprocess

Digg föreslår att Digg ska ansvara för utfärdandet av den statliga e-legitimationen och identitetskontrollerande myndighet ska kontrollera att sökandes identitet är styrkt vid personligt besök, det som i uppdraget benämns grundidentifiering.

Digg föreslår en utgivningsprocess som uppfyller kraven för den högsta tillitsnivån.

Av regeringsuppdraget framgår att Digg ska vara ansvarig för den statliga e-legitimationen och att den ska vara tillgänglig för så många som möjligt. Det framgår också att lösningar som leder till högre kostnadseffektivitet och kortare införandetid ska övervägas. Diggs förslag innebär att lösningen uppfyller kraven för den högsta tillitsnivån enligt Tillitsramverket för Svensk e-legitimation, och som en följd av det även kraven som ställs genom (EU) 2015/1502 för tillitsnivån *hög* enligt eIDAS-förordningen.

En utgångspunkt för Diggs förslag till fördelningen av förvaltningsuppgifter mellan Digg och de identitetskontrollerande myndigheterna har varit att identitetskontrollerande myndighet inte ska betungas i alltför stor uträckning. En annan utgångspunkt har varit att finna en modell där uppgifter och ansvar fördelas så att det, både för berörda myndigheter och för den som ansöker om statlig e-legitimation, ska vara tydligt vem som ansvarar för respektive del. Förslaget ska vara rättsenligt, administrativt hanterbart och hållbart över tid.

5.1 Vad avses med grundidentifiering?

Utgångspunkten är att den identitetskontrollerande myndigheten ska genomföra det som i uppdraget kallas för *grundidentifiering*.

Grundidentifiering är ett begrepp som inte förekommer i de regelverk som gäller för pass eller nationellt id-kort. Begreppets innebörd anges inte heller närmare i regeringsuppdraget. Utredningen om effektiv styrning av nationella digitala tjänster har i sitt slutbetänkande använt detta begrepp som beteckning på åtgärder som syftar till att koppla ihop en individ med uppgifter i folkbokföringsdatabasen och som resulterar i att en identitetshandling ges ut[61]. Med grundidentifiering avser Digg i denna rapport att kontrollera att en sökandes identitet är styrkt. Användningen av begreppet ansluter väl till

[61] SOU 2017:114 s. 173.

nuvarande regler inom området, exempelvis Polismyndighetens föreskrifter för pass och nationellt id-kort.[62]

5.2 Stegen i utgivningsprocessen

Processen som Digg föreslår för utgivningen av den statliga e-legitimationen utgår från att den identitetskontrollerande myndigheten kommer att utföra en grundidentifiering av den sökande genom personligt besök till ett utgivningsställe. Den identitetskontrollerande myndigheten kommer i processen att dokumentera resultatet av grundidentifieringen och hjälpa den sökande att upprätta och ge in en ansökan om statlig e-legitimation till Digg. Det blir således en fråga för de identitetskontrollerande myndigheterna att ge service åt enskilda i samband med ansökan om statligt e-legitimation. En ansökan om statlig e-legitimation registreras hos Digg och det är Digg som automatiserat kommer att fatta beslut om utfärdande. Den identitetskontrollerande myndigheten ska därefter tillhandahålla e-legitimationen till sökanden. Det kan övervägas om den identitetskontrollerande myndigheten i samband med tillhandahållandet även ska kunna hjälpa sökanden vid aktivering av den statliga e-legitimationen, för det fall sökanden av någon anledning inte kan aktivera e-legitimationen på egen hand. Nedan följer en kortfattad beskrivning av den föreslagna utgivningsprocessen.

5.2.1 Beställning av kortämnen

1. Ansvarig administratör vid utgivningsstället beställer kortämnen[63]. Beställningen läggs i Diggs system på visst antal kortämnen (lådor om något hundratal förproducerade kort).
2. Digg förmedlar beställningen till korttillverkare som packar lådorna i förslutet säkerhetsemballage och sänder kollit direkt till utgivningsstället.
    a. Säkerhetsemballagets serienummer förmedlas tillbaka via Diggs system.
    b. I kollit packas även motsvarande antal informationsfoldrar som ska tillhandahållas sökanden tillsammans med kortet.
3. Då kollit anländer kontrollerar ansvarig administratör det förslutna säkerhetsemballaget, verifierar serienummer och dokumenterar utfallet. Kortämnena plockas ur emballaget och förvaras på skyddad plats vid utgivningsstället.
    a. Om säkerhetsemballaget är skadat kasseras korten.

[62] Polismyndighetens föreskrifter och allmänna råd om pass och nationellt id-kort PMFS 2021:3.
[63] Blanka kort som inte tilldelats någon och som saknar egentligt värde

5.2.2 Ansökan om att få en e-legitimation

Processen från ansökan till aktivering kräver endast att sökanden genomför ett besök till ett utgivningsställe.

1. Sökanden beger sig till ett utgivningsställe. Information om adresser, öppettider och hur eventuell tidsbokning kan göras finns på Diggs webbplats.
2. Vid utgivningsstället inleds processen med att handläggaren tar betalt av sökanden.
3. Handläggaren noterar sedan sökandens person- eller samordningsnummer och öppnar samtidigt en ansökan i ett ärende om statlig e-legitimation[64].

5.2.3 Identifiering av sökanden och tillhandahållande av kort

1. Sökanden styrker sin identitet för handläggaren enligt de rutiner och krav identitetskontrollerande myndighet föreskrivit.

2. Efter genomförd identifiering av sökanden intygar handläggaren i Diggs system att identifiering är genomförd på föreskrivet sätt.
    a. Om handläggaren inte kan genomföra en identifiering på föreskrivet sätt meddelas detta till Digg via Diggs system som därvid fattar beslut om att inte utfärda en e-legitimation till sökanden.
3. Om inga hinder föreligger mot att utfärda en e-legitimation fattar Digg ett beslut att bifalla ansökan.
    a. Prövningen av ärendet hos Digg består bland annat i att kontrollera att grundidentifieringen kunde genomföras med positivt resultat samt att den åberopade identiteten finns registrerad i folkbokföringsdatabasen, och att denna inte är markerad som avliden, försvunnen eller falsk.
4. Om ansökan om en e-legitimation bifallits av Digg tar handläggaren ett kort ur lådan med kortämnen, registrerar kortets löpnummer i ärendet, och lämnar kortet tillsammans med kvitto och en informationsfolder till sökanden. Handläggningen vid utgivningsstället är nu avslutad.
    a. Om Digg avslår ansökan ska handläggaren vid utgivningsstället bistå i att expediera beslutet till sökanden inklusive återbetalning av erlagd avgift.

[64] Kraven i kommissionens genomförandeförordning (EU) 2015/1502, bilagans avsnitt 2.1.1, måste beaktas vid den närmare utformningen av ansökningsprocessen.

5.2.4 Aktivering och val av personlig kod

Sökanden har nu kortet i sin hand och måste aktivera det innan det kan användas. Detta följer av de krav som gäller för tillitsnivå *hög* enligt eIDAS-förordningen. Information om hur aktivering går till finns i den folder som sökanden erhöll tillsammans med kortet. Aktivering måste också ske inom viss tid från utlämnandet. Sökanden ges tre alternativ för att aktivera e-legitimationen:

1. Elektronisk aktivering i egen utrustning genom Diggs app. Detta alternativ är tillgängligt för den som har tillgång till en smarttelefon eller motsvarande, och som innehar ett giltigt svenskt pass eller giltigt svenskt nationellt id-kort.
    a. Sökanden laddar ner Diggs app till sin smarttelefon och startar den.
    b. Sökanden väljer *aktivera e-legitimation.*
    c. Sökanden läser av sin id-handling genom att först fotografera den så att kameran kan registrera det maskinläsbara fältet[65] och håller sedan id-handlingen mot baksidan av telefonen för avläsning via gränssnittet för närfältskommunikation[66].
    d. Om det existerar en icke-aktiverad e-legitimation för det avlästa personnumret ges sökanden valet att aktivera denna. Detta steg kan innefatta att läsa av kortet genom telefonen, för att säkerställa att sökanden fortfarande har det i sin kontroll.
    e. Sökanden väljer personlig kod, och vägleds i denna process i appen att välja en tillräckligt säker personlig kod med avseende på längd och komplexitet.
    f. E-legitimationen är nu klar att använda.
2. Elektronisk aktivering i självserviceterminal. Detta alternativ är tillgängligt för den som inte har tillgång till en smarttelefon eller motsvarande, men som innehar ett giltigt svenskt pass eller giltigt svenskt nationellt id-kort.
    a. Efter att sökanden fått kortet i sin hand går hen till självserviceterminalen på utgivningsstället. Självserviceterminalen består i en surfplatta i så kallat kioskläge, monterad på ett stativ och med uppkoppling via mobilnätsanslutning.
    b. Sökanden väljer *aktivera e-legitimation.*
    c. Sökanden läser av sin id-handling genom att först hålla upp den mot terminalen så att kameran kan registrera det maskinläsbara fältet och håller sedan id-handlingen mot angivet ställe på terminalen för avläsning via gränssnittet för närfältskommunikation.

[65] Machine-readable zone, MRZ
[66] Near Field Communication, NFC

d. Om det existerar en icke-aktiverad e-legitimation för det avlästa personnumret ges sökanden valet att aktivera. Detta steg kan innefatta att läsa av kortet genom terminalen, för att säkerställa att sökanden fortfarande har det i sin kontroll.
e. Sökanden väljer personlig kod, och vägleds i denna process i terminalen att välja en tillräckligt säker personlig kod med avseende på längd och komplexitet.
f. E-legitimationen är nu klar att använda.

3. Om inget av de två tidigare alternativen för aktivering skett inom 24 timmar från det att kortet tillhandahölls sänds en aktiveringskod till sökandens folkbokföringsadress (eller registrerad utlandsadress om sådan existerar). Aktiveringsalternativ ett och två ovan kvarstår även om en aktiveringskod skickats med post till sökanden.
    a. Efter att sökanden fått brevet med aktiveringskoden besöker denne Diggs webbplats. Om sökanden inte har tillgång till egen dator, eller är osäker på processen och behöver hjälp, kan detta ske på ett av Statens servicecenters kontor eller på ett kommunalt Digidel-center[67].
    b. Sökanden väljer *aktivera e-legitimation* och anger sitt person- eller samordningsnummer samt kortets löpnummer.
    c. Sökanden ombeds att ange aktiveringskoden som mottagits genom brevet.
    d. Om det existerar en icke-aktiverad e-legitimation med det angivna löpnumret och för det angivna person- eller samordningsnumret, samt att en giltig aktiveringskod angetts, ges sökanden valet att aktivera e-legitimationen.
    e. Sökanden väljer personlig kod, och vägleds i denna process i webbläsaren att välja en tillräckligt säker personlig kod med avseende på längd och komplexitet.
    f. E-legitimationen är nu klar att använda.

5.3 Tillgänglighetsanalys av utgivningsprocessen

Av regeringsuppdraget framgår att den statligt utfärdade e-legitimationen ska vara tillgänglig för så många som möjligt, och utgöra ett komplement till de privat tillhandahållna lösningarna. Digg delar denna bedömning och konstaterar att finns flera grupper av personer som riskerar ett digitalt utanförskap. Bland dessa personer kan det

[67] https://digidel.se/digidelcenter/

också finnas flera samverkande faktorer som bidrar till det digitala utanförskapet. Digg har i det här arbetet gjort en översiktlig analys, men vill betona att det krävs fördjupning av olika aspekter kopplade till digitalt utanförskap i ett nästa steg, inte minst när det gäller tillgänglighetsfrågor.

Enligt SCB:s undersökning Befolkningens IT-användning 2022[68] har 94 procent av befolkningen, eller nästan 8 miljoner personer, i åldrarna 16–85 år tillgång till internet i hemmet. I åldersgruppen 75–85 år var tillgången till internet drygt 90 procent och i åldersgruppen 75–85 år var siffran 86 procent. Hela 15 procent i åldrarna 75–85 år har dock aldrig använt internet. Samhället behöver ett kompletterande och fördjupande perspektiv på det digitala utanförskapet, vilket exempelvis kan skapas genom att titta närmare på olika särskilt utsatta samhällsgrupper och hur de använder internet. Vissa grupper osynliggörs dock i undersökningar som drar slutsatser om hela befolkningen. Detta beror till viss del på att individer i de här grupperna är relativt få till antalet. Metoderna som används för att samla in data når inte vissa personer och ger dem därför inte en chans att delta i undersökningar och enkäter. Denna svaghet i undersökningsmetodiken illustreras i en studie utförd av Linköpings universitet, i vilken det digitala utanförskapet undersöktes i en svensk mångkulturell förort[69]. Studien visade att 13 procent i den aktuella förorten inte använde internet alls och att 23 procent inte hade BankID. Hela 21 procent av deltagarna i studien uppgav att de inte kände sig delaktiga i det digitala samhället.

Föreningen Begripsam har genomfört en undersökning som slog fast att den digitala klyftan etableras i unga år och består livet ut[70]. Storleken på klyftan varierade beroende på funktionsförmåga. I många fall var skillnaden mellan de som har funktionsnedsättning och de utan runt 30 procent, och återfanns i alla åldersgrupper. En tredjedel av personerna med en funktionsförmåga som skiljer sig från normen hade enligt undersökningen till exempel inte någon e-legitimation, vilket i sin tur innebar att de var utestängda från digitala kontakter med myndigheter och företag där det krävs e-legitimation.

5.3.1 Svårigheter att ta sig till ett utgivningsställe

I en rapport från Trafikanalys bedömdes det att ungefär en tredjedel av Sveriges befolkning har minst en funktionsnedsättning som påverkade deras vardag och därmed

[68] Statistiska centralbyrån. *Befolkningens it-användning 2022.*
[69] Karin Skill och Ahmed Kaharevic. *Förorten svarar: En enkätmetod för att kartlägga digital delaktighet och hållbarhet i Skäggetorp.* DINO Rapport 2021:7, Linköpings universitet.
[70] Begripsam. *Svenskarna med funktionsnedsättning och internet.* 2019.

resandet[71]. Det är känt att personer med funktionsnedsättning reser mindre än den genomsnittliga personen i befolkningen. En person med nedsatt rörelseförmåga gör till exempel i genomsnitt hälften så många resor per dag i jämförelse med de som inte har någon funktionsnedsättning.

Det finns ett visst samspel mellan ett mindre resande bland personer med funktionsnedsättning och med ålder och sysselsättning. Bland personer med funktionsnedsättning finns det en större andel äldre och ekonomiskt utsatta i jämförelse med befolkningen i övrigt. Dessutom förvärvsarbetar personer med funktionsnedsättning i mindre utsträckning än andra. Förutom ålder och socioekonomiska faktorer kan dock inte det mindre resandet förklaras på andra sätt än att det finns reella barriärer och hinder i kollektivtrafiken.

Ett sätt att lösa utmaningen med att kunna ta sig till ett utgivningsställe är att handläggare vid en identitetskontrollerande myndighet istället tar sig till personen som vill skaffa sig en e-legitimation, men som av någon anledning inte kan ta sig till ett utgivningsställe. Detta skulle kunna lösas med hjälp av mobila enheter. Ett annat sätt att skapa en större tillgänglighet kan vara att bredda antalet utgivningsställen. Det kan handla om var i landet utgivningsställen placeras i kombination med ett utökat antal utgivningsställen.

5.3.2 Svårigheter med aktivering av e-legitimationen

Det kan också finnas svårigheter vid själva aktiveringen av e-legitimationen enligt de steg för aktivering som beskrivits i avsnitt 5.2.4. Den sökandes ekonomiska förutsättningar kan vara begränsande i alternativ ett, handhavandet och vardagskulturen kan vara begränsande i alternativ två och vad gäller alternativ tre behöver en korrekt folkbokföringsadress vara registrerad i folkbokföringsdatabasen. För alternativ tre krävs dessutom att den sökande har tillgång till dator. Det kan också förekomma fel i de registrerade folkbokföringsuppgifterna med avseende på folkbokföringsadress[72] eller att en person saknar folkbokföringsadress. Det finns uppskattningar som pekar på att ungefär 200 000 personer lever på en felaktig adress[73] och 33 000 personer i hemlöshet[74].

I de fall aktiveringen ska utföras på ett av Statens servicecenters kontor eller motsvarande uppstår samma svårigheter beträffande resandet som beskrevs i föregående avsnitt. Förutom att kognitiva utmaningar genomsyrar de olika delarna av aktiveringsprocessen

[71] Trafikanalys. *Kollektivtrafikens barriärer – kartläggning av hinder i kollektivtrafikens tillgänglighet för personer med funktionsnedsättning Rapport 2019:3.* 2019.

[72] SOU 2021:57. Utredningen om folkbokföring och samordningsnummer. *Om folkbokföring, samordningsnummer och identitetsnummer: slutbetänkande.*

[73] https://www.hemhyra.se/nyheter/har-aker-du-oftast-fast-for-fel-adress-vi-anmaler-jattemycket/

[74] https://www.socialstyrelsen.se/om-socialstyrelsen/pressrum/press/fler-atgarder-behovs-for-att-forebygga-hemloshet/

så finns det andra generella hinder. En aspekt att särskilt tänka på är den fysiska utformningen av utgivningsplatserna. En högre grad av tillgänglighet kan åstadkommas genom att erbjuda service och stöd, exempelvis att sökanden kan få hjälp av en handläggare med aktivering av kortet. Detta skulle kunna genomföras vid ett av Statens servicecenters kontor eller vid kommunala Digidel-center.

6 En e-legitimation för hela samhället

Digg föreslår att inrätta en statlig förlitandetjänst där Digg tillhandahåller både elektroniska identitetskontroller och identitetsintyg till offentlig sektor samt en statlig identifieringstjänst där Digg endast utför identitetskontroller utan att leverera identitetsintyg till privata leverantörer av identitetsintyg.

Digg föreslår att upphandlande myndigheter ska kunna ansluta sig till den statliga förlitandetjänsten genom valfrihetssystemet.

Digg föreslår att privata leverantörer av identitetsintyg ska kunna ansluta sig till den statliga identifieringstjänsten för att förse andra aktörer med identitetsintyg. Det gransknings- och tillståndsförfarande som följer av regelverket kring kvalitetsmärket Svensk e-legitimation ska tillämpas även för anslutning till den statliga identifieringstjänsten.

Digg föreslår att den statliga e-legitimationen ska kunna användas i hela samhället, alltså både i offentlig och privat sektor. Detta kräver dock olika lösningar, såväl ur tekniskt som rättsligt hänseende. I det följande beskrivs vilka tjänster Digg bör tillhandahålla, åt förlitande aktörer eller privata tjänsteleverantörer, för att en statlig e-legitimation ska kunna användas och tillföra det ytterligare skydd för samhället som krävs samt hur berörda rättsförhållanden bör regleras, med avseende på

- kontrollerna av om använd e-legitimation är giltig och vem som har brukat den (elektronisk identitetskontroll), respektive
- leveransen av identitetsintyg efter en elektronisk identitetskontroll (utställande av identitetsintyg).

6.1 En statlig förlitandetjänst och en statlig identifieringstjänst

Digg föreslår en uppdelning i tjänsterna för statlig e-legitimation. Förslaget innebär att en statlig förlitandetjänst inrättas genom vilken Digg tillhandahåller både elektroniska identitetskontroller och identitetsintyg. Utöver detta inrättas det även en statlig identifieringstjänst där Digg endast utför identitetskontroller utan att leverera identitetsintyg. Som en följd av uppdelningen i två olika tjänster behöver det rättsliga mellanhavandet konstrueras på delvis olika sätt. När den statliga förlitandetjänsten används uppkommer ett rättsförhållande direkt mellan Digg och förlitande aktör. När identitetsintygen istället tillhandahålls av en privat leverantör av identitetsintyg uppkommer dels ett rättsförhållande mellan Digg och den privata leverantören av identitetsintyg, dels ett rättsförhållande mellan den privata leverantören och den

förlitande aktör som den privata leverantören förser med identitetsintyg. För den statliga identifieringstjänsten behöver Digg bara tillhandahålla ett maskinellt gränssnitt, API[75], för att verifiera användares identitet.

6.2 Upphandlade myndigheter kan ansluta sig till den statliga förlitandetjänsten genom valfrihetssystemet

6.2.1 Valfrihet för användaren

Sedan e-legitimationer började användas i digitala tjänster har det varit en utmaning för myndigheter att anskaffa förlitandetjänster. Myndigheter är vanligtvis hänvisade till upphandlingsförfaranden där en vinnare ska utses. Men det är användaren som väljer vilken e-legitimation denne vill använda. En sedvanlig upphandling skulle därför resultera i att bara användare som valt just den typ av e-legitimation som tilldelats kontraktet i upphandlingen skulle kunde identifiera sig i den upphandlande myndighetens digitala tjänster.

För att erbjuda tillgång till identifierings- och intygstjänster för alla de e-legitimationer som en myndighet behöver kunna lita på infördes därför lagen om valfrihetssystem i fråga om tjänster för elektronisk identifiering[76]. Digg bedömer att den förlitandetjänst som här föreslås bör kunna omfattas av samma lag. Detta innebär att den statliga e-legitimationen ska ansöka om att ingå i valfrihetssystem i fråga om tjänster för elektronisk identifiering. På så sätt kan lagen om valfrihetssystem[77] tillämpas för upphandlande myndigheter för att få tillgång till identifieringstjänster för den statliga e-legitimationen.

6.3 Privata leverantörer av identitetsintyg kan ansluta sig till den statliga identifieringstjänsten

Digg föreslår att även privat sektor ska kunna erbjuda den statliga e-legitimationen i sina digitala tjänster. Idag finns det ungefär 6000 digitala tjänster som använder e-legitimation för elektronisk identifiering. Omkring 75 procent av dessa återfinns inom den privata sektorn. Digg bedömer att det finns ett stort behov även i privat sektor av att kunna erbjuda en statlig e-legitimation i de digitala tjänsterna.

[75] Application Programming Interface
[76] Lag (2013:311) om valfrihet i fråga om tjänster för elektronisk identifiering
[77] Ibid.

Eftersom olika samhällssektorer har skilda behov påverkas den teknik som är mest lämpad för informationsutbytet inom respektive sektor. Dessa behov representerar inte sällan motstående intressen som kan vara svåra att förena. Till detta kan läggas även andra utmaningar som uppkommer om ett anslutningsförfarande skulle omfatta alla privata aktörer och den hantering av till exempel sanktioner som därmed skulle krävas och utföras som en del i myndighetsutövning. Dagens modell med civilrättsliga avtal är inte ändamålsenlig för en sådan vidgad hantering. Den administration som skulle bli följden av att pröva en vid krets av aktörer, tekniskt validera, teckna avtal och sedan ansluta, följa upp och utöva tillsyn över dem skulle bli omfattande och ta tid att införa.

Digg föreslår därför att privata leverantörer av identitetsintyg ska få ansluta sig till en statlig identifieringstjänst för att i sin tur ställa ut identitetsintyg i det format och på det sätt som de överenskommer om med sina respektive kundgrupper. Det blir därmed den privata leverantören av identitetsintyg som gentemot de privata förlitande aktörerna får hantera förlitandeavtal, ansvarsfrågor, ersättningar, uppföljningar och sanktioner om en förlitande aktör bryter mot uppsatta regler. Diggs roll begränsas till att kontrollera om den använda e-legitimationen är giltig och vem som har brukat den för att sedan besvara den privata leverantörens fråga om en användares identitet kan verifieras eller inte.

6.3.1 Krav för att få anslutas till den statliga identifieringstjänsten

För att säkerställa att privata leverantörer av identitetsintyg producerar överenskomna tjänster på ett tillräckligt säkert sätt föreslås att Digg ska tillämpa rutiner för granskning och godkännande av dessa aktörer innan de får bli en del av den infrastrukturen.

Digg har redan infört ett gransknings- och tillståndsförfarande för sådana tjänster enligt det regelverk som omgärdar Kvalitetsmärket Svensk e-legitimation. Dessa regler och rutiner, innefattande tillitsramverkets krav, bör tillämpas även här. Därmed kan redan godkända utfärdare av Svensk e-legitimation omedelbart anslutas till den statliga identifieringstjänsten.

Ytterligare privata leverantörer vars verksamhet endast inriktas på att ställa ut identitetsintyg kan också granskas, godkännas och anslutas i enlighet med dessa redan etablerade granskningsrutiner och regler. Det gransknings- och tillståndsförfarande som följer av regelverket kring Kvalitetsmärket Svensk e-legitimation ska således tillämpas även för anslutning till den statliga identifieringstjänsten.

Dessa krav är högt ställda och relativt kostnadsdrivande. Förhållandet mellan dessa kostnader och de samlade intäkter det kan bli fråga om för att tillgodose marknadens behov av elektronisk identifiering med den statliga e-legitimationen kan antas begränsa det antal aktörer som vill verka på den svenska marknaden till en handfull sådana aktörer. Digg bedömer att det kan anses vara tillräckligt för att även inom privat sektor uppfylla

grundläggande behov av säkerhet, robusthet och tillförlitlighet i samhällskritisk infrastruktur.

6.3.2 Reglering i författning eller genom avtal

Digg föreslår att utfärdandet och tillhandahållandet av den statliga e-legitimationen ska regleras i författning, se även avsnitt 7.1. Vid utformningen av dessa regler har ledning hämtats i föreskrifter för pass och fysiska identitetshandlingar. Där är användningsfasen sparsamt reglerad. Detsamma gäller för de författningsförslag som lagts fram rörande elektronisk identifiering.

Utredningen om effektiv styrning av nationella digitala tjänster föreslog i sitt slutbetänkande en lag om statlig elektronisk identitetshandling där utfärdande av sådana handlingar reglerades[78]. Utredningen föreslog också, med sikte på användningsfasen, en lag och en förordning om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling. De föreslagna föreskrifterna skulle bland annat omfatta hur elektronisk identitetskontroll av en statlig elektronisk identitetshandling skulle utformas enligt tekniska specifikationer. Några regler om rättigheter och skyldigheter för leverantörer av identitetsintyg och förlitande aktörer föreslogs dock inte. Slutbetänkandet bereds i Regeringskansliet, men förslagen som utredningen lämnade har ännu inte föranlett några författningsändringar.

På liknande sätt föreslog 2017 års ID-kortsutredning i sitt slutbetänkande en reglering i lag och i förordning av bland annat statlig e-legitimation[79]. Vidare föreslog utredningen att regeringen eller den myndighet som regeringen bestämmer skulle få meddela föreskrifter om villkor för när och hur den statliga e-legitimationen skulle få användas. Utredningen lämnade inte några förslag gällande reglering av rättigheter och skyldigheter för leverantörer av identitetsintyg och förlitande aktörer. Utredningen bereds i Regeringskansliet och har i denna del ännu inte föranlett författningsändringar. Tjänster för elektronisk identitetskontroll och intygstjänster har istället reglerats genom avtal, se bland annat regleringen i Sweden Connect-avtalet[80] som fungerat väl och smidigt kunnat anpassas till de snabba förändringarna inom området.

Digg anser inte att det är ändamålsenligt att inom ramen för detta regeringsuppdrag lägga fram ytterligare förslag till författningsreglering av användningsfasen, särskilt inte vid beaktande av den korta tidsram som angetts som målsättning för att utveckla och ta funktioner för statlig e-legitimation i drift. Digg anser dock att det skulle behöva göras en

[78] SOU 2017:114.
[79] SOU 2019:14.
[80] https://www.digg.se/digitala-tjanster/e-legitimering#h2SwedenConnect

grundlig genomlysning över hur e-legitimationsområdet bör regleras. De avtal som Digg administrerar inom området kan dock utgöra en ändamålsenlig förebild i nuläget, i det fall en kort införandetid krävs.

7 Rättsliga analyser om utfärdandet av statlig e-legitimation

De rättsliga analyserna utgår till stora delar från det författningsförslag som Digg lämnar till regeringen i den här rapporten.

Digg lämnar i det följande förslag på hur förvaltningsuppgifterna mellan Digg och den identitetskontrollerande myndigheten lämpligen kan regleras. En utgångspunkt i föreslagen reglering av uppgifterna är att finna en rättslig modell för fördelning av uppgifter och ansvar som medför att det blir tydligt för respektive myndighet hur uppgiften ser ut, samt säkerställa att det inte finns delar som saknar en ansvarig eller behörig myndighet.

Digg analyserar i det följande vilka rollkonflikter som kan uppstå inom myndigheten i och med den nya roll som Digg enligt uppdraget får. Digg ger också förslag på hur risken för att rollkonflikter uppstår kan minskas.

Den statliga e-legitimationen förutsätter att personuppgifter behandlas hos Digg och den identitetskontrollerande myndigheten. Digg kommer att inte endast att behandla personuppgifter vid utfärdandet av den statliga e-legitimationen utan även vid användningen av densamma. Digg analyserar och bedömer vilka personuppgifter som behöver behandlas för att kunna ansvara för den statliga e-legitimationen. Digg ger en beskrivning av de personuppgiftsbehandlingar som sker inom respektive myndighets verksamhet med den statliga e-legitimationen. Det görs även en genomgång av på vilket sätt personuppgiftsbehandlingarna är förenliga dataskyddsregleringen samt om behov finns av eventuella författningsåtgärder.

7.1 En förordning om statlig e-legitimation

En förordning om statlig e-legitimation bör reglera hur ansökan och utfärdande av den statliga e-legitimationen går till, samt ge rättsliga förutsättningar för den personuppgiftsbehandling som behöver ske. Digg och den identitetskontrollerande myndigheten bör ges bemyndiganden att närmare föreskriva om den statliga e-legitimationen.

7.1.1 Legalitet

Digg föreslår att det genom författningsreglering ska föreskrivas att Digg ska utfärda och tillhandahålla statliga e-legitimationer.

Digg föreslår att även den identitetskontrollerande myndighetens uppgift att kontrollera sökandens identitet i samband med utfärdande ska författningsregleras.

Myndigheter får bara vidta åtgärder som har stöd i rättsordningen (legalitetsprincipen).[81] Legalitetsprincipen innebär att det ska finnas någon form av normmässig förankring för all typ av verksamhet som en myndighet bedriver. Sådan normmässig förankring finns vanligtvis i en myndighets instruktion, men kan också finnas i annan författnings-reglering eller komma till stånd genom ett förvaltningsbeslut, exempelvis om åtgärden har stöd i myndighetens regleringsbrev.[82]

Enligt aktuellt regeringsuppdrag föreslås Digg framöver ansvara för statlig e-legitimation. Detta ansvar föreslås innefatta både *utfärdande* av statliga e-legitimationer och kontroller vid *användningen* av dem. Dessa nya arbetsuppgifter omfattas inte idag av myndighetens instruktion och har heller inte annat stöd i rättsordningen. Diggs förslag är att sådant stöd ska ges genom reglering i en ny författning som närmare beskriver förutsättningarna för den statliga e-legitimationen.

Diggs förslag innebär dessutom att vissa förvaltningsuppgifter ska utföras av den identitetskontrollerande myndigheten. Dessa uppgifter är visserligen begränsade till att vid ett personligt besök fastställa den sökandes identitet och att kontrollera att de identitetshandlingar som åberopas är äkta, men resultatet blir av avgörande betydelse för möjligheten att få en statlig e-legitimation utfärdad. Även dessa förvaltningsuppgifter bör ges uttryckligt stöd.

[81] 5 § förvaltningslag (2017:900).
[82] Prop. 2016/17:180. *En modern och rättssäker förvaltning*, s. 58 och 289.

7.1.2 Normgivningsnivå och författningens namn

Digg föreslår att en författningsreglering av statlig e-legitimation sker i förordning. Förordningen bör benämnas förordning om statlig e-legitimation. I förordningen om statlig e-legitimation ska föreskrivas hur ansökan ska ske samt hur statlig e-legitimation ska utfärdas. Där delegeras också till Digg att meddela föreskrifter för denna hantering. Där delegeras också till den identitetskontrollerande att meddela föreskrifter om genomförande av kontroller i samband med identifiering av sökande.

Digg bedömer att föreskrifter om statlig e-legitimation inte bör föras in i författningar som reglerar fysiska identitetshandlingar.

Det blir av praktisk betydelse om de skyldigheter som följer med en ansökan om statlig e-legitimation kan regleras i förordning eller om de måste meddelas genom lag. En reglering i förordning framstår som ändamålsenlig vid beaktande av den snäva tidsram som har angetts som målsättning för att ta funktioner för statlig e-legitimation i drift.

Diggs bedömning är att det vid utfärdande och användning av en statlig e-legitimation inte förekommer några betydande intrång i den personliga integriteten som avses i 2 kap. 6 § andra stycket regeringsformen. Den statliga e-legitimationen och den anknytande hanteringen erbjuds som en ren serviceåtgärd. I övrigt gäller att föreskrifter ska meddelas genom lag bland annat om de avser skyldigheter för enskilda eller ingrepp i enskildas personliga eller ekonomiska förhållanden.[83] Regeringen får i övrigt meddela bland annat sådana föreskrifter som inte enligt grundlag ska meddelas av riksdagen.[84] Det innebär att gynnande eller neutrala föreskrifter kan meddelas av regeringen genom förordning.

Digg föreslår inte något krav på att ha en statlig e-legitimation eller att bruka en sådan. Medborgarna är inte heller beroende av en statlig e-legitimation för att styrka sin identitet eller skriva under handlingar digitalt. Det finns flera andra e-legitimationer att tillgå. Den som inte vill ansöka om statlig e-legitimation kan således låta bli utan det uppstår några särskilda konsekvenser. Regeringsformen kräver därmed inte en reglering i lag. Lagform krävs inte heller enligt Europakonventionen[85] eller av något annat skäl.[86] En författnings-reglering av statlig e-legitimation föreslås därmed i en ny förordning om statlig e-legitimation.

[83] 8 kap. 8 § första stycket 2 regeringsformen.
[84] Ibid.
[85] Europeiska konventionen om skydd för de mänskliga rättigheterna (EKMR).
[86] Motsvarande bedömning har gjorts vid införandet av det nationella identitetskortet se promemorian Ett nationellt identitetskort, Ju2003/00861/PO och Ds 2020:22 Ökad säkerhet för vissa identitets- och uppehållshandlingar s. 58.

Förordningen bör benämnas förordningen om statlig e-legitimation. Där bör föreskrifter ges om ansökan, villkor för utfärdande, aktivering, spärr och överklagbarhet. Där bör också föreskrivas om den identitetskontrollerande myndighetens uppdrag att utföra förvaltningsuppgifter vid identifiering av den sökande.

Regleringen av den statliga e-legitimationen behöver vara flexibel och inte alltför detaljstyrd. Därför föreslås ett bemyndigande för Digg att meddela föreskrifter om utfärdande av statlig e-legitimation. Vidare föreslås bemyndiganden för den identitetskontrollerande myndigheten att meddela föreskrifter om genomförande av kontroller i samband med identifiering av sökande. Detta förutsätter att den identitetskontrollerande myndigheten har den kompetens som krävs för att avgöra hur en tillförlitlig grundidentifiering sker.

Utredningen om effektiv styrning av nationella digitala tjänsters har föreslagit en reglering av statlig e-legitimation i andra författningar än dem som reglerar den fysiska identitetshandlingen[87] medan 2017 års ID-kortsutredning istället argumenterat för att fysiska och digitala identitetshandlingar ska regleras i samma författningar.[88]

Det förslag som Digg lägger fram här innebär att statlig e-legitimation utfärdas i annan ordning än fysiska identitetshandlingar. Den reglering som föreslås för statlig e-legitimation tar dessutom sikte på andra utfärdare än Digg och skiljer sig väsentligt från vad som gäller för de fysiska identitetshandlingarna. En statlig e-legitimation bör därmed regleras i den föreslagna förordningen om statlig e-legitimation.

7.1.3 Personuppgiftsbehandlingen regleras i förordning

Digg föreslår att ramarna för personuppgiftsbehandlingen bör slås fast i förordningen om statlig e-legitimation.

Det är vanligt att den personuppgiftsbehandling som utförs vid en viss myndighet eller inom ett visst område regleras genom registerförfattning, som innehåller bestämmelser som avviker från EU:s dataskyddsförordning. En särreglering av detta slag aktualiseras bland annat då det behövs ett förstärkt integritetsskydd eller att regelverket behöver anpassas till de särskilda förhållanden som råder inom den aktuella myndighetens verksamhet.

Den personuppgiftsbehandling som ska äga rum inom verksamheten med den statliga e-legitimationen kommer att, potentiellt sett, omfatta stora delar av Sveriges befolkning.

[87] SOU 2017:114.
[88] SOU 2019:14.

Känsliga personuppgifter kommer dock inte att behandlas. Uppgifter om lagöverträdelser kan visserligen bli aktuella men sådana uppgifter ska inte behandlas i det register som Digg föreslås föra över innehavare av statlig e-legitimation. Enligt Diggs mening behövs dock ett förstärkt integritetsskydd för dessa personuppgiftsbehandlingar. Ramarna för dem bör därför slås fast i förordningen om statlig e-legitimation.

7.1.4 Reglering av myndighetsuppgifter

Digg föreslår att myndigheternas respektive uppgifter ska regleras i förordning. Digg bedömer att det kan krävas någon form av förvaltningsgemensam överenskommelse mellan myndigheterna avseende de praktiska aspekterna av utfärdandet.

7.1.4.1 Myndigheternas uppgifter ska författningsregleras

Digg har i avsnitt 5.2 om utgivningsprocessen beskrivit hur utgivningsprocessen avseende den statliga e-legitimationen ska gå till. Frågan är hur myndigheternas, det vill säga Diggs och den identitetskontrollerade myndighetens, förvaltningsuppgifter ska regleras.

Myndigheter under regeringen styrs av regeringen genom förordningar, främst myndighetsförordningen (2007:515) och den förordning med instruktion som finns för varje myndighet, samt genom regleringsbrev och andra individuella regeringsbeslut. Därutöver styrs myndigheters handlande av de lagar och andra författningar som reglerar den verksamhet som myndigheten ansvarar för. Principiellt och i huvudsak fördelas alltså arbetsuppgifter och dras gränser mellan myndigheternas ansvarsområden på detta vis.[89] En utgångspunkt i regleringen av myndigheternas uppgifter är att *ansvars- och rollfördelningen* mellan berörda myndigheter ska vara tydlig.

Digg har studerat olika rättsliga konstruktioner för myndigheternas olika roller och fördelning av uppgifter. En modell som har studerats är den som gäller mellan Migrationsverket och utlandsmyndigheterna i fråga om migrationsärenden vid utlandsmyndigheterna.[90] En sådan konstruktion bygger i huvudsak på att Migrationsverket har huvudansvaret för migrationsärendena vid utlandsmyndigheterna. De närmre förutsättningarna för samarbetet framgår i sin tur av en förvaltningsöverenskommelse mellan myndigheterna.

Digg har övervägt att införa denna konstruktion för ansvarsfördelningen mellan myndigheter vid utfärdande av statlig e-legitimation. En närmare genomlysning har gett

[89] SOU 2017:14. Utredningen om ansvar för migrationsverksamheten vid utlandsmyndigheterna. *Migrationsärenden vid utlandsmyndigheterna: slutbetänkande*, s. 164 f.
[90] SOU 2017:14.

vid handen att myndigheternas ansvar i huvudsak bör regleras direkt i författning. En reglering i författning skapar tydliga ramar för myndigheternas uppgifter och bidrar till en hållbar och förutsägbar reglering över tid. I den föreslagna förordningen om statlig e-legitimation bör därför föreskrivas att identitetskontrollerande myndighet ska kontrollera att sökandes identitet är styrkt, det vill säga ansvara för grundidentifieringen.

Beträffande de praktiska aspekterna kring utfärdandet och samarbetet i övrigt får det antas att det kommer att behövas någon form av överenskommelse mellan myndigheterna.

7.1.4.2 Samverkan mellan myndigheterna

Även om det i författning pekas ut vilka förvaltningsuppgifter som åligger respektive myndighet kommer det att kvarstå frågor i gränslandet mellan berörda myndigheters ansvar och frågor som i övrigt rör samarbetet mellan dessa myndigheter. Detta gäller i synnerhet för de uppgifter som identitetskontrollerande myndighet ska utföra för Diggs räkning, såsom att upprätta en ansökan i Diggs system och att tillhandahålla e-legitimation till en sökande. Sådana frågor kan behöva regleras utan regeringens direkta inflytande.

I 8 § förvaltningslagen föreskrivs att en myndighet inom sitt verksamhetsområde ska samverka med andra myndigheter och i rimlig utsträckning hjälpa den enskilde genom att själv inhämta upplysningar eller yttranden från andra myndigheter. I myndighets-förordningen[91] riktas även en generell uppmaning till myndigheterna att ta till vara de fördelar som kan vinnas med samarbete. Samarbeten och överenskommelser mellan myndigheter behöver, om det avhandlade är av någon omfattning, ges en ordnad skriftlig form. En beteckning som har kommit att användas på sådana texter är ”förvaltnings-överenskommelse”. Texterna är utformade som avtal, fast mellan aktörer som är delar av staten och alltså inte självständiga rättssubjekt som kan ingå juridiskt bindande avtal med varandra.[92]

Digg ser att behovet av samverkan mellan identitetskontrollerande myndighet och Digg inom området för statlig e-legitimation blir betydande och att myndigheterna kommer att behöva reglera formerna för samverkan i någon form av överenskommelse. En sådan kan till exempel avse detaljer kring ansvarsfördelningen eller praktiska frågor om användningen av it-stöd och säkerhetsfunktioner.

[91] 6 § andra stycket myndighetsförordningen (2007:515).
[92] SOU 2017:14.

7.2 Rollkonflikter

Diggs nya roll som ansvarig för den statliga e-legitimation innebär att rollkonflikter inom myndigheten riskerar att uppstå. Det behöver vidtas organisatoriska åtgärder för att minska dessa risker.

7.2.1 Vad innebär rollkonflikter?

Det framgår av uppdraget att Digg ska analysera eventuella risker för rollkonflikter inom Digg eller andra myndigheter. Digg har inte identifierat några rollkonflikter inom andra myndigheter. I det här avsnittet beskrivs innebörden av begreppet rollkonflikt samt risken för rollkonflikter inom Digg och förslag på hur risken för rollkonflikter kan begränsas.

Det är inte ovanligt att en myndighet utför flera olika uppgifter och ikläder sig olika roller. Som exempel kan nämnas att en myndighet kan agera främjande, normerande, tillståndsgivande eller utföra någon form av tillsyn. Det finns inget generellt förbud mot att en myndighet har olika uppgifter. Vissa uppgifter kan dock vara svåra att förena eftersom det finns risk för rollkonflikter där de olika rollerna på något vis kan rubba förtroendet för att myndigheten utför uppgiften opartiskt.

7.2.2 Diggs uppgifter på e-legitimationsområdet idag

Idag har Digg har ett antal olika uppgifter på e-legitimationsområdet, dessa framgår i huvudsak av myndighetens instruktion.[93] Detta är en kort översikt över hur myndighetens uppgifter på området ser ut:

- Digg ska samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig
- Digg ska ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift
- Digg ska främja användningen av elektronisk identifiering och underskrift
- Digg ska ansvara för noderna i enlighet med eIDAS-förordningen samt att driva Sveriges eIDAS-nod (Sweden Connect)
- Vidare ska myndigheten bedriva arbetet med digitalisering av den offentliga förvaltning på ett sätt som säkerställer skyddet av säkerhetskänslig verksamhet och informationssäkerhet i övrigt samt skyddet av den personliga integriteten.

[93] Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning.

Digg ska dessutom administrera och tillhandahålla valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering (eLOV). I 1 § andra stycket föreskrivs att lagen gäller när en upphandlande myndighet har

- beslutat att tillämpa valfrihetssystem i fråga om tjänster för elektronisk identifiering av enskilda i myndighetens elektroniska tjänster,
- anslutit sig till ett system för säker elektronisk identifiering som tillhandahålls av den myndighet som regeringen bestämmer, och
- uppdragit åt den myndighet som avses i 2 att i den upphandlande myndighetens namn administrera valfrihetssystemet enligt 3 – 14 §§, föra dess talan i samband med mål om rättelse enligt 16 § och i förekommande fall vidta rättelse enligt 17.

7.2.3 Objektivitetsprincipen

Objektivitetsprincipen kommer till uttryck i regeringsformen där det föreskrivs att en myndighet ska iaktta saklighet och opartiskhet.[94] Principen innebär att myndigheterna är skyldiga att agera sakligt och opartiskt i alla lägen. Den kan också tolkas som ett förbud mot att myndigheterna ser till andra intressen än de som ska tillgodoses. Ytterst syftar principen till att upprätthålla allmänhetens förtroende för myndigheten.

Begreppen saklig och opartisk kan ibland uppfattas som synonyma, men begreppen tar sikte på olika aspekter av objektiviteten. Opartiskheten tar sikte på hur något uppfattas utifrån. Sakligheten handlar om att begränsa vad ett beslut kan grundas på, om likabehandling och om att myndigheten ska hålla sig till sina uppdrag.

Vidare finns det en objektiv och en subjektiv sida av principen. Med den subjektiva sidan menas hur myndigheten själv anser sig ha agerat medan den objektiva sidan avser hur myndighetens agerande kan uppfattas utifrån. Risken för att andra kan uppfatta att saklighet och opartiskhet inte iakttas är tillräcklig för att agerandet skulle kunna anses strida mot objektivitetsprincipen.

7.2.4 Jävsreglerna i förvaltningslagen

För att få en större förståelse för innebörden av objektivitetsprincipen kan det vara värt att söka ledning i de principer som kommer till uttryck i förvaltningslagens bestämmelser om jäv.[95]

[94] 1 kap. 9 § regeringsformen, se även 5 § andra stycket förvaltningslagen.
[95] 16 § förvaltningslagen.

Syftet med jävsreglerna är att myndigheter ska agera sakligt och opartiskt samt att allmänheten ska ha förtroende för myndigheternas arbete. Reglerna om jäv pekar ut vissa situationer där det allmänt sett finns en risk för att en anställd tar hänsyn till annat än reglerna och de sakliga omständigheterna i det enskilda fallet.

Förvaltningslagens regler om jäv gäller den som ska handlägga ett ärende. Reglerna gäller också självfallet för beslutsfattare. Om en konsult deltar i handläggningen av ett ärende vid en myndighet omfattas han eller hon av förvaltningslagens jävsbestämmelser på samma sätt som anställda vid myndigheten förutsatt att denne har en formell ställning som handläggare eller beslutsfattare.

Kraven för att jäv ska anses föreligga är låga. Det är tillräckligt att en person kan antas, i en inte oväsentlig utsträckning, påverkas av utgången i ett ärendeför att jäv anses föreligga.

7.2.5 Rollkonflikter kan uppstå inom Digg

Diggs bedömning är att rollkonflikter riskerar att uppstå på flera ställen inom myndigheten i och med Diggs nya roll som utfärdare och tillhandahållare av den statliga e-legitimationen.

Digg beslutar idag vilka krav som ska uppfyllas för att en e-legitimationsutfärdare ska få inga i valfrihetssystemet, fattar beslut om att godkänna e-legitimationsutfärdare i enlighet med kraven och ingår avtal med en godkänd e-legitimationsutfärdare.[96] I avsnitt 6.2 föreslås att den statliga e-legitimationen ska upphandlas genom valfrihetssystemet. Risken för en rollkonflikt inom Digg blir här tydlig. När Digg ansöker om att den statliga e-legitimationen ska få ingå i ett valfrihetssystem kommer myndigheten att pröva sig själv mot krav som myndigheten själv har satt upp, samt fatta beslut som rör den egna verksamheten. Det finns också en risk att det för utomstående kan väckas tvivel kring huruvida Digg lever upp till de krav som ställs för att ingå i ett valfrihetssystem.

Digg genomför idag granskningar och godkänner Svensk e-legitimation utifrån Tillitsramverket för Svensk e-legitimation. Digg skulle därmed granska och godkänna sig själv utifrån samtliga uppställda krav i avtal och tillhörande tillitsramverk (och tekniska ramverk). Här finns det alltså en risk att myndigheten kommer att granska sig själv mot krav som myndigheten själv har satt upp.

Ytterligare en fråga kopplad till rollkonflikter är att privata e-legitimationsutfärdare vid granskning och revision förväntas tillgängliggöra sådan information till Digg som kan

[96] 4, 12 och 14 §§ lag (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering.

anses vara affärshemligheter eller till någon del ha bäring på utfärdarnas affär eller vara sådan information som skyddas av immateriella rättigheter. Det kan visa sig olämpligt att Digg i rollen som utfärdare av statlig e-legitimation får del av kunskap och information som myndigheten kan ha nytta av och begagna för statlig e-legitimation.

7.2.6 Risken för rollkonflikter bör undvikas

Digg har inom ramen för uppdraget övervägt olika lösningar för att minska risken för rollkonflikter inom myndigheten. Det bör i vart fall krävas att myndigheten organisatoriskt skiljer på rollen som utfärdare av e-legitimationen från övriga uppgifter inom e-legitimationsområdet för att säkerställa att myndigheten lever upp till de krav som ställs på myndighetens verksamhet, framförallt vad gäller objektivitet, likabehandling och för att undvika en jävsproblematik.

Den del av Diggs verksamhet som innebär att Digg utfärdar och tillhandahåller den statliga e-legitimationen bör tillhöra en organisatorisk enhet som inte är samma organisatoriska enhet som ansvarar för infrastrukturen och tillhandahållande av valfrihetssystem. Digg behöver även tydliggöra hur beslutsförfarandet ska se ut samt när myndigheten agerar i de olika rollerna som infrastrukturansvarig, tillhandahållande myndighet av valfrihetssystem eller utfärdare av e-legitimationen.

Genom att skilja verksamheten åt anser Digg att det är möjligt att undvika de konflikter som annars riskerar att uppstå när Digg agerar i olika roller samtidigt. Vidare möjliggör en sådan uppdelning att intäkter och kostnader kopplade till den statliga e-legitimationen kan skiljas från övrig verksamhet. Det blir också tydligt vilka resurser som avsätts för den statliga e-legitimationen och att korssubventionering inte sker från andra verksamhets-grenar som kan skapa en otillbörlig fördel för den statliga e-legitimationen.

Det bör även eftersträvas att den organisatoriska uppdelningen får till följd att de olika verksamhetsgrenarna anses vara separerade i offentlighet- och sekretesslagens mening.[97] På så sätt kan myndigheten förhindra att sekretessbelagd information når en annan verksamhetsgren.

Det bör ankomma på Digg att bestämma de närmare formerna för hur myndigheten ska organiseras för att minska risken för rollkonflikter. Som exempel kan dock tjäna hur Försvarets materielverk har organiserats för att upprätthålla det krav på oberoende som följer av EU:s cybersäkerhetsakt.[98]

[97] Se 8 kap. 2 § offentlighets- och sekretesslag (2009:400).
[98] Se förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

7.3 Dataskydd

Det kommer att hanteras omfattande mängder personuppgifter inom verksamheten med den statliga e-legitimationen. De personuppgiftsbehandlingar som sker ska vara förenliga med det dataskyddsrättsliga regelverket.

7.3.1 Inledning

Den statliga e-legitimationen förutsätter att personuppgifter behandlas hos både den identitetskontrollerande myndigheten samt hos Digg. Digg kommer att inte endast att behandla personuppgifter vid *utfärdandet* av den statliga e-legitimationen utan även vid *användningen* av densamma. Det är fråga om omfattande mängder personuppgifter som kommer att behandlas eftersom att potentiellt sett hela Sveriges befolkning på sikt skulle kunna inneha en statlig e-legitimation. Den identitetskontrollerande myndigheten kommer att behandla personuppgifter vid grundidentifieringen samt vid utförandet av vissa andra förvaltningsuppgifter för Diggs räkning.

I uppdragsbeskrivningen anges att Digg ska *analysera* och *bedöma* vilka personuppgifter som behöver behandlas för att kunna ansvara för den statliga e-legitimationen. De förslag som lämnas ska vidare vara förenliga med dataskyddsregleringen. I denna del ges därför en beskrivning av de personuppgiftsbehandlingar som sker för att respektive myndighet ska kunna utföra sina uppgifter inom verksamheten med den statliga e-legitimationen. Det görs även en genomgång av på vilket sätt personuppgiftsbehandlingarna är förenliga dataskyddsregleringen. För det fall det krävs redogörs även för vilka eventuella författningsåtgärder som är nödvändiga för att personuppgiftsbehandlingen ska vara förenlig med gällande rätt. Som framgått i avsnitt 7.1.3 bör ramarna för personuppgifts-behandlingen framgå av den föreslagna förordningen om statlig e-legitimation.

7.3.2 EU:s dataskyddsförordning och dataskyddslagen

EU:s dataskyddsförordning[99] (hädanefter kallad dataskyddsförordningen) är i alla delar bindande och direkt tillämplig i samtliga EU:s medlemsländer. Dataskyddsförordningen kompletteras i Sverige av bland annat lagen (2018:218) med kompletterande bestämmelser till dataskyddsförordningen (dataskyddslagen) och förordningen (2018:219) med kompletterande bestämmelser till dataskyddsförordningen. Dessa författningar är av generell karaktär och reglerar bland annat frågor om rättslig grund för behandling av personuppgifter och känsliga personuppgifter. Dataskyddslagen är subsidiär i förhållande

[99] Europaparlamentets och rådet förordning (EU) 2016/679 av den 17 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning).

till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i registerförfattningar.

Dataskyddsförordningen är tillämplig på sådan behandling av personuppgifter som helt eller delvis sker på automatisk väg och på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register (artikel 2.1). Med personuppgifter avses enligt artikel 4 i förordningen varje upplysning som avser en identifierad eller identifierbar fysisk person. Med behandling avses enligt artikel 4.2 en åtgärd eller kombination av åtgärder avseende personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstörning.

Utöver det grundläggande kravet på att all behandling måste vara laglig, i betydelsen att någon av de rättsliga grunder som anges i artikel 6.1 ska vara tillämplig, omgärdas varje behandling av personuppgifter också av andra krav. Principerna för behandling av personuppgifter, det vill säga vilka allmänna krav som gäller för all personuppgifts-behandling, anges i artikel 5.1. Bland annat uppställs krav på att uppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

7.3.3 Personuppgiftsbehandling hos den identitetskontrollerande myndigheten

Digg bedömer att den identitetskontrollerande myndigheten är personuppgiftsansvarig för den personuppgiftsbehandling som sker i samband med grundidentifieringen.

Digg bedömer vidare att den identitetskontrollerande myndigheten är personuppgiftsbiträde åt Digg för den personuppgiftsbehandling som i övrigt sker för Diggs räkning vid utfärdandet av den statliga e-legitimationen.

7.3.3.1 Personuppgiftsbehandling vid utfärdande av e-legitimationen

Vid grundidentifiering av sökanden behandlar den identitetskontrollerande myndigheten personuppgifter om sökanden som finns i de handlingar som krävs för identifiering av sökanden, exempelvis i pass. Den identitetskontrollerande myndigheten behöver då ha tillgång till och ha möjlighet att göra kontroller i vissa register som krävs för att kontrollera att sökandens identitet är styrkt.

Vid grundidentifieringen torde den identitetskontrollerande myndigheten behandla känsliga personuppgifter i form av ras eller etniskt ursprung. I förarbetena till

genomförandet av tredje penningtvättsdirektivet[100] uttalade regeringen bland annat att passhandlingar innehåller bild som i förening med namn och uppgift om medborgarskap kan avslöja såväl ras som etniskt ursprung. Regeringen har i förarbetena till vissa ändringar i arbetsmiljölagen[101] bedömt att en isolerad uppgift om medborgarskap varken avslöjar ras eller etniskt ursprung. Vid grundidentifiering behandlas oundvikligen uppgifter om sökandens namn, person- eller samordningsnummer, födelseort och medborgarskap av den identitetskontrollerande myndigheten. Dessutom innehåller pass och nationella id-kort ansiktsbilder på sökanden. Digg gör därför bedömningen att den identitetskontrollerande myndigheten vid grundidentifiering av sökanden behandlar uppgifter som kan avslöja en persons ras eller etniskt ursprung. Den identitets-kontrollerande myndigheten behöver ha rättslig grund enligt artikel 9 i dataskydds-förordningen för att behandla känsliga personuppgifter för att genomföra grundidenti-fieringen.

Även vid ansökan och tillhandahållandet av den statliga e-legitimationen behandlar den identitetskontrollerande myndigheten a personuppgifter om sökanden. För att inleda ett ärende om statlig e-legitimation hos Digg behöver den sökande ansöka om en statlig e-legitimation. Ansökan görs på plats hos den identitetskontrollerande myndigheten men registreras hos Digg. Detta görs genom att den identitetskontrollerande myndigheten, i samband med grundidentifieringen, elektroniskt överför sökandes person- eller samordningsnummer till Digg i form av en fråga/svar-tjänst, se vidare avsnitt 7.3.4.12.

Utformningen av en fråga/svar-tjänst på det sätt Digg föreslår förutsätter att den identitetskontrollerande myndigheten har stöd i författning för att lämna ut personuppgifter elektroniskt till Digg.

Den identitetskontrollerande myndighetens behandling av person- eller samordnings-nummer anses motiverad med anledning av vikten av en säker identifiering som är nödvändig vid utfärdande av en statlig e-legitimation (3 kap. 10 § dataskyddslagen).

7.3.3.2 Personuppgiftsansvar

Den identitetskontrollerande myndigheten behandlar personuppgifter vid grundidenti-fieringen, ansökan samt tillhandahållandet av den statliga e-legitimationen. Enligt Diggs förslag är det den identitetskontrollerande myndigheten som bestämmer hur en godtagbar grundidentifiering sker genom att utfärda föreskrifter på området.

---

[100] Prop. 2008/09:70. *Genomförande av tredje penningtvättsdirektivet*, s. 142

[101] Prop. 2001/02:144. *Lag om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten*, s. 41

Den identitetskontrollerande myndigheten är därmed personuppgiftsansvarig för den personuppgiftsbehandling som sker i samband med grundidentifieringen. För tydlighetens skull anser Digg att deras personuppgiftsansvar ska framgå av den föreslagna förordningen om statlig e-legitimation.

Den identitetskontrollerande myndigheten agerar vid ansökan och tillhandahållandet av den statliga e-legitimationen helt på instruktion av Digg och har ingen bestämmanderätt över ändamål och medel vid personuppgiftsbehandlingen. Det är enbart Digg som bestämmer för vilka syften personuppgifterna får behandlas och på vilket sätt. Den identitetskontrollerande myndigheten behandlar vid ansökan och tillhandahållandet personuppgifter för Diggs räkning och ska således betraktas som personuppgiftsbiträden åt Digg i denna del.

Av artikel 28.2 dataskyddsförordningen framgår att när personuppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras antingen genom avtal eller genom annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet. Digg anser att det bör finnas en möjlighet för Digg att reglera villkoren för personuppgiftsbiträdets behandling av personuppgifter genom en rättsakt. Förslagsvis kan regleringen ske genom att Digg ges föreskriftsrätt. En jämförelse kan göras med Lantmäteriets föreskriftsrätt vad gäller personuppgiftsbiträdens behandling av personuppgifter i fastighetsregistret.[102]

7.3.3.3 Rättslig grund

För att behandla personuppgifter krävs en rättslig grund enligt artikel 6.1 dataskyddsförordningen. Den verksamhet som en statlig myndighet bedriver inom ramen för sin befogenhet är av allmänt intresse och det är vanligen den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen som bör tillämpas av myndigheter.[103] För att behandling av personuppgifter ska vara laglig enligt artikel 6.1 e i dataskyddsförordningen måste den uppgift som den personuppgiftsansvarige utför dels vara av allmänt intresse eller utgöra ett led i myndighetsutövning, dels vara fastställd i enlighet med unionsrätten eller den nationella rätten. Vidare måste behandlingen vara nödvändig för ett ändamål som är nödvändigt för att utföra uppgiften.

Digg har föreslagit att den identitetskontrollerande myndighetens uppgift att kontrollera att sökandes identitet är styrkt ska slås fast i förordningen om statlig e-legitimation. Det innebär att den identitetskontrollerande myndigheten kommer att ha stöd i nationell rätt

[102] 83 § förordningen (2000:308) om fastighetsregister.
[103] Prop. 2017/18:105. *Ny dataskyddslag*, s. 56

för att grunda den personuppgiftsbehandling som äger rum vid grundidentifieringen på allmänt intresse enligt artikel 6.1 e dataskyddsförordningen. Den behandling av personuppgifter som sker är nödvändig för att myndigheten ska kunna genomföra grundidentifieringen.

Denna behandling får därför anses nödvändig för att utföra en uppgift av allmänt intresse enligt artikel 6.1 e dataskyddsförordningen.

7.3.4 Personuppgiftsbehandling hos Digg

Digg bedömer att Digg är personuppgiftsansvarig för den personuppgiftsbehandling som sker i samband med utfärdandet och användningen av den statliga e-legitimationen.

7.3.4.1 Personuppgiftsbehandling vid utfärdande av e-legitimationen

Diggs föreslagna utgivningsprocess beskrivs närmre i avsnitt 5.2. Vid ansökan om den statliga e-legitimationen behöver Digg behandla sökandes personuppgifter såsom person- eller samordningsnummer, namn och i vissa fall adress. Innehavaren ska även frivilligt kunna registrera en elektronisk kontaktväg, e-post och/eller mobiltelefonnummer. Efter att en ansökan har registrerats av den identitetskontrollerande myndigheten i Diggs system handläggs automatiserat en ansökan hos Digg. När Digg automatiserat behandlar ansökan sker erforderliga kontroller gentemot bland annat folkbokföringsdatabasen och därefter fattas beslut avseende utfärdandet. Om Digg bifaller ansökan ser handläggaren vid den identitetskontrollerande myndigheten detta inom någon sekund och överlämnar ett kortämne med chip. Om Digg avslår ansökan ser handläggaren vid den identitets-kontrollerande myndigheten detta inom någon sekund och överlämnar en utskrift av avslagsbeslutet tillsammans med information om hur beslutet kan överklagas.

Sökanden som har tilldelats kortet med e-legitimationen måste aktivera det för att det ska vara brukbart. När sökande aktiverar sin e-legitimation med pass eller nationellt id-kort kommer MRZ-koden[104], vilket är en personuppgift, i passet eller det nationella id-kortet att läsas av. Det kommer inte att behandlas några biometriska eller andra känsliga personuppgifter vid avläsning av identitetshandlingen.

I sin roll som utfärdare av den statliga e-legitimationen kommer det krävas att Digg för ett register över innehavare av den statliga e-legitimationen. Digg kommer även i sina system att, via direktåtkomst, ha tillgång till Skatteverkets system för distribution av folkbok-

[104] Machine readable zone

föringsuppgifter; Navet.[105] Automatiska kontroller kommer att ske mot Navet via Diggs system. På så sätt säkerställer Digg att uppgifter om innehavaren är uppdaterade och korrekta.

7.3.4.2 Personuppgiftsbehandling vid användning av e-legitimationen

Det har beskrivits vilka personuppgiftsbehandlingar och vilka samlingar av personuppgifter som krävs för att Digg ska kunna utfärda statlig e-legitimation. Digg behöver också behandla personuppgifter vid användningen av den statliga e-legitimationen. Användningen av den statliga e-legitimationen består dels i att bruka den, dels i att kontrollera om användning e-legitimation är giltig och vem som har brukat den för att sedan besvara fråga om en användares identitet kan verifieras, dels i att ställa ut ett identitetsintyg. Digg föreslår en statlig förlitandetjänst och en statlig identifierings-tjänst där behandlingar av personuppgifter behöver äga rum, se avsnitt 6.1.

Innehavaren av en statlig e-legitimation (användaren) besöker en tjänst hos en offentlig förlitande part och väljer där statlig e-legitimation för identifieringen. Den förlitande parten skickar som en följd därav en begäran om identitetsintyg till den statliga förlitande-tjänsten och styr användaren till den funktion som Digg tillhandahåller åt användaren för att bruka sin e-legitimation. Där aktiverar användaren e-legitimationen genom att ange sin personliga kod. Digg genomför därefter automatiserade kontroller i flera led (elektronisk identitetskontroll), bland annat kontroll av att e-legitimationen inte är spärrad och att dess giltighetstid inte gått ut, samt en verifiering på kryptografisk väg som visar att användaren känner till sin personliga kod. Visar kontrollerna att e-legitimationen är giltig och att det inte finns indikationer på någon felaktighet ställer Digg ut ett identitetsintyg till förlitande part. Identitetsintyget innehåller de uppgifter som den förlitande aktören behöver för att kunna lita på att användaren är den som han eller hon utger sig för att vara.

Om det i efterhand uppstår någon tvekan om ett levererat identitetsintyg är korrekt ska Digg, i skälig utsträckning, tillhandahålla de ytterligare uppgifter som behövs i samband med att riktigheten av en identifiering ifrågasätts. Här blir det fråga om manuella förfaranden, eventuellt som förberedelse för en rättslig prövning, där åtgärdernas förenlighet med avtal och gällande rätt får bedömas i varje enskilt fall.

Förlitande part får använda mottaget identitetsintyg för att hantera frågor om identitet i anslutning till förlitande parts tjänst samt, för att under viss kortare tid därefter, identifiera användaren med avseende på annan tjänst som tillhandahålls av den förlitande

[105] 2 kap. 8 § lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet

parten. Användningen av identitetsintyget ska ske i enlighet med gällande lagar, andra författningar och myndighetsbeslut.

7.3.4.3 Personuppgiftsbehandling vid spärr av e-legitimationen

Digg föreslår att e-legitimationen ska kunna spärras vid ett antal olika omständigheter. Dessa omständigheter beskrivs närmare i förslaget till förordning om statlig e-legitimation.

För att Digg ska kunna veta om någon uppgift som är väsentlig och inte längre föreligger behöver myndigheten behandla sådana uppgifter som myndigheten har tillgång till enligt Skatteverkets folkbokföringsdatabas Navet. På så sätt kan Digg upptäcka en felaktig uppgift såsom att innehavaren har bytt namn eller avlidit.

För att Digg ska kunna veta om någon annan än den som ska förfoga över e-legitimationen eller om kontrollen över e-legitimationen är förlorad kan uppgifter om den som missbrukar en e-legitimation behöva behandlas. Detta kan avse namn, personnummer och kontaktuppgifter. Digg kan även i övrigt behöva ha kunskap om på vilket sätt e-legitimationerna eventuellt missbrukas eller om det finns fog för att anta att sådant missbruk kan komma att ske. I sådana fall kan Digg behöva behandla uppgifter om lagöverträdelser. Digg behöver inte behandla uppgifter om lagöverträdelser i registret över innehavare av statliga e-legitimationer.

För att kunna spärra en e-legitimation när en person avlider behöver Digg ha tillgång till och behandla uppgifter om att en person har avlidit. Sådana uppgifter får Digg tillgång till via Skatteverkets folkbokföringsdatabas Navet.

7.3.4.4 Personuppgiftsansvar

En personuppgiftsansvarig är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.[106]

Digg föreslås vara personuppgiftsansvarig för behandling av personuppgifter i sin roll som utfärdare och tillhandahållare av den statliga e-legitimationen. Även personuppgiftsansvaret för de behandlingar som Digg utför i samband med den elektroniska identitetskontrollen får anses vila på Digg. Detsamma gäller för de behandlingar som Digg utför i samband med utfärdandet av ett identitetsintyg. Digg bedömer att det av den föreslagna förordningen om en statlig e-legitimation bör framgå

[106] Artikel 4.7 EU:s dataskyddsförordning.

att Digg är personuppgiftsansvarig för behandling av personuppgifter i sin roll som ansvarig för den statliga e-legitimationen. Genom en bestämmelse som pekar ut personuppgiftsansvaret blir det tydligt att den myndighet som registerförfattningen avser är personuppgiftsansvarig.

7.3.4.5 Rättslig grund

För att behandla personuppgifter krävs en rättslig grund enligt artikel 6.1 dataskydds-förordningen. Den verksamhet som en statlig myndighet bedriver inom ramen för sin befogenhet är av allmänt intresse och det är vanligen den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen som bör tillämpas av myndigheter.[107] För att behandling av personuppgifter ska vara laglig enligt artikel 6.1 e i dataskyddsförordningen måste den uppgift som den personuppgiftsansvarige utför dels vara av allmänt intresse eller utgöra ett led i myndighetsutövning, dels vara fastställd i enlighet med unionsrätten eller den nationella rätten. Vidare måste behandlingen vara nödvändig för ett ändamål som är nödvändigt för att utföra uppgiften.

Diggs ansvar för den statliga e-legitimationen innebär inte enbart att Digg kommer att behandla personuppgifter vid *utfärdandet* av den statliga e-legitimationen utan även vid *användningen*. Det föreslås att Digg ges uttryckligt rättsligt stöd för sin roll som *utfärdare* och *tillhandahållare* av den statliga e-legitimation i förordningen om en statlig e-legitimation. Förutsatt att sådan författningsåtgärd vidtas kommer Digg att ha stöd i nationell rätt för att grunda den personuppgiftsbehandling som äger rum i myndighetens verksamhet med den statliga e-legitimationen på allmänt intresse enligt artikel 6.1 e dataskyddsförordningen. Den behandling av personuppgifter som sker är nödvändig för att Digg ska kunna uppfylla sina uppgifter som ansvarig för den statliga e-legitimationen. Denna behandling får därför anses nödvändig för att utföra en uppgift av allmänt intresse enligt artikel 6.1 e dataskyddsförordningen.

Grunden för behandlingen kommer enligt Diggs förslag att vara fastställd i författning på det sätt som krävs med hänsyn till artikel 6.3 i dataskyddsförordningen. Även kravet på proportionalitet, liksom övriga villkor enligt artikel 6.3 i dataskyddsförordningen bedöms vara uppfyllda. Vid behandlingen måste även övriga bestämmelser i EU:s dataskydds-förordning och dataskyddslagen tillämpas. Hänsyn måste exempelvis tas till de allmänna principerna i artikel 5, regleringen avseende den registrerades rättigheter och bestämmelserna om säkerhet för personuppgifter.

[107] Prop. 2017/18:105 s. 56.

7.3.4.6 Ändamål

Personuppgifter ska enligt artikel 5.1 b i dataskyddsförordningen samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifterna får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Det sistnämnda kallas för finalitetsprincipen. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska dock enligt samma bestämmelse inte anses vara oförenlig med de ursprungliga ändamålen.

Digg kommer att behandla personuppgifter i sin roll som utfärdande myndighet. Dels kommer Digg att behandla personuppgifter för ändamål vid utfärdandet av den statliga e-legitimationen, dels för ändamål vid användningen av den statliga e-legitimationen. Det kan även tänka sig att Digg behöver behandla personuppgifter för ytterligare ändamål inom ramen för sin verksamhet med den statliga e-legitimationen, såsom vid användar-support eller vid loggning och logguppföljning.

Det är svårt att i detalj förutse exakt för vilka specifika ändamål myndigheten kommer att behöva behandla personuppgifter för. Digg bedömer att det därför inte är ändamålsenligt att i den föreslagna förordningen om en statlig e-legitimation formulera specifika ändamål för vilka Digg ska få behandla personuppgifter i sin verksamhet med den statliga e-legitimationen. Av dataskyddsförordningen grundläggande principer följer redan att Digg i sin roll som personuppgiftsansvarig skyldig att själv i förväg specificera ändamålen med behandlingen.[108] Av den föreslagna förordningen ska det därför inte i detalj framgå för vilka specifika ändamål uppgifter får behandlas. Ändamålsregleringen bör istället ges en mer generell utformning. Digg föreslår att personuppgifter får behandlas om det är nödvändigt för att Digg ska kunna utföra sina uppgifter i verksamheten med den statliga e-legitimationen.

7.3.4.7 Rätten att göra invändningar

Rätten att göra invändningar regleras i artikel 21 i dataskyddsförordningen. Som anges ovan behandlas personuppgifterna hos Digg på den grunden att det är nödvändigt för att utföra en uppgift av allmänt intresse enligt artikel 6.1 e i dataskyddsförordningen. Rätten att göra invändningar enligt artikel 21.1 gäller vid sådan behandling. Begränsningar i rätten att göra invändningar får dock göras under de förutsättningar som anges i artikel 23.

[108] Prop. 2019/20:106. *Stärkt integritet i Rättsmedicinalverkets verksamhet*, s. 39.

I det lagstiftningsärende[109] där bland annat lagstiftningen beträffande id-kort för folkbokförda i Sverige sågs över med anledning av dataskyddsförordningen anförde regeringen att det är av stor betydelse att personuppgifter får behandlas oberoende av den registrerades inställning i de aktuella verksamheterna. Regeringen ansåg då att lagstiftningen uppfyllde de krav på bland annat skyddsåtgärder som uppställs i artikel 23.2 i dataskyddsförordningen.[110] Digg ser ingen anledning att göra någon annan bedömning beträffande den statliga e-legitimationen. Det ska därför införas en bestämmelse som anger att rätten att göra invändningar inte gäller vid sådan behandling som är tillåten enligt den föreslagna förordningen eller föreskrifter som har meddelats i anslutning till förordningen.

7.3.4.8 Register över innehavare av e-legitimationer

I sin roll som utfärdare kommer Digg att behöva föra ett register över innehavare av e-legitimationer, något som Digg inte gör idag.

Av den föreslagna förordningen bör det för tydlighetens skull framgå att Digg får föra ett register över innehavare av e-legitimationer. Digg anser inte att regleringen av personuppgiftsbehandlingen i den föreslagna förordningen enbart ska omfatta personuppgiftsbehandlingar i registret. Digg kommer även att behöva behandla personuppgifter utöver registerföringen såsom vid användningen av e-legitimationen samt vid loggning och logguppföljning. Det är således mer ändamålsenligt att bygga registerförfattningen på den personuppgiftsbehandling som sker i Diggs hela verksamhet med den statliga e-legitimationen och inte enbart på personuppgiftsbehandlingen som sker i registret.

Digg kommer i registret enbart hantera sådana personuppgifter som är nödvändiga med hänsyn till ändamålet. I dagsläget ser Digg att åtminstone följande personuppgifter att behandlas i registret:

- uppgifter om sökandens namn, personnummer, dag för utfärdande och giltighetstid
- uppgift om e-legitimationens unika identifierare (en hash av den unika kryptografiska nyckeln) och serienummer
- status för e-legitimationen såsom om den inte är aktiverad, spärrad eller utgången.
- aktiveringskod (tillfällig uppgift) och hash av innehavarens personliga kod
- kontaktuppgifter till innehavaren av e-legitimationen i form av e-post, bostadsadress och telefonnummer.

---

[109] Prop. 2017/18:95. *Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning.*
[110] Prop. 2017/18:95. *Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning*, s. 85 f.

Sökanden ombeds att frivilligt lämna uppgifter om e-post, bostadsadress och telefonnummer på utgivningsstället. Ändamålen med att inhämta dessa uppgifter är att kunna informera innehavaren om viktiga säkerhetshändelser och att verifiera begäran om spärr om en e-legitimation förkommit. Digg kommer även att göra automatiska slagningar mot folkbokföringsdatabasen Navet via Diggs register över e-legitimationer. På så sätt säkerställs att uppgifterna i registret är uppdaterade och korrekta. Exempelvis kan Digg på så sätt upptäcka om en innehavare har avlidit så att åtgärder kan vidta för att inaktivera eller spärra e-legitimationen.

Digg bedömer att registret inte är av så känslig karaktär att det av den anledningen finns skäl att detaljreglera innehållet i förordning. Den närmare regleringen av uppgifter som registret ska och får innehålla bör istället tas in i föreskrifter på lägre nivå.

7.3.4.9 Känsliga personuppgifter

Dataskyddsförordningen innehåller ett principiellt förbud mot att behandla vissa särskilda kategorier av personuppgifter (artikel 9.1). Förbudet omfattar behandling av uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Förbudet i dataskyddsförordningen kompletteras av ett antal undantag som gör det möjligt att behandla känsliga personuppgifter i vissa fall. Ett sådant undantag är om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades rättigheter och intressen (artikel 9.2 g).

Diggs bedömning är dock att Digg inte kommer att behandla några känsliga person-uppgifter i sin verksamhet med den statliga e-legitimationen. Digg kommer varken att behandla ansiktsbilder på sökanden, födelseort, medborgarskap eller andra uppgifter som tillsammans skulle kunna utgöra en uppgift om ras eller etniskt ursprung. Ingen av dessa uppgifter är nödvändiga för att utfärda den statliga e-legitimationen. Inte heller några andra känsliga personuppgifter kommer att behandlas av Digg inom sin verksamhet med den statliga e-legitimationen. Enligt Diggs förslag ska det därför i den föreslagna förordningen om statlig e-legitimation framgå att inga känsliga personuppgifter får behandlas inom Diggs verksamhet med den statliga e-legitimationen.

De handlingar som kommer in till Digg har dock myndigheten ingen möjlighet att påverka. Digg bör därför medges en möjlighet att behandla känsliga personuppgifter om

uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag. I propositionen Ny dataskyddslag gör regeringen bedömningen att den grundlagsfästa rätten att ta del av allmänna handlingar måste anses utgöra ett viktigt allmänt intresse.[111] I 3 kap. 3 § punkten 1 dataskyddslagen anges därför att känsliga personuppgifter får behandlas av en myndighet om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag. Bestämmelsen klargör att det är tillåtet för myndigheten att utföra sådan behandling av känsliga personuppgifter som krävs i myndighetens verksamhet som en direkt följd av framför allt offentlighets- och sekretesslagens och förvaltningslagens bestämmelser om hur allmänna handlingar ska hanteras, exempelvis genom krav på diarieföring och skyldighet att ta emot e-post.[112] Mot denna bakgrund bör det klargöras i den föreslagna förordningen om statlig e-legitimation att känsliga personuppgifter endast får behandlas med stöd av 3 kap. 3 § punkten 1 dataskyddslagen.

Som en integritetsskyddande åtgärd föreslår Digg att det i den föreslagna förordningen om statlig e-legitimation ska regleras att känsliga personuppgifter inte får användas som sökbegrepp.

7.3.4.10 Uppgift om lagöverträdelser

Uppgifter som rör lagöverträdelser tillhör inte de särskilda kategorier av personuppgifter som omfattas av förbudet mot behandling i artikel 9 i dataskyddsförordningen, men anses ändå vara en kategori personuppgifter som förtjänar särskilt skydd.[113] För behandlingar av uppgifter som rör fällande domar i brottmål samt överträdelser anges i artikel 10 dataskyddsförordningen att sådana behandlingar endast får utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller nationell rätt, där lämpliga skyddsåtgärder fastställts för de registrerades rättigheter och friheter. Ett sådant stöd i nationell rätt har införts i 3 kap. 8 § dataskyddslagen. Enligt bestämmelsen får personuppgifter som rör lagöverträdelser behandlas av myndigheter. Av ett rättsligt ställningstagande från Integritetsskyddsmyndigheten[114] framgår den närmare innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen.

Vid eventuella missbruk av e-legitimationer kan Digg komma att behöva göra vissa typer av utredningar innan en polisanmälan upprättas. Det är troligt att uppgifterna som Digg

[111] Prop. 2017/18:105 s. 86.
[112] Prop. 2017/18:105 s. 194.
[113] Prop. 2017/18:105 s. 97.
[114] Integritetsskyddsmyndighetens rättsliga ställningstagande (IMYRS 2021:1) - innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen.

registrerar till följd av missbruk av e-legitimation kommer att uppnå en sådan konkretionsgrad att de utgör sådana brottsmisstankar som omfattas av artikel 10 dataskyddsförordningen. Utgångspunkten är alltså att Digg i sin verksamhet med den statliga e-legitimationen kommer att behandla uppgifter om lagöverträdelser. Stöd för sådan behandling finns i 3 kap. 8 § dataskyddslagen. Digg kan dock inte se att uppgifter om lagöverträdelser kommer att behandlas i särskilt stor omfattning inom myndigheten. Uppgifterna kommer inte heller att behöva behandlas i myndighetens register över e-legitimationer.

Som en integritetsskyddande åtgärd föreslår Digg att det i den föreslagna lagen om statlig e-legitimation ska regleras att uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden inte får användas som sökbegrepp.

7.3.4.11 Personnummer och samordningsnummer

Med personnummer och samordningsnummer avses detsamma som i folkbokföringslagen (1991:481). Personnummer är inte en känslig personuppgift men har fått en särställning i svensk rätt. Enligt 3 kap. 10 § dataskyddslagen får personnummer och samordningsnummer behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Enligt Diggs förslag behöver Digg behandla uppgift om personnummer och samordningsnummer i verksamheten med den e-legitimationen, såsom vid utfärdandet och användningen av den statliga e-legitimationen. Behandlingen av personnummer och samordningsnummer är klart motiverat med hänsyn till vikten av en säker identifiering.

Enligt Diggs förslag kan den statliga e-legitimationen endast utfärdas till personer som har svenskt personnummer eller samordningsnummer. Endast sådana samordningsnummer där det inte råder osäkerhet om personens identitet, så kallat styrkt samordningsnummer, omfattas av Diggs förslag.[115] När förslagen i Stärkt system för samordningsnummer[116] har trätt i kraft, bör den grundidentifiering som genomförs i samband med utgivning av den statliga e-legitimationen i sig innebära att sökandes identitets styrkts i den grad som krävs för att uppgifterna i folkbokföringsdatabasen ska anses styrkta.

[115] 5 a § folkbokföringsförordningen samt prop. 2021/22:276, s.24.
[116] Prop. 2021/22:276.

7.3.4.12 Elektroniskt utlämnande av personuppgifter

I registerförfattningar görs åtskillnad mellan utlämnande via direktåtkomst och utlämnande på medium för automatiserad behandling, även benämnt elektroniskt utlämnande. Det kan konstateras att den tekniska utvecklingen har lett till att gränserna för direktåtkomst och utlämnande på medium för automatiserad behandling suddats ut. I det så kallade LEFI Online-målet (HFD 2015 ref. 61) fann domstolen att direktåtkomst avgränsas genom en prövning av om berörda upptagningar ska anses vara förvarade hos mottagande myndighet enligt 2 kap. 3 § andra stycket tryckfrihetsförordningen, TF. Domstolen fann vidare att teknisk tillgång enligt 2 kap. 3 § andra stycket TF inte föreligger om ett utlämnande förutsätter att den utlämnande myndigheten reagerar på en begäran om att de efterfrågade uppgifterna ska lämnas ut.

För att tillhandahållandet av den statliga e-legitimationen ska kunna ske hos den identitetskontrollerande myndigheten behöver ett elektroniskt utbyte av personuppgifter i realtid ske mellan denna myndighet och Digg. Vid direktåtkomst skapas överskottsinformation hos den mottagande myndigheten, vilket skapar risker för enskildas integritet. Av den anledningen anser Digg att det elektroniska informationsutbytet mellan den identitetskontrollerande myndigheten och Digg inte bör ske genom direktåtkomst. Digg bedömer att det elektroniska informationsutbyte som sker mellan den identitetskontrollerande myndigheten och Digg istället bör bygga på att elektroniskt utlämnande sker mellan myndigheterna i en fråga/svar-tjänst istället för genom direktåtkomst. Tjänsten för informationsutbyte bör tekniskt utformas så att Digg reagerar på en begäran om utlämnande.

Det är vanligt att formen för utlämnanden regleras i myndigheters särskilda registerförfattningar.[117] Det finns dock några myndigheter, såsom Skatteverket och Kronofogdemyndigheten, som inte begränsas av särskilda bestämmelser om utlämnande på medium för automatiserad behandling.[118] Regeringen har i de fallen anfört att under förutsättning att den utlämnande myndigheten har möjlighet att avgöra vilka uppgifter som ska lämnas ut saknas det anledning att reglera när uppgifter får lämnas ut på medium för automatiserad behandling. Regeringen har bedömt att inte finns några bärande skäl för att i informationsutbytet mellan myndigheter skilja på utlämnande som görs på papper och utlämnande som sker elektroniskt.[119]

---

[117] Se till exempel 16 § domstolsdatalagen (2015:728) samt 13 § lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten.

[118] Se lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet och lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet.

[119] Prop. 2000/01:33. *Behandling av personuppgifter inom skatt, tull och exekution*, s. 111 f.

Merparten av de utlämnanden som sker idag sker digitalt. Den tekniska utvecklingen har lett till att det numera saknas anledning att göra skillnad på utlämnanden på papper och digitalt. Digg anser att en reglering av formen på utlämnanden i registerförfattning riskerar att verka hämmande på myndighetens möjlighet till effektivt informationsutbyte. Utgångspunkten är att den nu föreslagna registerförfattningen bör vara teknikneutral och inte behöva ändras i takt med att den tekniska utvecklingen går framåt. Enligt Diggs förslag kommer Digg styras av ändamålsbestämmelser som anger när personuppgifter för behandlas. Det följer vidare av dataskyddsförordningens bestämmelser att Digg är skyldig att vidta lämpliga säkerhetsåtgärder för att skydda de uppgifter som behandlas.[120] Samtliga utlämnanden ska även vara förenliga med eventuella bestämmelser om sekretess. Digg anser således att myndigheten själv, utifrån beaktande av regelverk kring dataskydd, offentlighet och sekretess och informationssäkerhet i övrigt, ska göra bedömningen hur utlämnande av uppgifter ska ske. Det ska därför inte finnas några bestämmelser som reglerar formen för utlämnanden i den föreslagna registerförfattningen.

7.3.4.13 Längsta tid som personuppgifter får behandlas

Enligt huvudregeln i artikel 5.1 e i dataskyddsförordningen får personuppgifter inte förvaras i en form som möjliggör identifiering under längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna behandlas. När en personuppgift inte längre behöver behandlas för de ursprungliga ändamålen ska den alltså raderas eller avidentifieras. Personuppgifter får dock i enlighet med artikel 89.1 i dataskyddsförordningen lagras under en längre period i den mån uppgifterna enbart behandlas för arkivändamål av allmänt intresse eller för vetenskapliga och historiska forskningsändamål eller statistiska ändamål.

Digg bedömer att det inte finns anledning att reglera lagringstiderna i den föreslagna förordningen. En lämpligare hantering är istället att Digg själv i egenskap av personuppgiftsansvarig ställer upp lagringstider i förhållande till ändamålen med behandlingen i enlighet med EU:s dataskyddsförordning.

7.3.4.14 Automatiserat beslutsfattande

Med automatiserat beslut avses beslut som fattas maskinellt utan att någon enskild befattningshavare på myndigheten tar någon aktiv del i själva beslutsfattandet i det enskilda fallet.[121] Vid utgivning av den statliga e-legitimationen fattas ett automatiserat beslut av Digg i myndighetens system för statliga e-legitimationer. Vid det automatiserade

[120] Artikel 24 och 32 EU:s dataskyddsförordning.
[121] Prop. 2016/17:180 s. 315.

beslutsfattande sker en prövning av om förutsättningarna för att beviljas en statlig e-legitimation är uppfyllda. Enligt 28 § första stycket förvaltningslagen får myndigheter fatta automatiserade beslut.

8 Konsekvenser av Diggs förslag

I det här kapitlet redogörs för konsekvenser av Diggs förslag vad gäller kostnader och finansiering, tidplan samt konsekvenser för myndigheter och företag.

8.1 Kostnader

Digg bedömer att de sammantagna utvecklings- och uppbyggnadskostnaderna för Digg uppgår till cirka 80–100 miljoner kronor (mnkr). Dessa fördelar sig på kostnader för utveckling av system och programvara om cirka 50–70 mnkr och uppbyggnad av verksamheten vid Digg om cirka 30 mnkr.

Digg bedömer vidare att de årliga kostnaderna för verksamheten vid Digg uppgår till 63–71 mnkr. Dessa fördelar sig på kostnader för förvaltning om cirka 8–11 mnkr, kostnader för drift cirka 30 mnkr och Diggs kostnader för utgivningsprocessen till 25–30 mnkr. Baserat på utgivningsvolymerna kommer det över tid vara nödvändigt att se över beräkningarna.

De årliga kostnaderna för utgivningsprocessen hos de identitetskontrollerande myndigheterna uppskattas till sammanlagt cirka 21–30 mnkr, men även här kommer det över tid vara nödvändigt att se över beräkningarna.

Kostnadsanalysen bygger på uppskattningar av resursåtgång för respektive kostnadskategori. Försäkringskassan och Polismyndigheten har bistått Digg i att få en bild av uppskattade kostnader för drift och förvaltning samt för utgivningsprocessen. Det har dock inte varit möjligt att fullfölja analysen för verksamheten vid de identitetskontrollerande myndigheterna mot bakgrund av de nya förutsättningar för regeringsuppdragets genomförande som i ett sent skede uppkom genom Polismyndighetens ställningstagande, se bilaga 2. Givet avgränsningen i regeringsuppdraget har det inte heller varit möjligt för Digg att lämna förslag på annan identitetskontrollerande myndighet eller genomföra analyser som skulle följa av ett sådant förslag.

8.1.1 Utvecklings- och uppbyggnadskostnader

Den tekniska lösningen för en statlig e-legitimation föreslås alltså vara ett kontaktlöst aktivt kort och bygga på PIV-standarden. Ett flertal leverantörer tillhandahåller kompletta certifierade produkter på den öppna marknaden med de erforderliga funktioner som skulle krävas. Leverantörerna erbjuder vanligen även logistiklösningar och tjänster för att skapa visst innehåll på korten. Det innebär att korten bör kunna distribueras direkt från tillverkaren till utgivningsställena.

Digg kommer behöva utveckla nödvändig programvara och handledningar för att kunna använda kortet tillsammans med smarttelefoner och datorer. Genom att bygga på PIV-specifikationerna finns ett stort utbud av programbibliotek och standardapplikationer som kan användas, vilket kortar utvecklingstider och minskar kostnaderna. Vissa användargrupper kommer även ha behov av att använda kortet tillsammans med en vanlig dator, vilken då kan behöva kompletteras med en kortläsare. Det finns allmänt tillgänglig programvara att installera för att kunna använda kortet med en dator. Digg bedömer dock att det kan finnas behov av att utveckla ytterligare programvara för vanliga datorer och tillhörande handledning.

I sammanställningen nedan redogörs för resursåtgången för identifierade kostnadsposter. Beräkningarna har gjorts genom uppskattning av den tidsåtgång som skulle krävas för att utveckla varje steg, uttryckt som årsarbetskrafter. Ett ingående antagande i denna sammanställning är att en årsarbetskraft kostar 1,5 mnkr, inklusive overhead-kostnader[122]. Andra lösningsförslag eller identifiering av annan nödvändig utveckling kan dock komma att påverka utvecklingskostnaderna. Givet nuvarande antaganden uppskattar Digg de identifierade totala utvecklingskostnaderna till cirka 50–70 mnkr.

Utveckling av system och programvara

Kostnadsspecifikation	**Beskrivning**	**Uppskattad kostnad (mnkr)**
Tjänster för kommunikation med kortregistret	Maskingränssnitt (API-funktioner) för kommunikation med kortregistret behöver utvecklas. Dessa utformas i minst två olika varianter. Uppskattat två årsarbetskrafter.	3
Funktioner för att identifiera innehavare och ställa ut identitetsintyg	Intygsfunktioner ska tas fram, sannolikt i två olika skepnader för att möta krav på teknisk interoperabilitet (SAML resp. OIDC). Uppskattat 4–5 årsarbetskrafter.	6–7,5
Funktioner för hantering av metadata	Stödverktyg för att förlitande parter säkert ska kunna kommunicera med Diggs intygsfunktioner. Uppskattat en halv årsarbetskraft.	1
Programvara för användning i	En app behöver utvecklas för användning i mobiltelefon. Motsvarande programvara för	15

[122] 1,1 mnkr exklusive overhead-kostnader

innehavarens mobiltelefon eller dator	användning i dator behöver tas fram. Uppskattat två årsarbetskrafter multiplicerat med antal andra versioner av programvara för vanliga datorer. Tillkommande arbete med tillgänglighetsanpassning, användartester, kvalitetssäkring osv.	
Påbyggnadskomponent underskriftscertifikat	Påbyggnadskomponent innebär att man förser den elektroniska id-handlingen med ett underskriftscertifikat på distans. Kostnader drivs av certifieringsarbete mot eIDAS krav. Fyra årsarbetskrafter.	6
Övriga kostnadsposter	Kravställning, upphandling, projekt- och utvecklingsledning, rapportering och uppföljning, juridiska analyser, framtagande av allmänna villkor, förlitandeavtal, kontakter med intressenter, osv.	20–40
Register över innehavare	Ett register där alla kort som tillverkas ska registreras. Rutiner för kvalitet och säkerhet driver kostnader. Kostnadsuppskattningen kräver ytterligare utredning av tekniska och administrativa säkerhetskrav och har därför inte kunnat beräknas.	n/a
Summa	**Uppskattade utvecklingskostnader (exklusive kortregister)**	**50–70**

Utöver utveckling av system och programvara kommer uppgiften att ansvara för en statlig e-legitimation kräva bland annat uppbyggnad av ny verksamhet, förstärkningar av funktioner och anpassningar av lokaler hos Digg. Totalt beräknas dessa kostnader uppgå till 30 mnkr.

Uppbyggnad av verksamheten vid Digg

Kostnadsspecifikation	Beskrivning	Uppskattad kostnad (mnkr)
Rekrytering och utbildning av personal	Förstärkning till Digg för rekrytering och utbildning av personal	6
Informations- och cybersäkerhet	Utveckling av processer och rutiner för att leda och styra säkerhetsarbetet, anpassning av lokaler, säkerhetsprövning av personal	15
Rättsliga frågor och upphandling	Utredning av rättsliga frågor, framtagning av nya avtal, upphandling av kort, teknik och drift	6
Kommunikation	Framtagning av informationsmaterial och webbplats	3
Summa	**Uppskattade kostnader för uppbyggnad av verksamheten vid Digg**	**30**

8.1.2 Drift och förvaltning

Digg bedömer att vägval gällande driften bör göras i anslutning till den i Regeringskansliet pågående beredningen av förslagen som it-driftsutredningen lämnade i sitt slutbetänkande[123]. Viktiga frågor om till exempel redundans och geografisk spridning behöver en strategisk inriktning och hanteras i ett större sammanhang tillsammans med övrig samhällskritisk digital infrastruktur. Det bör exempelvis övervägas om tjänster och infrastruktur för digital identitet kräver flera likvärdiga instanser som kan ta över vid bortfall i en instans, och huruvida dessa också bör vara utspridda geografiskt[124]. Digg anser vidare att det även ur ett kostnadseffektivitetsperspektiv vore fördelaktigt att den dagliga driften läggs inom statlig verksamhet som redan har bemanning för närliggande tjänster. Exempelvis är eIDAS-noden en typ av intygstjänst och det bör därför utredas vidare om funktionerna för den statliga e-legitimationen skulle kunna tillhandahållas på likartat sätt.

I tidigare projekt har Digg beräknat förvaltningskostnader genom en procentuell schablon av uppskattade utvecklingskostnader. Så gjordes till exempel i Diggs genomförandeplan

[123] SOU 2021:97. It-driftsutredningen. *Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift: slutbetänkande.* 2021.
[124] SOU 2021:9. Utredningen om betrodda tjänster. *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen: delbetänkande.* 2021.

för införandet av bevisutbyte enligt engångsprincipen (SDG) där berörda myndigheter tillfrågades om sina förvaltningskostnader. Utifrån dessa togs sedan en schablon fram[125]. Förvaltningskostnaderna i det projektet visade sig ligga i ett intervall mellan 6–25 procent av utvecklingskostnaderna, och Digg valde då att använda ett medelvärde på 15 procent. Digg har applicerat samma schablon vid beräkning av förvaltningskostnaderna för den statliga e-legitimationen, vilket ger en uppskattning på cirka 8–11 mnkr årligen. Därtill uppskattas de årliga driftskostnaderna till cirka 30 mnkr, men Digg vill här betona att ytterligare analys behövs, bland annat mot bakgrund av förslagen från it-driftsutredningen[126].

8.1.3 Utgivningsprocessen

8.1.3.1 Kostnader hos Digg

Digg kommer i sin roll som utfärdare av den statliga e-legitimationen att få ökade kostnader på årlig basis. Dessa är till viss del volymberoende, men det finns också andra aspekter som Digg särskilt behöver beakta, exempelvis vad gäller behovet av att undvika rollkonflikter vid granskning och utfärdande. Vissa funktioner hos Digg kan därför behöva separeras organisatoriskt. Digg förutser också att ökade säkerhetskrav kommer att gälla för delar av verksamheten. Beräkningarna i sammanställningen nedan bygger på uppskattad tidsåtgång i form av årsarbetskrafter[127].

Utgivningsprocessen – uppskattade årliga kostnader för Diggs verksamhet

Kostnadsspecifikation	Beskrivning	Uppskattad kostnad (mnkr)
Juridik och upphandling	Upphandling av kort, förvaltning av avtal, upphandling och övriga juridiska frågor	3
Informations- och cybersäkerhet	Förvaltning och vidareutveckling av åtgärder i enlighet med lagkrav, incidenthantering, samverkan med andra myndigheter, kontinuerlig omvärldsbevakning inkl. 24/7-beredskap, intern kontroll, säkerhetsprövning av personal m.m.	4,5–6

[125] Myndigheten för digital förvaltning. *Genomförandeplan för införandet av bevisutbyte enligt engångsprincipen.* 2021.
[126] SOU 2021:97.
[127] 1,5 mnkr inklusive overhead-kostnader

Stöd till användare	Kundservice, administration, första linjens support, hantering av frågor från allmänheten, informationsmaterial och webb	9
Stöd till förlitande parter och identitetskontrollerande myndighet	Kundservice, administration, första linjens support, förvaltning av Sweden Connect, informationsmaterial och webb	4,5–6
Andra linjens support	Ärenden från användare, förlitande parter och identitetskontrollerande myndighet som skickas vidare från första linjen	4,5–6
Summa	**Uppskattade kostnader hos Digg för hantering av utgivningsprocessen**	**25,5–30**

Digg bedömer att beräkningarna endast är en grundnivå för Diggs hantering av den statliga e-legitimationen. Nivån kan komma att ändras vid större förändringar i volymerna av utgivna e-legitimationer.

8.1.3.2 Kostnader hos identitetskontrollerande myndighet

Digg har varit i kontakt med Polismyndigheten och, för utlandsmyndigheternas del, Utrikesdepartementet för att förstå hur myndigheternas processer avseende ansökan, betalning, identitetskontroll och utlämnande ser ut idag. Baserat på denna information har sedan uppskattningar gjorts gällande kostnader för utgivningsprocessen hos identitetskontrollerande myndighet. En viktig kostnadsdrivande faktor är mängden ansökningar som direkt påverkar dimensionering av personal och lokaler. Digg konstaterar att det är mycket svårt att uppskatta hur många ansökningar om den statliga e-legitimationen som kommer att göras. En bedömning baserat på målgruppsanalysen nedan är att antalet ansökningar i Sverige och i utlandet kan komma att uppgå till 160 000–300 000 de första två åren. Digg har valt att beräkna volymerna på två års basis då det kan antas att det initialt kan komma att röra sig om väldigt små volymer för att därefter öka. Ett tvåårsperspektiv utgör då en mer realistisk tidshorisont.

Uppskattning av ansökningsvolymer i Sverige de första två åren

Målgrupp	**Uppskattat antal ansökningar**
Personer med samordningsnummer	50 000
Tekniskt intresserade personer inräknat de som av olika skäl inte vill använda en smarttelefon	10 000
De som vill skaffa en statlig e-legitimation för att i nästa led skaffa en annan e-legitimation på distans.	50 000
Personer med funktionsnedsättning som har svårt att använda existerande lösningar och för vilka den statliga e-legitimationen skulle passa bättre	10 000
Personer som inte använder e-legitimation på dator eller mobiltelefon, men vill kunna göra vissa ärenden med lånad utrustning	50 000
Personer som har behov av den högsta tillitsnivån för gränsöverskridande identifiering	10 000
Personer med samordningsnummer som av olika skäl kan ha svårt att skaffa en annan e-legitimation	50 000
Uppskattade ansökningsvolymer år 1–2	**230 000**

Digg har här gjort ett konservativt antagande och gör bedömningen att volymerna sannolikt kommer att påverkas av för vilket användningsområde som de olika målgrupperna behöver en statlig e-legitimation i förhållande till andra existerande lösningar. På nationell nivå skulle användningen av den statliga e-legitimationen markant öka vid ett framtida beslut om att alla godkända e-legitimationer ska kunna användas i den offentliga förvaltningens tjänster. Digg bedömer vidare att volymerna också kommer öka i takt med användningen av den kommande europeiska digitala identitetsplånboken, där den statliga e-legitimationen kommer att användas vid inloggning. Om exempelvis körkortsbehörighet läggs in i den digitala plånboken så skulle ansökningarna om den statliga e-legitimationen årligen kunna uppgå till 500 000. Det finns således faktorer som gör Diggs uppskattningar här osäkra och det finns därför anledning att se över beräkningarna när förutsättningarna framöver förändras.

För att kunna uppskatta kostnaderna för utgivningsprocessen hos de identitets-kontrollerande myndigheterna behövs, förutom de uppskattade ansökningsvolymerna, även en uppskattning av tidsåtgång för handläggning. Polismyndigheten har bistått Digg med siffror från processen för utfärdande av pass och id-kort. En genomsnittlig ansökan beräknas ta cirka 10 minuter och utlämning av det färdiga passet eller id-kortet beräknas till i genomsnitt 3 minuter. Ansökan och utlämning av pass och id-kort sker idag vid två separata tillfällen. I Diggs förslag till utgivningsprocess för den statliga e-legitimationen har de aktiviteterna lagts ihop till ett och samma tillfälle, vilket borde leda till en effektivisering av administrationen och att handläggningstiden vid de identitets-kontrollerande myndigheterna kortas. Hur denna effektivisering rent praktiskt ska kunna ske är ännu inte fastställt. Digg har därför valt att utgå från befintlig administrationstid som ett konservativt scenario, det vill säga cirka 13 minuter.

Ett ingående antagande i denna sammanställning är att en årsarbetskraft motsvarar 1,5 mnkr, och fördelningen i utgivningsvolym mellan åren uppskattas till 40 procent av utgivningsvolymen det första året, och 60 procent av volymen år två. Givet en grov uppskattning av utgivningsvolym inom Sverige på cirka 230 000 statliga e-legitimationer under de första två åren, skulle detta innebära en uppskattad utgivningsvolym på ungefär 92 000 det första året, och 138 000 år två. Detta motsvarar i sin tur ett tillkommande bemanningsbehov för den identitetskontrollerande myndigheten på ungefär 10 årsarbetskrafter under år ett, och 15 årsarbetskrafter år två. Digg uppskattar den tillkommande kostnaden för den identitetskontrollerande myndigheten vid utfärdande av statlig e-legitimation därför till cirka 15 mnkr det första året, och 22 mnkr kronor under år två. Digg bedömer att siffrorna kan komma att behöva revideras baserat på hur många utgivningsställen i Sverige som kommer att utfärda den statliga e-legitimationen.

Även om utgivningsprocessen på utlandsmyndigheterna inte är identisk med den som beskrivs i föregående avsnitt, så är resonemanget i kostnadsanalysen detsamma. I nuläget bor närmare 700 000 svenskar utomlands[128]. Digg uppskattar att cirka 10–20 procent av dessa personer skulle kunna vara intresserade av en statlig e-legitimation för att kunna utföra vissa ärenden. Givet samma antaganden rörande tidsåtgång som ovan, med justering för en genomsnittslön baserat på de lönekostnader som framräknats av Statskontoret[129], skulle utlandsmyndigheternas administrativa kostnader för utfärdande av den statliga e-legitimationen ligga på cirka 4 årsarbetskrafter det första året, och 7 årsarbetskrafter år två. Detta motsvarar en tillkommande kostnad på ungefär 6 mnkr det

[128] Swedenabroad.se (aug 2022).

[129] Statskontoret. *Migrationsverksamheten vid Utlandsmyndigheterna – en analys av vad det skulle kosta om Migrationsverket tar över ansvaret. Statskontoret 2017:23.* 2017.20. (s. 20: 1 545 000 kr för utsänd personal + 302 000 för lokalt anställd personal, inkl. OH om 655 000 kr per årsarbetskraft baserat på år 2016.).

första året, och 8 mnkr år två. Digg bedömer att siffrorna kan komma att behöva revideras baserat på hur många av utlandsmyndigheterna som kommer att utfärda den statliga e-legitimationen.

Kostnader för utbildning, nyanställning, investeringar i ny hårdvara och annan verksamhetsanpassning är delar som kräver ytterligare utredning för den identitetskontrollerande myndigheten.

8.2 Finansiering

I detta avsnitt presenterar Digg sina ställningstaganden kring vilken typ av finansiering som är lämplig för de berörda myndigheterna. Generellt bedömer Digg att anslagsfinansiering skapar bättre förutsättningar än avgiftsfinansiering för berörda myndigheter att planera och bemanna sin verksamhet, och kan ge bättre möjligheter för att tillhandahålla en statlig e-legitimation på ett långsiktigt, stabilt och förutsägbart sätt.

8.2.1 Finansiering av Diggs kostnader

Digg föreslår att kostnader för utveckling av system och programvara samt uppbyggnad av verksamheten vid Digg ska finansieras genom ett tillfälligt förstärkt förvaltningsanslag till Digg (2:6 ap.1) under utvecklings- och uppbyggnadsfasen och att de årliga kostnaderna därefter finansieras genom en permanent höjning av samma anslagspost.

8.2.2 Finansiering av verksamheten hos de identitetskontrollerande myndigheterna

Polismyndighetens och utlandsmyndigheternas verksamheter och uppdrag utgår från samtliga kostnader kopplade till hanteringen av pass och id-kort ska täckas fullt ut. Digg bedömer att samma förhållanden bör gälla för de identitetskontrollerande myndigheterna.

Utrikesdepartementet har gällande utlandsmyndigheterna har uttryckt en önskan att hantera kostnaden för utfärdande av den statliga e-legitimationen via en kostnadsdelning i likhet med den som idag finns mellan utlandsmyndigheterna och Migrationsverket gällande migrationsverksamheten[130]. Det skulle innebära en användning av befintligt tidsmätningssystem för att mäta den tid det tar att handlägga ett utgivningsärende och i efterhand fakturera denna kostnad för tidsåtgång till ansvarig förvaltningsmyndighet, i detta fallet Digg. För att minimera administrationen, vore det lämpligt att i ett sådant fall,

[130] Utrikesdepartementet. *Förvaltningsöverenskommelse mellan Utrikesdepartementet och Migrationsverket, avseende administrativt samarbete och kostnadsdelning för migrationsverksamheten vid utlandsmyndigheterna, UD2019/19279/PLAN.* 20191220. Samt bilagor 1-4: Förvaltningsöverenskommelse Utrikesdepartementet och Migrationsverket.

undersöka förutsättningarna för att Migrationsverket, i likhet med den befintliga överenskommelsen, hanterar den tillkommande administrationen för fakturering mellan myndigheter.

8.2.2.1 Avgifter för den statliga e-legitimationen

Digg föreslår att en avgift tas ut för den statliga e-legitimationen i samband med ansökan. Den uttagna avgiften bör användas till att finansiera de ökade kostnaderna som uppstår hos myndigheterna. Digg bedömer dock att avgifterna till fullo inte kommer att kunna täcka dessa kostnader och föreslår därför att ytterligare medel tillförs via anslag. Digg har valt att inte lämna förslag till nivån på avgiften då det bland annat krävs fördjupad analys av målgruppernas betalningsvilja och -förmåga. Digg bedömer också att nivån på avgiften kan vara en politisk fråga. En lämplig utgångspunkt för att bestämma nivån skulle kunna vara dagens avgifter för pass och id-kort. Digg rekommenderar att inriktningen att den statliga e-legitimationen ska kunna skaffas av så många som möjligt tas i beaktande när nivån på avgiften fastställs. En för hög avgift skulle sannolikt påverka efterfrågan, men Digg förespråkar ändå att en viss avgift tas ut då det leder till att kortet får ett monetärt värde för användaren och därmed uppmuntrar till försiktighet att inte slarva bort kortet.

Riksdagen har i generella bemyndiganden i annan form än lag överlåtit åt regeringen att meddela föreskrifter om ansöknings- och expeditionsavgifter.[131] Regeringens bemyndigande till myndigheten att ta ut avgifter ska ges i den förordning som reglerar prövningen, i förekommande fall förordning om statlig e-legitimation.

I förordning om statlig e-legitimation föreslås att 11 – 14 §§ avgiftsförordningen ska gälla för prövningen i övrigt. Detta innebär bland annat att avgiften som huvudregel ska betalas när ansökan ges in (11 §), att avgiften ska betalas för varje avgiftsbelagt ärende som ansökan avser (12 §) och att en myndighet får, om det finns särskilda skäl, betala tillbaka hela eller delar av ansökningsavgiften (13 §). Av 14 § framgår att ett beslut om ansökningsavgift får överklagas i samma ordning som gäller för det ärende som ansökan avser.

8.3 Översiktlig tidplan

Givet att nödvändiga beslut har fattats av regering och riksdag gällande finansiering, författningsförändringar och annan myndighetsstyrning bedömer Digg att utvecklingstiden för en statlig e-legitimation är minst 24 månader. I bedömningen ingår ett antal aktiviteter som i vissa delar kan bedrivas parallellt, men i andra delar måste bedrivas

[131] SOU 2007:96. Avgiftsutredningen. *Avgifter: slutbetänkande*, s. 89.

sekventiellt. På nationell nivå består aktiviteterna bland annat i att bygga upp organisationen hos Digg, till exempel rekrytera och utbilda personal, utreda rättsliga frågor, upphandla lösningar för de fysiska korten samt utveckla processer och rutiner för att leda och styra säkerhetsarbetet. Andra omfattande aktiviteter består i utveckling, användartester, tillgänglighetsanpassningar och införande av den tekniska lösningen.

När det gäller EU och eIDAS-förordningens tidsramar så tillkommer en parallell tidplan där den statliga e-legitimationen ska föranmälas till EU-kommissionen och granskas av andra medlemsländer för att slutligen godkännas för användning vid gränsöverskridande e-legitimering. Enligt det kompromissförslag som antogs av medlemsländerna i december 2022 ska en e-legitimation på högsta tillitsnivån finnas på plats senast 24 månader efter att genomförandeakterna trätt i kraft. Genomförandeakterna ska i sin tur antas senast sex månader efter antagandet av eIDAS-förordningen. Givet att tidsramarna inte ändras under återstoden av förhandlingen av eIDAS-förordningen så får den totala tidsåtgången högst uppgå till 30 månader. Även här finns det beroenden till att nödvändiga beslut har fattats av regering och riksdag.

8.4 Konsekvenser för myndigheter och företag

Den statliga e-legitimationen föreslås tillhandahållas via Diggs valfrihetssystem för elektronisk identifiering. Detta innebär i sak ingen skillnad för de myndigheter som redan har tecknat avtal med Digg om valfrihetssystem. Myndigheterna behöver därefter lägga till den statliga e-legitimationen som ett val i sin anvisningstjänst så att användaren får möjlighet att logga in.

Sammantaget kommer en statlig e-legitimation innebära att fler individer som idag befinner sig i ett digitalt utanförskap får möjlighet att identifiera sig digitalt. Därmed kommer användningen av de digitala tjänsterna att öka, såväl i offentlig som privat sektor, samtidigt som behovet av stöd via exempelvis kundtjänst och telefonsupport torde minska. Digg bedömer således inte att införandet av en statlig e-legitimation skulle innebära ökade kostnader för myndigheter eller företag.

9 Förslag till nästa steg

Digg har under utredningsarbetet identifierat frågor som kräver ytterligare fördjupning. Utifrån frågor kopplade till den pågående förhandlingen av eIDAS-förordningen bedöms vissa som mer brådskande, men för att få ihop helheten kring en statlig e-legitimation behövs också ett större samlat grepp. Detta gäller särskilt frågor som berör det digitala utanförskapet och där Digg uppfattat att det finns höga förväntningar på att den statliga e-legitimationen ska bidra till att fler får möjlighet att ta tillvara sina rättigheter och utföra sina skyldigheter i den digitala världen. Det är också ytterst angeläget att säkerhetsfrågorna får högsta prioritet i det fortsatta arbetet.

9.1 Starta utvecklingsarbetet

I kompromissförslaget till den reviderade eIDAS-förordningen som antogs av medlemsländerna den 6 december 2022 anges att varje land ska ha notifierat en e-legitimation på högsta tillitsnivå senast 24 månader efter att förordningen trätt i kraft. Denna tid kan komma att kortas efter förhandling med Europaparlamentet. Parallellt med att författningsförslag och andra frågor kopplat till genomförandet av eIDAS-förordningen nu hanteras av regeringens särskilda utredare[132] behöver utveckling och testning av den statliga e-legitimationen inledas för att det ska vara möjligt att realisera förslaget inom dessa tidsramar. Digg föreslår därför att regeringen ger Digg i uppdrag att påbörja utvecklingsarbetet.

Lösningen som Digg föreslår utgör en möjliggörare för fortsatt utveckling. I ett förnyat uppdrag till Digg bör det därför också ingå att ytterligare undersöka hur den statliga e-legitimationen även kan tillhandahållas via de nationella id-korten.

9.2 Sätt säkerheten i fokus

Under detta förhållandevis korta utredningsuppdrag har det inte varit möjligt att genomföra fördjupade analyser avseende säkerheten i den föreslagna tekniska lösningen. Digg har, tillsammans med MSB, gjort bedömningen att i ett nästa steg bör myndigheterna i det Nationella cybersäkerhetscentret ges i uppdrag att tillsammans genomföra en analys av säkerheten. Utöver en teknisk säkerhetsanalys som Försvarets radioanstalt föreslås få ett särskilt ansvar för att utföra bör även vald lösning belysas ur ett samhällsperspektiv. Där bör exempelvis beroenden till annan infrastruktur och även samhällsviktig verksamhets beroenden till systemet, samt exempelvis frågor om digital suveränitet,

[132] Dir. 2022:142

hanteras. Dessa frågor kan MSB ta ett särskilt ansvar för liksom att hålla ihop uppdrags-arbetet i sin helhet.

9.3 Ställ krav på användningen

Digg bedömer att det tidigare lämnade förslaget om att alla e-legitimationer som Digg granskat och godkänt ska kunna användas i offentliga aktörers digitala tjänster fortsatt är aktuellt. Utöver att erbjuda en ny lösning för e-legitimation krävs ytterligare åtgärder för att den statliga e-legitimationen ska nå sina användare. Den statliga e-legitimationen måste erbjudas vid inloggning hos alla aktörer i den offentliga förvaltningen och det ska inte vara valbart för aktören vilka e-legitimationer som erbjuds. Detta kräver en ny reglering, ett obligatorium. Digg välkomnar därför att den nyligen tillsatta utredningen[133] har fått i uppdrag att analysera och lämna författningsförslag om det bör ställas krav på förlitande parter som tillhandahåller digitala tjänster inom offentlig sektor att acceptera alla e-legitimationsalternativ på marknaden förutsatt att de lever upp till den tillitsnivå som tjänsterna kräver. Digg anser att även avgiften i valfrihetssystemet behöver utredas, mot bakgrund av kommande krav i eIDAS-förordningen.

9.4 Minska det digitala utanförskapet

Som Digg visat i rapporten finns det ett omfattande digitalt utanförskap i Sverige. Införande och användning av en statlig e-legitimation förväntas bidra till att minska detta utanförskap, men det finns behov av ytterligare åtgärder. E-legitimationer ska vara säkra och enkla att använda, fast ibland är det inte så enkelt. Då måste det finnas möjlighet att få stöd i användningen. Digg anser att mer arbete behövs för att öka den digitala kompetensen hos medborgare. Ett sådant stöd skulle kunna tillhandahållas via offentliga aktörer, till exempel Statens servicecenter, kommunala Digidel-center och bibliotek, men även via andra åtgärder såsom kompetenslyft och informationskampanjer.

För att minska det digitala utanförskapet krävs också ett särskilt fokus på tillgänglighets-frågor. Digg bedömer att det finns behov av utförliga tester av tillgängligheten i den lösning som föreslås och att sådana tester måste vara en prioriterad del i det fortsatta arbetet.

Digg har i en tidigare rapport framfört till regeringen att en utredning bör tillsättas som föreslår sätt att hantera de restriktioner ett förvaltarskap medför med avseende på e-legitimationer[134]. Frågan har fallit mellan stolarna i offentliga utredningar och det

[133] Dir. 2022:142
[134] Myndigheten för digital förvaltning. Utveckling av det svenska e-legitimationssystemet. 2021.

saknas idag förslag till åtgärder. En ny utredning enligt Diggs tidigare förslag skulle även kunna omfatta förslag till åtgärder som förhindrar personer som är misstänkta eller dömda för bedrägerier att fortsätta använda e-legitimationer i brottsligt syfte. Ju fler som får tillgång till e-legitimation, desto viktigare är denna fråga.

Inom Ena-Sveriges digitala infrastruktur pågår ett arbete med en förvaltningsgemensam ombudslösning som förväntas bidra till att minska det digitala utanförskapet och möjliggöra spårbarhet i vem som agerat ombud[135]. För att en ombudslösning ska fungera även för de som har gode män eller förvaltare behövs ett register över gode män och förvaltare. Ett sådant register föreslogs av Ställföreträdarutredningen och skulle kunna underlätta för en god man eller förvaltare att hjälpa sina huvudmän att även sköta ärenden som kräver e-legitimation[136]. Digg föreslår att regeringen går vidare med förslagen från utredningen så att människor kan företrädas digitalt av ombud utifrån korrekta data.

Digitalt utanförskap kan också bero på ekonomiska faktorer. Det kostar inte något att få tillgång till en e-legitimation från en privat leverantör av e-legitimationer. Detta skiljer sig från förslaget i avsnitt 8.2.2 att det ska tas ut en avgift för ansökan om den statliga e-legitimationen. Digg bedömer att det är relevant att ta ut en avgift för ansökan, men vill även framhäva att detta kan utesluta eller försvåra för vissa personkretsar att skaffa en statlig e-legitimation. Digg föreslår därför att förutsättningarna för att ansökningsavgiften för den statliga e-legitimationen skulle kunna ingå i försörjningsstödet ska utredas.

9.5 Utred utestående frågor

9.5.1 Sekretess

Det kan förekomma uppgifter inom verksamheten för den statliga e-legitimationen som behöver skyddas av sekretess. Digg har i denna rapport inte tagit ställning till frågor om sekretess eftersom det inte har omfattats av uppdragsbeskrivningen. Digg har inte heller analyserat om det finns tillräckligt stöd för att skydda uppgifter som kan omfattas av sekretess i nuvarande sekretesslagstiftning eller om detta kräver författningsåtgärd. För att samarbetet med de identitetskontrollerande myndigheterna ska fungera kan det finnas behov av sekretessbrytande bestämmelser. Digg föreslår därför att frågor om sekretess och behov av sekretessbrytande bestämmelser inom verksamheten med den statliga e-legitimationen utreds vidare.

[135] https://www.digg.se/ledning-och-samordning/ena---sveriges-digitala-infrastruktur
[136] SOU 2021:36. Ställföreträdarutredningen. *Gode män och förvaltare – en översyn: slutbetänkande*. 2021.

9.5.2 Skydd mot missbruk av e-legitimationer

Så länge en e-legitimation kan brukas kan den missbrukas. Det finns inga tekniska sätt att få e-legitimationen att tänka åt dess innehavare. Problemen med dagens bedrägerier handlar många gånger om att förvilla och lura innehavare att använda sin e-legitimation till att göra det som bedragaren vill. Vissa modus kan förenklas eller försvåras av viss teknisk utformning, men möjligheterna kommer alltid att finnas. Den som har de bästa möjligheterna att motverka bedrägerierna är varken innehavaren eller utfärdaren av e-legitimationen, det är den förlitande aktören som i den digitala tjänsten kan bygga in spärrar och rimlighetskontroller så att de blir säkrare att använda. Digg bedömer att vissa riskindikatorer, framställda ur tekniska parametrar från användningen av e-legitimationen, skulle kunna tjäna som ett värdefullt verktyg för förlitande aktörer i att kontrollera att en viss åtgärd inte genomförs obehörigen. De rättsliga förutsättningar som behövs för att det ska kunna bli möjligt att förmedla sådana uppgifter behöver utredas vidare.

Idag har innehavare av BankID ibland ett slags "konsumentskydd" genom bestämmelser i lag (2010:751) om betaltjänster (jfr. kap 5 a)[137]. Detta skydd stärktes nyligen genom HD:s avgörande i mål nr. T 4623-21 från 21 juni 2022[138]. Då en statlig e-legitimation inte omfattas av lagen om betaltjänster saknas såväl de aktsamhetskrav som ansvars-begränsningar som där föreskrivs. Detta kan få allvarliga konsekvenser för en statlig e-legitimation, och det finns behov av att utreda skyddet för konsumenten.

9.5.3 Biometriska personuppgifter

Möjligheten att läsa och äkthetskontrollera id-handlingar maskinellt, vilket främst är tillämpligt för nationella id-kort och pass, skulle bidra till en högre tillförlitlighet i identifieringen. En sådan maskinell avläsning skulle även göra det möjligt att på maskinell väg göra biometrijämförelser av såväl ansiktsbild som fingeravtryck. Dessa åtgärder skulle avsevärt försvåra missbruk av traditionella id-handlingar. För att en statlig e-legitimation ska kunna vara mer tillförlitlig krävs att den så kallade grundidentifieringen kan göras på ett noggrant och säkert sätt, möjligen genom att identitetskontrollerande myndighet i handläggningen av ett ansökningsärende har tillgång till och får behandla biometriska personuppgifter. Digg föreslår därför vidare utredning av förutsättningar för att behandla biometriska personuppgifter i samband med utfärdande av den statliga e-legitimationen.

[137] Lag (2010:751) om betaltjänster
[138] Högsta domstolen, mål: T 4623-21

9.5.4 Förvaltningsrättsliga frågor

Digg föreslår att olika myndigheter ska ansvara för olika delar av utgivningsprocessen för e-legitimationen och att ansvarsfördelningen ska framgå av förordning, vilket kan väcka rättsliga frågeställningar i förvaltningslagens mening. En konsekvens av Diggs föreslagna utgivningsprocess är att olika myndigheter – Digg och den identitetskontrollerande myndigheten – är involverade i olika skeende av en ärendeprocess. Digg anser att vissa förvaltningsrättsliga frågor, exempelvis överklagbarheten hos beslut hos identitets-kontrollerande myndighet, bör utredas vidare i nästa steg.

9.5.5 Upphandling och konkurrens

I Sverige finns det en fungerande marknad för e-legitimationer där idag endast privata e-legitimationsutfärdare verkar. Det finns konkurrensrättsliga bestämmelser som kan komma att aktualiseras när offentliga aktörer ägnar sig åt säljverksamhet på en sådan marknad. Den statliga e-legitimationen behöver utformas på ett sådant sätt att konkurrensen inte snedvrids på ett otillbörligt sätt. Beroende på hur finansierings-modellen av den statliga e-legitimationen utformas, kan användningen aktualisera upphandlingsplikten hos upphandlande myndigheter. Digg anser att eventuella upphandlingsrättsliga aspekter, inklusive statsstödsfrågor, bör utredas vidare i ett nästa steg.

Diggs förslag bygger på öppna standarder, vilket minskar risken för inlåsning i specifika tekniska lösningar[139]. Digg har också för avsikt att publicera bland annat stödprogram-varor som öppen källkod.

9.5.6 Säkerhetsskydd

För det fall den statliga e-legitimationen är en sådan verksamhet som är av betydelse för Sveriges säkerhet kan den komma att omfattas av säkerhetsskyddslagstiftningen. Detta kan innebära än högre krav på hur lösningarna kring den statliga e-legitimationen utformas och tillhandahålls, samt medföra att det ställs ännu högre krav på ansvarig myndighet avseende säkerheten. Digg bedömer därför att frågan om säkerhetsskyddet i förhållande till den statliga e-legitimationen behöver utredas i ett nästa steg.

[139] Konkurrensverket. *IT-standarder, inlåsning och konkurrens. En analys av policy och praktik inom svensk förvaltning.* Uppdragsforskningsrapport 2016:2. 2016.

Källförteckning

Författning

Domstolsdatalagen (2015:728)

Europeiska konventionen om skydd för de mänskliga rättigheterna (EKMR)

Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

Europaparlamentets och rådet förordning (EU) 2016/679 av den 17 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning)

Europaparlamentets och rådets direktiv (EU) 2016/2102 av den 26 oktober 2016 om tillgänglighet avseende offentliga myndigheters webbplatser och mobila applikationer

Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster

Folkbokföringslagen (1991:481)

Förordningen (2000:308) om fastighetsregister

Förordningen (2018:219) med kompletterande bestämmelser till dataskyddsförordningen

Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning

Förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt

Förvaltningslag (2017:900)

Föräldrabalken (1949:381)

Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

Lag (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet

Lag (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet

Lag (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet

Lag (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten

Lag (2010:751) om betaltjänster

Lag (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering

Lag (2015:899) om identitetskort för folkbokförda i Sverige

Lag (2018:218) med kompletterande bestämmelser till dataskyddsförordningen

Lag (2022:1697) om samordningsnummer

Myndighetsförordningen (2007:515)

Offentlighets- och sekretesslag (2009:400)

Polisdatalagen (2010:361)

Regeringsformen (1974:152)

Säkerhetsskyddslagen (2018:585)

Tryckfrihetsförordningen (1949:105)

Förarbeten

Dir. 2020:133. *Statens roll på betalningsmarknaden.*

Dir. 2022:142. *Säker och tillgänglig digital identitet.*

Regeringskansliet. *Auktorisationssystem för elektronisk identifiering och digital post: promemoria.* 21 december 2020.

SOU 2007:96. Avgiftsutredningen. *Avgifter: slutbetänkande.* 2007.

SOU 2007:100. Id-kortsutredningen. *Id-kort för folkbokförda i Sverige: slutbetänkande.* 2007.

SOU 2009:86. E-delegationen. *Strategi för myndigheternas arbete med e-förvaltning: delbetänkande.* 2009.

SOU 2010:104. Utredningen om bildande av en e-legitimationsnämnd. *E-legitimationsnämnden och Svensk e-legitimation: slutbetänkande.* 2010.

SOU 2017:14. Utredningen om ansvar för migrationsverksamheten vid utlandsmyndigheterna. *Migrationsärenden vid utlandsmyndigheterna: slutbetänkande.* 2017.

SOU 2017:37. Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden. *Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra: slutbetänkande.* 2017.

SOU 2017:114. Utredningen om effektiv styrning av nationella digitala tjänster. *reboot – omstart för den digitala förvaltningen: slutbetänkande.* 2017.

SOU 2019:14. 2017 års ID-kortsutredning. *Ett säkert statligt ID-kort – med e-legitimation: slutbetänkande.* 2019.

SOU 2021:9. Utredningen om betrodda tjänster. *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen: delbetänkande.* 2021.

SOU 2021:36. Ställföreträdarutredningen. *Gode män och förvaltare – en översyn: slutbetänkande.* 2021.

SOU 2021:42. Utredningen om stärkta åtgärder mot penningtvätt och finansiering av terrorism. *Stärkta åtgärder mot penningtvätt och finansiering av terrorism: slutbetänkande.* 2021.

SOU 2021:57. Utredningen om folkbokföring och samordningsnummer. *Om folkbokföring, samordningsnummer och identitetsnummer: slutbetänkande.* 2021.

SOU 2021:97. It-driftsutredningen. *Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift: slutbetänkande.* 2021.

Prop. 2000/01:33. *Behandling av personuppgifter inom skatt, tull och exekution.*

Prop. 2001/02:144. *Lag om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten.*

Prop. 2007/08:160. *Utökat informationsutbyte.*

Prop. 2008/09:70. *Genomförande av tredje penningtvättsdirektivet.*

Prop. 2012/13:74. *Förfalsknings- och sanningsbrotten.*

Prop. 2016/17:180. *En modern och rättssäker förvaltning.*

Proposition 2017/18:77. *Nya regler om betaltjänster.*

Prop. 2017/18:95. *Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning.*

Prop. 2017/18:105. *Ny dataskyddslag.*

Prop. 2019/20:106. *Stärkt integritet i Rättsmedicinalverkets verksamhet.*

Prop. 2021/22:276. *Stärkt system för samordningsnummer.*

Ds 2020:22. *Ökad säkerhet för vissa identitets- och uppehållshandlingar.*

Rättsfall

Hovrätten för Västra Sveriges domar den 18 juni 2018 i mål nr T 3583-17 och den 29 november 2018 i mål nr T 2473-18

Högsta domstolen, mål: T 4623-21.

LEFI Online-målet (HFD 2015 ref. 61)

Åklagarkammarens ärende AM-61001-16

Åklagarmyndigheten Utvecklingscentrum Stockholms beslut (ärende ÅM 2016/4817)

Rapporter

Begripsam. *Svenskarna med funktionsnedsättning och internet.* 2019.

Digitaliseringsrådet. *En lägesbild av digital trygghet.* 2018.

Digitaliseringsrådet. *Delaktighet i en digital tid – fördjupningsrapport med förslag.* 2019.

Finansinspektionen. *Förstärkt digital motståndskraft hos företag i den finansiella sektorn.* 2022.

Försvarets radioanstalt. *Medarbetare i demokratins tjänst.* Årsrapport 2021.

Internetstiftelsen. *Svenskarna och internet 2022.*

Konkurrensverket. *IT-standarder, inlåsning och konkurrens. En analys av policy och praktik inom svensk förvaltning.* Uppdragsforskningsrapport 2016:2. 2016.

Myndigheten för digital förvaltning. *Genomförandeplan för införandet av bevisutbyte enligt engångsprincipen.* 2021.

Myndigheten för digital förvaltning. *Utveckling av det svenska e-legitimationssystemet.* 2021.

Myndigheten för digital förvaltning. *Digital plånbok*. 2022.

Nationella underrättelsecentret. *Identitetsrelaterad brottslighet.* 2015.

Polismyndigheten. *Myndighetsgemensam lägesbild om organiserad brottslighet.* Dnr A457.772/2019.

Polismyndigheten. *De dödliga bedrägerierna, En rapport om bedrägeribrottslighet och skjutvapenvåldet.* 2022.

RISE. *Cyberhot mot Sverige - En sammanfattning för ledare och beslutsfattare.* 2022.

Skill, Karin och Kaharevic, Ahmed. *Förorten svarar: En enkätmetod för att kartlägga digital delaktighet och hållbarhet i Skäggetorp*. DINO Rapport 2021:7, Linköpings universitet.

Statistiska centralbyrån. *Befolkningens it-användning 2022.*

Statskontoret. *Migrationsverksamheten vid Utlandsmyndigheterna – en analys av vad det skulle kosta om Migrationsverket tar över ansvaret. Statskontoret 2017:23.* 2017.20.

Statskontoret. *Perspektiv på omprövning*. 2021.

Säkerhetspolisen. *Säkerhetspolisen 2021.*

Trafikanalys. *Kollektivtrafikens barriärer – kartläggning av hinder i kollektivtrafikens tillgänglighet för personer med funktionsnedsättning Rapport 2019:3.* 2019.

Övrigt material

Betänkande 2021/22:TU6. *Digitaliserings- och postfrågor.*

Dagens Nyheter, DN Debatt. *Sverige måste införa en statlig e-legitimation.* 16 november 2022.

Dagens Nyheter, ledarsidan. *Blir e-legitimation ett nytt statligt it-haveri?* 3 januari 2023.

ISO/IEC 7816-15:2016. *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application.* 2016.

Integritetsskyddsmyndighetens rättsliga ställningstagande (IMYRS 2021:1) - innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskyddsförordningen.

Ju2003/00861/PO Ett nationellt identitetskort.

Näringsdepartementet. *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi.* N2017/03643/D.

Polismyndigheten. *Skrivelse från Nationellt bedrägericentrum*. 2022-09-06.

Polismyndighetens föreskrifter och allmänna råd om pass och nationellt id-kort PMFS 2021:3.

Riksbanken. *Remissvar om betänkandet Ett säkert statligt id-kort med e-legitimation (SOU 2019:14)*. Dnr 2019-00588.

Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR.

Utrikesdepartementet. *Förvaltningsöverenskommelse mellan Utrikesdepartementet och Migrationsverket, avseende administrativt samarbete och kostnadsdelning för migrationsverksamheten vid utlandsmyndigheterna, UD2019/19279/PLAN*. 20191220.

Westberg, Mikael och Furberg, Per. *Kan man lita på e-legitimationen? Om missbruk av urkund i den digitala miljön*. Juridisk Tidskrift nr 2 2017/18.