Skatteverket

PROMEMORIA

Datum
2019-01-21

Bilaga till
Dnr 2 02 27351-19/113

Fördjupad utredning rörande koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar

Postadress: 171 94 SOLNA **Telefon**: 0771-567 567
Mejl via "Kontakta oss" på www.skatteverket.se

Innehållsförteckning

Sammanfattning

Regeringen har genom beslut den 17 maj 2018 (Fi2018/02044/S3) lämnat i uppdrag till Skatteverket att vidareutveckla myndighetens promemoria Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer och lämna förslag som syftar till att möjliggöra ökad gränsöverskridande åtkomst till svenska digitala myndighetstjänster. Skatteverkets uppdrag ska slutredovisas senast den 31 januari 2019. Denna promemoria utgör rapporteringen av uppdraget.

Skatteverket föreslog 2016 ett register över kopplingar mellan utländska eID-handlingar och svenska personnummer eller styrkta samordningsnummer för att ge användare med utländska eID-handlingar och svenska identitetsbegrepp tillgång till svenska myndigheters digitala tjänster och för att tillhandahålla identifiering av dessa användare till de svenska myndigheterna.

För att möta risker och utmaningar med ett kopplingsregistersystem har Skatteverket nu renodlat förslaget om hur en koppling ska kunna registreras till en inledande tvåstegsmodell där användaren först efter fysisk inställelse hos Polisen kan få en koppling registrerad mellan sin utländska eID-handling och sitt svenska personnummer. För att komma fram till denna modell har Skatteverket bland annat gjort avvägningar i missbruks- och bedrägerihänseende, informationssäkerhetsmässiga bedömningar och en ny genomsyn av personuppgiftsansvaret mot bakgrund av EU:s dataskyddsreform 2018 och den kompletterande svenska lagstiftningen.

Skatteverket har varit i kontakt med de övriga myndigheter som var involverade i arbetet med den förra promemorian 2016. De flesta av dem har uppdaterat sin inställning med ökad medvetenhet om säkerhet och personuppgiftsansvar. Till övervägande del är de övriga myndigheterna fortfarande positivt inställda till en central funktion för koppling. Skatteverket har därför inte gjort någon omprövning av behovet, utan kvarstår i bedömningen att det finns ett behov av en central kopplingstjänst och tillhörande kopplingsregister.

Förslaget om kopplingsregister finns därför kvar sedan den förra promemorian men med begränsningar av tillvägagångssätt för hur en koppling ska kunna registreras. Av säkerhetsskäl ska ett tillvägagångssätt för koppling startas i taget. Först efter att det har utvärderats tillsammans med en uppdaterad behovsbild kan det bli aktuellt att starta flera tillvägagångssätt för att registrera koppling.

Användaren startar processen för att registrera koppling genom att logga in med den eID-handling som hen vill koppla till ett svenskt personnummer i en digital tjänst och där skapa en väntande koppling. Därefter inställer sig användaren fysiskt hos Polisen, som ska utföra identitetskontroll, och styrker sin identitet på motsvarande sätt som krävs för utfärdande av svenska pass och id-kort. Efter kontroll använder handläggaren den väntande kopplingen för att slutföra registreringen av koppling mellan eID-handlingen och det svenska personnumret. Modellen för registrering av koppling är framtagen med avsikt att minimera risker för missbruk och bedrägerier.

Informationssäkerheten i kopplingsregistret ska säkerställas genom vedertagna åtgärder som syftar till att information i kopplingsregistret inte sprids till obehöriga, att informationen är korrekt och fullständig samt att informationen är tillgänglig för behöriga vid behov. Åtgärderna innefattar också en spårbarhetsdimension som innebär att möjliggöra säkerställande av vem eller vilka som har läst, bearbetat, förändrat eller förstört specifik information och när eller var det har skett.

Skatteverket bedömer att det för närvarande inte är lämpligt att skapa en koppling mellan en utländsk eID-handling och en användares styrkta samordningsnummer. För att tillräcklig säkerhet ska uppnås genom hela identifieringsprocessen behövs ordentlig grundidentifiering av användaren vid tilldelning av samordningsnummer. Detta kan enligt Skatteverkets uppfattning bara utföras vid personlig inställelse. I dagsläget ansvarar den myndighet som begärt tilldelning av samordningsnumret för identifieringen och avgör själv hur identifieringen ska gå till. Skatteverket har den 17 december 2018 i promemorian Samordningsnumrens funktion i samhället (Dnr 2 04 319440-17/113) lämnat förslag om hur tilldelningen av samordningsnummer kan förbättras säkerhetsmässigt så att samordningsnummer i framtiden ska kunna kopplas samman med utländska eID-handlingar.

När det gäller personuppgiftsbehandlingen i kopplingsregistret har Skatteverket gjort en ny genomgång och beskrivit ändamålen samt bedömt proportionaliteten och den rättsliga grunden för förslagen. Skatteverket föreslår även att kopplingsregistret ska regleras med samma typ av sekretess som gäller för folkbokföringsdatabasen.

I frågan om ansvar för kopplingsregistret kvarstår Skatteverkets bedömningar när det gäller att Skatteverket ska ansvara för kopplingsregistret och tjänsten för att registrera koppling och Polisen för identifieringskontrollen och handläggningen vid registrering av kopplingsärenden. Utlandsmyndigheter i Europa som är passmyndigheter har enligt Utrikesdepartementet för närvarande inte resurser eller kompetens nog för att utföra identifieringskontroller. Skatteverket anser därför att de inte i inledningsskedet bör registrera kopplingar.

De kostnadsmässiga konsekvenserna av förslaget förväntas för Skatteverket uppgå till 12,3 miljoner kronor för utveckling av systemet och därefter 7,8 miljoner kronor per år för drift och förvaltning. I samband med att Skatteverket har samrått med Polisen har Polisen lämnat uppgift om att deras kostnader förväntas uppgå till 128 000 kronor för utbildning av personal samt 350 kronor per besökande användare.

Ordlista och definitioner

Anvisningstjänst	Digitala tjänster kan styra sina användare till en anvisningstjänst där användaren väljer identifieringstjänst. Det avlastar de enskilda digitala tjänsterna från att själva implementera stöd för hur användare väljer att identifiera sig.
Användare	Fysisk person som vill logga in i en myndighets digitala tjänst.
API	API kommer av engelskans application programming interface och översätts till applikations-programmeringsgränssnitt. Det är en specifikation av hur olika applikationsprogram kan använda och kommunicera med en specifik programvara.
Applikation	Typ av datorprogram som användaren tillämpar i ett direkt syfte, t.ex. ordbehandling, kommunikation eller nöje, till skillnad från program som behövs för att driva datorn eller skapa program (se även Webb-applikation).
DIGG	Myndigheten för digital förvaltning.
Digital tjänst	Service som erbjuds på digital eller elektronisk väg.
eID-handling	Sådan handling för elektronisk identifiering som avses i artikel 6 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Ofta används begreppet e-legitimation för sådana handlingar. Skatteverket menar att legitimation ska användas när det gäller behörighet och identitetshandling när det gäller identifiering. I promemorian använder Skatteverket begreppet eID-handling som en förkortning av elektronisk identitetshandling.[1]
eID-koppling	Att med hjälp av en redan registrerad eID-handling koppla en ny eID-handling till en svensk identitetsbeteckning. Användaren loggar in med en svensk eller annan eID-handling och godkänner att ytterligare en eID-handling kopplas till samma identitet. Det förutsätts att det är styrkt att innehavaren av en viss utländsk eID-handling är identisk med innehavaren av en viss svensk identitetsbeteckning.

[1] SOU 2017:114, s. 171 f.

eIDAS	Electronic identification (eID) and electronic trust services (eTS)
eIDAS-förordningen	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.
eIDAS-ID	För att få användas för gränsöverskridande identifiering enligt eIDAS-förordningen ska en eID-handling innehålla en minimiuppsättning av personidentifieringsuppgifter som är unika för en person. En av dessa uppgifter är en unik identitetsbeteckning som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering och som är mest beständig i tid. Detta regleras i Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i eIDAS-förordningen. Denna identitetsbeteckning benämns eIDAS-ID i detta sammanhang.
Elektronisk underskrift	Krypterade uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form, för att säkerställa de senares ursprung och dataintegritet.
Folkbokföringsdatabasen	Folkbokföringen förs i folkbokföringsdatabasen. I folkbokföringsdatabasen finns uppgifter om varje person som är eller har varit folkbokförd. Även uppgifter om personer med samordningsnummer ingår i databasen. Där görs alla registreringar som påverkar folkbokföringen, till exempel vigsel, namnändring eller dödsfall. Uppgifter från folkbokföringsdatabasen lämnas i huvudsak ut genom personbevis (utdrag ur databasen) via aviseringssystemet Navet som utgör en del av folkbokföringsdatabasen, eller ett separat register, det statliga personadressregistret, SPAR.
Gränssnitt	Gränssnitt är utformningen av en viss förbindelse mellan olika objekt. Inom informationsteknologi avser det hur man kommunicerar mellan olika mjuk- eller hårdvaror, eller interaktionen mellan människa och maskin (användargränssnitt).
Identitetsintyg	När en användare autentiserar sig hos en identitetsleverantör skickar denna sedan ett identitetsintyg till tjänsten som användaren vill

	använda. Identitetsintyget innehåller enligt eIDAS-förordningen bland annat information om användarens förnamn, efternamn, födelsedatum, ett identitetsbegrepp och vilken tillitsnivå som har använts vid autentiseringen.
Identitetsleverantör	Den organisation som har den grundläggande informationen om användarna och den part som också utför autentiseringen. Benämns även som Utfärdare eller Identity Provider (IdP).
Kopplingsregister	Ett i denna promemoria föreslaget register över kopplingar mellan utländska eID-handlingar och svenska identitetsbeteckningar. Benämns även som kopplingsdatabas.
Matchning	Processen för att para ihop en utländsk eID-handling med en svensk identitetsbeteckning och kontrollera att uppgifterna stämmer överens.
Nationell nod	En nod är en omkopplingspunkt för datatrafik. Med nationell nod avses den svenska eIDAS-noden. Se även utländsk nod.
Navet	Ett aviseringssystem som hämtar sina uppgifter ur, och är en del av folkbokföringsdatabasen.
Samordningsnummer	Ett samordningsnummer kan användas av svenska myndigheter som identitet på personer som inte är eller har varit folkbokförda i Sverige, men ändå är registrerade i folkbokföringsdatabasen. Det kan gälla för utländska personer som arbetar tillfälligt i landet, som pendlar från grannland, studerar vid universitet, är sjöman på svenskt fartyg, äger sommarstuga eller svenskregistrerad bil, behöver svenskt körkort, får en ordningsbot eller blir åtalade för brott med flera situationer.
Tillitsnivå	Nivå av säkerhet för eID-handlingar. Ju högre tillitsnivå desto säkrare kan den digitala tjänst som använder eID-handlingar för identifiering av användarna vara på att det är rätt användare som man kommunicerar med.
Translitterering	Omskrivning av ett skriftsystem till ett annat så att varje främmande tecken motsvarar ett translitterert tecken. En text kan då göras läsbar för dem som inte känner till det skriftsystem varmed originaltexten är skriven, samtidigt som teckenmängden i den translitterade texten varken ökar eller minskar. Denna egenskap kan vara fördelaktig vid

	databehandling där intakt teckenmängd är av vikt, t.ex. när det gäller id-handlingar.
Utländsk nod	En nod är en omkopplingspunkt för datatrafik. I detta sammanhang avses europeiska eIDAS-noder. Varje medlemsstat kommer att ha en egen eIDAS-nod. Se även nationell nod.
Validera	Bekräfta, förklara giltig, göra gällande.
Webb-applikation	Datorprogramvara som man kommer åt genom att använda en webbläsare och som används i ett speciellt syfte (se även Applikation).

1 Författningsförslag

1.1 Förslag till lag om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar

Härigenom föreskrivs följande.

Databas

1 § Skatteverket ska föra en databas för registrering av personer som både har en svensk identitetsbeteckning och en eller flera sådana handlingar för elektronisk identifiering som avses i artikel 6 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eID-handling) och som har begärt att en sådan registrering ska ske.

Polisen ska handlägga ärenden om koppling och föra in uppgifter i kopplingsregistret.

Myndigheten för digital förvaltning ska kontrollera förekomst av koppling i databasen och förmedla identitetsinformation till myndighet som tillhandahåller digital tjänst och till vilken den registrerade digitalt har begärt tillträde.

Lagens tillämpningsområde och förhållande till annan reglering

2 § Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddförordning), här benämnd EU:s dataskyddsförordning.

Vid behandling av personuppgifter enligt denna lag gäller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Denna lag gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställnings enligt särskilda kriterier.

Ändamål

3 § Personuppgifter får behandlas i databasen för att visa kopplingen mellan en persons utländska eID-handling och dennes svenska identitetsbeteckning. Uppgifterna får även behandlas för att handlägga ärenden enligt denna lag.

Uppgifterna i databasen får också behandlas för att tillhandahålla information som behövs hos Skatteverket, Polisen eller Myndigheten för digital förvaltning för tillsyn, kontroll, uppföljning och planering av verksamheten.

Uppgifter får också behandlas i databasen för tillhandahållande av information som behövs i Myndigheten för digital förvaltnings verksamhet att förmedla identitetsinformation till myndigheter som tillhandahåller digitala tjänster.

Personuppgifter som behandlas för ändamålet enligt första stycket får också behandlas om det behövs för att fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning.

4 § Databasen får innehålla uppgifter om personer som har tilldelats personnummer. För de ändamål som anges i 3 § får följande uppgifter behandlas:

1. namn,
2. personnummer,
3. födelsedatum,
4. eID-handlingarnas unika identitetsbeteckningar, och

Regeringen får föreskriva att också andra uppgifter ska få behandlas i databasen.

5 § De övriga uppgifter och handlingar som behövs för att handlägga ett ärende enligt denna lag och som har kommit in till eller upprättats i ett ärende får behandlas i databasen.

Sådana personuppgifter av särskilda kategorier som anges i artikel 9 i Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EC (dataskyddsförordningen) får behandlas i en handling som lämnats i ett ärende. Sådana uppgifter får behandlas även i en handling som upprättats i ett ärende, om de är nödvändiga för ärendets handläggning. Motsvarande gäller uppgift om fällande domar i brottmål och överträdelser m.m. enligt artikel 10 i samma förordning.

Personuppgiftsansvar

6 § Skatteverket är personuppgiftsansvarigt för den behandling av person-uppgifter som myndigheten utför i databasen.

Polisen är personuppgiftsansvarig för den behandling av personuppgifter som sker i ärendehantering som avser koppling mellan utländska eID-handlingar och svenska identitetsbegrepp. Polisen är också personuppgiftsansvarig för införande av uppgifter och handlingar i databasen.

Myndigheten för digital förvaltning är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför för att kontrollera förekomst av koppling samt för att förmedla identitetsinformation till andra myndigheter.

Ansökan och registrering

7 § En ansökan om registrering i databasen enligt 1 § ska göras skriftligen och ska innehålla de uppgifter som behövs för prövningen.

En koppling ska registreras efter ansökan av den som kopplingen avser, om ansökan gjorts på föreskrivet sätt och om den sökande har styrkt sin identitet enligt den svenska identitetsbeteckningen samt styrkt kopplingen med eID-handlingen.

8 § En ansökan om registrering av koppling mellan en svensk identitetsbeteckning och en eID-handling ska avslås om det som anges i 7 § eller som har föreskrivits av regeringen i fråga om ansökan inte har iakttagits och sökanden inte har följt en uppmaning att avhjälpa bristen.

9 § En registrering av en koppling enligt 1 § ska tas bort om den registrerade skriftligen ansöker om det.

En registrering av en koppling ska även tas bort om det framkommer att eID-handlingen inte längre gäller, inte längre ska erkännas eller det finns skäl att anta att eID-handlingen inte avser den registrerade.

10 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om ansökan och registrering av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Digitalt utlämnande

11 § Myndigheten för digital förvaltning får ha direktåtkomst till uppgift enligt 1 § tredje stycket.

Polisen får ha direktåtkomst till uppgifter och handlingar i databasen om det behövs för myndighetens ärendehandläggning enligt denna lag.

En enskild får ha direktåtkomst till person- och ärendeuppgifter om sig själv i databasen

Till andra myndigheter får uppgiften lämnas ut på medium för automatiserad databehandling.

Myndigheten för digital förvaltning får på medium för automatiserad databehandling lämna uppgift om att det finns en registrerad koppling mellan viss utländsk eID-handling och en svensk identitetsbeteckning i databasen i samband med ett förfarande för att verifiera en eID-handling.

Sökbegrepp

12 § Vid sökning i databasen får uppgifter som avses i 5 § andra stycket inte användas.

Gallring

13 § Uppgifter och handlingar som finns i databasen ska gallras senast fem år efter att beslut om kopplingen mellan den utländska eID-handlingen och den svenska identitetsbeteckningen registrerades.

Överklagande

14 § Ett beslut enligt denna lag får överklagas till Förvaltningsrätten i Stockholm.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 juli 2020.

1.2 Förslag till lag om ändring i offentlighets- och sekretesslag (2009:400)

Härigenom föreskrivs att 22 kap. 1 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
22 kap.	
1 §[2]	
Sekretess gäller för uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs och uppgiften förekommer i verksamhet som avser	
1. folkbokföringen eller annan liknande registrering av befolkningen och, i den utsträckning regeringen meddelar föreskrifter om det, i annan verksamhet som avser registrering av en betydande del av befolkningen, *eller*	1. folkbokföringen eller annan liknande registrering av befolkningen och, i den utsträckning regeringen meddelar föreskrifter om det, i annan verksamhet som avser registrering av en betydande del av befolkningen,
2. förande av eller uttag ur sjömansregistret.	2. förande av eller uttag ur sjömansregistret*, eller*
	3. koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Sekretess gäller i verksamhet som avses i första stycket 1 för uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 juli 2020.

[2] Senaste lydelse 2009:400.

1.3 Förslag till förordning om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar

Härigenom föreskrivs följande.

1 § Denna förordning innehåller kompletterande bestämmelser till lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

2 § Med identitetsbeteckning avses, i lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar och denna förordning, svenskt personnummer.

Ansökan och registrering

3 § Ansökan ska innehålla fullständigt namn, svensk identitetsbeteckning, uppgift om utländsk eID-handling samt en försäkran på heder och samvete att den digitala identiteten avser samma person som har den svenska identitetsbeteckningen.

4 § En registrering av en koppling mellan en utländsk eID-handling och en svensk identitetsbeteckning får bara göras om det är styrkt att sökanden är identisk med innehavaren av den svenska identitetsbeteckningen.

En koppling kan registreras efter att sökanden personligen inställt sig hos Polisen för kontroll av identiteten.

Bemyndigande

5 § Skatteverket får meddela de ytterligare föreskrifter som behövs för verkställigheten av lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar och för verkställigheten av denna förordning.

Polisen får meddela de ytterligare föreskrifter som behövs för verkställigheten av den kontroll av identiteten som avses i 3 § 2 stycket.

Denna förordning träder i kraft den 1 juli 2020.

1.4 Förslag till förordning om ändring i förordningen (2014:1102) med instruktion för Polismyndigheten

Härigenom föreskrivs att det i förordningen (2014:1102) med instruktion för Polismyndigheten ska införas en ny paragraf med följande lydelse.

6 a § Polismyndigheten ansvarar för handläggning av ärenden om koppling enligt lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Denna förordning träder i kraft den 1 juli 2020.

1.5 Förslag till förordning om ändring i förordningen (2017:154) med instruktion för Skatteverket

Härigenom föreskrivs att det i förordningen (2017:154) med instruktion för Skatteverket ska införas en ny paragraf med följande lydelse.

12 a § Skatteverket ansvarar för kopplingsregistret enligt lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Denna förordning träder i kraft den 1 juli 2020.

2 Bakgrund

2.1 Uppdraget

I mitten av september 2014 publicerades 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 (eIDAS-förordningen). Den svenska lagen (2016:561) och förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering trädde i kraft den 1 juli 2016, vilket sammanföll med datumet för eIDAS-förordningens tillämpning.

E-legitimationsnämnden har i en rapport ”E-legitimationer enligt eIDAS” den 16 december 2015 slutrapporterat ett uppdrag från regeringen (N2015/2620/EF) avseende analys av konsekvenserna av ett införande av EU-förordningen och dess genomförandeakter. I slutrapporten anförs bl.a. att det finns ett behov av att möjliggöra för individer att på ett frivilligt och säkert sätt kunna koppla sin EU-godkända europeiska eID-handling till sitt redan utfärdade svenska personnummer eller identitetsstyrkta samordningsnummer. Även E-delegationen har i slutbetänkandet En e-förvaltning som håller ihop framhållit behovet av att Skatteverket får lagra kopplingen mellan samordningsnummer och en utländsk eID-handling.[1]

Regeringen gav den 23 mars 2016 i uppdrag (N2016/2307/EF) till Skatteverket att utreda behoven av och förutsättningarna för en tjänst för koppling mellan en utländsk eID-handling och en individs svenska personnummer eller styrkta samordningsnummer vid användning av svenska digitala myndighetstjänster. Skatteverket skulle även lämna förslag på nödvändig författningsreglering. E-legitimationsnämnden fick samtidigt i uppdrag att ansvara för den svenska noden för elektronisk identifiering enligt eIDAS-förordningen.

Skatteverket skulle enligt uppdragsbeskrivningen genomföra en övergripande analys av offentlig sektors behov och förväntade nytta av en tjänst för koppling mellan en utländsk eID-handling och en individs svenska personnummer eller styrkta samordningsnummer. Vidare skulle Skatteverket ta fram ett lösningsförslag för utformning och förvaltning av en sådan tjänst, såväl avseende ansvarig myndighet som teknisk lösning. I uppdraget ingick även att bedöma kostnader och konsekvenser av förslaget. Vidare skulle Skatteverket utreda de juridiska förutsättningarna för tjänsten och lämna förslag till nödvändiga författningsändringar för att möjliggöra en koppling mellan den utländska eID-handlingen och individens svenska personnummer eller styrkta samordningsnummer. Skatteverket skulle även redovisa konsekvenserna av eventuella författningsförslag. Författningsförslagen skulle inte innefatta några ändringar av grundläggande förutsättningar för folkbokföringen eller tilldelning av person- eller samordningsnummer. Inom uppdraget skulle Skatteverket även identifiera och beskriva viktiga frågor som behöver utredning i annan form. Uppdraget slutredovisades den 24 oktober 2016 i promemorian Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer.

Regeringen har därefter genom beslut den 17 maj 2018 (Fi2018/02044/S3) lämnat i uppdrag till Skatteverket att vidareutveckla promemorian från 2016 och lämna förslag som syftar till att möjliggöra ökad gränsöverskridande åtkomst till svenska digitala myndighetstjänster.

[1] SOU 2015:66 s. 35

Skatteverket ska analysera riskerna för att det föreslagna kopplingsregistret kan angripas och nyttjas i missbrukssyfte och lämna förslag på hur sådana eventuella risker ska hanteras för att förhindra missbruk av identitetshandlingar och därigenom förebygga bedrägerier och brott mot välfärden. Vidare ska Skatteverket analysera och bedöma vilka åtgärder som bör vidtas för att säkerställa en god informationssäkerhet i det föreslagna kopplingsregistret.

Skatteverket ska även överväga om det för närvarande kan anses lämpligt att skapa en koppling mellan en utländsk eID-handling och en individs styrkta samordningsnummer.

I uppdraget ingår även att överväga om det finns behov av sekretessbestämmelser och sekretessbrytande bestämmelser för hantering av uppgifter i kopplingsregistret som är skyddade i andra länder eller som rör personer med skyddade personuppgifter samt utföra en förnyad och fördjupad bedömning av personuppgiftsbehandlingen i det föreslagna kopplingsregistret.

Skatteverket ska också överväga om registrering av koppling mellan en europeisk eID-handling och ett svenskt identitetsbegrepp som sker vid personlig inställelse bör utföras vid vissa svenska utlandsmyndigheter som även är passmyndigheter. Därutöver ska Skatteverket utföra en fördjupad utredning om de tekniska förutsättningarna för ett kopplingsregister.

I uppdraget ingår även att bedöma kostnader och konsekvenser som förslaget kan komma att medföra. Vidare ska Skatteverket lämna förslag till nödvändiga författningsändringar samt redovisa konsekvenserna av eventuella författningsförslag. Denna promemoria utgör rapporteringen av uppdraget.

2.2 Övriga förutsättningar

Grundtanken med den gränsöverskridande identifieringen enligt eIDAS-förordningen är att de medverkande länderna ska ha tillit till varandras lösningar för eID-system och därmed även tillit till varandras processer när det gäller grundidentifiering och utfärdande av alla sorters id-handlingar.

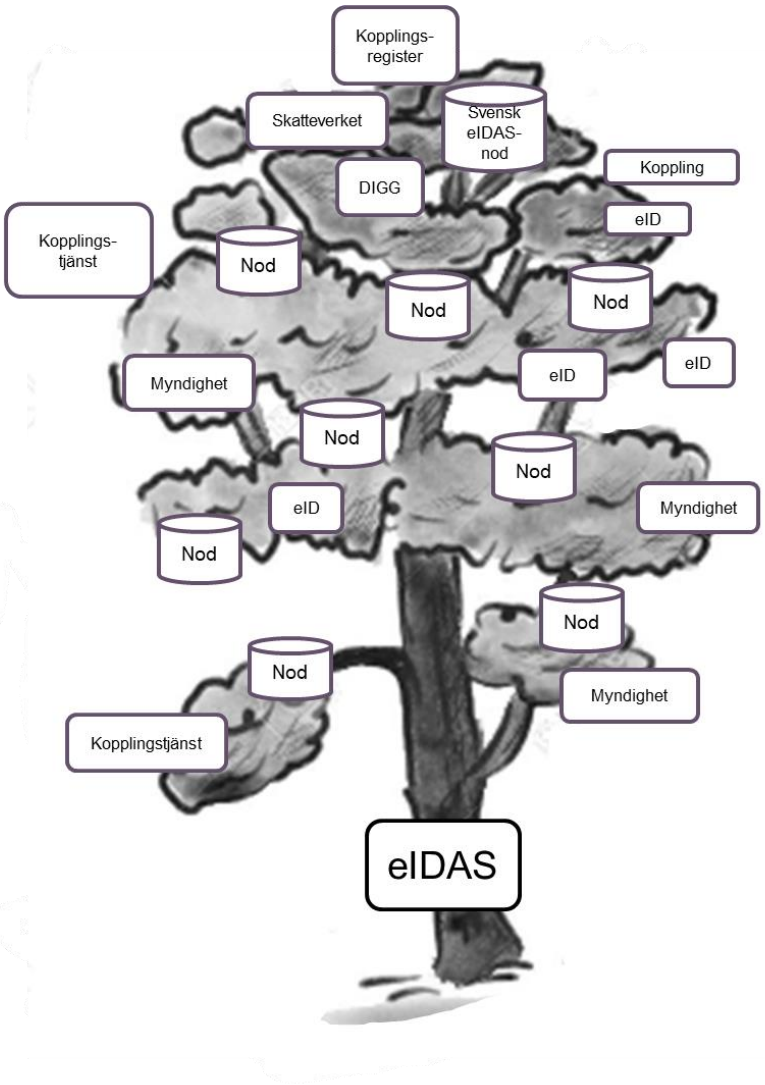
Länderna accepterade dessa förutsättningar när eIDAS-förordningen förhandlades fram och är bundna att leva upp till de åtaganden som gäller enligt förordningen. Det får med andra ord inte förekomma diskriminering av något lands godkända eID-handlingar även om det skulle visa sig att det finns skäl att ifrågasätta tilliten till dem.

Ett svenskt kopplingsregister är en länk i en lång kedja av händelser när en användare vill logga in i en svensk myndighets digitala tjänst. Innan det är dags att koppla samman en utländsk eID-handling med en svensk identitetsbeteckning har användaren någon gång grundidentifierats i det land som har utfärdat eID-handlingen. Användaren har fått en eID-handling och den utländska noden har förmedlat kontakt mellan eID-utfärdaren och Sverige. Under denna process kan det inträffa något fel utan att det uppmärksammas på vägen. Sådana fel kan så att säga ”ärvas” in i systemet och orsaka fel i slutändan som inte har med kopplingen i Sverige att göra. Oavsett kvaliteten på kopplingstjänsten och kopplingsregistret kan det uppstå problem som Sverige inte kan råda över. Om ett sådant fel inträffar är medlemsstaten som anmält eID-systemet i och för sig ansvarig och skadeståndsskyldig gentemot de fysiska eller juridiska personer som lidit skada. Det följer av Artikel 11 i eIDAS-förordningen.

Tillitssystemet mellan länderna kan jämföras med ett träd där stammen består av eIDAS-förordningen. Därefter kommer alla länders noder och eID-handlingar som ska användas för gränsöverskridande identifiering. Alla medlemsstater avgör

själva vilka system de ska använda och hur de ska bygga upp sina lösningar för att ta emot eID-handlingar. Detta regleras inte av eIDAS-förordningen. Längre ut i trädkronan följer ländernas ansvariga myndigheter och först efter det kommer lösningar för att koppla samman eID-handlingar med inhemska identitetsbeteckningar. Det svenska exemplet illustreras med fyra centrala komponenter längst ut i trädets grenverk; Myndigheten för digital förvaltning (DIGG), den svenska noden, Skatteverket och kopplingsregistret. Detta kan se helt olika ut i varje medlemsstat. Vissa länder kan ha ett departement eller myndighet som ansvarar för alla deras delkomponenter och andra kan dela upp ansvaret mellan olika offentliga och privata aktörer. I vissa länder finns inga centrala kopplingslösningar.

Med illustrationen avser Skatteverket att visa att det svenska kopplingsregistret är en liten gren i ett stort komplicerat nät av sammanlänkade händelser. Kopplingsregistret kan inte isoleras från vad som pågår i övriga delar. Om något inträffar på vägen fram till kopplingsregistret får det följder för det svenska systemet.



3 Gällande rätt

3.1 EU:s förordning om elektronisk identifiering

I artikel 1, i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen), anges att målet med förordningen är att säkerställa en väl fungerande marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster. I skäl 2 till förordningen anges att den syftar till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan företag, medborgare och offentliga myndigheter. Därigenom ska effektiviteten öka hos offentliga och privata digitala tjänster samt i elektronisk affärsverksamhet och e-handel i unionen. Enligt artikel 2 gäller förordningen system för elektronisk identifiering som en medlemsstat har anmält.

Enligt artikel 6 ska medel för elektronisk identifiering under vissa förutsättningar omfattas av ömsesidigt erkännande. Det gäller sådana medel för elektronisk identifiering som är utfärdade inom ramen för ett system för elektronisk identifiering som har anmälts av en medlemsstat och förts upp på en särskild förteckning som offentliggörs av Europeiska kommissionen.

System för elektronisk identifiering ska anmälas till kommissionen enligt ett särskilt förfarande som framgår av artikel 7–9. Där anges vilka system som får anmälas, hur anmälan ska gå till och vilka krav som ställs på de anmälda systemen och de medel för elektronisk identifiering som utfärdas inom dessa.

Enligt eIDAS-förordningen har offentliga organ en skyldighet att erkänna en utländsk elektronisk identitetshandling senast ett år efter att denna publicerats i en för ändamålet avsedd förteckning som förs av EU. Innan en identitetshandling förs upp på förteckningen ska den anmälande medlemsstaten först ha spridit information om identitetshandlingen under en sexmånadersperiod.

Enligt eIDAS-förordningen ska det i varje medlemsstat finnas en nationell nod som har ansvar för trafiken avseende elektronisk identifiering till och från landet. När det gäller trafik till landet är det tillåtet att ha flera mottagande noder men i Sverige finns det för närvarande en nod hos DIGG som sköter den inkommande trafiken. Uppgift om en eID-handling som utfärdats av land X ska således skickas från land X:s nod till den svenska nationella noden. En svensk myndighet eller annan svensk tillhandahållare av en digital tjänst kan kontrollera att det är en godkänd eID-handling via den svenska och den utländska noden. Det är land X som ansvarar för att det är en korrekt utfärdad eID-handling. Land X kan däremot inte ansvara för om det finns en koppling mellan denna eID-handling och en svensk identitetsbeteckning.

3.2 Kommissionens genomförandeförordningar

Som komplement till eIDAS-förordningen finns en rad genomförande-förordningar med mer specificerad information om tekniska krav och definitioner av vissa centrala begrepp.

3.2.1 Unika personidentifieringsuppgifter

Av betydelse för Skatteverkets uppdrag är bland annat kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets

förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Där fastställs vissa tekniska och operativa krav, bland annat minimiuppsättningen av personidentifierings-uppgifter som är unika för en fysisk person. Dessa uppgifter eller attribut är de som kommer att ingå i identitetsintygen från medlemsstaterna när användare från andra medlemsstater vill logga in i svenska digitala tjänster.

Enligt artikel 11 ska en minimuppsättning av personidentifieringsuppgifter som är unika för en fysisk person uppfylla kraven i bilagan vid användning i ett gränsöverskridande sammanhang. I bilagan specificeras att en minimiuppsättning av uppgifter för en fysisk person ska innehålla följande obligatoriska attribut: nuvarande efternamn, nuvarande förnamn, födelsedatum och en unik identitetsbeteckning som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering.

En minimiuppsättning för en fysisk person kan dessutom innehålla ett eller flera av följande attribut: förnamn och efternamn vid födseln, födelseort, nuvarande adress och kön.

3.2.2 Tillitsnivåer

I kommissionens genomförandeförordning (EU) 2015/1502 fastställs bland annat tekniska minimikrav rörande tillitsnivåer. Även kartläggning av nationella tillitsnivåer för anmälda system för elektronisk identifiering ska följa de krav som fastställs i samma förordning. Resultaten av kartläggningen ska anmälas till kommissionen med hjälp av en mall som fastställs i kommissionens genomförandebeslut (EU) 2015/1505.

Enligt Artikel 1, första punkten i kommissionens genomförandeförordning (EU) 2015/1502 ska tillitsnivåerna låg, väsentlig och hög för medel för elektronisk identifiering utfärdade inom ett anmält system för elektronisk identifiering fastställas med hänvisning till specifikationerna och förfarandena i förordningens bilaga.

I artikelns andra punkt klargörs att tillitsnivåerna för medel för elektronisk identifiering specificeras genom att tillförlitlighet och kvalitet fastställs för följande beståndsdelar: inskrivning, hantering av medel för elektronisk identifiering, autentisering samt hantering och organisering. Alla beståndsdelar angående en viss tillitsnivå ska uppfyllas för att motsvara den hävdade tillitsnivån.

Varje beståndsdel består i sin tur av flera delar. För varje del inom varje beståndsdel finns i bilagan till genomförandeförordningen varierande detaljbeskrivningar av vad som krävs för att nå upp till tillitsnivåerna låg, väsentlig och hög.

För att nå upp till tillitsnivå låg krävs för alla delar och beståndsdelar en del säkerhetsåtgärder men ofta räcker det att det kan antas att det som presenteras är riktigt eller att det finns en tillförlitlig källa som styrker påståendet. Tillitsnivå väsentlig kräver detsamma som tillitsnivå låg med påbyggnad av säkerhetsåtgärder såsom ytterligare tillförlitliga källor eller fler processer för att minimera risker. Den högsta tillitsnivån nås genom ännu fler säkerhetsåtgärder. Det kan handla om fotografiskt eller biometriskt identifieringsbevis eller hög kapacitet mot angrepp.

I eIDAS-förordningens Artikel 6 om ömsesidigt erkännande finns de villkor som krävs för att ett medel för elektronisk identifiering (eID-handling) som utfärdats i en annan medlemsstat ska erkännas i den första medlemsstaten. Dels ska eID-handlingen finnas med på kommissionens förteckning (se vidare avsnitt 3.1). Tillitsnivån för eID-handlingen ska motsvara tillitsnivån väsentlig eller hög.

Dessutom ska myndigheten använda tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten.

3.3 Svenska tillitsnivåer

Svenska tillitsnivåer specificeras i Tillitsramverket för Svensk e-legitimation.[2] Skalan för svenska eID-handlingars tillitsnivåer går från 1 till 4 där nivå 4 svarar mot den högsta graden av skydd. Nivåindelningen motsvarar den som används i den internationella standarden ISO/IEC 29115.

Även de svenska tillitsnivåerna kan delas in i beståndsdelar som i sin tur består av flera delar. Beståndsdelarna är:

– Organisation och styrning
– Fysisk, administrativ och personorienterad säkerhet
– Teknisk säkerhet
– Ansökan, identifiering och registrering
– Utfärdande och spärr av eID-handling
– Kontroll av innehavares elektroniska identiteter
– Utställande av identitetsintyg

I tillitsramverket finns varierande detaljbeskrivningar av vad som krävs för att inom varje beståndsdel uppnå tillitsnivåerna 2, 3 och 4.

De vanligaste svenska eID-handlingarna BankID och Mobilt bankID antas uppfylla tillitsnivå 3. Vad det innebär framgår av tillitsramverket. Vid de bedömningar som gjorts har tidigare E-legitimationsnämnden, numera DIGG, ansett att den svenska tillitsnivå 3 håller något högre säkerhetsgrad än eIDAS-förordningens tillitsnivå väsentlig men når inte upp till eIDAS-förordningens tillitsnivå hög. Det innebär att de utländska eID-handlingarna håller minst samma tillitsnivå som de svenska men att säkerheten kan vara något lägre för de som har tillitsnivå väsentlig.

3.4 Kompletterande nationella bestämmelser

Det finns en svensk lag (2016:561) och en förordning (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. De kompletterande bestämmelserna handlar i nuläget enbart om betrodda tjänster och inte om elektronisk identifiering. Regeringen eller den myndighet som regeringen bestämmer ska enligt lagen få meddela föreskrifter dels om vad som krävs av organ för bedömning av överensstämmelse som enligt eIDAS-förordningen ska granska kvalificerade tillhandahållare av betrodda tjänster, dels om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för skapande av kvalificerade elektroniska stämplar. Vidare innehåller lagen bestämmelser om tillsyn, överklagande och avgifter.

Utöver införandet av lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering har det gjorts en rad nödvändiga följdändringar i andra lagar för att anpassa skrivningar och begrepp till eIDAS-förordningen.[3]

Utredningen om nationella digitala tjänster föreslog i sitt slutbetänkande ytterligare kompletteringar i nämnda författningar. Förslagen gällde bl.a.

[2] Tillitsramverk för Svensk e-legitimation, Myndigheten för digital förvaltning, Ärendenr 2018-158.
[3] Prop. 2015/16:72.

lagstiftning om den svenska noden, anmälan av svenska medel för elektronisk identifiering, att DIGG ska vara ansvarig för noden samt att Försvarets radioanstalt ska göra tekniska säkerhetsgranskningar av noden.[4]

3.5 Offentlighet och sekretess

Offentlighetsprincipen innebär att allmänheten ska ha insyn i statens och kommunernas verksamhet. Principen kommer bl.a. till uttryck genom rätten att ta del av allmänna handlingar. Bestämmelser om rätten att ta del av allmänna handlingar finns i 2 kap. tryckfrihetsförordningen.

I OSL finns bl.a. bestämmelser om tystnadsplikt i det allmännas verksamhet och om förbud att lämna ut allmänna handlingar (sekretess). Dessa bestämmelser avser förbud att röja uppgift, vare sig detta sker muntligen, genom utlämnande av allmän handling eller på något annat sätt (1 kap. 1 § OSL).

Enligt 8 kap. 1–2 §§ OSL gäller sekretessen gentemot enskilda och andra myndigheter. Det förekommer situationer när andra myndigheters eller enskildas intresse av att ta del av en sekretessbelagd uppgift väger tyngre än det intresse som sekretessen ska skydda. I OSL finns därför bestämmelser av innebörden att sekretess under vissa förutsättningar inte hindrar att sekretessbelagda uppgifter lämnas till myndigheter eller enskilda. Sekretessregleringen innehåller därför särskilda s.k. sekretessbrytande bestämmelser.

Sekretessbrytande regler finns i 10 kap. OSL och i anslutning till berörda sekretessbestämmelser i de olika avdelningarna i lagen. I vissa fall kan det finnas ett behov av att identifiera den som begär att få ta del av en handling eller uppgift för att kunna bedöma om en sekretessbrytande bestämmelse är tillämpbar.

3.6 Personlig integritet

Någon enhetlig definition av begreppet personlig integritet finns inte i svensk rätt. I 1 kap. 2 § regeringsformen, förkortad RF, föreskrivs att det allmänna ska värna om den enskildes privatliv. Även Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna innehåller sådana bestämmelser, t.ex. artikel 8 om rätt till skydd för privat- och familjeliv.

Av 2 kap. 6 § andra stycket RF framgår att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

3.7 Registerförfattningar och datalagen

Svenska myndigheter har fört register av olika slag sedan lång tid tillbaka. Under 1900-talets andra hälft började sådana register föras i datoriserad form. Redan på 1960-talet började datoriseringens inverkan på samhället debatteras i många länder, så också i Sverige. Debatten och ett antal utredningar ledde fram till införandet av datalagen (1973:289).

Även före datalagen fanns en del registerförfattningar. I huvudsak handlade dock äldre registerlagar om att ett register av visst innehåll skulle föras för att tillgodose något allmännyttigt syfte eller liknande. Syftet i dessa äldre författningar var som regel inte att värna om den enskildes integritet. Vissa äldre

[4] SOU 2017:114, reboot – omstart för den digitala förvaltningen s. 42 ff.

registerförfattningar hade dock enstaka bestämmelser om t.ex. gallring, inhämtande och spridande av uppgifter i register som motiverades av hänsyn till de registrerades integritet.

Genom datalagen sattes fokus på att hindra att hanteringen av ADB-förda personregister medförde otillbörliga intrång i den personliga integriteten. Registrering skulle få förekomma, men det krävdes att vissa regler iakttogs. Lagen var tillämplig inom både den offentliga och privata sektorn och byggde på ett tillståndssystem. Enligt lagens ursprungliga lydelse krävdes – med visst undantag – tillstånd av den då nyinrättade Datainspektionen för att starta eller föra ett personregister med ADB. Detta gällde register hos såväl myndigheter som privata aktörer. Tillståndskravet kom senare att i vissa fall ersättas av ett anmälningsförfarande. Utöver tillstånd förutsattes Datainspektionen meddela föreskrifter om registrets ändamål, vilka personuppgifter som fick ingå samt, vid behov, föreskrifter om bl.a. inhämtandet av personuppgifter, tillåtna ADB-bearbetningar, utlämnande av personuppgifter, bevarande och gallring eller kontroll och säkerhet.

Från datalagens krav på tillstånd undantogs dock personregister vars inrättande beslutats av riksdagen eller regeringen, s.k. statsmaktsregister. Undantaget gällde oberoende av om beslutet om registrets inrättande gavs formen av lag eller annan författning eller kom till uttryck på annat sätt.[5] Innan sådant beslut fattades skulle dock yttrande inhämtas från Datainspektionen. När Datainspektionen avgav ett sådant yttrande skulle en bedömning av registret ske enligt samma grunder som vid prövning av ett tillståndsärende.

Datainspektionen kunde även meddela föreskrifter för registret i den mån riksdagen eller regeringen inte hade gjort det, t.ex. om ändamål eller bevarande och gallring. Dessutom omfattades även statsmaktsregister av Datainspektionens tillsyn enligt datalagen.

Även efter datalagens införande fortsatte datoranvändningen och den personliga integriteten att debatteras i samhället och nya utredningar tog vid. Datalagstiftningskommittén fick 1976 uppdraget att göra en översyn av bl.a. datalagen. Kommittén lämnade flera delbetänkanden. Beträffande statliga register förordade kommittén att dessa var för sig borde regleras genom lagar eller förordningar med, så långt som möjligt, uttömmande föreskrifter om användningen.[6]

Data- och offentlighetskommittén hade senare likartade tankar:

> Vi har övervägt möjligheten att sammanföra alla registerförfattningar under ett paraply. En sådan lösning skulle medverka till enhetlig utformning av lagstiftningen och ge utrymme för såväl behövlig modernisering av befintliga författningar som en ny reglering på de områden där sådan behövs. I en gemensam registerlag blir det emellertid svårt att reglera sådana centrala frågor som de olika registrens ändamål och innehåll. Det är också troligt att en för alla specialreglerade register gemensam registerlag blir alltför svåröverskådlig för att fylla sitt syfte. En möjlighet vore att ge registerlagen karaktären av ramlag och att komplettera med registerförordningar eller föreskrifter från DI [Datainspektionen] för varje enskilt register. En sådan ramlag skulle t.ex. kunna innehålla föreskrifter om vilka frågor som skall regleras i olika registerförfattningar. I princip ger dock datalagen redan vägledning på den punkten. Denna lösning ger också

[5] Prop. 1973:33 s. 97.
[6] SOU 1978:54 s. 110.

riksdagen mindre inflytande än vad som har varit fallet vid tillkomsten av befintliga registerlagar.[7]

Data- och offentlighetskommittén stannade således för att fortsatta särförfattningar var att föredra. Kommitténs överväganden kom att få stor betydelse i den fortsatta framväxten av registerlagstiftningen. Under 1990-talet tillkom allt fler registerlagar.

Det finns i dag ett stort antal olika registerförfattningar. I Informationshanteringsutredningens slutbetänkande Myndighetsdatalag (SOU 2015:39) har i avsnitt 4.2 gjorts en redovisning av utredningens inventering av registerförfattningar.

3.8 Dataskyddsdirektivet och personuppgiftslagen

Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, det s.k. dataskyddsdirektivet, syftade till att garantera dels att en hög skyddsnivå förelåg när det gällde enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter, dels att alla medlemsländerna höll en likvärdig skyddsnivå.

Dataskyddsdirektivet genomfördes i svensk rätt bl.a. genom personuppgiftslagen. Lagen gällde för behandling av personuppgifter om uppgifterna ingick i eller var avsedda att ingå i en strukturerad samling av personuppgifter som var tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Lagen var subsidiär i den meningen att avvikande bestämmelser i annan lag eller i förordning gällde i stället för bestämmelserna i personuppgiftslagen. Sådana avvikande bestämmelser fanns bl.a. i s.k. registerförfattningar, t.ex. lagen om behandling av uppgifter i Skatteverkets beskattningsverksamhet.

3.9 Dataskyddsförordningen och kompletterande svensk rätt

Sedan den 25 maj 2018 ska dataskyddsförordningen tillämpas direkt. Förordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU. Från förordningens tillämpningsområde undantas bl.a. behandling av personuppgifter som utgör ett led i verksamhet som inte omfattas av unionsrätten, som utförs av en fysisk person som ett led i verksamhet av privat natur eller som har samband med dennes hushåll eller som utförs av behöriga myndigheter för ändamålen att förebygga, utreda, upptäcka eller lagföra brott, verkställa straff eller skydda mot och förebygga hot mot allmän säkerhet.

Dataskyddsförordningen baseras till stor del på det tidigare gällande dataskyddsdirektivets[8] struktur och innehåll men innebär även en rad nyheter såsom vissa utökade rättigheter för registrerade. Dataskyddsförordningen både förutsätter och möjliggör kompletterande nationella bestämmelser av olika slag. Enligt artikel 6.2 får medlemsstaterna behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen med hänsyn till behandling som är nödvändig för att utföra en uppgift av allmänt

[7] SOU 1987:31, s.159.

[8] Europaparlamentet och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, det s.k. dataskyddsdirektivet.

intresse eller som led i den personuppgiftsansvariges myndighetsutövning. Enligt artikel 6.3 kan den rättsliga grunden i en medlemsstats författning för en sådan behandling innehålla särskilda bestämmelser om bl.a. de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål.

De grundläggande principer för behandling av personuppgifter som anges i artikel 5 stämmer till den allra största delen överens med tidigare gällande principer. Detta innebär bl.a. att uppgifter ska samlas in för särskilt uttryckliga angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål samt att uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Vidare ska uppgifterna behandlas på ett sätt som säkerställer lämplig säkerhet för dem, inbegripet skydd mot bl.a. obehörig eller otillåten behandling, med användning av lämpliga tekniska eller organisatoriska åtgärder. I dataskyddsförordningen finns också bestämmelser om bl.a. enskildas rättigheter och om skyldigheter för den personuppgiftsansvarige och personuppgiftsbiträden.

I Sverige har det dessutom antagits kompletterande bestämmelser till dataskyddsförordningen. Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning trädde även den ikraft den 25 maj 2018. Författningarna innehåller bland annat bestämmelser om att dataskyddsförordningen med vissa undantag ska gälla även utanför sitt egentliga tillämpningsområde, till exempel i verksamhet som rör nationell säkerhet. Lagen är dock subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i andra registerförfattningar.

Dataskyddslagen förtydligar även under vilka förutsättningar personuppgifter får behandlas med stöd av dataskyddsförordningen. Bland annat kan ett barn som är minst 13 år samtycka till behandling av personuppgifter i samband med användning av informationssamhällets tjänster.

När det gäller personnummer och samordningsnummer får de enligt dataskyddslagen 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. Regeringen får meddela ytterligare föreskrifter om i vilka fall behandling av personnummer och samordningsnummer är tillåten.

Vidare behandlas sanktionsavgifter, begränsning av de registrerades rättigheter samt skadestånd och överklagande. Slutligen anges att dataskyddsförordningen och den nya lagen inte ska tillämpas i den utsträckning det strider mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

3.10 Utlämnande via direktåtkomst

Det finns inte någon legaldefinition av begreppet direktåtkomst. Den grundläggande innebörden anses dock vara att någon har direkt tillgång till information hos någon annan och på egen hand kan söka i uppgiftssamlingen utan att den utlämnande myndigheten måste reagera. Den sökande kan dock inte själv påverka innehållet i informationen.

I begreppet direktåtkomst ligger att den utlämnande myndigheten i det enskilda fallet inte har någon kontroll över vilka uppgifter mottagaren vid ett visst söktillfälle tar del av. Den myndighet som lämnar ut uppgifter fattar med andra ord inte beslut om utlämnande i varje enskilt fall. Prövningen av om ett utlämnande är förenligt med OSL måste därför ske redan då uppgifterna görs tillgängliga genom direktåtkomst, oavsett om någon mottagare vid den tidpunkten tar del av dem. En

bestämmelse om direktåtkomst är inte en sådan sekretessbrytande regel som avses i offentlighets- och sekretesslagen. En förutsättning för att direktåtkomst ska kunna tillåtas är därför att åtkomsten antingen endast avser offentliga uppgifter eller att den avser sådana sekretessbelagda uppgifter som enligt lag eller förordning får lämnas ut till den som har direktåtkomst.

3.11 Annat utlämnande i elektronisk form än genom direktåtkomst

För annat elektroniskt utlämnande än genom direktåtkomst brukar ofta begreppet ”utlämnande av uppgifter på medium för automatiserad behandling” användas. Sådant utlämnande kan exempelvis innebära att elektronisk information överförs via digital post, genom utlämnande av uppgifter på ett flyttbart lagringsmedium – t.ex. flashminne (s.k. USB-minne) – eller genom direkt överföring från ett datorsystem till ett annat. Många författningar om behandling av personuppgifter innehåller bestämmelser som begränsar när uppgifter får lämnas ut på medium för automatiserad behandling.

3.12 Folkbokföring

Skatteverket har ansvaret för folkbokföringen i Sverige. Ett huvudsakligt syfte med folkbokföringen är att samla in och organisera viss grundläggande information om personer i landet, för att dessa uppgifter ska kunna användas i samhället.

Bestämmelser om folkbokföring finns bl.a. i folkbokföringslagen (1991:481) FoL och i lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet (FdbL).

För varje folkbokförd person fastställs enligt 18 § FoL ett personnummer som identitetsbeteckning. Personnumret innehåller födelsetid, födelsenummer och kontrollsiffra. En person som inte är eller har varit folkbokförd får enligt 18 a § FoL tilldelas ett samordningsnummer. Det ska alltså inte vara möjligt att ha både ett person- och ett samordningsnummer. Om en person med samordningsnummer senare blir folkbokförd ska samordningsnumret kopplas samman med det nya personnumret och därefter ska personnumret användas.

Den som avlider eller dödförklaras ska avregistreras från folkbokföringen. Den som kan antas komma att regelmässigt tillbringa sin dygnsvila utom Sverige under minst ett år ska avregistreras från folkbokföringen som utflyttad förutom i vissa undantagsfall. Att man är utflyttad innebär inte att man förlorar sitt personnummer. Personnumret är fortfarande den identitetsbeteckning man ska använda i kontakt med svenska myndigheter om man någon gång har tilldelats ett sådant.

3.12.1 Folkbokföringsdatabasen

Folkbokföringen förs i ett särskilt datasystem, folkbokföringsdatabasen. I folkbokföringsdatabasen finns uppgifter om varje person som är eller har varit folkbokförd. Även uppgifter om personer med samordningsnummer ingår i databasen. Där görs alla registreringar som påverkar folkbokföringen, till exempel vigsel, namnändring eller dödsfall. Uppgifter från folkbokföringsdatabasen lämnas i huvudsak ut genom personbevis (utdrag ur databasen), via aviseringssystemet Navet som utgör en del av folkbokföringsdatabasen eller via ett separat register, det statliga personadressregistret, SPAR.

Uppgifter om personer som har tilldelats samordningsnummer får behandlas i folkbokföringsdatabasen enligt 2 kap. 2 § FdbL. Av 3 § framgår vilka uppgifter som får behandlas i databasen, bland annat namn, födelsetid, medborgarskap, födelseort och adress. I ärenden om tilldelning av bland annat samordningsnummer får även anges grunden för tilldelningen och de handlingar som har legat till grund för identifiering samt om det råder osäkerhet om personens identitet enligt 3 § tredje stycket.

Navet är Skatteverkets system för distribution av folkbokföringsuppgifter. Via Navet sprider Skatteverket maskinellt folkbokföringsuppgifter till andra myndigheter. Navet får i första hand användas av statliga och kommunala myndigheter för aktualisering, komplettering och kontroll av personuppgifter. Navet uppdateras kontinuerligt när uppgifter registreras i folkbokföringsdatabasen. Navet innehåller samtliga personer som är eller har varit folkbokförda eller av annan anledning har tilldelats personnummer eller samordningsnummer. För personer med samordningsnummer redovisas samordningsnummer (inklusive födelsetid och kön), namn, adress i Sverige, medborgarskap och födelseort (och land) samt om dessa uppgifter är styrkta eller inte. Det finns också hänvisningsnummer vilket innebär att för de personer som har bytt personnummer eller samordningsnummer anges tidigare person- eller samordningsnummer.

De uppgifter som lämnas ut från Navet har alltid samma innehåll och format. Vilka uppgifter som aviseras beror på vilket lagstöd respektive myndighet har för att ta emot uppgifter. Hur uppgifterna sedan hanteras hos mottagarna varierar mycket, såväl vad avser vilka uppgifter som tas om hand som hur de presenteras för användaren. Varje myndighet är ansvarig för sina egna personregister. Det innebär att det är myndigheten själv som, utifrån sina verksamhetsbehov, bestämmer vad som ska presenteras för användarna.

4 Offentlig sektors behov och förväntade nytta av kopplingstjänsten

Om en myndighet tillhandahåller en digital tjänst som kräver eID-handling för att komma in och där myndigheten behöver kunna klarlägga att användaren är identisk med innehavaren av en viss identitetsbeteckning, finns ett problem om användaren identifierar sig med en utländsk eID-handling. Personen har identifierat sig men eID-handlingen kommer inte att i sig ge någon koppling till en svensk identitetsbeteckning. Med enbart eID-handlingen kommer användaren att kunna autentiseras av myndigheten men det krävs något mer för att göra kopplingen till den svenska identitetsbeteckningen och därmed ge förutsättningen för att användaren också ska kunna använda tjänsten. Det ytterligare steget kan vara utformat på olika sätt. En avgörande faktor för vilka sätt som kan vara godtagbara för en viss tjänst är vilken nivå på säkerhet som behövs för att godta att sökanden är identisk med innehavaren av en viss identitetsbeteckning.

Den enklaste nivån är att myndigheten kan godta sökandens påstående om att denne har en viss identitetsbeteckning. För det alternativet krävs endast att användaren får möjlighet att lämna uppgiften i tjänstens gränssnitt.

Ett alternativ är att användaren får lämna uppgift om svensk identitetsbeteckning i gränssnittet och att en kontroll av uppgifterna i eID-handlingen (namn och födelsetid) görs mot motsvarande uppgifter i den svenska folkbokföringen. Det ger en större säkerhet för att det råder identitet men lämnar samtidigt utrymme för att det rör sig om två olika personer med samma namn och födelsetid.

Ett tredje alternativ är att genomföra en mer utförlig kontroll av att det råder identitet mellan innehavaren av eID-handlingen och innehavaren av den svenska identitetsbeteckningen. Sådana kontroller behöver vara på samma nivå som för utfärdande av en id-handling om säkerhetsnivån ska upprätthållas.

Dessa frågor har betydelse för att bedöma vilket behov av en central kopplingstjänst som olika myndigheter har. Skatteverket gjorde inför rapporten 2016 en kartläggning av de mest berörda myndigheternas behov av en sådan kopplingstjänst. Genomgången gjordes ur myndigheternas perspektiv.

Inför denna rapport har myndigheterna på nytt fått möjlighet att komplettera med nya uppgifter som kan ha framkommit sedan 2016.

4.1 Arbetsförmedlingen

Efter inskrivning hos Arbetsförmedlingen måste den arbetssökande inom fem dagar boka ett fysiskt möte och besöka ett Arbetsförmedlingskontor för att visa att man är aktivt arbetssökande. Eftersom den sökande ändå måste visa upp sig fysiskt inom fem dagar är behovet av kopplingstjänst inte så stort i detta skede.

De behov som Arbetsförmedlingen ser av en kopplingstjänst hänger främst samman med den övriga inskrivningsprocessen när en arbetssökande ska lägga in sina meriter eller åter anmäla sig till Arbetsförmedlingen efter att ha varit utskriven en period. En kopplingstjänst skulle även kunna komma till användning vid olika digitala tjänster där man behöver identifiera sig hos en handläggare, t.ex. på ”Min sida” som är en handlingsplan mellan Arbetsförmedlingen och den arbetssökande.

För arbetssökande inom Öresundsregionen och vid gränserna mellan Sverige, Norge och Finland kan en kopplingstjänst bli intressant. Det rör människor som kan tänka sig att komma till Sverige och arbeta och där processen skulle kunna underlättas av att kopplingstjänsten finns.

En annan grupp som kan tänkas ha behov av kopplingstjänsten är arbetsgivare som vill kunna skapa annonser för att kunna ansöka om arbetsgivar- eller anställningsstöd, svenska arbetsgivare i andra EU-länder som vill anställa svenskar bosatta i dessa länder samt tillhandahållare av arbetsmarknadsutbildningar och andra tjänster som kräver att man har eID-handling för att kunna upprätta gemensamma utbildningsplaner med arbetssökande. Dessa aktörer utgörs dock främst av juridiska personer och omfattas därför inte av den kopplingstjänst som nu utreds.

De digitala tjänster som finns hos Arbetsförmedlingen i dag är uppdelade i två kategorier, de som kräver eID-handling och de som kräver användarnamn och lösenord. För att kunna registrera t.ex. en meritförteckning behövs bara användarnamn och lösenord men för att kunna ta del av egna uppgifter krävs eID-handling. Det innebär pedagogiska svårigheter att förklara övergången från lägre till högre nivå av säkerhet för användarna. Därför vill Arbetsförmedlingen se över om man ska begära eID-handling i alla tjänster istället.

Arbetsförmedlingen har svårt att uppskatta volymer för det framtida behovet av kopplingstjänst eftersom lösningen inte finns i dag. Om en lösning fanns så skulle den kanske användas i större omfattning än man kan tro nu. Volymerna kan öka bara tack vare att tillgängligheten ökar om digitala vägar används mer.

För att en kopplingstjänst ska vara användbar måste kopplingen hålla samma säkerhetsnivå som de svenska eID-handlingarna gör i dag, dvs. nivå 3. Om kopplingen inte kan komma upp i samma nivå är det bättre att bara använda eIDAS-förordningen direkt. Man får då använda sin utländska identitet i eID-handlingen istället, utan koppling till sin svenska identitetsbeteckning. Arbetsförmedlingen kan tänka sig att förlita sig till den ”egna relationen” med sina kunder utan ett centralt kopplingsregister i framtiden. Det skulle i så fall leda till att man tvingas hålla ett eget litet kopplingsregister men det ser man inte som så problematiskt eftersom man ändå inte kan förlita sig till fullo på svenska identitetsbeteckningar.

4.2 Centrala Studiestödsnämnden (CSN)

CSN ser både behov och nytta av en kopplingstjänst. Myndigheten vill kunna knyta ärendebehandlingen till personnummer och man ser effektivitetsvinster i minskad pappershantering.

Myndigheten har många digitala tjänster som fungerar antingen med eID-handling eller med pinkod. CSN jobbar aktivt för att öka användandet av eID-handling samt att utveckla digitala tjänster.

CSN:s verksamhet (kärnverksamheten) är uppdelad i tre delar – kundmötesavdelningen, utbetalningsavdelningen och inbetalningsavdelningen. Kundmötesavdelningen ansvarar bland annat för ansökan om studiemedel på webben (Mina Sidor). Utbetalningsavdelningen ansvarar i huvudsak för prövningen av ansökningar om studiestöd. Om man vill ansöka om studiemedel kan man i dag göra det elektroniskt och man kan då använda svensk eID-handling eller pinkod. En ansökan om studiehjälp sker via fysisk blankett. År 2015 inkom 72 000 ansökningar om studiemedel från utländska medborgare. Samma person kan skicka mer än en ansökan. Antal utländska personer som ansökte om studiemedel år 2015 var ca 40 000. Av dessa var ca 22 500 från en EU- eller EES-stat. Ungefär hälften av ansökningarna signerades med svenska eID-handlingar. Många av de utländska studenterna är folkbokförda i Sverige och har därför möjlighet att få en svensk eID-handling.

När det gäller återbetalning finns det också digitala tjänster som kan bli aktuella för personer som har studerat i Sverige men därefter flyttat utomlands. Det handlar om att flytta förfallodagar, ändra betalningsintervall, betalningssätt eller adress. Antalet svenska medborgare som den 31 augusti 2016 var bosatta utomlands med en studieskuld var 65 790 personer. Av dessa bodde drygt 40 000 i EU- eller EES-stater och skulle kunna ha tillgång till en eID-handling.

CSN är angelägna om att uppgifter om registrerade kopplingar ska gå att spåra under lång tid som del i myndighetens skuldsäkring av studielån. Återbetalningstiden för studieskulder är upp till 25 år eller mer och myndigheten kan därför behöva tillgång till gamla uppgifter långt efter att de inte längre gäller.

CSN har 2018 kompletterat med att myndigheten fortfarande har behov av ett kopplingsregister eftersom deras digitala tjänster är byggda på att deras kunder har svenska person- eller samordningsnummer. CSN anser att det finns säkerhetsproblem med samordningsnummer och har inga invändningar mot att de i nuläget inte ska kunna kopplas till utländska eID-handlingar. CSN ser dock behov av att samordningsnummer ska ingå i tjänsten på sikt.

4.3 Datainspektionen

Datainspektionen har inga digitala tjänster som kräver eID-handling och saknar därför behov av en kopplingstjänst för sina användare. I sin roll som tillsynsmyndighet lyfter Datainspektionen fram ett antal synpunkter, t.ex. att person- och samordningsnummer ska användas i så liten utsträckning som möjligt av integritetsskäl. När de aktuella digitala tjänsterna utvecklas krävs det att analyser har genomförts i förhållande till dataskyddsförordningen innan de digitala tjänsterna träder i kraft.

Datainspektionens inställning är att svenska person- och samordningsnummer inte bör kopplas direkt till eID-handlingar från hela EU. Om det blir aktuellt att använda ytterligare attribut för eID-handlingar genom överenskommelser med andra medlemsstater, måste det även här genomföras analyser hur detta förhåller sig till dataskyddsförordningen. Datainspektionen har upparbetade samarbetsformer med tillsynsmyndigheter i andra länder i frågor som berör dataskyddsförordningen.

Datainspektionen har 2018 kompletterat med att de är positivt inställda till att Skatteverket gör en förnyad och fördjupad bedömning av personuppgiftsbehandlingen i det föreslagna kopplingsregistret. När nya författningar tas fram, krävs det att konsekvenserna för den personliga integriteten vid personuppgiftsbehandling analyseras. En sådan analys ska svara på frågan om förslaget är förenligt med reglerna om skydd för den personliga integriteten i grundlagarna och EU-rätten. En förutsättning för detta är en noggrann kartläggning och beskrivning av den föreslagna personuppgiftsbehandlingen och en utredning av vilka konsekvenser för den personliga integriteten behandlingen medför eller kan medföra.

4.4 eHälsomyndigheten

eHälsomyndigheten har få egna digitala tjänster men det finns andra aktörer som har digitala tjänster mot eHälsomyndighetens bastjänst. eHälsomyndighetens aktuella digitala tjänster är Hälsa För Mig, MinFörskrivning, Läkemedelskollen och leverantörsportalen till VARA-registret. Bastjänsterna till receptregistret fungerar

för utländska användare redan i dag, men i och med eIDAS-förordningen finns möjlighet att stärka upp säkerheten genom inloggning med utländsk eID-handling.

VARA-registret innehåller alla läkemedel samt de handelsvaror som kan förskrivas inom förmånen. Det kommer att finnas behov för svenska och utländska företag att kunna logga in och fylla på med information i leverantörsportalen till VARA-registret. Det råder inga höga autentiseringskrav i dag men eIDAS-förordningen skulle kunna underlätta hanteringen om man i framtiden kan kräva inloggning av företrädare med eID-handling. Vidare finns det vinster för läkemedelsföretag om alla myndigheter som de har kontakt med använder samma mekanism för inloggning. I dag loggar företrädare in med användarnamn och lösenord.

Behov av identifiering finns även för läkare, sjuksköterskor och farmaceuter som bor i annat land. De behöver identifiera sig för att få del av information om en viss patient. Den digitala tjänsten MinFörskrivning innebär att läkare kan jämföra sin förskrivning mot hur andra läkare skriver ut recept. Även verksamhetschefer kan göra jämförelser av hur läkare på en enhet skrivit ut recept.

Inom vården kan det finnas behov som inte är knutna till eHälsomyndigheten. Mina vårdkontakter är en sådan tjänst som kan vara aktuell om en utländsk patient till exempel vill boka möte med svensk läkare. I dag finns möjlighet att logga in med svensk eID-handling alternativt via personnummer och lösenord.

Receptregistret är en databas med tillhörande bastjänster till vilken vårdgivaren via journalsystem skickar in ett recept och därefter kan kunden hämta ut läkemedel via apoteken. Det krävs personnummer för den som ska hämta ut läkemedel. Den som inte har personnummer får till vårdgivaren ange födelsedatum och vilket apotek man ska plocka ut läkemedel från. Lösningen upplevs som osäker. Att kunna hantera andra personliga ID-handlingar (t.ex. pass och passnummer) är ett sätt att säkra hanteringen.

Inom ramen för en EU-finansieringsmekanism (CEF) pågår arbete för att tillgängliggöra digitala recept och patientöversikt till medborgare som vistas utomlands. Sverige planerar att tillgängliggörande av svenska e-recept ska ske via en så kallad nationell kontaktpunkt (NCP). Även här kan det komma att finnas digitala tjänster som påverkas av eIDAS-förordningen.

4.5 Försäkringskassan

Försäkringskassan har huvudsakligen relation med personer som omfattas av svensk socialförsäkring. Det finns ett begränsat antal situationer där personer är bosatta i en annan EU- eller EES-stat, har svensk identitetsbeteckning, och har en relation med Försäkringskassan.

Det kan gälla familjemedlemmar till utländska personer som arbetar i Sverige. Familjemedlemmarna kan ha rätt till sjukvård i hemlandet men den ska betalas av Sverige. Dessa personer kan i dag inte komma åt sin information elektroniskt. Det kan också gälla svenskar som arbetar utomlands och som är sjukskrivna mer än 14 dagar. I den situationen lämnar den utländska arbetsgivaren en sjukanmälan. För att komma åt informationen skulle en företrädare för arbetsgivaren kunna logga in med sin utländska eID-handling. En annan grupp som kan bli aktuell är utländska doktorander i Sverige som kan omfattas av svensk socialförsäkring. Ytterligare ett exempel är familjer där en part arbetar i annan EU- eller EES-stat och partner eller barn bor i Sverige.

I alla nämnda situationer handlar det om väldigt små volymer som skulle bli aktuella för att använda sig av en kopplingstjänst men det finns grupper inom Försäkringskassans verksamhet som kan ha nytta av tjänsten.

I komplettering 2018 anger Försäkringskassan att även om nyttan med gränsöverskridande identifiering är uppenbar är riskerna och utmaningarna betydande. De problem som finns enbart i en svensk kontext med svenska lösningar blir exponentiellt större i ett internationellt perspektiv. Försäkringskassan bedömer att genom att avgränsa Skatteverkets utredningsuppdrag till kopplingsregistret och inte hela processen och ekosystemet riskerar allvarliga risker och problem att inte analyseras. Uppdraget innehåller en analys av sekretessbestämmelser och sekretess i själva kopplingsregistret men Försäkringskassan bedömer att denna granskning inte ska avgränsas till bara kopplingsregistret utan behöver omfatta den fulla processen från utfärdande av eID-handling till avregistrering av koppling.

4.6 Migrationsverket

Inom Migrationsverkets kategorier av ärenden finns olika behov av en kopplingstjänst. När det gäller asylansökningar är behovet inte stort eftersom de inte kan lämnas eller kompletteras genom någon digital tjänst. Det är inte heller aktuellt att utveckla någon sådan digital tjänst.

En ärendekategori som kan bli aktuell är vissa ansökningar om arbetstillstånd. Det rör sig om regler inom EES-regelverket där tredjelandsmedborgare som har status som varaktigt bosatta i ett EU-land kan ansöka om uppehållstillstånd för att t.ex. arbeta i Sverige. Där utvecklas digitala tjänster nu och identifieringen sker i dag med pinkod. Det rör i dag drygt 100 ansökningar per år men av dessa saknas vetskap om hur många som eventuellt skulle ha tillgång till en eID-handling från något annat medlemsland.

Med arbetstillstånden följer även arbetsanhöriga. Detta rör sig om tredjelandsmedborgare, som är anhöriga till en EU-medborgare som kommer till Sverige i enlighet med reglerna för den fria rörligheten, t.ex. för att arbeta. Dessa anhöriga ska ansöka om ett s.k. uppehållskort. Detta är en kategori som kan komma att bli aktuella för framtida digitala tjänster. Det handlar i dagsläget om 1 800 ansökningar per år. Av dessa kan åtskilliga ha utländska eID-handlingar.

Migrationsverket är skeptiskt inställt till en gemensam kopplingstjänst. Det finns farhågor om att det kan komma att innebära en onödig komplexitet, i synnerhet med ett centralt kopplingsregister, som inte är jämförbart med någon annan verksamhet i Sverige.

De digitala tjänsterna riskerar att få en eIDAS-nivå och en svensk nivå. Diffusa tillitsnivåer leder till tillitsproblem mellan myndigheterna. Man kommer inom varje myndighet att behöva avgöra vilken tillitsnivå som krävs för varje digital tjänst. Migrationsverket kommer sannolikt själva att utveckla en egen kopplingstjänst där den digitala tjänsten eller myndigheten själva gör en jämförelse med uppgifter i Navet.

Migrationsverket anser sig tillämpa tillitsnivå 4 när det gäller asylsökande eftersom de då kräver personlig inställelse. När en person fått en svensk eID-handling och ska kunna nyttja digitala tjänster räcker dock nivå 3. Migrationsverket går mot allt högre säkerhetsnivåer efter rekommendationer från MSB. Informationssäkerheten blir bättre även om det innebär att det blir svårare och trögare för användaren.

I komplettering 2018 anger Migrationsverket att deras synpunkter mot ett kopplingsregister kvarstår. Samtidigt anges när det gäller kostnader kring införande av ett eventuellt kopplingsregister att Migrationsverket förutsätter att det kommer att tas fram en förvaltningsgemensam tjänst för detta ändamål. Migrationsverket har inget att erinra mot att utländska eID-handlingar inte kopplas till styrkta samordningsnummer.

4.7 Myndigheten för samhällsskydd och beredskap (MSB)

MSB har inga digitala tjänster som kräver eID-handlingar och har därför inte något eget behov av en kopplingstjänst. Genom sitt uppdrag inom cybersäkerhet och skydd av samhällsviktig verksamhet har myndigheten ändå synpunkter på en sådan funktion.

Det grundläggande skälet för en myndighetsgemensam lösning är kostnadseffektivitet. Det blir dyrare om varje myndighet ska bygga upp en egen lösning för att hantera utländska eID-handlingar.

Säkra sätt att bygga upp ett kopplingsregister kan vara genom att personen inställer sig fysiskt på en ambassad eller ett konsulat och legitimerar sig innan man kopplar eID-handlingen till ett personnummer eller styrkt samordningsnummer. Man kan även, i förekommande fall, koppla en befintlig svensk eID-handling till en utländsk eID-handling.

Skatteverket har under utredningstiden 2018 träffat MSB och diskuterat informationssäkerhetsaspekter samt gått igenom de tänkta tekniska lösningar som Skatteverket arbetar med. De risker MSB ser handlar om att nyttja systemet för att skapa sig fördelar i samhället eller ekonomisk vinning (gentemot olika myndigheter t.ex. CSN m.fl.) penningtvätt, finansiering av terrorism, främmande makt, social engineering.

4.8 Pensionsmyndigheten

Många pensionärer och pensionssparare bor utomlands och har behov av att kunna använda Pensionsmyndighetens digitala tjänster. Det finns cirka 345 000 personer som får ett orange kuvert som är utlandsbosatta och någon gång arbetat i Sverige och tjänat in till allmän pension och kan ha ett intresse av fondbyten och pensionsprognoser. Det kräver eID-handling. När det gäller fondbyten finns det även ett förfarande via blankett fortfarande men man funderar på att avsluta den möjligheten.

Pensionsmyndigheten upplever att det största hindret i dag för de utlandsbosatta är kravet på eID-handling. Det är svårt att få en svensk eID-handling då BankID förutsätter personlig inställelse för utfärdandet. Pensionsmyndighetens digitala tjänster är knutna till inloggning med personnummer.

Myndigheten har årlig kontakt med ca 160 000 utlandsbosatta personer med svensk pension för att säkerställa att pensionärerna lever. I dag skickar Pensionsmyndigheten uppgifter på papper, s.k. levnadsintyg, till ca 60 000 av dessa personer. Därefter krävs personlig inställelse vid en myndighet eller liknande där någon intygar personens identitet och undertecknar intyget som sedan skickas tillbaka till Pensionsmyndigheten. Viss infrastruktur för sådan personlig inställelse finns utbyggd genom att man använder sig av ambassader, konsulat, svenska

kyrkan, notarius publicus, utländska socialförsäkringsinstitutioner, polismyndighet eller någon annan registerförande myndighet.

De övriga ca 100 000 löses genom elektroniskt informationsutbyte med pensionsinstitutionen i bosättningslandet ex med de nordiska länderna och med Tyskland.

Ett antal utlandsbosatta som uppnår pension utomlands behöver kunna hanteras i samband med att de ska få ut sin pension. Ansökan sker via det land de bor i om det är ett EU land. Ansökan sker manuellt och handläggningen likaså, bland annat ställs kontrollfrågor beträffande t.ex. födelsetid, ort, vilket namn föräldrarna hade innan de gifte sig osv. för att säkerställa identiteten.

Pensionsmyndigheten välkomnar möjligheten att kunna använda utländska eID-handlingar. För deras kundgrupper finns det ett stort behov. Ett kopplingsregister vore bra men det måste hålla hög säkerhet.

Användarbarhetsaspekten får inte undervärderas. Det är viktigt att användare inte ”faller mellan stolarna”. Om kopplingarna inte sker centralt finns det risk för att myndigheter gör olika bedömningar som leder till att användare kommer åt vissa myndigheters digitala tjänster men inte andra. Synpunkter kommer ibland från främst svenskar i Norge som klagar på att det inte går att använda norska eID-handlingar. Det är redan en pedagogisk utmaning att förklara varför det inte fungerar.

I komplettering 2019 anger Pensionsmyndigheten att det vore mycket bra om Skatteverket har ansvar för att förvalta och utveckla registret även om man gärna ser ett samarbete avseende kravställning på uppbyggnad och innehåll. Pensionsmyndigheten nämner även behovet av analys av hur befintliga digitala eller maskinella informationsutbyten kan användas och vidareutvecklas samt hur säkerhetsnivån kan höjas för utlandsmyndigheternas hantering av t.ex. levnadsintyg.

4.9 Skatteverket

Skatteverkets verksamhet rör en rad olika aspekter av frågan om behov av en kopplingstjänst mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Personer som varit bosatta här men som lämnat Sverige och inte längre har någon giltig svensk eID-handling kan fortfarande i vissa fall vara skattskyldiga här och ha behov av att kunna använda sig av Skatteverkets digitala tjänster. De kan förutom att deklarera inkomster även äga fastighet eller ha behov av att anmäla deklarationsombud. Många av dessa personer kan deklarera papperslöst med hjälp av koder via telefon eller via sms och behöver inte använda digitala tjänster med eID-handling. År 2018 var det dock drygt 15 000 personer bosatta inom EU- eller EES-stater som, bland annat på grund av att de behövde lämna en deklarationsbilaga, inte kunde deklarera via telefon eller sms och som därför deklarerade på papper. Om dessa personer har en utländsk eID-handling skulle de i stället kunna deklarera via Skatteverkets digitala tjänster.

Personer som arbetar i Sverige utan att vara folkbokförda här tilldelas normalt ett samordningsnummer för beskattningsändamål. Skatteverket tilldelar varje år omkring 30 000 samordningsnummer på uppdrag av den egna beskattnings-verksamheten. De flesta av de personer som får ett sådant till följd av tillfälligt arbete i Sverige kan antas komma från EU- och EES-stater eftersom fri rörlighet för arbetstagare råder inom detta område. Som beskrivs senare (avsnitt 6.2) anser Skatteverket inte att utländska eID-handlingar bör kopplas till

samordningsnummer i nuläget men om samordningsnummersystemet stramas upp och säkerheten vid tilldelning höjs kan skattskyldiga med samordningsnummer på sikt vara en grupp som kommer att kunna ha nytta av en kopplingstjänst.

Utländska fastighetsägare är en kundgrupp med sannolikt behov av en kopplingstjänst för sina kontakter med t.ex. kommuner. De flesta utländska fastighetsägare har ännu inte någon svensk identitetsbeteckning men de har starka behov av att kunna sköta sina åtaganden genom att använda utländsk eID-handling eftersom det ofta handlar om att de äger ett fritidsboende i Sverige och tillbringar stor del av tiden utomlands.

Företrädare för bolag kan ha behov av att logga in i digitala tjänster med eID-handling utfärdad i annat EU-land. Det är svårt att uppskatta hur stor andel av dem som har svenska identitetsbeteckningar.

Det finns förmodligen behov av en kopplingstjänst för användarna av de digitala tjänsterna Kassaregister och Personalliggare bygg, dock är det oklart vilken omfattning och vilka volymer som kan vara aktuella.

Kassaregisterbestämmelserna omfattar sedan maj 2017 även utländska torg- och marknadshandlare som kan behöva logga in med sina utländska eID-handlingar.

När det gäller den digitala tjänsten Personalliggare bygg kan det förekomma utländska byggherrar med utländska anmälare som kan vilja logga in med utländska eID-handlingar. Med utländska företag avses i sammanhanget de företag som inte har svenskt organisations- eller personnummer.

En kategori där säkerheten skulle kunna höjas avsevärt med hjälp av användning av utländska eID-handlingar är digitala tjänster utan krav på eID-handling som t.ex. rot- och rutavdrag. Om man inte är folkbokförd i Sverige och därför inte kan få svensk eID-handling och har utfört rot- eller rutarbete får man i dagsläget begära utbetalning genom en blankett som skickas till Skatteverket. Personen som begär utbetalningen kan då inte identifieras på annat sätt än genom sin underskrift. Möjligheten till användning av utländska eID-handlingar innebär en välkommen säkerhetshöjning.

4.10 Sveriges kommuner och landsting (SKL)

Skatteverket har träffat företrädare för SKL som i sin tur har stämt av med flera kommunförbund och andra för att försöka identifiera behovet av en kopplingstjänst hos de myndigheter som de representerar. Vid dessa kontakter har sammanfattningsvis följande synpunkter lämnats.

När det gäller vårdsektorn är de flesta digitala tjänster reserverade för invånare i Sverige. Inom vården används dessutom andra nummersystem när identiteten inte är känd, s.k. reservnummer, som inte är unika och inte omfattas av uppdraget. Det är därför svårt att se behovet av en kopplingstjänst mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Inom viss skolverksamhet kan man tänka sig att det kan finnas behov för föräldrar som bara har en utländsk eID-handling och vill kunna logga in i skolornas system för att få tillträde till information om sitt barns skolgång. I dessa fall torde det dock inte vara nödvändigt för skolorna att koppla samman förälderns identitetsbeteckning med deras utländska eID-handling.

En grupp användare som skulle ha nytta av att kunna logga in i svenska kommuners digitala tjänster är utländska fastighetsägare. De kan tänkas ha behov av att ansöka om bygglov samt ordna med sophämtning, anslutning till fiber och andra kommunala tjänster som har med fastighetsägandet att göra. Ett problem är att utländska fastighetsägare i Sverige inte har svenska identitetsbeteckningar i dag.

På längre sikt kommer det för kommunala digitala tjänster som ger service åt utländska fastighetsägare att finnas behov av en kopplingstjänst mellan den utländska eID-handlingen och svensk identitetsbeteckning.

Det finns andra digitala tjänster hos kommuner där det kan bli fråga om att användare med utländska eID-handlingar vill logga in. Det kan röra sig om ansökan om förskoleplats, ansökan om gymnasieplats, bokning av idrotts- och fritidsanläggningar men det är än så länge ganska vagt definierat och man ser inte någon anstormning av användare inom dessa kategorier.

SKL har kompletterat 2018 och anger att det som är avgörande för om ett kopplingsregister kan realiseras eller inte, är hur kopplingen ska utföras på ett säkert sätt så att rättsverkan kan uppnås och att det inte öppnar upp för identitetsstölder.

SKL lyfter även problemet med att nummerserierna för både person- och samordningsnummer inte räcker till för de inhemska behoven.

4.11 Transportstyrelsen

Transportstyrelsen hanterar flera skilda verksamheter med olika målgrupper som alla har sina respektive nyttor och behov av möjlighet till inloggning med utländska eID-handlingar. Transportstyrelsen har ca 50 digitala tjänster som kräver autentisering. Beroende på den digitala tjänstens syfte, nivå på informationssäkerhet och vilka användare den riktar sig till erbjuds olika inloggningsalternativ. Exempel är CAPTCHA, användarnamn och lösenord, organisationsnummer och PIN-kod eller eID-handling i olika former. För vissa tjänster erbjuds olika nivåer på autentisering men den digitala tjänstens funktioner kan då vara begränsade om användaren väljer den lägre nivån. Exempel är vissa digitala tjänster där ägaren kan hantera sina fordon genom autentisering via eID-handling, men där också begränsad funktionalitet erbjuds om användaren väljer autentisering genom fordonets registreringsnummer tillsammans med behörighetskod från registreringsbeviset.

Inom yrkestrafik på väg finns bl.a. digitala tjänster för ansökan om olika personliga yrkesbehörigheter och färdskrivarkort, ansökan om olika trafiktillstånd och digitala tjänster för att hantera anmälningar inom sitt tillstånd. För privatpersoner tillhandahålls flera olika digitala tjänster inom körkortsområdet. För utbildningsanordnare inom dessa båda områden finns digitala tjänster för att rapportera genomförda utbildningar.

Transportstyrelsen har viss utbildningsverksamhet där digitala tjänster förekommer när en elev har utfört vissa delar i en utbildning och detta ska rapporteras in till Transportstyrelsen

För fordonsägare finns det möjlighet att ta del av skulder kopplade till fordonet. När det gäller intag av trängselskatt och infrastrukturavgift för utländska förare med utlandsregistrerade bilar finns i dag en lösning med en upphandlad tredjepartsleverantör som spårar det utländska fordonet och kontaktar folkbokföringsmyndigheten i det andra landet för att komma i kontakt med föraren eller fordonsinnehavaren. När det gäller t.ex. trängselskatt är det viktigt att man kan identifiera rätt person, det får inte vara möjligt att kunna ta del av annan persons trängselskatter.

Inom luftfart finns i dag endast öppna digitala tjänster, dvs. inga som kräver autentisering, men det pågår utvecklingsarbete.

Inom sjöfart finns olika digitala tjänster som riktar sig till t.ex. sjömän, redare och läkare. Exempel är att sjömannen kan ansöka om olika behörigheter, läkare kan hantera och rapportera in läkarintyg, skolor rapporterar in godkända

utbildningar. Sjömän ansöker t.ex. via digitala tjänster om att få vistas i maskinrum, vistas på fartyg, framföra fartyg, ansöka om sjömansböcker samt intyg om tjänstgöring. För vissa digitala tjänster erbjuds både eID-handling och användarnamn och lösenord, för andra digitala tjänster erbjuds enbart användarnamn och lösenord.

Transportstyrelsen har tagit fram praktiska lösningar för att de digitala tjänsterna ska fungera för alla men användarna borde egentligen i fler fall använda eID-handling. Därför kommer det att underlätta och stärka säkerheten med möjlighet att logga in med utländska eID-handlingar

Möjlighet till en kopplingstjänst mellan utländska eID-handlingar och svenska identitetsbeteckningar kan bli användbart för svenska fordonsägare i andra länder som behöver kunna ta del av sina uppgifter, men det kan även handla om utländska medborgare i Sverige. Det kommer sannolikt krävas en hel del analys om hur detta kan hanteras med hjälp av eIDAS-förordningens möjligheter till inloggning med utländska eID-handlingar. Frågorna är mycket komplexa.

Transportstyrelsen har 2018 kompletterat och anger att nyttan med kopplingsregistret kommer att bli mycket begränsad för Transportstyrelsens del om man inte kopplar samman utländska eID-handlingar med samordningsnummer. Samtidigt delar Transportstyrelsen uppfattningen att säkerhetsaspekten måste väga tyngst i detta sammanhang. Transportstyrelsen utgår dock ifrån att Skatteverket samtidigt arbetar vidare med frågan om samordningsnummer för att kopplingsregistret inom en inte alltför avlägsen framtid även ska kunna hantera sådana.

4.12 Tullverket

Tullverkets behov av koppling av utländska eID-handlingar till svenska identitetsbeteckningar är svårt att avgöra. Det vanliga när det gäller Tullverkets verksamhet är att utländska företag har ett svenskt ombud i Sverige som omhändertar hela eller delar av processen. Mycket av tullhanteringen är redan i dag elektronisk men sker då maskin till maskin. Tullverket har ett behörighetsregister över företrädare för bolag. Företagen administrerar själva vem eller vilka som får företräda ett specifikt bolag

Tullverket har i dag inte några digitala tjänster som kräver inloggning med eID-handling. Dock har Tullverket digitala tjänster som kräver inloggning med en egen tvåfaktors autentisering baserad på användar-ID och lösenord samt ett sms med OTP (one time pincode).

Tullverket avser att gå över mot nyttjandet av eID-handling dels av serviceskäl, dels av effektivitetsskäl då det kan minska administration och kostnader på sikt genom att nyttja en redan genomförd identifieringsprocess i stället för att själva ansvara för denna.

Tullverket är med i ett EU-projekt som heter UUM&DS och som syftar till att näringslivet ska kunna nyttja EU-centrala tjänster baserat på en nationell inloggning och behörighet. I Sverige administreras och hanteras den nationella delen av Tullverket. UUM&DS är kompatibel med eIDAS-förordningen.

Från Tullverkets perspektiv är en digitalt säkerställd koppling mellan fysisk och juridisk person av stort intresse, för att kunna identifiera en initial företagsadministratör som sedan ansvarar för att dela ut behörighet till andra fysiska personer.

4.13 Universitets- och högskolerådet (UHR)

Universitets- och högskolerådet har inget stort behov av en kopplingstjänst i dag men det skulle kunna fungera som en säkerhetshöjare i framtiden. I nuläget har man bedömt att det räcker med användarnamn och lösenord eller pin- och aktiveringskod.

Utlandssvenska studenter med personnummer är en grupp som skulle kunna ha behov då de inte kan få aktiveringskod skickad. Det handlar om små volymer, ca 500 personer per år som i dag hanteras manuellt. En framtida kopplingstjänst skulle underlätta hanteringen och vara till hjälp istället för den manuella hantering som sker i dag. Om tio år är behovet sannolikt större, bland annat med anledning av ökade strömningar av människor som väljer att studera och bo på nya platser.

Universitets- och högskolerådet följer SUNETs[9] riktlinjer när det gäller informationssäkerhet på internet. När studenten skriver in sig vid lärosätet görs en identitetskontroll. Även vid tentamenstillfällen sker en identitetskontroll. Utmaningar finns i dag främst vid högskoleprovet då det är svårt att säkerställa att rätt person genomför provet.

Universitets- och högskolerådet hanterar inte utbetalning av pengar eller integritetskänslig data. Däremot mottar och administrerar UHR inbetalning av anmälningsavgifter från sökande utanför EU. En kopplingstjänst skulle fungera mer som en säkerhetslösning än en servicelösning. Samtidigt är myndighetens kunder i dag mer betjänta av god service än av en högre säkerhetsnivå.

UHR har 2018 kompletterat och anger att deras behov av ett kopplingsregister fortfarande är begränsat även om digitaliseringen medför förändringar där kopplingsregistret kommer att bli en viktig pusselbit. UHR anser att en kopplingstjänst gör mest nytta om den är centraliserad men också att det ställer höga krav på säkerhet.

4.14 Sammanställning av offentlig sektors behov och förväntade nytta av en kopplingstjänst

I vissa fall förutsätter en hantering i en svensk myndighets digitala tjänst att den som vill använda tjänsten kan redovisa ett svenskt identitetsbegrepp. En utländsk eID-handling kommer, till skillnad från svenska eID-handlingar, inte att innehålla den uppgiften.

Det finns några olika sätt som frågan kan hanteras på. Den första åtgärden för varje myndighet med digitala tjänster bör vara att överväga om det finns ett behov av att ha en koppling till en svensk identitetsbeteckning. Om det inte finns ett tvingande behov av en sådan koppling bör det övervägas att ändra utformningen av tjänsten så att den kan användas utan kopplingen. Exempel på digitala tjänster utan behov av svenskt identitetsbegrepp är inom universitetsverksamhet när det gäller ansökningar och inskrivning, inom kommunal verksamhet för någon som planerar att flytta till en viss kommun eller inom Transportstyrelsens verksamhet vid ansökan om olika tillstånd och behörigheter eller rapportering av uppgifter inom viss utbildning.

Myndigheternas behov av kopplingstjänsten varierar. Även inom samma myndighet finns det olika behov av kopplingstjänst för olika digitala tjänster. Det kan dock konstateras att för vissa större myndigheter (Pensionsmyndigheten och

[9] SUNET står för Swedish University computer Network och är en enhet på Vetenskapsrådet. Enligt instruktioner från Utbildningsdepartementet ska Vetenskapsrådet särskilt "ansvara för kommunikationssystemet och beakta intresset hos forskning och andra berörda". www.sunet.se 2019-01-16.

Skatteverket) finns tydliga behov och stora grupper av möjliga användare. För andra myndigheter är behovet inte lika tydligt och det råder viss skepsis mot att det går att konstruera en service som är tillräckligt säker för att myndigheterna ska våga använda den.

Skatteverket anser efter analys av både verkets och andra myndigheters behovsbedömningar att det finns ett behov av en central funktion för att göra kopplingar mellan utländska eID-handlingar och svenska identitetsbegrepp. Den fortsatta bedömningen kvarstår kring att Skatteverket ska ansvara för kopplingsregistret.

I detta sammanhang kan även nämnas möjligheten att forma kopplingstjänsten efter de myndigheter som har störst nytta och behov. I nuläget är det Pensionsmyndigheten och Skatteverket som i så fall är aktuella. Genom att utveckla registret tillsammans avseende kravställning på uppbyggnad och vidareutveckling av registret kan hänsyn tas från början till de eventuella särlösningar dessa myndigheter har behov av. Registret kan rentav formas efter dessa myndigheters önskemål. På så sätt ser man också till att involvera stora grupper av användare från starten och minskar risken för att bygga upp ett kostsamt system som inte blir använt.

5 Alternativ till central kopplingstjänst

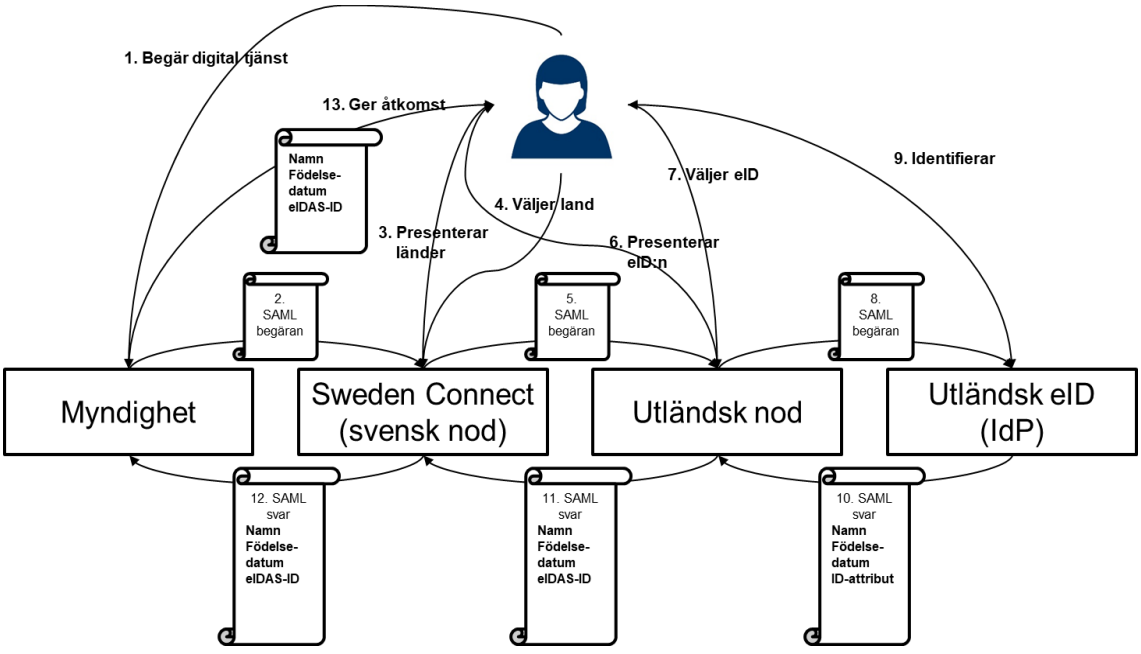
5.1 Digitala tjänster utan behov av kopplingstjänst

Bedömning: De digitala tjänster som saknar behov av en central kopplingstjänst kan använda sig av befintlig struktur och myndighetsservice.

Skälen för bedömningen: Olika myndigheter har olika stora behov av en central tjänst för att koppla ihop utländska eID-handlingar med svenska identitetsbeteckningar. De myndigheter som har digitala tjänster där det inte krävs att användaren har en svensk identitetsbeteckning kommer inte att ha behov av en kopplingstjänst alls utan kan använda sig direkt av den utländska eID-handlingen och den information som förmedlas genom den om man vill.

Sådana tjänster kan förekomma inom universitetsverksamhet när det gäller ansökningar och inskrivning, inom kommunal verksamhet för någon som planerar att flytta till en viss kommun eller inom Transportstyrelsens verksamhet vid ansökan om olika tillstånd och behörigheter eller rapportering av uppgifter inom viss utbildning.

Följande bild visar, något förenklat, hur identifieringen går till i en sådan digital tjänst.



1. Användaren begär åtkomst till en digital tjänst och väljer att logga in med en utländsk eID-handling.
2. Myndigheten skickar en begäran om identifiering via den svenska noden.
3. Den svenska noden presenterar valbara länder för användaren.
4. Användaren väljer det land som har utfärdat eID-handlingen.
5. Den svenska noden skickar begäran vidare till den valda utländska noden.

6. Den utländska noden presenterar valbara eID-handlingar för användaren.
7. Användaren väljer den eID-handling som hen vill identifiera sig med.
8. Den utländska noden skickar begäran om identifiering till utfärdaren av eID-handlingen.
9. Utfärdaren identifierar användaren.
10. Utfärdaren skickar svar innehållande användarens namn, födelsedatum och eventuella övriga ID-attribut till den utländska noden.
11. Den utländska noden skickar svaret vidare till den svenska noden och lägger till ett unikt eIDAS-ID som ska vara så beständigt som möjligt.
12. Den svenska noden skickar svaret till den svenska myndigheten.
13. Myndigheten väljer, baserat på den information som förmedlas, om användaren ska ges åtkomst till tjänsten.

Här ansvarar respektive myndighet själv för vad man väljer att göra med den information man får, om man anser att säkerheten är tillräcklig för att ge åtkomst till tjänsten.

5.2 Jämförelse med uppgifter i folkbokföringsdatabasen

Bedömning: En kopplingstjänst utan register skulle innebära svårigheter med matchningen av namn och födelsetid från eID-handling mot svensk identitetsbeteckning. En sådan kopplingstjänst når tillitsnivå 2 men inte nivå 3 (se avsnitt 3.2.2 ang. tillitsnivåer). Det räcker inte för de myndigheter som kräver tillitsnivå 3 i sina digitala tjänster. Skatteverket lämnar därför inget förslag om en sådan kopplingstjänst. Det utesluter inte att enskilda myndigheter kan använda en sådan lösning om det räcker med tillitsnivå 2 för deras digitala tjänster. Nödvändiga uppgifter finns tillgängliga för dem via Navet.

Skälen för bedömningen: Det finns digitala tjänster där man använder sig av svenska identitetsbeteckningar utan att kraven på säkerhet i övrigt är så stora. Noden kan göra en jämförelse mellan identitetsintyget och uppgifter i folkbokföringsdatabasen och förmedla resultatet till myndigheten som har tjänsten.

Det finns också myndigheter som föredrar att göra en egen koppling efter jämförelse mellan de uppgifter som tillhandahålls via den utländska eID-handlingen och de uppgifter som finns i folkbokföringsdatabasen. Alla myndigheter har via Navet tillgång till aktuella uppgifter från folkbokföringsdatabasen.

Det finns stora risker och nackdelar med en kopplingstjänst utan centralt register. Utan register måste jämförelsen mot folkbokföringsdatabasen göras vid varje inloggningstillfälle. Det är tidskrävande och kostsamt både för användaren och för myndigheten som tillhandahåller den digitala tjänsten. Det finns även en stor risk att myndigheterna gör olika bedömningar om kopplingen kan användas eller inte. Det leder till dålig förutsebarhet för användaren och fara för att användaren i en kedja av myndighetskontakter fastnar mellan myndigheter och inte kan lösa sina ärenden på samma sätt genom processen.

Matchningen av en identitet från ett utländskt identitetsintyg med uppgifter i folkbokföringsdatabasen kan också innebära svårigheter. Det är vanligt att namn stavas på olika sätt eller att presentationen av namndelar skiftar. Det kan även skilja någon siffra i födelsedatumet. Skatteverket kan ha fastställt ett personnummer som innehåller en annan födelsedag än den som är personens faktiska födelsedag om det inte finns lediga personnummer för personens födelsetid. Det kan även inträffa att personens födelsetid är felaktigt registrerad.

En lösning är att bara godkänna kopplingar där uppgifterna helt och hållet stämmer överens. I de fall uppgifterna inte stämmer överens kan den sökande hänvisas till att rätta sina uppgifter i den svenska folkbokföringen eller vända sig till utfärdaren av den utländska eID-handlingen för att rätta uppgifterna där så att de stämmer överens med de som registrerats i Sverige.

Denna lösning vore enkel eftersom det inte lämnar utrymme för bedömningar. Det skulle dock ge ett stelt system som eventuellt inte kan underlätta för användarna på det sätt som avsågs med eIDAS-förordningen.

Man kan också tänka sig att bygga in acceptans av en viss grad av bristande överensstämmelse i kopplingssystemet. Då måste inte överensstämmelsen vara hundraprocentig. Det återstår dock ändå svårigheter i var gränsen ska dras för vad som är en tillräckligt bra matchning. Olika myndigheter har olika behov av överensstämmelse och så länge matchningen sker maskinellt är systemet stelt och saknar utrymme för bedömningar.

En annan tänkbar svårighet med matchning är att det finns flera personer med samma namn och födelsetid. Så länge individen behöver ange sin identitetsbeteckning vid inloggningen bör det ändå gå enkelt att göra kopplingen till rätt individ.

Den största riskfaktorn när det gäller koppling utan register är säkerheten. Utan möjlighet att lagra information om användaren blir det mycket enkelt att utge sig för att vara någon annan än den man är vid inloggningen. För någon som vill ”kapa” en identitet vore det lätt att genomföra. Det är enkelt att byta för- och efternamn i många länder. Om man därefter skaffar en eID-handling i det nya namnet och har ett födelsedatum som stämmer överens med någon med samma namn och födelsedatum i Sverige skulle man kunna ansöka om en koppling till den personens identitetsbeteckning. De minimiattribut (se avsnitt 3.2.1) som bifogas av den utländska noden; nuvarande efternamn, nuvarande förnamn, födelsedatum och en unik identitetsbeteckning, skulle stämma överens med uppgifterna i folkbokföringsdatabasen. Om inga ytterligare kontroller görs skulle en koppling därefter kunna registreras.

Den beskrivna kopplingstjänsten uppnår inte tillitsnivå 3 eller väsentlig eftersom användaren själv anger identitetsbeteckning utan att detta kontrolleras närmare vid t.ex. fysisk inställelse. Nivå 3 eller väsentlig är den nivå som måste kunna erbjudas för de tjänster som kräver att nuvarande tillitsnivå bibehålls i alla led. Myndigheter med stora säkerhetskrav som Pensionsmyndigheten och Skatteverket kan därför inte använda sig av en kopplingstjänst utan register.

6 Överväganden och förslag

6.1 Säkerhet och förtroende

Bedömning: Kopplingstjänsten får inte innebära försämrad säkerhet eller sänkta tillitsnivåer.

Skälen för bedömningen: I eIDAS-förordningen anges att den syftar till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan företag, medborgare och offentliga myndigheter. Avgörande för förtroendet är att de lösningar som föreslås håller tillräcklig säkerhet för att myndigheter och medborgare ska våga lita på att de fungerar. Det är också av väsentlig betydelse att upprätthålla skyddet för den personliga integriteten.

En konstruktion som kopplar olika identitetsbegrepp till varandra och som är lätt att manipulera riskerar att urholka förtroendet för kopplingarna och i förlängningen för hela eIDAS-förordningen.

Det finns farhågor bland myndigheter, medborgare och i de övriga medlemsländerna för att problem med missbruk av urkund, urkundsförfalskning och bedrägerier kommer att öka om säkerheten försämras av att det lättare ska gå att få åtkomst till myndigheters digitala tjänster. Det kan vara lättare att orsaka stora problem i den elektroniska världen än i den fysiska. Pappershantering innebär en viss tröghet som ibland kan fungera som skyddsbarriär mot systematiska angrepp.

Enligt Polisens Nationella bedrägericenter anmäldes 116 760 identitetsintrång och 27 261 fall av olovlig identitetsanvändning under 2017. Anmälningar till polisen och frågeundersökningar talar för att bedrägerierna har ökat kraftigt de senaste fem åren när det gäller id-kapningar på nätet. Det bör ses i relation till att också handeln på nätet har ökat med 15–20 procent årligen under samma period.[10] Olika former av identitetsmissbruk utgör ofta grunden för att kunna utföra bedrägeri.[11] Det har bland annat lett till att brottet olovlig identitetsanvändning har införts i brottsbalken. Straffbestämmelsen syftar till att motverka missbruk av identitetsuppgifter och ge skydd mot den integritetskränkning det innebär att få dessa utnyttjade. För att kunna dömas för brottet krävs att någon utger sig för att vara en annan person genom att olovligen använda den personens identitetsuppgifter och därigenom ger upphov till skada eller olägenhet för honom eller henne. I förarbetena till författningsändringen, prop. 2015/16:150 s. 10 beskrivs behovet:

> Problemet med denna typ av olovlig identitetsanvändning har vuxit stort under senare år. Utvecklingen är parallell med ökningen av antalet anmälda bedrägeribrott, som ökat från cirka 116 100 år 2010 till ungefär 156 100 år 2014. Det går inte att ur den officiella brottsstatistiken utläsa något om antalet identitetskapningar eller brott som begås med hjälp av kapade identiteter. Uppgifter som Polisens nationella bedrägericentrum i samarbete med UC AB tagit fram pekar dock på att det totala antalet bedrägerier med hjälp av kapade identiteter utgör en stor del av dessa brott och avser betydande värden.

Acceptans för en kopplingstjänst och eIDAS-förordningen kommer att vara avhängigt att det går att tillgodose kraven på säkerhet som omgärdar gränsöverskridande identifiering och legitimering. Systemen behöver fungera väl för att skapa tillit så att myndigheter och medborgare vågar använda sig av den

[10] https://www.svd.se/id-kapningar-pa-natet-okar--igen, 18 september 2018.
[11] Brå rapport 2016:9 s. 9-12

tillgängliga tekniken. Ett extra led i identifieringen utgör en extra risk för att något kan bli fel, med eller utan avsikt.

En koppling som görs av Skatteverket kan vara förtroendeingivande och utstråla legitimitet enbart på grund av att den är gjord av en myndighet som medborgarna har förtroende för. Myndigheterna behöver ha beredskap och vara medvetna om vilka risker som kan uppstå i deras respektive digitala tjänster. För enskilda kan det vara svårt att skydda sig. Det är därför av största vikt att den lösning som Skatteverket föreslår inte innebär ökad risk för medborgarna att utsättas för brott.

Skatteverket anser sammantaget att kopplingar inte får förmedlas till priset av försämrad säkerhet. Den lösning som Skatteverket föreslår behöver uppnå samma tillitsnivå som gäller i dag, dvs. svensk tillitsnivå 3 eller eIDAS-förordningens tillitsnivå väsentlig. Vid identifieringen måste därför samma grad av säkerhet krävas som vid utfärdandet av en id-handling.

Utfärdande av id-handlingar genomförs av polisen (pass och nationella id-kort) och av Skatteverket (identitetskort). I Rikspolisstyrelsens föreskrifter och allmänna råd om polismyndigheternas hantering av pass och nationellt identitetskort (RPSFS 2009:14) anges bl.a. att polismyndigheten noggrant ska kontrollera sökandens identitet. Identiteten ska styrkas genom att sökanden i första hand uppvisar giltig id-handling som ska granskas med avseende på äkthet.

Enligt Skatteverkets föreskrifter om identitetskort (SKVFS 2009:14) ska sökanden i första hand styrka sin identitet och övriga personuppgifter genom att visa upp en godtagbar identitetshandling. Vad som räknas som godtagbar identitetshandling anges i föreskrifterna. Vidare ska sökandens längd kontrolleras i samband med ansökan.

I augusti 2017 tillsattes 2017 års ID-kortsutredning, med uppdrag att utreda och lämna förslag till förändringar av de krav och rutiner som gäller för svenska identitetshandlingar. Av direktiven framgår att utredningen ska föreslå hur antalet identitetshandlingar och utfärdare ska begränsas, analysera och föreslå hur verifieringen av äktheten och giltigheten av identitetshandlingar kan förbättras, utreda och vid behov föreslå hur identitetshandlingar bör utfärdas och utformas för att bli säkrare samt analysera och ta ställning till om fysiska identitetshandlingar bör innehålla en eID-handling på högsta tillitsnivå. Uppdraget ska redovisas senast den 29 mars 2019.[12]

Skatteverket har samrått med 2017 års ID-kortsutredning. Uppdraget till 2017 års ID-kortsutredning handlar i stort om att öka säkerheten runt gällande svenska id-handlingar och se till att nya svenska id-handlingar når upp till högre säkerhetsnivåer än vad vi har i dag. Beroende av vad utredningen föreslår kan det komma att påverka förslagen i denna rapport. En utgångspunkt för Skatteverket är att samma grad av säkerhet måste krävas för att registrera en koppling som vid utfärdandet av en svensk id-handling. Annars blir koppling via utländsk eID-handling en väg in i svenska digitala tjänster utan samma grad av säkerhet och kontroll som vid användning av svenska eID-handlingar.

6.2 Koppling till styrkt samordningsnummer

Bedömning: Det är för närvarande inte lämpligt att skapa en koppling mellan en utländsk eID-handling och en individs styrkta samordningsnummer.

[12] Dir. 2017:90.

Skälen för bedömningen: Enligt uppdragsbeskrivningen ska Skatteverket överväga om det för närvarande kan anses lämpligt att skapa en koppling mellan en utländsk eID-handling och en individs styrkta samordningsnummer.

I rapporten om kopplingsregister från 2016 föreslog Skatteverket att kopplingar skulle kunna lagras mellan utländska eID-handlingar och både personnummer och styrkta samordningsnummer men först efter att systemet för samordningsnummer har setts över genom vidare utredning.[13] Utredningen om nationella digitala tjänster bedömde i sitt slutbetänkande också att samordningsnummersystemet behöver ses över och identitetskontrollen skärpas.[14]

Skatteverket har tidigare lämnat flera förslag om regelförändringar för att öka kvaliteten på samordningsnummer[15] och nyligen slutfört ytterligare ett regeringsuppdrag i frågan. I promemorian Samordningsnumrens funktion i samhället från den 17 december 2018 lämnar Skatteverket en rad författningsförslag för att stärka samordningsnummersystemet och underlätta både för de personer som tilldelas samordningsnummer att få sina behov tillgodosedda och de myndigheter och organisationer som hanterar samordningsnummer i sina system. Dessutom har Skatteverket inom ramen för uppdraget påbörjat ett arbete med att informera och utbilda både internt och externt om hur samordningsnummer fungerar, tilldelas och kan användas.

När det gäller tilldelning av styrkta samordningsnummer kräver regelverket i dag inte personlig inställelse hos Skatteverket för den som ska få samordningsnumret. Den myndighet som från Skatteverket rekvirerar ett samordningsnummer till en person ansvarar för identifieringen av personen. Det kan räcka med en passkopia för att samordningsnumret ska anses vara styrkt. Skatteverket har utvecklat en digital tjänst för att rekvirera samordningsnummer där den rekvirerande myndigheten skickar in rekvisition och uppvisade handlingar elektroniskt till Skatteverket. Vid användningen av tjänsten ska en kopia av underlaget som styrkt identiteten skickas in elektroniskt.

Dessutom utfärdas i dag inte svenska eID-handlingar till personer med samordningsnummer, främst av säkerhetsskäl eftersom identiteten inte är kontrollerad på ett tillräckligt säkert sätt. Om styrkta samordningsnummer kan kopplas samman med utländska eID-handlingar skulle personer med samordningsnummer som inte får en svensk eID-handling, ändå ges möjlighet till åtkomst till myndigheters digitala tjänster genom att använda en utländsk eID-handling.

Det råder alltså i praktiken en viss skillnad mellan personnummer och styrkta samordningsnummer. För att tillräcklig säkerhet ska uppnås genom hela kedjan behövs ordentlig grundidentifiering av personen vid tilldelning av samordningsnummer. Detta kan enligt Skatteverkets bedömning bara utföras vid personlig inställelse.

Skatteverket har i promemorian från december 2018 lämnat förslag om att införa ytterligare en grad av säkerhet genom att den som ska tilldelas samordningsnummer får inställa sig för identitetskontroll hos Skatteverket. Samordningsnummer skulle först därefter kunna tilldelas med en säkerhetsgrad som motsvarar den som används vid utfärdande av id-handlingar. Innan ett sådant system är genomfört och utvärderat är det inte lämpligt att skapa en koppling mellan en utländsk eID-handling och en individs styrkta samordningsnummer.

---

[13] Skatteverkets rapport Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer från den 24 oktober 2016, s. 64.
[14] SOU 2017:114, s. 325 ff.
[15] Skatteverkets promemoria Samordningsnummer och utländska fastighetsägare – en översyn från den 18 augusti 2014, dnr. 131 430148-14/113 samt Skatteverkets promemoria Samordningsnummer till asylsökande från den 25 april 2016, dnr. 131 176575-16/113.

6.3 Kopplingsregister

6.3.1 En central funktion

Förslag: Ett kopplingsregister skapas för att behandla och spara kopplingar mellan eID-handlingar och svenska identitetsbeteckningar. För att få en koppling registrerad ska samma grad av säkerhet krävas vid identifieringen som vid utfärdandet av en id-handling.

Skälen för förslaget: Ett nytt centralt register måste byggas för att uppgifter om användarens identiteter ska kunna lagras och behandlas. Bara genom att ha tillgång till detta register kan kopplingar sparas och förmedlas med den säkerhet som krävs.

För att en kopplingstjänst med ett centralt register ska kunna ge service åt de myndigheter som har de största behoven krävs att tjänsten omgärdas av tillräckligt hög grad av säkerhet. Skatteverket anser därför att samma grad av säkerhet måste krävas vid registreringen och identifieringen som vid utfärdandet av en id-handling. Det innebär att koppling kan registreras först efter noggrann identitetskontroll av användaren vid fysisk inställelse hos den myndighet som ska utföra kontrollen.

Förutom säkerhetsaspekten finns det ytterligare fördelar med att skapa ett register. Uppgifterna i registret kommer att finnas tillgängliga för den nationella noden så att användaren av en digital tjänst inte vid varje inloggningstillfälle behöver vänta på att jämförelse ska göras med uppgifter i folkbokföringsdatabasen.

Skatteverket har övervägt om det ska finnas möjlighet att spärra sin identitetsbeteckning mot kopplingar till utländska eID-handlingar. Det kan ge skydd åt alla som är helt säkra på att de inte kommer att behöva registrera någon koppling. För de flesta som bor i Sverige är det ett troligt scenario. Samtidigt måste en sådan spärr kunna hävas och det skulle i så fall ske efter grundlig identitetskontroll. Kraven vid tillfället för registrering motsvarar därför de krav som skulle ställas vid hävandet av en sådan spärr. Därför bedömer Skatteverket att en spärr mot kopplingar till utländska eID-handlingar skulle sakna funktion.

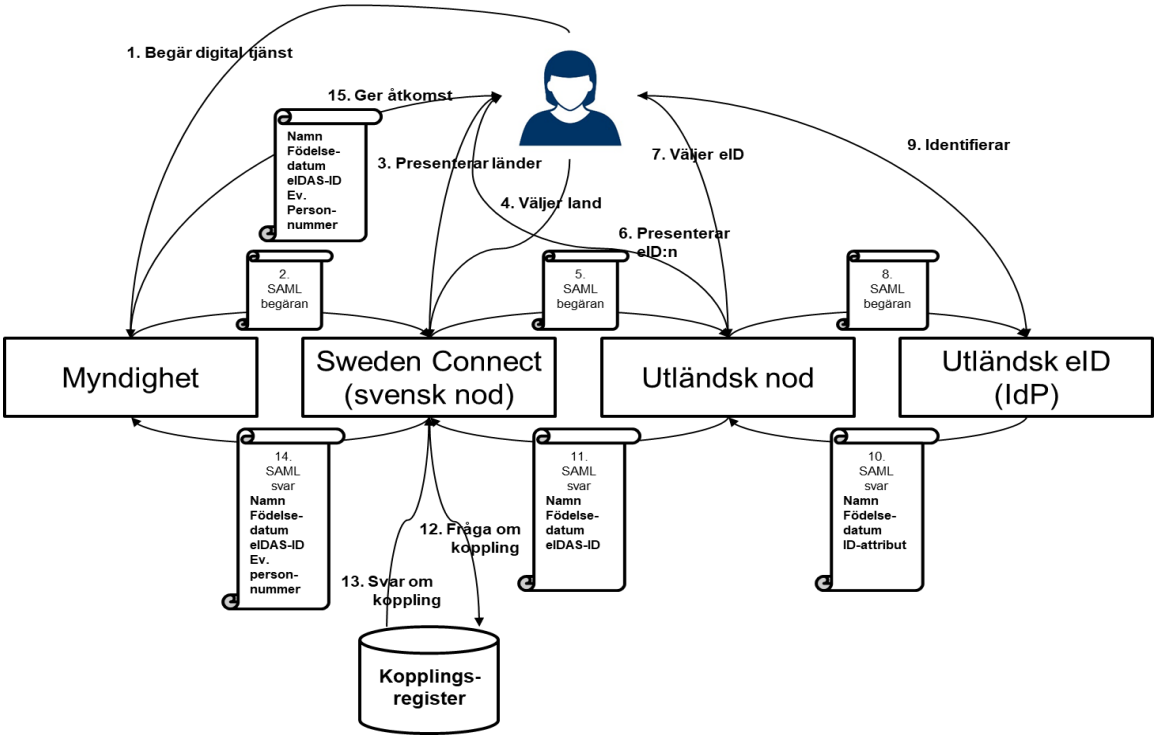
I följande avsnitt beskrivs först hur kopplingen ska förmedlas genom den svenska noden och därefter hur man ska gå tillväga för att registrera kopplingar med tillräcklig säkerhet.

6.3.2 Noden förmedlar uppgift om koppling

Förslag: Uppgift om att det finns en registrerad koppling ska förmedlas via den svenska noden i samband med att en eID-handling verifieras. Den uppgift som ska förmedlas är vilken identitetsbeteckning som finns kopplad till den använda eID-handlingen eller att det inte finns någon sådan registrerad koppling.

Skälen för förslaget: Att kopplingen förmedlas genom den svenska noden ger möjlighet till ett automatiserat förfarande som är snabbt och enkelt både för användaren och för den myndighet som tillhandahåller den digitala tjänsten. Det gör det också möjligt att begränsa tillgången till uppgifterna om befintliga kopplingar i kopplingsregistret, till värdmyndigheten för den svenska noden.

Följande bild visar, något förenklat, hur identifieringen går till när en registrerad person vill logga in i en digital tjänst och det finns ett kopplingsregister.



1. Användaren begär åtkomst till en digital tjänst och väljer att logga in med en utländsk eID-handling.
2. Myndigheten skickar en begäran om identifiering via den svenska noden.
3. Den svenska noden presenterar valbara länder för användaren.
4. Användaren väljer det land som har utfärdat eID-handlingen.
5. Den svenska noden skickar begäran vidare till den valda utländska noden.
6. Den utländska noden presenterar valbara eID-handlingar för användaren.
7. Användaren väljer den eID-handling som hen vill identifiera sig med.
8. Den utländska noden skickar begäran om identifiering till utfärdaren av eID-handlingen.
9. Utfärdaren identifierar användaren.
10. Utfärdaren skickar svar innehållande användarens namn, födelsedatum och eventuella övriga ID-attribut till den utländska noden.
11. Den utländska noden skickar svaret vidare till den svenska noden och lägger till ett unikt eIDAS-ID som ska vara så beständigt som möjligt.
12. Den svenska noden skickar en fråga till kopplingsregistret om det finns någon svensk identitetsbeteckning kopplad till den utländska eID-handlingen.
13. Om det finns en koppling registrerad mellan den utländska eID-handlingen och en svensk identitetsbeteckning skickas identitetsbeteckningen från kopplingsregistret till den svenska noden.
14. Den svenska noden skickar svaret till den svenska myndigheten.

15. Myndigheten väljer, baserat på den information som förmedlas, om användaren ska ges åtkomst till tjänsten.

Noden har direktåtkomst till kopplingsregistret och gör slagningen för att se om användaren är registrerad eller inte. Identitetsbeteckningen skickas till myndigheten som har den digitala tjänsten. Därefter är det myndigheten som avgör om tillträde ska ges till tjänsten.

Man kan tänka sig olika lösningar när det gäller vilken aktör som gör slagningen mot kopplingsregistret. Myndigheten som har den digitala tjänsten eller Skatteverket kan också utföra slagningen. Eftersom det här handlar om en helt maskinell lösning kan funktionen dock byggas in i den svenska noden.

Förslaget är utformat för att säkerställa att tillitsnivån i systemet bibehålls, men det är fortfarande fullt möjligt för tjänster som inte har sådana krav att ta fram egna lösningar i enlighet med vad som beskrivits i kapitel 5.

6.4 Modell för att åstadkomma koppling

6.4.1 Tvåstegsprocess med personlig inställelse

Förslag: Användaren startar processen för att registrera koppling genom att logga in med den eID-handling som hen vill koppla till ett svenskt personnummer i en digital tjänst och där skapa en väntande koppling. Därefter inställer sig användaren fysiskt hos den myndighet som ska utföra identitetskontroll och styrker sin identitet på motsvarande sätt som krävs för att utfärda svenska id-handlingar. Efter kontroll använder handläggaren den väntande kopplingen för att slutföra registreringen av koppling mellan eID-handlingen och den svenska identitetsbeteckningen.

Skälen för förslaget: För att uppnå samma grad av säkerhet vid registreringen som vid utfärdandet av en id-handling kan identifieringen genomföras enligt samma mönster som vid utfärdandet av en id-handling. Användaren inställer sig fysiskt vid den myndighet som ska utföra identifieringen. Myndigheten ska noggrant kontrollera användarens identitet. Vid myndigheten ska det finnas personal som är utbildad för att göra identifieringen och riktlinjer och rutiner för hur en identifiering ska gå till. Identiteten ska styrkas genom att användaren i första hand uppvisar giltig svensk id-handling som ska granskas med avseende på äkthet. Vidare kan t.ex. användarens längd kontrolleras i samband med ansökan.

Användaren måste också logga in med den eID-handling som ska kopplas till det svenska personnumret. Möjlighet till sådan inloggning är svår för en svensk myndighet att tillhandahålla eftersom eID-handlingar är konstruerade på olika sätt. Ibland har innehavaren en dosa eller ett kort men en eID-handling kan också vara installerad i en stationär dator som inte kan flyttas med till en myndighets kontor. Skatteverket arbetar därför med en tvåstegslösning där användaren först loggar in hemifrån och skapar en väntande koppling. Därefter inställer sig användaren hos den myndighet som ska göra identitetskontrollen och kan slutföra registreringen av kopplingen. Processen kan beskrivas i följande steg:

1. Användaren som önskar koppla sitt svenska personnummer till en eID-handling begär åtkomst till den självserviceapplikation som kopplingsregistersystemet tillhandahåller för detta.

2. Användaren omdirigeras till anvisningstjänst för att välja eID-handling för inloggning.

3. Användaren väljer att logga in med den eID-handling som ska kopplas.

4. eIDAS-systemet (svensk och utländsk nod) hanterar identifieringen och skickar sedan användaren tillbaka till självserviceapplikationen.

5. Användaren väljer ”Koppla eID” i självserviceapplikationen.

6. Applikationen visar en vy för att ange uppgifter för kopplingen.

7. Användaren uppger det personnummer som ska kopplas (samt telefonnummer om överföring av en engångskod ska ske via SMS).

8. Användaren initierar kopplingssekvensen i självserviceapplikationens användargränssnitt.

9. Självserviceapplikationen genererar en engångskod/sekvens-ID.

10. Anrop till API-applikationen för att skapa en ”väntande koppling”. I anropet skickas informationen från sessionen/eID-handlingen (namn, födelsedatum och PRID/eIDAS-ID), angivet personnummer samt engångskod/kopplingsidentifierare.

11. API-applikationen hämtar uppgifter (namn, födelsedatum) från folkbokföringen baserat på uppgivet personnummer.

12. Kontroll att uppgifter från eID-handlingen och uppgifter från folkbokföringen stämmer överens. Kontrollen består i att namn och födelsedatum ska stämma överens. Vad gäller namnet kan man antingen kräva att de är exakt samma eller tillåta mindre skillnader (t.ex. orsakat av att namnet translittererats olika)

13. En ”väntande koppling” skapas i databasen. Uppgifter sparas om sessions-information från eID-handlingen, personnummer samt den genererade engångskoden/sekvens-ID.

14. Information om att en väntande koppling har skapats visas i självserviceapplikationen.

15. Engångskoden/sekvens-ID som ska visas i nästa steg, hos myndigheten, skickas som SMS till angivet telefonnummer.

Användaren går till ansvarig myndighet med sin engångskod för att fortsätta kopplingssekvensen.

1. Användaren besöker ansvarig myndighet med engångskod/sekvens-ID för att fortsätta kopplingssekvensen.

2. Användaren identifierar sig hos handläggaren. Handläggaren genomför erforderliga rutiner och granskningar för identitetskontroll.

3. Användaren överlämnar den engångskod/sekvens-ID som erhölls via SMS till handläggaren.

4. Handläggaren fyller i personnummer och övriga uppgifter från användarens fysiska id-handling, samt engångskoden/sekvens-ID i handläggarapplikationen.

5. Handläggarapplikationen hämtar personuppgifter om personnumret från folkbokföringen.

6. Handläggarapplikationen begär att hämta upp den väntande kopplingen via API-applikationen från databasen baserat på engångskoden/sekvens-ID.

7. Uppgifter från folkbokföringen och den väntande kopplingen presenteras i handläggarapplikationen.

8. Handläggaren kontrollerar och jämför uppgifterna från den fysiska id-handlingen och de upphämtade uppgifterna.

9. De upphämtade uppgifterna visas upp för användaren för godkännande.

10. Handläggaren godkänner att koppling etableras i handläggarapplikationen.

11. Handläggarapplikationen anropar API-applikationen för att etablera koppling. I anropet skickas personnummer, engångskod/sekvens-ID, samt information (namn, födelsedatum) från den fysiska id-handlingen.

12. API-applikationen hämtar personuppgifter från folkbokföringen baserat på personnummer från väntande kopplingen.

13. Uppgifter från den väntande kopplingen, folkbokföringen och ifyllda uppgifter från den fysiska id-handlingen kontrolleras så att de stämmer överens. Uppgifter som kontrolleras är namn och födelsedatum (maskinell kontroll).

14. API-applikationen skriver till databasen för att etablera kopplingen mellan eID-handlingen och användarens personnummer.

15. API-applikationen skriver till databasen för att markera den väntande kopplingen som utförd (baserat på engångskod/sekvens-ID).

16. Handläggarapplikationen visar ”koppling utförd”-vy.

17. Handläggaren visar användaren att kopplingen är klar och informerar om hur man själv kan hantera kopplingar i och med att den första kopplingen nu är på plats. Alternativt överlämnas ett kvitto och en informationsbroschyr om detta.

Matchningsproblematiken (t.ex. olika stavningar av namn, skillnader på någon siffra i födelsedatumet etc.) kommer lättare att kunna lösas om personen vid något tillfälle inställer sig vid en myndighet för identifiering. Vid detta tillfälle kan utredas vad skillnaderna beror på och vid behov kan ytterligare information hämtas in från sökanden. Det är då inte fråga om att jämföra uppgifter i två identiteter, utan att kunna styrka att dessa två identiteter avser samma person. Mindre avvikelser mellan

stavningar och födelsetidpunkt blir inte så betydelsefulla. Större avvikelser kan ge skäl att ifrågasätta om de två identiteterna avser samma fysiska person.

6.5 Informationssäkerhet

Skatteverket ska enligt uppdragsbeskrivningen analysera och bedöma vilka åtgärder som bör vidtas för att säkerställa en god informationssäkerhet i kopplingsregistret.

Åtgärderna ska syfta till att information i kopplingsregistret inte sprids till obehöriga, att informationen är korrekt och fullständig samt till att informationen är tillgänglig för behöriga vid behov. Åtgärderna behöver också innefatta en spårbarhetsdimension som innebär att möjliggöra säkerställande av vem eller vilka som har läst, bearbetat, förändrat eller förstört specifik information och när eller var det har skett.

6.5.1 Åtgärder innan driftsättning

Informationsklassning

Informationsklassning genomförs för att värdera informationen utifrån Konfidentialitet (vem får ta del av information), Riktighet (att informationen alltid är korrekt och aktuell) och Tillgänglighet. Därefter anpassas lösningen utifrån informationsklassningsvärden, KRT, när det gäller behörighetsstyrning, kommunikationssäkerhet, kontinuitetsplanering, tillgänglighetskrav samt spårbarhet, backup rutiner, spegling av informationen samt möjliga andra IT-säkerhetstekniska åtgärder. Klassning av informationstillgångar utifrån Konfidentialitet, Riktighet och Tillgänglighet möjliggör identifiering och klargörande av vilken effekt ett otillräckligt skydd av informationstillgångarna får. Klassning syftar främst till att ge informationstillgångar skydd som motsvarar deras värde, men också till att undvika överskydd med onödigt höga kostnader som följd.

Säkerhetsbedömning

Säkerhetsbedömning görs med målsättningen att identifiera behov av säkerhetsrelaterade aktiviteter som en verksamhetsförändring behöver hantera. Syftet är identifiering av risker som kan påverka värdmyndighetens tillgångar på ett negativt sätt och lämna förslag på åtgärder i ett tidigt stadium. Säkerhetsbedömningen visar även om fördjupad riskanalys rekommenderas. Säkerhetsbedömningen börjar med en övergripande riskanalys och övergår sedan eventuellt till en Säkerhetsskyddsbedömning. Om behov av säkerhetsskydd finns, är det ofta ett omfattande arbete över tid som tillkommer och därför är det viktigt att det tidigt görs en bedömning av behovet.

Kontinuitetsplan

Kopplingsregistrets tillgänglighet måste säkerställas i händelse av haveri och störningar.

Kontinuitetsplanering är en metod för säkerställande av leveransförmågan genom planering för fortsatt verksamhet vid en eventuell förlust av operativ förmåga. Till affärskritiska processer räknas alla de processer som är viktiga för uppnåendet av ställda verksamhetsmål. Dessa processer kan vara beroende av stödprocesser, aktiviteter och resurser. Säkerhetskopior av systemet ska tas fram och testas regelbundet för att garantera tillgängligheten.

6.5.2 Åtgärder relaterade till design- och testfas

Kravställning enligt ISO-standard

ISO 27000 är ett internationellt erkänt ramverk eller ledningssystem för att organisationer ska kunna ha bättre kontroll över sin informationssäkerhet. Kravställning på systemets infrastruktur bör följa standarder och praxis inom informationssäkerhetsområdet enligt ISO 27000-serien.

Säkerhetsgranskning av programkod

Granskning av programkoden avseende sårbarheter och vidtagande av åtgärder för eliminering av sårbarheter och skadlig programkod bör genomföras.

Kommunikationssäkerhet

Kommunikationssäkerhet handlar om att implementera och upprätthålla säkerhetsåtgärder som är relaterade till kommunikation eller nätverk. Kommunikationssäkerhetsarbetet innefattar ett säkerställande av att informationen skyddas i alla lägen, såsom under transport mellan kopplingsregistret och den svenska eIDAS-noden. Kommunikationssäkerhetsarbetet innefattar även säkerställande av att tillräckliga åtgärder vidtas för att motverka informationsförvanskning, störning, avlyssning, felkopplingar, kapning, missbruk och bedrägerier relaterade till systemet och dess kommunikation.

Spårbarhet

Säkerställande av att det finns tillräckligt god spårbarhet i registret för att möjliggöra spårning och klarläggande av oegentligheter och missbruk samt för att möjliggöra analyser av systemfel är viktigt för att uppnå spårbarhet.

6.5.3 Åtgärder efter driftsättning

Systemrevision

Revision av hela systemet ur ett informationssäkerhetsperspektiv är lämpligt att genomföra när den tekniska lösningen har etablerat sig i dess olika delar, dvs. när systemet är i drift. Vidare rekommenderas revision av hela systemet ur ett informationssäkerhetsperspektiv vid förändringar av systemet och återkommande revisioner av systemet i sin helhet med lämplig regelbundenhet.

Kontinuerlig övervakning

Övervakning utförs i syfte att påvisa nätverkstrafik och aktiviteter som avviker från normaltillståndet, s.k. anomalier. Arbetet innefattar även periodisk granskning av loggar.

Säkerställande av skydd mot skadlig programkod

Ingående systemenheter i kopplingsregistersystemet bör avsökas efter skadlig programkod med lämplig regelbundenhet.

Teknisk säkerhetsgranskning

Återkommande tekniska säkerhetsgranskningar, penetrationstest, av hela systemet ur ett IT-säkerhetsperspektiv är lämpligt att genomföra när den tekniska lösningen

har etablerat sig i dess olika delar, dvs. när systemet är i drift. Återkommande tester bör göras för att säkerställa att kopplingsregistret har förmågan att hantera olika typer av överbelastningsattacker.

6.5.4 Om informationssäkerhet i den föreslagna lösningen

Bedömning: Kopplingsregistret och den föreslagna lösningen för registrering av koppling kräver inte extraordinära skyddsåtgärder utöver de som vanligtvis vidtas när det kommer till lösningar som utgörs av registerhållning med tillhörande tekniska komponenter.

Skälen för bedömningen: Det kopplingsregistersystem som Skatteverket fått i uppdrag att analysera utgörs av flera olika komponenter. Bland dessa delar återfinns kopplingsregistret, kopplingstjänsten (genom vilken man kan koppla utländska eID-handlingar till svenska personnummer) och kopplingen till den svenska eIDAS-noden.

I samtliga komponenter bearbetas eller lagras ett antal uppgifter. De uppgifter som kommer att behandlas är bl.a. användarens personnummer, förnamn, efternamn, uppgift om befintlig koppling och aktuellt eIDAS-ID.

Utöver de faktiska komponenter som infrastrukturen består av samt de uppgifter som bearbetas eller lagras inom ramen för infrastrukturen finns även processen för att knyta en utländsk eID-handling till den svenska identitetsbeteckningen och kontrollera att uppgifterna stämmer överens.

Efter en inledande analys är Skatteverkets uppfattning att den föreslagna lösningen ur ett informationssäkerhetsperspektiv inte utgör en sådan lösning som kräver extraordinära skyddsåtgärder utöver de som vanligtvis vidtas när det kommer till lösningar som utgörs av registerhållning med därtill kommande tekniska komponenter. De säkerhetsåtgärder som vidtas behöver också stå i proportion till de risker och hot som kan föreligga mot den aktuella lösningen. Skatteverket vill i sammanhanget emellertid poängtera att en mer detaljerad analys utifrån ett informationssäkerhetsperspektiv kommer behöva genomföras i samband med utveckling av det föreslagna kopplingsregistret med därtill hörande kopplingstjänst.

Två ytterligare parametrar som faller utanför informationssäkerhetsbedömningen men som ändå kan medföra konsekvenser i förlängningen är det gemensamma ansvaret mellan myndigheter och risk för nedärvda fel.

En lösning som baseras på en infrastruktur där tre myndigheter samverkar (enl. tidigare förslag Skatteverket, Polismyndigheten och Myndigheten för digital förvaltning, se avsnitt 6.7) kan medföra risker i ljuset av att ingen myndighet har helhetsansvaret i sammanhanget. Lösningen behöver därför ha inbyggda mekanismer för att säkerställa att helheten omhändertas.

Det utredningsuppdrag Skatteverket har omfattar inte den process för grundidentifiering som sker i samband att användare skaffar sig en eID-handling. Detta är en del inom ramen för eIDAS-förordningen som baseras på tillit mellan medlemsstaterna. Skatteverket vill i dock belysa det faktum att en felaktigt eller bristfälligt genomförd grundidentifiering riskerar ärvas in i ett kommande kopplingsregister. Något som i förlängningen kan få till följd att det finns kopplingar mellan utländska eID-handlingar och svenska personnummer där innehavaren av den utländska eID-handlingen inte är den hen utger sig för att vara.

6.6 Juridiska förutsättningar för kopplingsregistret

6.6.1 En ny kopplingsregisterlag och förordning

Förslag: En ny lag och tillhörande förordning som reglerar kopplingsregistret införs. Författningarna innehåller bestämmelser om tillämpningsområde och relation till annan reglering, om registrets ändamål, innehåll, ansökningar, registreringar, när registreringar ska tas bort, gallring och överklagande.

Skälen för förslaget: Regleringen av ett kopplingsregister kan struktureras på olika sätt. Skatteverket föreslår ett fristående register som kan knytas till valfri myndighet beroende på omfattning och framtida utveckling.

Ett fristående register behöver regleras i en egen lag. Det är lämpligt att reglera att ett sådant register ska föras och att lägga fast några regler för hanteringen för att lägga ramar som tar tillvara den enskildes intressen och samtidigt fyller det behov som redovisats i kapitel 4 av ett centralt register över kopplingar mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Dessutom föreslår Skatteverket en tillhörande förordning för kompletterande bestämmelser som lämpar sig bättre i en förordning.

Ansökningsförfarandet för att registrera en koppling beskrivs i avsnitt 6.4.1. Den webbaserade tjänsten förutsätter att användaren skriftligen fyller i de uppgifter som behövs för prövningen. Den som har ett svenskt personnummer skulle efter ansökan ha rätt att få en koppling till en utländsk eID-handling registrerad i kopplingsregistret. Det förutsätter dock att det inte finns skäl att ifrågasätta att den elektroniska identiteten avser samma person som har personnumret. I sådana fall får ansökan avslås. Ansökan får även avslås om sökanden inte har lämnat de uppgifter som behövs eller iakttagit vad som har föreskrivits av regeringen i fråga om ansökan och sökanden inte har följt en uppmaning att avhjälpa bristen. Ansökan ska även innehålla en försäkran på heder och samvete att den elektroniska identiteten avser samma person som har personnumret.

En registrering av en koppling till en utländsk eID-handling ska bygga på frivillighet. Det måste därför också vara möjligt att ta bort en registrerad koppling om den registrerade inte längre vill ha kopplingen registrerad.

Det måste även vara möjligt för den registerförande myndigheten att ta bort en koppling utan en ansökan från den registrerade personen om kopplingen avser en eID-handling som inte längre gäller, inte längre ska erkännas eller om det finns skäl att anta att den inte avser den registrerade personen.

Det behövs också en möjlighet för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om ansökan och registrering av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Slutligen föreslår Skatteverket att beslut enligt lagen får överklagas till Förvaltningsrätten i Stockholm och att prövningstillstånd ska krävas vid överklagande till kammarrätten.

Den föreslagna regleringen beskrivs närmare i avsnitt 6.6.2–6.7.2.

6.6.2 Tillämpningsområde och förhållande till annan reglering

Förslag: Lagen innehåller bestämmelser som kompletterar EU:s dataskyddsförordning. Dessutom gäller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av den föreslagna lagen eller

föreskrifter som meddelas i anslutning till lagen. Regleringen ska gälla om personuppgiftsbehandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställnings enligt särskilda kriterier.

Skälen för förslaget: Dataskyddsregleringen för verksamheten att åstadkomma kopplingar mellan utländska eID-handlingar och svenska identitetsbegrepp kommer inte bara att bestå av den föreslagna lagen utan även av dataskyddsförordningen och dataskyddslagen. Det är därför lämpligt att den föreslagna lagens förhållande till dataskyddsförordningen och dataskyddslagen klargörs.

Lagen ska innehålla en upplysning om att den kompletterar dataskyddsförordningen. Dataskyddsförordningen är direkt tillämplig och har företräde framför nationell lagstiftning. Den nya lagen om koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar kommer därför endast att innehålla bestämmelser som kompletterar dataskyddsförordningen där det är tillåtet. Dataskyddslagen ska vidare gälla, om inte annat följer av den föreslagna lagen eller föreskrifter som har meddelats med stöd av den.

Tillämpningsområdet för lagen och förordningen ska vara att de ska gälla vid behandling av personuppgifter i verksamhet som rör koppling av utländska eID-handlingar och svenska personnummer och som sker helt eller delvis automatiserat eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier. Tillämpningsområdet blir då detsamma som för dataskyddsförordningen och dataskyddslagen. Manuella behandlingar av personuppgifter som inte ingår i en strukturerad samling enligt ovan, t.ex. minnesanteckningar i anslutning till ärendehanteringen, omfattas inte av den nya lagen.

Förslaget tas in i 2 § i lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

6.6.3 Ändamålen med personuppgiftsbehandling

Förslag: Ändamålen med personuppgiftsbehandlingen i det föreslagna kopplingsregistret är att skapa och lagra kopplingar mellan utländska eID-handlingar och svenska personnummer, hantera ärenden i kopplingsregistret, tillgodose behov av spårbarhet, förvaltning av kopplingsregistret samt uppgiftslämnande.

Skälen för förslaget: Skatteverket har i avsnitt 5 redovisat alternativa lösningar för att möjliggöra koppling mellan utländska elektroniska identiteter och svenska personnummer. Skatteverkets slutsats och förslag, som redovisas i avsnitt 6.3, är att ett centralt kopplingsregister är att föredra såväl ur säkerhet- och tillitsperspektiven som ur ett kostnadsperspektiv. Det centrala kopplingsregistret tillgodoser behovet hos de digitala tjänstägarna, dvs. myndigheterna, se redovisning i avsnitt 4, av att upprätthålla en inloggningsprocess med hög tillitsnivå vilket är en förutsättning för en säker och tillförlitlig informationshantering inom myndigheternas digitala tjänster. Kopplingsregistret tillgodoser även enskildas behov av att möjliggöra en koppling mellan identitetsbegrepp på ett sätt som tillgodoser högt ställda integritetskrav.

Behov, ändamål och personuppgiftsbehandlingar

Syftet med eIDAS-förordningen är bl.a. att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan företag, medborgare och offentliga myndigheter. Att kunna genomföra elektroniska transaktioner där parternas identitet kan fastställas på ett tillförlitligt och säkert sätt är av stor betydelse för den inre marknadens utveckling och för enskilda medborgarens möjlighet att ta del av varu- och tjänsteutbud som tillhandahålls både av enskilda företag och av myndigheter. För svenska förhållanden är användningen av personnummer dominerande som identifieringsbegrepp.

Behovet av att kunna koppla utländska eID-handlingar med svenska personnummer är, enligt Skatteverkets slutsatser av redogörelsen i kapitel 4, stort. Behovet är givetvis kopplat till individer som både har svenskt personnummer och en utländsk eID-handling. Det är behovsnivån i den gruppen som bedömts som betydelsefull.

Det primära ändamålet med behandling av personuppgifter i ett kopplingsregister är att skapa den eftersträvade kopplingen mellan en utländsk eID-handling och ett svenskt personnummer. Genom kopplingen kommer den utländska eID-handlingen att medge tillträde till svenska digitala tjänster där normalt en svensk eID-handling krävs. Kopplingen förutsätter en ärendehantering där omständigheter som rör den utländska eID-handlingen och den svenska identiteten kommer att behandlas. Förekomsten av ett kopplingsregister med uppgift om genomförda kopplingar ställer också krav på att registret kan visa upp en spårbarhet avseende kopplingar mellan olika identitetsbegrepp som tidigare gjorts men som inte längre är giltiga.

Utöver ovanstående centrala ändamål med kopplingsregistret och de behandlingar som ska utföras inom ramen för registret så bör det också framhållas att ett ändamål för personuppgiftsbehandlingen i registret är dess förvaltning. Det kan t.ex. vara av betydelse att generera statistikunderlag från registret eller genomföra behandlingar i registret för att beräkna resursåtgång eller liknande. För att kunna genomföra den typen av behandlingar bör ett särskilt ändamål för förvaltning beskrivas i författningstexten.

Utöver de behandlingar i kopplingsregistret som redovisats ovan bör också nämnas behandlingar som kommer att vara möjliga men som är av sekundär natur. Framställningar till kopplingsregistret som sker med stöd av tryckfrihetsförordningen eller med stöd av 6 kap. 4-5 §§ offentlighets- och sekretesslagen (2009:400) kommer att kräva behandlingar i registret. För att det ska vara tydligt att också sådana behandlingar är tillåtna föreslår Skatteverket att det ska införas ett särskilt ändamål i den föreslagna författningstexten som avser uppgiftslämnande.

Förslaget tas in i 3 § i lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

6.6.4 Utlämnande

Förslag: DIGG får ha direktåtkomst till uppgift om koppling finns samt får på medium för automatiserad behandling förmedla identitetsinformation till värdmyndigheter för digitala tjänster som registrerade användare begär tillträde till. Polisen får ha direktåtkomst till de uppgifter som behövs för

ärendehandläggningen. Enskilda får ha direktåtkomst till uppgifter om sig själva. Skatteverket får lämna ut uppgifter till andra myndigheter på medium för automatiserad behandling.

Skälen för förslaget: När utlämnande ur kopplingsregistret aktualiseras med stöd av en uppgiftsskyldighet till andra myndigheter föreslår Skatteverket att det ska vara möjligt att lämna ut uppgifterna på medium för automatiserad behandling. I författningstexten föreslås detta regleras särskilt. Motsatsvis bör av lagtexten förstås att om enskilda begär uppgifter eller handlingar ur kopplingsregistret så får utlämnandet verkställas endast genom konventionella pappershandlingar. Inskränkningen i den här delen är ett sätt att stärka integritetsskyddet för den enskilde som är registrerad i kopplingsregistret.

Myndigheten för digital förvaltning föreslås däremot få direktåtkomst när det gäller att kontrollera förekomst av koppling i databasen och förmedla identitetsinformation till myndighet som tillhandahåller digital tjänst och till vilken den registrerade digitalt har begärt tillträde. Även Polisen föreslås få direktåtkomst till databasen när det behövs för den ärendehandläggning som myndigheten ska utföra med anledning av en initierad koppling.

Enskilda föreslås få direktåtkomst till person- och ärendeuppgifter om sig själva. Avsikten med regleringen är att möjliggöra en utveckling av digitala tjänster i anslutning till databasen. Det bör t.ex. vara möjligt att utveckla en tjänst där en enskild kan se vilka kopplingar som gjorts mellan utländska eID-handlingar och hans eller hennes svenska identitetsbeteckning. I en sådan tjänst bör det också kunna framgå när den enskilde behöver göra en ny koppling.

Förslaget tas in i 11 § i lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

6.6.5 Vilka personuppgifter ska behandlas?

Förslag: Databasen får innehålla uppgifter om personer som har tilldelats personnummer. Uppgifter om namn, födelsedatum och den utländska eID-handlingens unika beteckning får behandlas för de angivna ändamålen. För ärendehanteringen får också adressuppgifter, telefonnummer och eventuellt e-postadress bli föremål för behandling.

Regeringen får föreskriva att också andra uppgifter ska få behandlas i databasen.

Skälen för förslaget: I kopplingsregistret ska det i huvudsak vara förutsägbart vilka personuppgifter som ska behandlas. Vilka uppgifter som kommer att levereras med de utländska eID-handlingarna kan dock i någon mån variera. I normalfallet bör den levererade informationen innehålla uppgift om namn, födelsedatum och den utländska eID-handlingens unika beteckning. I vissa fall kommer uppgifterna som avser den utländska eID-handlingen vara pseudonymiserade. I kopplingsregistret, där ärendehanteringen avseende kopplingen ska ske, kommer också personuppgifter om användarens svenska identitet att behandlas t.ex. namn och personnummer. För ärendehanteringen kommer också adressuppgifter, telefonnummer och ev. e-postadress att kunna bli föremål för behandling.

Vid ärendehandläggning som avser att skapa en koppling såväl som att bringa en koppling att upphöra kan det inte uteslutas att känsliga personuppgifter eller uppgifter om lagöverträdelser kan komma att behandlas. T.ex. skulle det kunna bli aktuellt att pröva om en genomförd koppling är korrekt med hänsyn till inkomna

uppgifter om någon form av identitetsrelaterad brottslighet. I ett sådant fall måste myndigheten kunna dokumentera nödvändig information som har betydelse för kopplingens beständighet.

I kopplingsregistret kommer sökandes personnummer att bli föremål för behandling. Av 3 kap. 10 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning framgår att personnummer får behandlas utan samtycke endast om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. I fråga om kopplingsregistret så är dess primära ändamål att skapa en säker koppling mellan två identitetsbegrepp varav det ena är svenska personnummer. Behandlingen av personnummer i kopplingsregistret bör därför anses som tillåten.

Vilka uppgifter som får behandlas i kopplingsregistret ska begränsas i så stor omfattning som möjligt. För att värna den enskildes anspråk på skydd för sina personuppgifter föreslår Skatteverket att uppgifterna i kopplingsregistret ska vara sekretessreglerade, se avsnitt 6.6.13. Skatteverkets bedömning är att samma sekretessreglering bör gälla för identitetsuppgifterna i kopplingsregistret som gäller för motsvarande uppgifter i andra register, t.ex. folkbokföringsregistret. En sekretess med ett rakt skaderekvisit bör alltså gälla för uppgifterna i kopplingsregistret.

För att säkerställa skyddsbehovet för enskilda med sekretessmarkering införd i folkbokföringsregistret och för att möjliggöra för dem att också kunna begära koppling mellan en utländsk eID-handling och deras svenska personnummer ska kopplingsregistret få innehålla uppgift om sekretessmarkering. Härigenom kan också den här gruppen av enskilda omfattas av ambitionerna med eIDAS-förordningen.

En typ av uppgift som Skatteverket inte bedömt som aktuell att behandla i kopplingsregistret är uppgift om enskilds användning av genomförd koppling. Till kopplingsregistret kommer i stället endast fråga att ställas om existerande koppling. Frågan kommer i samtliga fall att komma från den svenska eIDAS-noden. Skatteverket har inte bedömt det som lämpligt eller som en del av kopplingsregistrets uppgift att innehålla användningsinformation. Det innebär för den enskilde att risken för kartläggning eller övervakning minskar genom att utnyttjandet av digitala tjänster där koppling krävs inte kommer att vara en registeruppgift. Å andra sidan innebär ställningstagandet att varken den enskilde själv eller någon annan kan få en samlad beskrivning av den enskildes användning av kopplingstjänsten.

För att skapa möjlighet att i framtiden förändra antalet och karaktären av uppgifter som får behandlas i kopplingsregistret bör regeringen medges möjlighet att genom förordning föreskriva sådana ändringar.

Förslaget tas in i 4 och 5 §§ i lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Insamling av personuppgifter till kopplingsregistret

En koppling i kopplingsregistret förutsätter att den enskilde begär att en sådan koppling ska registreras. Det är därför också den enskilde som i första hand ska se till att försörja systemet med information. När den enskilde begär att koppling ska ske kommer det att resultera i att den enskilde dirigeras till att identifiera sig med sin utländska eID-handling. Härigenom kommer den utländska eID-handlingens uppgifter att tillföras kopplingsregistret. Det är sedan upp till den enskilde att ange

det svenska personnummer som ska kopplas till den aktuella utländska eID-handlingen.

Inom ramen för ärendehandläggningen av begärd koppling kan det bli aktuellt för den ansvariga myndigheten att registrera kontaktuppgifter till den enskilde. Det kan vara fråga om adress, telefonnummer eller e-postadress. Det kan inte uteslutas att den begärda kopplingen behöver utredas och i det sammanhanget kommer kontaktuppgifter att vara nödvändiga att hantera.

Utöver ovanstående kommer det föreslagna kopplingsregistret att bekräfta angivet personnummer genom slagning mot folkbokföringsdatabasen. Slagningen kommer att ske mot systemet Navet. Slagningen kommer i de flesta fall inte att tillföra ärendet någon ny information. Från Navet kommer ny information att tillföras kopplingsregistret endast om det personnummer som den enskilde angivit är felaktigt, eller om den enskilde som begärt koppling har en registrerad sekretessmarkering i folkbokföringsdatabasen. Är det angivna personnumret felaktigt kommer någon typ av felmeddelande att skickas till kopplingsärendet och har den enskilde en sekretessmarkering kommer den uppgiften att tillföras kopplingsregistret.

För att skapa överblick och transparens kring personuppgiftsbehandlingen vid kopplingen måste den enskilde få utförlig information om den behandling som kommer att ske vid kopplingen. Att den enskilde ska informeras i anslutning till att personuppgifter samlas in från denne framgår av art. 13 i EU:s dataskyddsförordning. Det bör finnas goda möjligheter att lämna tillräcklig och nödvändig information till den enskilde om de behandlingar som krävs för att åstadkomma en koppling mellan identitetsbegreppen. Vilken information som ska lämnas framgår av art. 13.

För uppgifter som kan tillföras ärendehanteringen av annan än den enskilde gäller att information ska lämnas till den enskilde i enlighet med art. 14 i EU:s dataskyddsförordning. Det kan t.ex. vara sådan information som kommit in till den myndighet som ansvarar för kopplingsregistret och som ifrågasätter en kopplings riktighet. I ett sådant fall bör information om uppgifterna i normalfallet lämnas i samband med att kopplingen utreds på nytt.

Givetvis innebär också art. 15 i EU:s dataskyddsförordning att den enskilde har möjlighet att få kunskap om vilka personuppgifter som behandlas i kopplingsregistret och för vilka ändamål behandlingen sker.

Kopplingsregistret kommer på sikt att utgöra den uppgiftssamling där samtliga kopplade utländska eID-handlingar och kopplade svenska personnummer finns registrerade. Kopplingen som sådan och kopplingsregistret kommer att regleras i särskild ordning genom den författning som föreslås i denna utredning. För att stärka integritetsskyddet för enskilda som finns registrerade i uppgiftssamlingen bör kopplingsregistret betraktas som en självständig verksamhetsgren hos de myndigheter som får ansvaret för registret och för handläggning av ärenden om koppling. Genom en sådan ordning kommer antalet personer som är behöriga att behandla uppgifter i registret att hållas nere och det blir enklare att administrera de behörigheter till registret som kommer att krävas. Skatteverket anser att det är lämpligt att de myndigheter som slutligen får ansvaret för kopplingsregistret och för ärendehandläggning om koppling får arbetsuppgiften inskriven i sina respektive instruktioner.

6.6.6 Sökbegrepp

Förslag: Känsliga personuppgifter eller personuppgifter som avser lagöverträdelse får inte användas som sökbegrepp.

Skälen för förslaget: I kopplingsregistret har Skatteverket övervägt behovet av begränsningar av sök- och sammanställningsmöjligheter. Det ska vara möjligt att söka fram kopplingar mellan utländska eID-handlingar och svenska personnummer genom användning av personnummer eller formatet för utländska eID-handlingar. Skatteverkets bedömning är att det också ska vara möjligt att söka i kopplingsregistret utifrån nationell tillhörighet på elektroniska identiteter, t.ex. hur många franska eID-handlingar som finns registrerade i kopplingsregistret och vilka dessa är. Den senare typen av sökmöjlighet är viktig för att kunna leva upp till förvaltningskrav som kommer att ställas på kopplingsregistret. Skatteverket bedömer att den inskränkning i sökmöjligheter som bör författningsregleras är att det inte ska vara möjligt att i kopplingsregistret söka på känsliga personuppgifter eller på personuppgifter som avser lagöverträdelse.

Förslaget tas in i 12 § i lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

6.6.7 Uppgifternas livscykel och gallring

Förslag: Uppgifterna och handlingarna som finns lagrade i databasen ska gallras senast fem år efter att beslut om koppling mellan den utländska eID-handlingen och den svenska identitetsbeteckningen har registrerats.

Skälen för förslaget: Uppgifter och behandlingar i kopplingsregistret följer en viss livscykel. Såsom har beskrivits ovan initieras behandlingen av den enskilde själv som önskar få sitt svenska personnummer kopplat till en utländsk eID-handling. Uppgifterna som inkommer används för ärendehandläggning anknuten till frågan om en koppling kan etableras och därefter att visa att en koppling finns.

I kopplingsregistret kommer också någon form av förvaltning att ske. Andra myndigheter kommer att begära uppgifter ur kopplingsregistret för annat ändamål än att möjliggöra användning av deras digitala tjänster. Ett exempel är att brottsutredande myndigheter kan komma att intressera sig för en koppling och när den är gjord. Man kan också tänka sig att både organ inom EU och svenska myndigheter kommer att vilja ha uppgifter ur kopplingsregistret för statistiskt ändamål, t.ex. för att följa upp hur anslutningsgraden ser ut från olika länder inom EU samt om det är övervägande män eller kvinnor, unga eller gamla som begär koppling.

I ett livscykelperspektiv kommer kopplingen förr eller senare att upphöra. Det kan ske på begäran av den enskilde eller p.g.a. att giltigheten för den utländska eID-handlingen löper ut. En koppling kan också upphöra p.g.a. att omständigheter framkommer som gör att kopplingen inte längre är tillförlitlig. Efter att kopplingen har upphört behöver kopplingsregistret fortsätta att hålla information om tidigare kopplingar mellan svenskt personnummer och utländska eID-handlingar. Detta beror på att en koppling mellan olika identitetsbegrepp kräver spårbarhet över tid.

Livscykelperspektivet avslutas genom att uppgifter och ev. handlingar avseende en koppling som finns i kopplingsregistret gallras. Gallringen ska omfatta samtliga uppgifter som tillförts kopplingsregistret p.g.a. av att en enskild begärt koppling och som därefter tillförts under ärendehandläggningen. Skatteverket har bedömt

att en gallringsfrist om fem år från att beslut om koppling fattats är tillräcklig för att både tillgodose enskildas behov av beständighet i kopplingen och enskildas anspråk på att personuppgifter inte ska behandlas längre än nödvändigt. Gallringsfristen bedöms även tillgodose behovet av spårbarhet avseende gjorda kopplingar.

Förslaget tas in i 13 § i lagen om behandling av koppling mellan utländska eID handlingar och svenska identitetsbeteckningar.

6.6.8 Proportionalitetsbedömning

I avsnittet ovan har Skatteverket redovisat behovsbilden för kopplingsregistret och närmare beskrivit vilka uppgifter som kommer att behandlas och behandlingar som kan förväntas ske inom ramen för ett kopplingsregister. Avgränsningar till nödvändig information och ett begränsat antal behandlingar m.m. har redovisats för att skydda enskildas personliga integritet. I avsnitt 6.5 och 7 redovisar utredningen den riskanalys som genomförts kring behandlingen av personuppgifter i ett kopplingsregister.

Skatteverkets bedömning är att de integritetsrisker som kopplingsregistret innebär för den enskilde balanseras av de åtgärder som vidtas dels kring själva informationssamlingen i form av säkerhetsåtgärder, dels regleringen kring själva behandlingen av personuppgifter i kopplingsregistret. I sammanhanget har det också betydelse att det är den enskilde själv som initierar behandlingen i kopplingsregistret, och den enskilde kan också själv få behandlingen att upphöra. Med hänsyn härtill och till att behovet av att åstadkomma en koppling i varje givet ögonblick avgörs av den enskilde själv så bör behandlingen av personuppgifter enligt ovan anses som proportionerlig i förhållande till det integritetsintrång som samma behandling innebär.

6.6.9 Rättslig grund för personuppgiftsbehandling i kopplingsregistret

Av 2 kap. 6 § andra stycket regeringsformen (RF) framgår att var och en är gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Sådana åtgärder får endast begränsas genom lag i den utsträckning det är tillåtet enligt de allmänna förutsättningarna för begränsning av fri- och rättigheter som anges i 2 kap. 21 § RF. Avgörandet för om en åtgärd ska anses innebära övervakning eller kartläggning är inte dess huvudsakliga syfte utan vilken effekt åtgärden har.

Vid bedömningen av vilka åtgärder som kan anses utgöra ett ”betydande intrång” ska både åtgärdens omfattning och arten av det intrång åtgärden innebär beaktas.[16] Med andra ord innebär detta att åtgärder som är av sådant slag som anges i 2 kap. 6 § andra stycket RF bara får vidtas om det finns lagstöd för detta (jfr 2 kap. 20-22 §§ RF).

Den bedömning som här måste göras är om den personuppgiftsbehandling som utförs inom kopplingsregistret är av sådan karaktär att den kan anses utgöra sådant intrång i den personliga integriteten som avses i 2 kap. 6 § RF.

Syftet med den föreslagna regleringen om kopplingsregister är att skapa förutsättningar för att förenkla för enskilda med utländska eID-handlingar att använda dessa i samband med användning av en svensk myndighets digitala tjänst

[16] Prop. 2009/10:80 s. 171 ff.

i fall där tjänsten förutsätter att en svensk identitetsbeteckning ska kunna styrkas. Det föreslagna registret bygger på att den enskilde själv ansöker om registrering och att den enskilde när som helst kan begära att registreringen tas bort. Om den enskilde väljer att inte registrera kopplingen kan det innebära att han eller hon på annat sätt får styrka sin svenska identitetsbeteckning och eventuellt att kontakten med den svenska myndigheten får skötas på annat sätt än genom en digital tjänst. Den behandling som innebär koppling av identiteter i registret och efterföljande behandlingar sker således på frivillig väg, då registreringen i kopplingsregistret görs efter önskemål från den enskilde själv. Mot bakgrund av ovanstående finner Skatteverket att det utökade grundlagsskyddet i 2 kap. 6 § RF inte är tillämpligt. Personuppgiftsbehandlingen i kopplingsregistret är inte av sådan karaktär att den innebär övervakning eller kartläggning av den enskildes personliga förhållanden som avses i 2 kap. 6 § RF.

Det framgår av artikel 6 EU:s dataskyddsförordning att det måste finnas en rättslig grund för att det ska vara lagligt att behandla personuppgifter. En behandling kan vara tillåten om den är nödvändig för att utföra en uppgift av allmänt intresse (artikel 6.1 e). Det krävs då att det allmänna intresset är fastställt i gemenskapsrättslig lagstiftning eller nationell lagstiftning[17] (artikel 6.3). För att kunna säkerställa den rättsliga grunden allmänt intresse för behandlingen i kopplingsregistret föreslår Skatteverket därför en särskild lagstiftning. Övergripande syftar den föreslagna rättsliga regleringen till att tillgodose ett allmänt intresse och skapa ett ändamålsenligt kopplingsregister som motsvarar dagens och framtidens behov.

Genom att i särskild lag avgränsa för vilka ändamål uppgifterna i kopplingsregistret får behandlas och även tydligt avgränsa vilka uppgifter som får omfattas av behandlingen begränsas riskerna för integritetsintrång mot enskilda. De behandlingar som kan komma att utföras med aktuella personuppgifter blir förutsebara för den enskilde samtidigt som myndighetens möjligheter att behandla uppgifterna tydligt avgränsas. Även ändamålsregleringen som avgränsar när en myndighet får ha direktåtkomst till kopplingsregistret bidrar till förutsebarheten i vilka behandlingar som kan aktualiseras för uppgifterna i registret.

Skatteverket föreslår även att den självständiga verksamhetsgren som tillhandahållande av kopplingsregister bör utgöra ska regleras särskilt i den myndighetsinstruktion som gäller för aktuell värdmyndighet. Detta medför ett tydligt utpekat ansvar för den myndighet som har att tillhandahålla kopplingsregistretregistret samt visar lagstiftarens intentioner vad gäller den rättsliga grunden för behandlingen i registret.

Känsliga personuppgifter

Det stadgas i 3 kap. 3 § 2 p. kompletterande dataskyddslagen att känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning om behandlingen är nödvändig för handläggningen av ett ärende. Skatteverket anser att behandlingen av känsliga personuppgifter vid ärendehandläggningen i kopplingsregistret är nödvändig för att kunna säkerställa att kopplingar i registret är korrekta. Möjligheten att behandla känsliga personuppgifter vid handläggningen av ett ärende utgör därför ett viktigt allmänt

[17] Det stadgas i 2 kap. 2 § 1 p. lagen (2018.218) med kompletterande bestämmelser till EU:s dataskyddsförordning att personuppgifter får behandlas med stöd av artikel 6.1 e i EU:s dataskyddsförordning, om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

intresse, då det ämnar säkerställa att en koppling eller borttagande av en koppling i registret kan ske på ett effektivt och rättssäkert sätt.

Personuppgifter som rör lagöverträdelser

Uppgifter om lagöverträdelser får enligt 3 kap. 8 § 1 st. kompletterande dataskyddslagen behandlas av myndigheter (se artikel 10 EU:s dataskyddsförordning). Detta innebär att myndigheter inte behöver uttryckligt stöd i föreskrifter eller särskilda beslut för att få behandla sådana uppgifter.[18] Skatteverket gör därför bedömningen att uppgifter om lagöverträdelser kan behandlas vid ärendehandläggning för att t.ex. pröva om en genomförd koppling är korrekt med hänsyn till inkomna uppgifter om någon form av identitetsrelaterad brottslighet.

6.6.10 Ansvar för uppgifters riktighet

Förslag: Ansökan om registrering i kopplingsregistret ska innehålla en försäkran på heder och samvete att eID-handlingen avser samma person som identitetsbeteckningen.

Skälen för förslaget: Skatteverket anser att ansökan ska innehålla en försäkran på heder och samvete att det råder identitet mellan användarens identitetsbeteckning och den person som avses med den elektroniska identitetshandlingen. Enligt 15 kap. 10 § brottsbalken kan den som lämnar osann uppgift, när uppgiften enligt lag eller annan författning lämnas på heder och samvete, göra sig skyldig till osann försäkran och dömas för det. Ansvaret för uppgiftens riktighet läggs därmed på den ansökande personen.

Den registerförande myndighetens ansvar för registrerade uppgifter är att uppgifterna registreras och i övrigt behandlas i enlighet med gällande bestämmelser. Ansvaret för att den utländska eID-handlingen är riktig ligger hos behörig myndighet i det utfärdande landet.

Förslaget tas in i 3 § i förordningen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

6.6.11 Personuppgiftsansvar

Förslag: Skatteverket är personuppgiftsansvarigt för behandlingar av personuppgifter som myndigheten utför i kopplingsregistret. Även för andra behandlingar som närmast är att hänföra sig till förvaltningen av kopplingsregistret vilar ansvaret hos Skatteverket.

Polisen är personuppgiftsansvarig för behandlingar av personuppgifter som sker i anslutning till ärendehanteringen för att pröva och besluta om kopplingar. Det är normalt polisen som vid ärendehanteringen för in uppgifter i kopplingsregistret. För den behandlingen ska polisen vara personuppgiftsansvarig.

DIGG är personuppgiftsansvarig för de behandlingar av personuppgifter myndigheten behöver göra för att kontrollera förekomsten av koppling samt för att förmedla identitetsinformation till andra myndigheter.

Skälen för förslaget: Personuppgiftsansvarets placering och omfattning är en central fråga för reglerna gällande dataskydd. Det är avgörande för skyddet av den

[18] Prop. 2017/18:105 s. 99.

enskildes integritet och för att dataskyddsreglerna ska fungera att personuppgiftsansvaret uppfattas korrekt av den som utför behandlingar av personuppgifter. Någon tvekan om vilken myndighet som bär ansvaret för bristande regelefterlevnad får därför inte finnas. Ansvaret för att den enskildes rättigheter inte kränks ankommer på den personuppgiftsansvarige att axla och det måste stå klart till vem den registrerade ska vända sig till för att kunna ta tillvara sina rättigheter.

Personuppgiftsansvarig är den offentliga myndighet som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller av medlemsstaternas nationella rätt kan det skrivas ut vem som är personuppgiftsansvarig i unionsrätten eller i medlemsstaternas nationella rätt (artikel 4.7 EU:s dataskyddsförordning). Det är alltså den som bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till som har ansvaret för behandlingen. Det finns med andra ord inte någon generell regel eller definition av vem eller vilka som har personuppgiftsansvaret. Det är de faktiska omständigheterna i det enskilda fallet som avgör vem som är personuppgiftsansvarig. Vem som är personuppgiftsansvarig kan dock särskilt anges i lag eller förordning, till exempel i särskilda registerlagar.

För behandlingar som sker i kopplingsregistret bör personuppgiftsansvaret vila hos den myndighet som får uppdraget att hålla registret. Skatteverket föreslår i avsnitt 6.7. att Skatteverket ska vara ansvarig myndighet för kopplingsregistret. Personuppgiftsansvaret i den delen bör omfatta behandlingar som innebär förvaltning av kopplingsregistret. Behandlingar av personuppgifter som Skatteverket bör ansvara för är t.ex. uttag av statistsammanställningar, tillhandahållande av utdrag enligt art. 15 EU:s dataskyddsförordning och gallring. Det är även Skatteverket som ansvarar för den tekniska utformningen och säkerhetsarrangemangen kring kopplingsregistret.

I denna promemoria föreslår Skatteverket att Polisen ska ansvara för identifieringen av sökanden i samband med den personliga inställelsen (se avsnitt 6.7). I praktiken innebär det att polisen är den myndighet som kommer att handha ärendehanteringen där kopplingen mellan en utländsk eID-handling och ett svenskt personnummer ska prövas. Ärendehandläggningen kan i vissa fall innebära att en ansökan avskrivs om sökanden inte fullföljer sin begäran. Normalt sett borde dock ärendehandläggningen innebära att beslut fattas om att etablera en koppling mellan identiteter eller att beslut fattas om att inte medge en koppling. För den behandling av personuppgifter som sker inom ramen för ärendehandläggningen bör polisen vara personuppgiftsansvarig. Personuppgiftsansvaret som kommer att vila på polisen avser t.ex. att de uppgifter som sökanden lämnar i ärendet registreras in på ett korrekt sätt.

Av denna promemoria framgår även att DIGG ska vara ansvarig för den svenska nod som är tänkt att användas för att kontrollera förekomsten av koppling samt för att förmedla identitetsinformation till andra myndigheter (se avsnitt 3.1 och 3.4). Skatteverket föreslår därför att DIGG ska vara personuppgiftsansvarig för dessa behandlingar.

Skatteverket bedömer också att det är lämpligt att särskilt reglera personuppgiftsansvaret i författning. Genom att i särskild lag reglera personuppgiftsansvaret skapas en överblick och en transparens som motverkar att oklarheter uppstår för den registrerade om vem som är personuppgiftsansvarig för de olika behandlingarna i kopplingsregistret. Ett utpekat personuppgiftsansvar i

författning gör det också enklare för den registrerade att kunna tillvarata sina rättigheter.

Förslaget tas in i 6 § i lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

6.6.12 Ansökan och registrering

Förslag: Ansökan om registrering ska göras skriftligen och innehålla de uppgifter som behövs för prövningen. Koppling ska registreras om ansökan har gjorts på föreskrivet sätt och den sökande har styrkt både sin identitet och kopplingen med eID-handlingen. Ansökan ska avslås om det som har föreskrivits i fråga om ansökan inte har iakttagits och sökanden inte har följt en uppmaning att avhjälpa bristen. En registrering ska tas bort om den registrerade skriftligen ansöker om det, om det framkommer att eID-handlingen inte längre gäller, inte längre ska erkännas eller det finns skäl att anta att eID-handlingen inte avser den registrerade.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om ansökan och registrering.

Skälen för förslaget: Ansökan om att få en koppling registrerad kommer bara att kunna göras genom den digitala tjänst som har beskrivits i avsnitt 6.4.1. Som stöd för det behövs regler om att ansökan måste vara skriftlig. Det innefattar även digital skrift. För att kunna pröva ärendet om koppling ska registreras måste vissa uppgifter lämnas av den sökande; namn, svensk identitetsbeteckning och uppgift om utländsk identitetsbeteckning. Den sökande behöver också kunna styrka dessa uppgifter på samma sätt som när man ansöker om en fysisk id-handling i Sverige. Kopplingen till den utländska eID-handlingen styrks genom att användaren loggar in hemifrån och skapar en väntande koppling.

Om ansökan inte har gjorts på rätt sätt ska den sökande informeras om vad som behöver åtgärdas. I de fall den sökande inte uppfyller kraven för ansökan ska den avslås.

En registrerad koppling ska enkelt kunna tas bort om den enskilde skriftligen begär det. Om det framkommer att eID-handlingen inte längre gäller, inte längre ska erkännas eller det finns skäl att anta att eID handlingen inte avser den registrerade ska den registrerade kopplingen också tas bort.

Det kan komma att behövas fler regler om ansökan och registrering. Skatteverket föreslår därför att regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om ansökan och registrering. Skatteverket föreslår även i denna promemoria mer detaljerade regler om vad ansökan ska innehålla och vad som krävs för att koppling ska registreras i förordningsform (se avsnitt 1.3 och 6.4.1).

Förslagen tas in i 7-10 §§ i lagen om behandling av koppling mellan utländska eID handlingar och svenska identitetsbeteckningar samt i 3-4 §§ i förordningen om behandling av koppling mellan utländska eID handlingar och svenska identitetsbeteckningar.

6.6.13 Fråga om sekretess för uppgifter i registret

Förslag: Uppgifterna i kopplingsregistret bör sekretessregleras på ett sätt som erbjuder motsvarande skydd som likartade uppgifter har i andra databaser med identitetsinformation.

För att säkerställa att också enskilda med sekretessmarkerade personuppgifter ska kunna använda och koppla sin utländska eID-handling ska kopplingsregistret få innehålla uppgift om sekretessmarkering.

Skälen för förslaget: De uppgifter som ska behandlas enligt förslaget om kopplingstjänst och register kan vara integritetskänsliga. I kopplingsregistret ska bl.a. svenska personnummer och utländska identitetsbeteckningar behandlas. Även känsliga personuppgifter kan komma att behandlas inom ramen för ett kopplingsärende. I Sverige gäller som huvudregel att offentlighet gäller för enskildas identitetsbegrepp, t.ex. personnummer och namn. I register och databaser som innehåller identitetsuppgifter gäller normalt sekretess med ett rakt skaderekvisit, t.ex. enligt 22 kap. 1 § offentlighets- och sekretesslagen. Det bör därför övervägas om också uppgifterna i kopplingsregistret ska åtnjuta samma sekretesskydd som likartade uppgifter har i andra sammanhang.

Kopplingsregistret kommer att innehålla uppgifter om enskilda individer såsom deras svenska personnummer, namn, adress och ev. andra kontaktuppgifter. Motsvarande uppgifter finns i t.ex. Skatteverkets folkbokföringsdatabas och i Skatteverkets identitetskortsdatabas. För uppgifter i båda dessa databaser gäller sekretess enligt 22 kap. 1 § offentlighets- och sekretesslagen. Sekretessen gäller med ett rakt skaderekvisit vilket innebär att det råder en presumtion för att uppgifterna är offentliga. Det finns dock en möjlighet att åberopa sekretessbestämmelsen om det i ett enskilt fall finns särskild anledning att anta att den enskilde eller någon närstående till denne lider men om uppgiften röjs. Sekretessregeln ger uttryck för en avvägning av sekretesskyddet som är vanligt förekommande i uppgiftssamling där motsvarande personuppgifter förekommer. Enligt Skatteverkets mening finns det inte någon anledning att göra en annan bedömning av sekretessbehovet för uppgifter i kopplingsregistret än vad som traditionellt görs för motsvarande uppgifter i andra sammanhang.

Inom vissa andra länder som omfattas av eIDAS-förordningen finns en från svenskt perspektiv avvikande uppfattning om behovet av sekretesskydd för identitetsuppgifter. Presumtionen är att sekretess gäller för uppgiften och det råder stor försiktighet i hanteringen av uppgifterna för att förhindra spridning. För att skydda identitetsuppgifterna har många medlemsländer i sin anpassning till eIDAS-förordningen beslutat att använda pseudonymer i stället för att i systemet skicka över identitetsuppgifterna i klartext. Användning av pseudonymer vid elektroniska transaktioner ska enligt Artikel 5.2 eIDAS-förordningen inte förbjudas. Det står alltså medlemsstaterna fritt att skydda sina medborgares personuppgifter genom pseudonym. Med hänsyn härtill bör det förhållandet att synen på skyddsbehovet för identitetsuppgifter i andra länder kan avvika från synen på skyddsbehovet i Sverige, inte föranleda någon annan bedömning än ovan.

En annan sekretessaspekt gäller personer med skyddade personuppgifter. För folkbokförda personer som har behov av skydd kan Skatteverket föra in en markering i folkbokföringsdatabasen som innebär en varningssignal om behovet av att göra en noggrann sekretessprövning innan uppgifter lämnas ut. Om skyddade personuppgifter lämnas ut till andra myndigheter följer sekretessmarkeringen med, och uppgifterna ska skyddas på samma sätt hos nästa myndighet som tar emot dem.

Personer som har sekretessmarkering i folkbokföringsregistret och som begär koppling mellan sin utländska eID-handling och sitt svenska personnummer bör få sitt sekretessbehov tillgodosett också vid behandlingar inom kopplingsregistret. För att tillgodose deras behov och därigenom tillgängliggöra

kopplingsfunktionaliteten för den här gruppen av människor föreslår Skatteverket att kopplingsregistret ska få innehålla uppgift om enskildas sekretessmarkering från folkbokföringsdatabasen.

Sekretessmarkeringen och skyddsbehovet kan komma att ändras över tid vilket innebär att kopplingsregistret då skulle innehålla en felaktig uppgift. Eftersom livscykeln är så pass kort, fem år, anser Skatteverket att intresset av att människor med skyddade personuppgifter ska kunna använda kopplingsfunktionen väger tyngre än att registret kan innehålla inaktuella uppgifter en kortare tid. I samband med ett utlämnandeärende bör man också rutinmässigt kontrollera mot folkbokföringen om spärren kvarstår.

Förslaget föranleder en ändring i 22 kap. 1 § offentlighets- och sekretesslagen (2009:400).

6.7 Ansvarig myndighet

Förslag: Skatteverket blir ansvarig myndighet för kopplingsregistret. Polisen blir ansvarig myndighet för kontroll av identitet vid personlig inställelse.

Skälen för förslaget: Det finns några tänkbara olika lösningar för vilken myndighetsorganisation som skulle kunna ha ansvaret för kopplingsregistret. Skatteverket gör dock avgränsningen att endast befintliga myndigheter kan komma ifråga för uppdraget. Det finns, enligt Skatteverkets mening, inga skäl för att inrätta en ny myndighet för uppdraget.

För att få en koppling registrerad behöver det klarläggas att användaren är identisk med innehavaren av en viss identitetsbeteckning. Samma grad av säkerhet ska krävas vid identifieringen som vid utfärdande av en id-handling för att övriga myndigheter ska kunna lita på att uppgifterna i registret är korrekta. Annars blir kopplingsregistret inte användbart.

Förslaget är utformat så användaren startar processen för att registrera koppling genom att logga in med den eID-handling som hen vill koppla till ett svenskt personnummer i en digital tjänst och där skapa en väntande koppling. Därefter inställer sig användaren fysiskt hos Polisen, som ska utföra identitetskontroll, och styrker sin identitet på motsvarande sätt som krävs för utfärdande av svenska pass och id-kort. Efter kontroll använder handläggaren den väntande kopplingen för att slutföra registreringen av koppling mellan eID-handlingen och det svenska personnumret. Inledningsvis ska det alltså utvecklas en tvåstegsprocess med personlig inställelse för att få en koppling registrerad. Därefter kan helt elektroniska lösningar utvecklas genom id-koppling och bilaterala avtal.

Skatteverket har gedigen erfarenhet av att utveckla och förvalta register och digitala tjänster med höga krav på säkerhet. Skatteverket har även en bred erfarenhet av verksamhet som innebär bedömning, kontroll och registrering av identitet och andra personuppgifter, exempelvis vid ärenden om invandring. Skatteverket föreslår därför att Skatteverket blir ansvarig myndighet för att förvalta kopplingsregistret och fortsättningsvis utveckla de elektroniska alternativen för att registrera kopplingar.

När det gäller identitetskontroll vid personlig inställelse finns olika tänkbara lösningar för vilken myndighet som ska vara ansvarig.

Sedan juni 2009 utfärdar Skatteverket identitetskort för folkbokförda i Sverige. Årligen utfärdas cirka 100 000 id-kort. Ansökan kan göras vid 27 kontor i landet, som en del av de arbetsuppgifter som förekommer vid ett servicekontor.

Genomförda kvalitetssäkringar av arbetet på servicekontoren visar på en god kvalitet och id-kortet har stort förtroende hos användare av identitetshandlingar i samhället. Skatteverket skulle därmed också kunna ansvara för identitetskontrollen vid personlig inställelse men är i sammanhanget inte den myndighet som kan antas ha bäst förutsättningar för service när det gäller att utföra fysisk identifiering på ett besökskontor.

Polisen utför identitetskontroller i samband med utfärdande av olika typer av resehandlingar för svenska medborgare, t.ex. pass och nationellt identitetskort. Dessa handlingar accepteras som identitetshandling i Sverige. Utfärdandet sker på ett hundratal expeditioner runt om i landet med hjälp av egen personal som har särskild utbildning för att hantera arbetsuppgiften. Polisen utfärdar årligen cirka 1,8 miljoner pass och nationella identitetskort. Myndigheten får därför anses ha stor erfarenhet av identitetskontroll, även om denna kontroll endast avser svenska medborgare. Verksamheten har, på samma sätt som Skatteverkets id-kort, stort förtroende hos användare av identitetshandlingar i samhället. Med hänsyn till omfattningen av Polisens verksamhet, tillgängligheten samt medarbetarnas erfarenhet och kunnande har Polisen sammantaget goda förutsättningar för att ansvara för den fysiska identifieringen vid personlig inställelse för att få en koppling registrerad i kopplingsregistret.

Skatteverket föreslår alltså att ansvaret delas mellan två myndigheter. Det är inte olikt det system som råder i dag när det gäller t.ex. rekvirering och tilldelning av samordningsnummer. Det är den rekvirerande myndigheten som ansvarar för identitetskontrollen och Skatteverket som ansvarar för tilldelning, registerföring och digitala tjänster.

I mars 2019 kommer resultatet av 2017 års ID-kortsutredning[19] att presenteras. Det kan hända att utredningen föreslår någon sorts organisationsförändring för att hantera frågor om id-handlingar men innan utredningens betänkande är offentligt utgår Skatteverket från den rådande situationen. Den princip som kan framhållas när det gäller Skatteverkets resonemang om ansvarig myndighet är att det vore bra för id-handlingarnas kvalitet om hanteringen av dessa centraliserades till den myndighet som har störst kompetens för att utföra identitetskontroller. Samma myndighet bör också ansvara för den fysiska inställelsen för registrering av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

Förslaget tas in i 1 § i lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.

6.7.1 Kopplingsregistret ska vara en självständig verksamhetsgren

Förslag: Bestämmelser om att kopplingsregistret ska vara en självständig verksamhetsgren införs i Polisens och Skatteverkets instruktioner.

Skälen för förslaget: Tillhandahållande av kopplingsregister bör utgöra en självständig verksamhetsgren. Detta bör regleras särskilt i värdmyndighetens instruktion. Skatteverket föreslår därför en ändring av den egna instruktionen samt i Polisens instruktion. Det medför ett tydligt utpekat ansvar för Skatteverket att tillhandahålla kopplingsregistret samt visar lagstiftarens intentioner när det gäller den rättsliga grunden för personuppgiftsbehandlingen i registret. Det visar även en gränsdragning mot Polisens ansvar som gäller för handläggning av ärenden om koppling.

[19] Dir. 2017:90 Åtgärder för att minska bedrägeribrottsligheten – skärpta krav och rutiner för svenska identitetshandlingar.

I kopplingsregistret kommer samtliga kopplade utländska eID-handlingar och kopplade svenska personnummer finnas registrerade. Genom att det som rör kopplingsregistret görs till en egen verksamhetsgren hos respektive myndighet stärks integritetsskyddet för enskilda som finns registrerade. Antalet personer som är behöriga att behandla uppgifter i registret och i handläggningen av kopplingsärenden kommer då att lättare kunna hållas nere och det blir enklare att administrera de behörigheter till registret som krävs.

Förslaget föranleder en ny 6 a § i förordningen (2014:1102) med instruktion för Polismyndigheten och en ny 12 a § i förordningen (2017:154) med instruktion för Skatteverket.

6.7.2 Ikraftträdandebestämmelser

Förslag: De föreslagna bestämmelserna ska träda i kraft den 1 juli 2020.

Skälen för förslaget: Skatteverket behöver tid för att bygga upp den beskrivna tjänsten för koppling och kopplingsregistret. Även Polisen behöver tid för systemintegrering och för att inrätta rutiner och struktur för identitetskontroll vid personlig inställelse. Skatteverket föreslår därför att bestämmelserna ska träda i kraft den 1 juli 2020.

6.7.3 Registrering av koppling vid utlandsmyndigheter som är passmyndigheter

Bedömning: De europeiska utlandsmyndigheter som är passmyndigheter är för närvarande inte bemannade med den kompetens som krävs för att genomföra säkra identitetskontroller och granska id-handlingar. Möjligheten att registrera kopplingar efter personlig inställelse hos utlandsmyndigheter bör införas först efter att identitetskontroll vid personlig inställelse har testats hos Polisen och det är klart att det finns ett tydligt behov av att erbjuda samma tjänst hos vissa större utlandsmyndigheter i Europa.

Skälen för bedömningen: Enligt det förslaget om identitetskontroll vid personlig inställelse som lämnas i denna promemoria ska användaren uppsöka Polisen för att identiteten ska kunna kontrolleras. Ett ytterligare alternativ är att identifieringen även skulle kunna ske vid vissa svenska utlandsmyndigheter. Det skulle underlätta för användare som inte regelbundet kommer till Sverige. Ett sådant förslag bör kopplas till att personalen i fråga utför arbetsuppgifter som innebär kontroll av identitet vid utfärdande av olika typer av resehandlingar som kan användas som id-handling i Sverige. De utlandsmyndigheter som då kan bli aktuella är de som även är passmyndigheter i utlandet. Detta måste i så fall regleras i en förordning.

Skatteverket har samrått med utrikesdepartementet i frågan. Då framkom bl.a. följande. Sverige har endast två större ambassader inom EU som även är passmyndigheter, i Berlin och i Paris. Flera befattningar på dessa utlandsmyndigheter som tidigare var bemannade med utsänd personal har omorganiserats och är numera bemannade med lokalt anställd personal. Passfrågor och identifieringsfrågor ska skötas av utsänd personal. Det är ingen uppgift som lokalt anställda kan eller får ta över, annat än under mycket särskilda förhållanden och i så fall krävs bemyndigande från UD:s säkerhetsenhet. Identifieringsfrågor – som detta gäller - kan dessutom vara mycket komplicerade. UD ser därför inte att svenska passmyndigheter i Europa har möjlighet att ta på sig ytterligare

arbetsuppgifter i form av identifiering och andra frågor i samband med koppling av utländska eID-handlingar till svenska personnummer.

Utlandsmyndigheterna hjälper till med s.k. levnadsintyg trots att den frågan ligger hos Pensionsmyndigheten under Socialdepartementet. Där kräver man inte lika hög säkerhet som när det gäller utfärdande av pass och ID-handlingar.

Skatteverket är av uppfattningen att förslaget om kopplingsregister och tjänst för registrering behöver tas i flera steg. Det första sättet att registrera kopplingar mellan utländska eID-handlingar och svenska personnummer bör vara efter identitetskontroll vid personlig inställelse hos Polisen. Därefter kan utlandsmyndigheterna bli aktuella efter att man fått en uppfattning om hur stor efterfrågan är och vilka utlandsmyndigheter som kan komma i fråga innan man bemannar dem med den kompetens som behövs.

6.8 Utvecklingsmöjligheter

I rapporten om kopplingsregister som Skatteverket lämnade 2016 föreslogs tre alternativa sätt att registrera kopplingar mellan utländska eID-handlingar och svenska identitetsbeteckningar. Efter ytterligare utredning föreslår Skatteverket i denna rapport att ett av alternativen, fysisk inställelse och identitetskontroll, ska vara det sätt som inledningsvis ska användas för att registrera kopplingar.

Det utesluter inte att de övriga alternativen kan komma att bli aktuella vid senare tillfälle. Nedan beskrivs därför de övriga sätt att registrera kopplingar som Skatteverket har övervägt. Dessa alternativ kan ses som vägar att utveckla kopplingstjänsten och kopplingsregistret en tid efter att systemet har startat, använts och utvärderats.

6.8.1 Koppling till svensk eID-handling och vidare eID-kopplingar

Användaren genomför en eID-koppling genom att registrera en koppling mellan en tidigare registrerad eID-handling och en ny eID-handling. För användare som har en svensk eID-handling kan denna eventuellt användas i ett förfarande med koppling till en utländsk eID-handling.

Det finns inget som hindrar att en användare kan ha flera eID-handlingar utfärdade i olika länder. En digital väg att registrera en koppling till en utländsk eID-handling är att användaren själv kan göra en eID-koppling. Det innebär att användaren loggar in med en tidigare kopplad eID-handling och godkänner att ytterligare en utländsk eID-handling kopplas till den svenska identitetsbeteckningen, s.k. id-växling. Detta ger en möjlighet till registrering med motsvarande säkerhetsnivå som vid fysisk inställelse.

Att använda eID-koppling skulle ge möjlighet till digital registrering för en grupp användare som snabbt kan öka i antal. Myndigheter kan i framtiden informera privatpersoner inför utlandsflytt om eventuell möjlighet att göra en sådan eID-koppling medan de fortfarande har en giltig svensk eID-handling. I sådant fall kan det röra sig om alla svenska invånare som flyttar ur landet.

För att stärka säkerheten kan en bekräftelse skickas till den registrerade adressen som tillhör den person vars identitetsbeteckning ska kopplas ihop med en eID-handling. En sådan rutin skulle medföra bättre skydd mot felaktiga kopplingar. Det är samtidigt en trög lösning eftersom det skulle ta betydligt längre tid innan personen kan logga in i tjänsten. Det skulle också bli svårt att nå personer eftersom utländska adresser inte behöver uppdateras i den svenska folkbokföringen.

En förutsättning för id-växling är att utfärdaren av eID-handlingen tillåter att den får användas för id-växling. Privata utfärdare kan inte tvingas tillåta id-växling. De får själva avgöra hur de vill att deras produkt ska kunna användas. Utredningen om nationella digitala tjänster föreslog i sitt slutbetänkande att staten ska utfärda en eID-handling på högsta tillitsnivå som ska kunna användas att id-växla från. Det skulle avhjälpa problemet.[20]

Av flera skäl, även beskrivna i avsnitt 6.4, anser Skatteverket att det första steget när det gäller registrering av kopplingar mellan utländska eID-handlingar och svenska personnummer bör innehålla identifiering vid fysisk inställelse. Som nästa fas i utvecklingen kan man dock tänka sig en process enligt följande steg:

1. Användaren som önskar koppla sitt svenska personnummer till en eID-handling begär åtkomst till den tjänst som kopplings-registersystemet tillhandahåller för detta ändamål.

2. Användaren omdirigeras till anvisningstjänsten för att välja eID-handling för inloggning.

3. Användaren väljer att logga in med den eID-handling som ska kopplas till (motsvarande identitets) personnummer.

4. eIDAS-systemet (svensk och utländsk nod) hanterar identifieringen och skickar sedan användaren tillbaka till tjänsten.

5. Användaren väljer ”Koppla eID själv” i tjänsten.

6. Applikationen visar en vy för att ange uppgifter för kopplingen.

7. Användaren uppger det personnummer som ska kopplas.

8. Tjänsten genererar en engångskod/sekvens-ID.

9. Anrop till API-applikationen för att skapa en ”väntande koppling”. I anropet skickas informationen från sessionen/eID-handlingen (namn, födelsedatum och PRID/eIDAS-ID), angivet personnummer samt engångskod/kopplingsidentifierare.

10. API-applikationen hämtar uppgifter (namn, födelsedatum) från folkbokföringen baserat på uppgivet personnummer.

11. Kontroll att uppgifter från eID-handlingen och uppgifter från folkbokföringen stämmer överens. Kontrollen består i att namn och födelsedatum ska stämma överens. Vad gäller namnet kan man antingen kräva att de är exakt samma eller tillåta mindre skillnader (t.ex. orsakat av att namnet translittererats olika).

12. En ”väntande koppling” skapas i databasen. Uppgifter som sparas är sessions-information från eID-handlingen, personnummer samt den genererade engångskoden/kopplingsidentifieraren.

[20] SOU 2017:114, s. 187 ff.

13. Information om uppgifter hämtade från eID-handlingen och folkbokföringen presenteras sida vid sida i användargränssnittet, inklusive personnummer. (Engångskoden/sekvens-ID sparas i sessionen.)

14. Användaren uppmanas att ”på heder och samvete” skriva under att kopplingen ska genomföras och informeras om att underskriften ska ske med en elektronisk id-handling som bär med sig det personnummer som eID-handlingen ska kopplas till (dvs. en svensk elektronisk id-handling, eller en sedan tidigare kopplad eID-handling). En lista över elektroniska id-handlingar presenteras.

15. Användaren godkänner enligt ovan genom att välja elektronisk id-handling och trycka ”skriv under”.

16. Tjänsten initierar en underskrift med vald elektronisk id-handling samt uppgivet personnummer genom att en underskriftsbegäran skickas till underskrifttjänsten (ev. via stödtjänst).

17. Användaren autentiserar sig för underskrift. I fallet att en redan kopplad eID-handling används sker först val av eID-handling eftersom den IdP som anges i anropet lär bli den svenska eIDAS-noden(?).

18. Underskrifttjänsten mottar identitetsintyg, personnummer används som identifierare (i fallet att kopplad eID-handling används gäller alltså att plocka ut ”rätt” identifierare, dvs. personnummer, som ju den svenska eIDAS-noden i detta fall lagt till ”på väg in”).

19. Underskriftstjänsten skapar nyckel och certifikat och underskrift.

20. Underskriften skickas till tjänsten.

21. Tjänsten (ev. med hjälp av stödtjänst) validerar och sätter samman dokumentet med underskriften.

22. Tjänsten anropar API-applikationen för att etablera koppling. I anropet skickas personnummer, engångskod/sekvens-ID, samt information (namn, födelsedatum) från underskriften (dvs. från den elektroniska id-handlingen/identitetsintyget som bär personnummer som identifierare), samt det underskrivna dokumentet.

23. API-applikationen hämtar uppgifter om väntande koppling baserat på engångskoden.

24. API-applikationen hämtar personuppgifter från folkbokföringen baserat på personnummer från väntande kopplingen.

25. Uppgifter från den väntande kopplingen, folkbokföringen och uppgifter från underskriften jämförs. Uppgifter som jämförs är namn och födelsedatum.

26. API-applikationen skriver till databasen för att etablera kopplingen mellan eID-handlingen och personnumret. Det underskrivna dokumentet sparas som bevis i anslutning till kopplingen.

27. API-applikationen skriver till databasen för att markera den väntande kopplingen som utförd (baserat på engångskoden).

28. Tjänsten visar en vy för användaren som berättar att koppling mellan eID-handling och personnummer är skapad.

6.8.2 Bilaterala överenskommelser

Sverige kan komma att träffa överenskommelser med andra länder i bi- eller multilaterala avtal och i så fall enas om att eID-handlingarnas unika identitetsbeteckningar ska innehålla personnummer eller motsvarande beständiga identitetsbeteckningar. En eID-handling ska kunna kopplas mot en svensk identitetsbeteckning i enlighet med ett sådant avtal via ett elektroniskt system.

För att kunna få till stånd elektroniska lösningar för att registrera kopplingar enligt denna modell behöver Sverige ingå överenskommelser med de andra medlemsstaterna. De medlemsstater som använder identitetsbeteckningar som är beständiga över tid kan vara lämpliga att börja utbytet med (Norden). Det kan också vara värdefullt att ingå avtal med länder dit många svenskar flyttar (t.ex. Spanien).

De nordiska länderna har liknande system som Sverige i dag, med personbeteckningar i nästan samma format som de svenska som är bestående över lång tid. Det finns intresse bland de nordiska länderna för ett fördjupat samarbete tack vare de möjligheter som kan tillvaratas med anledning av våra liknande system. Ett sådant samarbete skulle även gagna säkerheten för kopplingar länderna emellan. Det är troligt att många av de europeiska användarna av svenska digitala tjänster kommer att vara nordiska medborgare som arbetar eller studerar eller äger fastigheter eller fordon i Sverige som en följd av den geografiska närheten.

Bilaterala överenskommelser mellan de nordiska länderna kan användas för att fördjupa samarbetet i de frågor som blir aktuella för att underlätta kopplingar mellan nordiska eID-handlingar och svenska identitetsbeteckningar. I detta sammanhang behöver Sverige tillgång till de nordiska personnumren för att med tillräcklig säkerhet kunna registrera en koppling till en eID-handling. Därför bör man avtala om att eID-handlingarnas unika identitetsbeteckningar ska innehålla personnumren.

För att kunna använda de uppgifter som förmedlas via identitetsintyg i eID-handlingen behöver den registerförande myndigheten ha möjlighet att lagra uppgifter som kan jämföras med dessa. Uppgifter för jämförelse kan tas in när identitetsbeteckningen tilldelas. Det finns redan i dag stöd i 2 kap. 3 § 16 p. lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet, FdbL, för att behandla nordiska personnummer i folkbokföringsdatabasen. Bestämmelsen kan på sikt utökas med identitetsbeteckningar från andra medlemsstater.

Ett alternativ är att även lagra uppgifterna i kopplingsregistret. När användaren ansöker om att få en koppling registrerad finns uppgifterna då direkt tillgängliga att jämföra med identitetsintyget från eID-handlingen.

Bilaterala avtal är beroende av att det finns en ömsesidig vilja från de aktuella länderna att ingå sådana avtal. Det finns mycket som tyder på att sådana här överenskommelser kan slutas inom en snar framtid. Under nordiska ministerrådets möte i Oslo hösten 2018 lyftes eID-frågor fram som ett prioriterat område. Norge och Direktoratet for forvaltning og ikt (Difi) leder det nordisk-baltiska eID-projektet (Nobid). Samarbetet utgår från den nordisk-baltiska ministerförklaringen (Digital North), där användning av nationella eID-handlingar över landsgränserna är ett centralt insatsområde.

7 Risker för angrepp och missbruk

Skatteverket ska i det fördjupade utredningsuppdraget särskilt analysera riskerna för att det föreslagna kopplingsregistret kan angripas och nyttjas i missbrukssyfte och lämna förslag på hur sådana eventuella risker ska hanteras för att förhindra missbruk av identitetshandlingar och därigenom förebygga bedrägerier och brott mot välfärden.

Som tidigare beskrivits i avsnitt 2.2 är riskerna för angrepp och missbruk inte bara beroende av Skatteverkets förslag till lösning när det gäller kopplingsregister och registrering av koppling. Systemet som följer av eIDAS-förordningen är ett komplext nät av komponenter i alla medlemsstater som genom förordningen har förbundit sig att lita på varandras grundidentifieringar och eID-lösningar. Om det inträffar en incident som påverkar tilliten mellan länderna kan det även få stor betydelse när det gäller risker för angrepp och missbruk av det svenska kopplingsregistret trots att Sverige inte behöver vara inblandat i den del av systemet där incidenten inträffade.

För att lösa denna del av uppdraget har Skatteverket haft möten och kontakter med Polisens nationella bedrägericenter och Gränspolisen. Nedan följer en redogörelse för de analyser som har gjorts baserade på scenarier över hur kopplingstjänsten skulle kunna angripas i missbrukssyfte.

7.1 Identitetskapning

Bedömning: För att förebygga identitetskapning och missbruk av den kapades registrerade kopplingar behövs tydlig och lättillgänglig information om eIDAS-förordningen samt hur kopplingstjänsten och registret fungerar.

Skälen för bedömningen: En identitetskapning tar sig uttryck genom att någon lyckas komma över tillräckligt många uppgifter om en annan person för att kunna utföra handlingar i denna persons namn. För kaparen handlar det ofta om att tillskansa sig pengar genom att i en annan persons namn t.ex. ta lån, beställa varor som går att sälja vidare eller få dyra tjänster utförda utan att behöva betala för dem.

Vid en identitetskapning är syftet kanske inte först och främst att komma över en koppling till ett svenskt identitetsbegrepp. Om kaparen känner till identiteten på den kapade personen väl kan det genom en central kopplingstjänst ändå uppstå att identitetskapningen även ger tillgång till ett svenskt identitetsbegrepp. Kaparen kan då utföra handlingar i svenska digitala tjänster genom att utge sig för att vara den kapade personen.

Handlingarna skulle kunna gå till på samma sätt som om en svensk eID-handling utsätts för kapning. De mest använda svenska eID-handlingarna BankID och Mobilt BankID har hittills inte blivit kapade på teknisk väg såvitt är känt. Däremot använder sig bedragare av s.k. social engineering, dvs. att de genom kontakter med offret lurar honom eller henne att lämna ut sina inloggningsuppgifter till kaparen. Det kan gå till så att kaparen utger sig för att vara en försäljare eller komma från en myndighet och vilja hjälpa offret att t.ex. välja fonder eller på annat sätt erbjuda någon tjänst.

Kaparen skulle kunna åsamka stor skada, både gentemot den kapade och gentemot svensk välfärd och svenska system. I detta scenario är kapningen av kopplingen dock bara en följd av den egentliga avsikten att kapa identiteten. För att kunna dra nytta av kapningen av kopplingen behöver kaparen känna till att den finns och hur man ska kunna använda sig av den.

När det kommer till bedrägerisituationer har det visat sig att användarnas brist på kunskap och avsaknaden av information om hur man ska använda sin eID-handling, vad man ska tänka på, vad man inte ska göra osv. har varit avgörande för att kunna genomföra id-kapningar. Att redan i ett tidigt skede ta kontroll över den information som lämnas om eIDAS-förordningen vore bra så att inte andra aktörer ”kapar” möjligheten till att lämna information.

Information bör lämnas både om svenska eID-handlingar och utländska samt möjligheterna till koppling.

7.2 Kapning av ett svenskt identitetsbegrepp

Bedömning: För att förebygga kapningar av svenska identitetsbegrepp genom att använda en koppling till en utländsk eID-handling har Skatteverket tagit fram en modell för registrering av koppling som innehåller en inbyggd tröghet. Genom att dessutom starta ett tillvägagångssätt för koppling i taget samt att skapa spårbarhet i systemet och använda de vedertagna standarder och rutiner för informationssäkerhet som har beskrivits i avsnitt 6.5 förebyggs missbruk av identitetshandlingar och bedrägerier ytterligare.

Skälen för bedömningen: En risk för angrepp är att en kapare från början känner till och är ute efter att kapa ett svenskt identitetsbegrepp för att kunna agera som någon annan i svenska digitala tjänster. Det skulle innebära att någon med ett svenskt identitetsbegrepp ofrivilligt kopplas mot en annan persons (kaparens) utländska eID-handling. En sådan felaktig koppling kan leda till stor skada, både för den vars identitetsbeteckning har blivit kapad och för svensk välfärd och svenska digitala system.

Det kan vara svårt för tillhandahållare av digitala tjänster att ifrågasätta en registrerad koppling. Vitsen med ett centralt kopplingsregister är att kopplingen inte ska behöva ifrågasättas utan att man ska kunna lita på att kopplingen är säker. Här är det viktigt att informationssäkerhetsarbetet som beskrivits i avsnitt 6.5 genomförs av den ansvariga myndigheten. Det handlar om att utföra alla de aktiviteter som beskrivits och kontinuerligt se till att informationssäkerheten upprätthålls.

Inbyggd tröghet för att åstadkomma koppling

Att tillämpa ett komplicerat och långsamt sätt för att åstadkomma koppling skulle motverka missbruk eftersom det gör det svårare och krångligare att konstruera ett sätt att ta sig runt gällande regler. Samtidigt strider ett sådant förfarande mot användarvänlighet och servicetänkande. Det är här fråga om en tröghet vid ett enstaka tillfälle när kopplingen ska registreras. Därefter kommer den digitala vägen att kunna användas snabbt varje gång användaren nyttjar en digital tjänst. Vid en avvägning av dessa intressen menar Skatteverket därför att det kan finnas anledning att låta själva registreringen ta tid genom att tillämpa en tvåstegsvariant vid alternativet med identitetskontroll vid personlig inställelse eftersom ett sådant förfarande kan hjälpa till att motverka missbruk och bedrägerier.

Starta ett tillvägagångssätt för koppling i taget

Ett sätt att hantera risk för missbruk är att starta ett sätt att koppla åt gången och använda det en period för att hitta brister och hinna åtgärda dem innan man startar nästa sätt att åstadkomma koppling. Det blir svårare att ha överblick om man

startar alla sätten samtidigt. Det är även svårare för användare att förstå flera parallella vägar på en gång. Det skulle kunna förebygga s.k. ”social engineering” att starta ett sätt i taget och låta det nyttjas och analysera följder och resultat innan man startar nästa tillvägagångssätt.

Skatteverkets förslag är därför numera att börja med den tidigare beskrivna tvåstegsprocessen där användaren hemifrån skapar en väntande koppling med den eID-handling som ska kopplas och därefter inställer sig fysiskt för identitetskontroll hos Polisen. Denna process behöver sättas igång, prövas och utvärderas innan nästa steg tas i utvecklingen av alternativ för att registrera kopplingar mellan utländska eID-handlingar och svenska identitetsbeteckningar.

7.3 Felkoppling av misstag

Bedömning: Felkopplingar av misstag kommer att minimeras genom att kraven på identifieringskontrollen är desamma som vid utfärdande av id-handlingar.

Skälen för bedömningen: En koppling mellan en utländsk eID-handling och fel svenska identitetsbeteckning kan registreras antingen uppsåtligen från den som begär kopplingen eller genom ett misstag. Felkopplingar av misstag borde inte få lika allvarliga följder men kan ändå leda till stor skada. Den vars identitetsbeteckning är kopplad till en utländsk eID-handling som den inte känner till kan uppleva obehag genom att någon agerar i dess namn. Den som innehar eID-handlingen kan få tillgång till uppgifter som inte ska spridas och upptäcka möjligheter att tillskansa sig fördelar även om det inte varit syftet från början.

Genom att i författningsförslaget och i rutiner för identifieringskontroll skapa krav på identifiering inför koppling som motsvarar kraven vid utfärdande av id-handlingar kan riskerna för uppsåtliga eller av misstag betingade kopplingar minimeras. Skatteverket bedömer att detta förfarande bör utgöra en effektiv ordning för att minimera felaktiga registreringar i kopplingsregistret.

7.4 Spridande av uppgifter

Bedömning: Det informationssäkerhetsarbete som har beskrivits i avsnitt 6.5 kommer att förebygga obehörigt spridande av uppgifter genom att enligt vedertagna standards och rutiner minimera identifierade risker.

Skälen för bedömningen: Ytterligare en integritetsrisk som identifierats med ett kopplingsregister som innehåller identitetsbegrepp, både svenska och utländska, är att uppgifterna kan komma att behandlas för en mängd olika ändamål. Om någon med ont uppsåt angriper registret för att få tillgång till registrerade uppgifter kan dessa snabbt spridas digitalt och det är svårt att förutse följderna.

Genom det informationssäkerhetsarbete som beskrivits i avsnitt 6.5 menar Skatteverket att man åtgärdar risken för digitalt spridande av uppgifter.

8 Konsekvensanalys

I detta kapitel beskrivs konsekvenserna av Skatteverkets förslag och det fördjupade uppdrag Skatteverket redovisar i övrigt i denna promemoria.

8.1 Alternativa lösningar

Skatteverket har bedömt att det finns behov av ett kopplingsregister och kostnaderna för detta beskrivs nedan.

En mer kostsam och komplicerad lösning är sannolikt att alla myndigheter själva bygger upp egna kopplingsregister, vilket skulle innebära merarbete både för berörda personer och för myndigheterna själva. Detta är därför ingen framkomlig väg. Ett annat alternativ skulle kunna vara att inte skapa något kopplingsregister alls. Mot detta talar att många myndigheter har uttryckt ett behov av ett kopplingsregister och att det sannolikt ökar möjligheterna för den enskilde att faktiskt kunna använda sig av svenska myndigheters digitala tjänster. Skatteverket förordar därför en lösning som ställer krav på teknisk utveckling och anpassning och därmed medför kostnader för berörda myndigheter.

8.2 Offentligfinansiella effekter

Sedan den 29 september 2018 har svenska myndigheter som har digitala tjänster som kräver inloggning med eID-handling en skyldighet att erkänna utländska eID-handlingar som har anmälts enligt eIDAS-förordningen. Dessa regler påverkar dock inte en persons rättigheter och skyldigheter, som t.ex. rätt till pension eller skyldighet att deklarera innehav av fastighet i Sverige. Det kan dock antas att hanteringen av dessa rättigheter och skyldigheter kommer att underlättas något, eftersom det kan bli enklare för personer bosatta utomlands att sköta sina ärenden. Digitala tjänster av typen Mina sidor eller Mina meddelanden kan också bidra till att informationen snabbare når mottagaren oavsett postgång, adressändringar etc. Den offentligfinansiella effekt som därmed kan uppstå är kopplad till att skyldigheter att t.ex. deklarera uppfylls i mer rätt tid eller överhuvudtaget.

Dessutom kan mindre tid från myndigheternas sida (och därmed minskade kostnader för staten) behöva läggas på att försöka nå personer utomlands och påminna dem om deras skyldigheter. På motsvarande sätt kan en person också lättare hävda en rättighet, exempelvis pension, vilket kan leda till ökade pensionsutbetalningar (men samtidigt troligtvis minska kostnaderna för manuell hantering). I de fall uteblivna eller försenade betalningar till en myndighet beror på bristande tekniska lösningar, kan möjligheterna att använda en utländsk eID-handling leda till att dessa i större utsträckning sker i rätt tid, vilket kan medföra positiva offentligfinansiella effekter. Om en digital tjänst är säkrare när det gäller identifiering än ett manuellt förfarande kan detta även antas leda till mer korrekta beslut, vilket i sin tur kan motverka felaktiga utbetalningar.

Införandet av ett kopplingsregister kan i och för sig underlätta användandet av svenska myndigheters digitala tjänster för personer som har utländska eID-handlingar även om rätten att använda en godkänd utländsk eID-handling följer redan av eIDAS-förordningen.

Det är mycket svårt att bedöma både hur stort användandet av utländska eID-handlingar kommer att bli och i vilken omfattning ett kopplingsregister kommer att underlätta detta användande, dvs. leda till att fler personer kan använda svenska digitala tjänster. De berörda myndigheterna har inte kunnat precisera effekterna av

ett kopplingsregister, eftersom det är okänt bland annat hur många berörda som har både en utländsk eID-handling och ett svenskt personnummer. Det saknas som en följd av detta också information om hur vanligt det är att dessa personer är sena med att fullgöra sina skyldigheter eller helt låter bli och vilket samband detta i så fall har med bristande tillgång till digitala tjänster. De offentligfinansiella effekterna av det föreslagna kopplingsregistret har därför inte kunnat bedömas. Eftersom reglerna inte påverkar rättigheter eller skyldigheter i sig, utan endast en individs möjligheter att uppfylla dessa, torde effekterna dock vara av mindre betydelse.

8.3 Konsekvenser för enskilda

Det är viktigt att ha i åtanke att endast personer med personnummer kan bli berörda av de föreslagna reglerna i första skedet. I nedanstående personkategorier kan i vissa fall även personer utan personnummer ingå, men dessa är då inte berörda av reglerna. I dagsläget är det nämligen mycket svårt att veta hur många potentiella användare av digitala tjänster som har svenska personnummer men saknar svensk eID-handling. Det är också svårt att bedöma hur angelägna dessa personer är att använda svenska myndigheters digitala tjänster.

De föreslagna reglerna berör främst personer med enbart utländsk eID-handling som har eller tidigare har haft anknytning till Sverige. Det kan t.ex. röra sig om följande kategorier av personer:

8.3.1 Personer som bor utomlands men äger fastigheter i Sverige

Med utländsk fastighetsägare avses personer från utlandet som äger en fastighet i Sverige utan att vara folkbokförda på den. Skatteverket har år 2014 beräknat antalet utländska fastighetsägare till 65 000 stycken. Detta antal omfattar dock även personer som varit folkbokförda här och kan ha ett svenskt personnummer. Vissa av dessa kan alltså redan ha tillgång till svensk eID-handling. Dessutom finns personer som bor utanför EU och EES också medräknade i detta antal.

8.3.2 Personer som utvandrat men är skattskyldiga i Sverige

Personer som inte är bosatta i Sverige, inte stadigvarande vistas här och inte heller har väsentlig anknytning hit är begränsat skattskyldiga i Sverige. Begränsat skattskyldig är också i vissa fall den som arbetar vid en utländsk ambassad eller karriärkonsulat (se nedan). Begränsad skattskyldighet innebär att endast vissa inkomster, som har anknytning till Sverige, beskattas här (källstatsprincipen). Personer som varit bosatta här men som lämnat Sverige och inte längre har någon giltig svensk eID-handling kan således fortfarande i vissa fall vara skattskyldiga här och ha behov av att kunna använda sig av Skatteverkets digitala tjänster. De kan förutom att deklarera inkomster även äga fastighet eller ha behov av att anmäla deklarationsombud. Många av dessa personer kan deklarera papperslöst med hjälp av koder via telefon eller via sms och behöver inte använda digitala tjänster. År 2018 var det dock drygt 15 000 personer bosatta inom EU och EES som, bland annat på grund av att de behövde lämna en deklarationsbilaga, inte kunde deklarera via telefon eller sms och som därför deklarerade på papper. Om dessa personer har en enligt eIDAS-förordningen godkändutländsk eID-handling skulle de i stället kunna deklarera via Skatteverkets digitala tjänster.

8.3.3 Anställda vid utländska ambassader och anhöriga till dessa personer

Det finns mer än 150 utländska beskickningar i Sverige. Det stora flertalet av dessa representerar inte länderna inom EU och EES, men flera av de anställda kan självklart ha varit bosatta i ett sådant land innan de flyttade till Sverige. Enligt 5 § folkbokföringslagen ska en anställd vid främmande makts beskickning folkbokföras endast om han eller hon är svensk medborgare eller, utan att vara svensk medborgare, var bosatt här när han eller hon kom att tillhöra beskickningen. Detsamma gäller för den anställdes familjemedlemmar. Utländska medborgare som flyttar till Sverige för att arbeta vid en utländsk beskickning tilldelas visserligen personnummer enligt 18 b § folkbokföringslagen, men har sannolikt svårt att få en svensk eID-handling eftersom de inte är folkbokförda här. Om de har en utländsk eID-handling (beskickningen tillhör en medlemsstat eller de har tidigare varit bosatta i ett sådant land) kan de däremot beröras av de nya reglerna. Dessa personer kan ha ett intresse av att använda digitala tjänster hos t.ex. Skatteverket och kommunerna (ansöka om förskoleplats eller skola).

8.3.4 Personer (både utvandrade svenskar och andra) som arbetat i Sverige och har rätt till pensioner härifrån

En stor grupp personer har rätt till pension från arbete i Sverige. Det kan röra sig både om personer som arbetat ett helt yrkesliv i Sverige och sedan flyttat utomlands och om personer som tillfälligt arbetat i Sverige. Det finns cirka 345 000 personer som får ett orange kuvert som är utlandsbosatta och någon gång arbetat i Sverige och tjänat in till allmän pension. Därtill kommer ca 160 000 personer som får pension utbetald. Pensionsmyndigheten har uppgivit att behovet av att kunna använda digitala tjänster är stort både för svenska pensionärer som bor utomlands och för andra som har rätt till pension härifrån. Behovet gäller inte bara de som redan får pension utan också alla de som ännu inte uppnått pensionsåldern, men ändå vill få tillgång till pensionsprognoser, kunna byta pensionsfonder m.m.

8.3.5 Utländska studenter som tillfälligt studerar i Sverige

De senaste uppgifterna som finns tillgängliga om den internationella studentmobiliteten gäller de inresande studenter som var nybörjare i svensk högskoleutbildning (nya inresande studenter) höstterminen år 2017. Då uppgick antalet studenter från EU- och EES-stater till 8 640 stycken.[21] Det totala antalet inresande utbytesstudenter och s.k. freemoverstudenter var läsåret 2017/2018 37 837 stycken. Av dessa kom ungefär 17 500 stycken från medlemsstaterna.[22] Utländska studenter som studerar i Sverige kan ha behov av att använda sina utländska eID-handlingar under förutsättning att de uppfyller kraven för att tilldelas ett svenskt personnummer.

[21] Universitetskanslersämbetet, UKÄ ÅRSRAPPORT 2018, s. 93
[22] Statistik & analys, Antal inresande studenter 2017/18 fördelat på lärosäte, grupp och land, www.uka.se. 2018-12-12.

8.3.6 Personer som omfattas av svensk socialförsäkring men bor i en annan medlemsstat

Personer som arbetar i Sverige ska normalt tillhöra svensk socialförsäkring. Detta gäller även den som bor i ett annat land inom EU eller EES eller i Schweiz. Den som är försäkrad i Sverige kan ha rätt till ersättningar från Försäkringskassan, till exempel barnbidrag och sjukpenning. Dessa personer kan därför ha ett behov av att kunna använda Försäkringskassans digitala tjänster.

8.3.7 Svenska studenter

Svenska studenter som har personnummer, men studerar lång tid utomlands kan ha svårt att förnya sin svenska eID-handling. De kan därför ha behov av att i stället koppla en utländsk eID-handling till sitt personnummer. Detta kan t.ex. behövas för att kunna använda CSN:s digitala tjänster. Även f.d. studenter som bor utomlands och har skulder till CSN kan behöva använda digitala tjänster för att sköta sina återbetalningar.

8.4 Konsekvenser för företag

De regler som föreslagits har endast begränsade konsekvenser för företag. Det kan bli enklare att använda olika digitala tjänster för företag för utländska personer som driver eller vill starta näringsverksamhet i Sverige utan att vara bosatta här. Detta gäller dock endast under förutsättning att bolagets företrädare har ett personnummer, så att koppling kan registreras till detta nummer. Även när det gäller digitala tjänster för företag är det alltså företrädaren som är direkt berörd av reglerna. För digitala tjänster som kräver inloggning med eID-handling krävs det nämligen att en företrädare för bolaget använder sig av sin personliga eID-handling. En företrädare för ett utländskt företag som saknar svensk eID-handling kan med förslaget använda sig av sin utländska eID-handling och därmed nå fler digitala tjänster än i dag. Ett utländskt företag som saknar fast driftställe i Sverige beskattas inte här och många av Skatteverkets digitala tjänster är därför inte aktuella att använda. Däremot kan det bland annat bli aktuellt att betala arbetsgivaravgifter för personal som anställts i Sverige eller till vilka ett utländskt företag betalar ut ersättning.

Även om en enskild näringsidkare varken är skattskyldig i Sverige eller omfattas av svensk socialförsäkring kan det finnas digitala tjänster som han eller hon skulle vilja ha tillgång till. Ett exempel på detta är den digitala tjänsten för rot- och rututbetalningar. Möjligheten till utbetalning för rot- och rutarbete gäller oavsett om arbetet utförts i Sverige eller i ett annat EES-land.

En person som är verksam och registrerad näringsidkare i en annan medlemsstat än Sverige kan alltså erbjuda svenska kunder rot- eller rutavdrag för arbeten både i en svensk och i en utländsk bostad. Om den person som utfört rot- och rutarbeten inte kan få en svensk eID-handling, kan personen ändå begära utbetalning för rot- och rutarbete. Exempel på detta kan vara en snickare från Polen eller Baltikum som monterar ett kök i Sverige på uppdrag av en fastighetsägare eller en spansk rörmokare som reparerar ett badrum i en lägenhet på spanska solkusten, som ägs av en svensk. För att förslaget ska beröra dessa hantverkare krävs dock att de sedan tidigare har tilldelats svenskt personnummer.

För arbeten utförda utanför Sverige är Spanien, Frankrike, Finland, Norge och Italien de vanligaste länderna.

Utförare som saknar eID-handling ska visserligen begära utbetalning elektroniskt, genom ett så kallat e-formulär, men blanketten signeras med hjälp av mus, pekplatta eller annat verktyg (underskrift) och inte genom elektronisk signering. Det är ett fåtal företag som använder e-formuläret för att begära utbetalning. De flesta av dessa är verksamma utomlands och utför arbete i svenskägda bostäder utomlands.

Bland de företagare som är aktiva i Sverige och kanske skulle kunna ha nytta av förslaget använder sig många redan i dag av möjligheten att begära utbetalning genom den digitala tjänsten via ombud. Har dessa företagare personnummer, skulle de kunna begära utbetalning själva, vilket kan vara enklare men att den digitala tjänsten endast finns på svenska kan vara ett hinder. Skatteverkets arbete med att registrera ombud kan också minska.

En möjlighet att använda utländsk eID-handling vid begäran om utbetalning för rot- och rutarbete skulle visserligen innebära att vissa personer med eID-handlingar från andra medlemsstater skulle kunna använda den vanliga digitala tjänsten. Detta innebär dock inte att någon särlösning inte längre behövs. Merparten av de som ansöker om utbetalning kommer även framöver att sakna personnummer.

8.5 Konsekvenser för Skatteverket och Polisen

8.5.1 Kostnader

Skatteverket föreslår en teknisk lösning som kan uppfylla kraven på tillitsnivå. Denna lösning kan visserligen leda till högre kostnader för berörda myndigheter än andra lösningar, men är enligt Skatteverket den enda lösning som är användbar utifrån myndigheternas behov.

För att beräkna kostnaderna för olika delar har Skatteverket tillämpat den s.k. successivmetoden[23] där en grupp analyserar och registrerar ett min- och ett maxvärde och diskuterar sig fram till ett troligt värde. Gruppens sammansättning har bestått av informationssäkerhetsexperter, IT-arkitekter, jurister och verksamhetsutvecklare.

Det osäkerhetsspann som fanns vid beräkningarna 2016 har minskat eftersom Skatteverket har arbetat med frågorna under en längre tid och numera vet med större säkerhet vad som behöver göras för att få igång en kopplingstjänst och register. Samtidigt vill Skatteverket framhålla att siffrorna är baserade på att uppdraget att ta fram kopplingsregister tilldelas Skatteverket som är inlästa och förberedda på att fortsätta arbetet. Om någon annan myndighet eller konsulter skulle tilldelas uppdraget tillkommer ytterligare kostnader för inläsning.

Utveckling av kopplingsregister för Skatteverket

Utvecklingskostnader för Skatteverket beräknas bli 12 245 000 kronor. I beräkningarna har inkluderats kostnader för att genomföra projektuppstart och projektadministration. Vidare ingår kostnader för utveckling av kopplingstjänst samt införandeprojekt. Inom dessa poster ingår bland annat informationssäkerhetsarbete, rättsligt arbete, IT-säkerhetsarbete, processflöde, implementation, integration, kommunikation, utbildning m.m.

[23] Successivmetoden, successivprincipen eller successiv kalkylering har sitt ursprung i den danske forne professorn och managementkonsulten Steen Lichtenberg, www.lichtenberg.org 2018-12-14.

Kostnad per år för förvaltning och drift för Skatteverket

Förvaltningskostnader för Skatteverket beräknas bli 7 800 000 kronor per år. När det gäller drift och förvaltning så finns förutom den faktiska förvaltningen även inräknat kostnader för licenser för nödvändig programvara. När det gäller personella resurser finns inräknat kostnader för drift, teknisk förvaltning och verksamhetsnära handläggning.

Kostnader för Polisen

Polisen beräknar att ett besök för att registrera koppling kommer att kosta lika mycket som ett besök för att göra ett pass. För pass stämmer kostnaden överens med den avgift sökanden får betala för passet, nämligen 350 kr. I de 350 kronorna ingår direkta kostnader för bland annat personal, utrustning och lokaler samt indirekta kostnader i form av s.k. over head-kostnader. De 350 kronorna kan enligt Polisen ligga till grund för att multipliceras med det potentiella antal besök som kan förutses.

I övrigt tillkommer kostnad för utbildning av personal. Den beräknar Polisen till 128 000 kr.

Det kan uppstå situationer när det blir otydligt för Polisen om en eID-handling och en fysisk person är identisk. Det kan vara till följd av ett namnbyte eller i ett fåtal fall ändring av födelsetid. Det kan också förekomma situationer när någon vill registrera en koppling vid personlig inställelse men inte längre har en giltig svensk id-handling som styrker att personen har det personnummer som den uppger. Det inträffar även i dag att personer vill ha en id-handling utfärdad utan att kunna visa en giltig id-handling till grund. Man kan låta andra personer intyga att det är rätt person men det är en sista utväg där säkerheten är lägre än vad som är önskvärt. Dessa situationer kommer att kräva utredningsresurser hos Polisen. Samtidigt är det jämförbart med situationer som uppstår hos Polisen i dagsläget vid utfärdandet av id-handlingar. Kostnaderna för dessa extra utredningsresurser får därför bedömas ingå i underlaget.

8.5.2 Övriga konsekvenser

Konsekvenserna för myndigheterna kan delas in i rent kostnadsmässiga konsekvenser och andra konsekvenser för förvaltningen som i och för sig också i förlängningen utmynnar i kostnader men som först yttrar sig i form av arbetsuppgifter. Det kan exempelvis uppstå ökat tryck på kundtjänst hos myndigheter där användare inte kan logga in. Detta gäller inte bara Skatteverket och Polisen utan alla de myndigheter som använder sig av kopplingsregistret.

I uppdragsbeskrivningen ingick ursprungligen att genomföra en övergripande analys av offentlig sektors förväntade nytta av en kopplingstjänst. De myndigheter som anser sig ha behov av en kopplingstjänst har ändå en likvärdig gemensam bild av vad nyttorna kan tänkas vara. De förväntade nyttorna uppges av dessa myndigheter vara ökad service, mindre pappershantering, snabbare handläggningstid och stora kostnadsbesparingar.

9 Författningskommentar

9.1 Förslaget till lag om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar

Databas

1 §

I paragrafen regleras att det ska föras en databas över koppling mellan en sådan utländsk eID-handling som ska godtas av svenska myndigheter enligt eIDAS-förordningen å ena sidan och en svensk identitetsbeteckning å andra sidan.

I *första stycket* regleras att det är Skatteverket som ska föra databasen samt att registrering förutsätter att den som uppgifterna avser har begärt att registreringen ska göras.

I *andra stycket* regleras att det är Polisen som ansvarar för handläggning av ärenden om koppling och därmed även ska föra in uppgifter i registret.

I *tredje stycket* ges grunderna för att föra in en kontroll mot den nu föreslagna databasen i ett förfarande av kontroll av en eID-handling när en sådan används för att logga in i en digital tjänst som tillhandahålls av en svensk myndighet. I samband med en sådan inloggning skickas en fråga via den svenska noden och berört lands nod till utfärdaren av eID-handlingen. Från utfärdaren skickas via samma väg ett certifikat tillbaka. I den svenska noden kan en kontroll mot databasen göras och om det finns en koppling kan den svenska identitetsbeteckningen bifogas i försändelsen till den svenska myndigheten. Ansvarig myndighet för den svenska noden är Myndigheten för digital förvaltning (DIGG).

Skälen för att det ska föras en databas över kopplingar behandlas i avsnitt 6.3.1.

Skälen för att Skatteverket ska ansvara för databasen och Polisen för handläggning av ärenden behandlas i avsnitt 6.7.

Skälen för att uppgift om koppling ska förmedlas via den svenska noden behandlas i avsnitt 6.3.2.

Lagens tillämpningsområde och förhållande till annan reglering

2 §

I paragrafens *första stycke* beskrivs relationen till EU:s dataskyddsförordning. Dataskyddsförordningen är direkt tillämplig och har företräde framför nationell lagstiftning.

I paragrafens *andra stycke* beskrivs relationen till dataskyddslagen. Dataskyddslagen är subsidiär i förhållande till den föreslagna lagen.

I paragrafens *tredje stycke* anges att lagen omfattar helt eller delvis automatiserad behandling av personuppgifter och annan behandling om uppgifterna ingår eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier. Tillämpningsområdet är detsamma som för dataskyddsförordningen och dataskyddslagen. Manuella behandlingar av personuppgifter som inte ingår i en strukturerad samling enligt ovan, t.ex. minnesanteckningar i anslutning till ärendehanteringen, omfattas inte av den nya lagen.

Skälen för bestämmelsen behandlas i avsnitt 6.6.2.

Ändamål

3 §

I paragrafen regleras för vilka ändamål personuppgifter får behandlas i databasen.

I *första stycket* regleras ändamålet att kunna visa en koppling mellan en eID-handling och en svensk identitetsbeteckning. En svensk myndighet kan i samband med att en digital tjänst tillhandahålls ha behov av att kunna kontrollera att en sådan koppling finns. I stycket anges vidare att personuppgifter får behandlas för handläggningen av ett ärende enligt den aktuella lagen.

I *andra stycket* regleras att uppgifter får behandlas för att tillhandahålla information som behövs hos de myndigheter som ansvarar för kopplingssystemet; Skatteverket, Polisen och DIGG för tillsyn, kontroll, uppföljning och planering av verksamheten.

I *tredje stycket* anges att uppgifter även får behandlas för förmedling av identitetsuppgifter via den svenska noden till en svensk myndighet i samband med att en användare vill logga in med en utländsk eID-handling till en digital tjänst som den svenska myndigheten tillhandahåller. Ansvarig myndighet för den svenska noden är DIGG.

I *fjärde stycket* anges att uppgifter som behandlas för ändamålet enligt första stycket, att visa koppling, också får behandlas för att fullgöra annat uppgiftslämnande i enlighet med lag eller förordning.

Skälen för ändamålsbestämmelsen behandlas i avsnitt 6.6.3.

4 §

I *första stycket* regleras de personuppgifter som databasen får innehålla. Databasen får bara innehålla personuppgifter om personer som tilldelats ett svenskt personnummer.

De uppgifter som minst behövs för att konstatera om det finns en koppling är eID-handlingens identitetsbeteckning och den svenska identitetsbeteckningen. Personens namn och födelsetid behövs också i registret för att kunna jämföra uppgifter när kopplingen ska registreras. Födelsedatum ingår som regel i den svenska identitetsbeteckningen, men det finns fall då det kan finnas avvikelser. Det kan inträffa när nummerserien för en viss dag har tagit slut.

I *andra stycket* anges att regeringen får föreskriva om att ytterligare uppgifter ska få behandlas.

Bestämmelsen behandlas i avsnitt 6.6.5.

5 §

I *första stycket* anges att utöver vad som följer av 4 § får även andra uppgifter och handlingar som kommit in i eller upprättats i ett ärende och som behövs för handläggningen av ärendet, behandlas.

I *andra stycket* regleras behandling av känsliga uppgifter och om lagöverträdelser i inkomna och upprättade handlingar. Även dessa uppgifter får behandlas om de är nödvändiga för ärendets handläggning.

Bestämmelsen behandlas i avsnitt 6.6.3 och 6.6.5.

Personuppgiftsansvar

6 §

I paragrafen regleras hur personuppgiftsansvaret ska vara fördelat.

I *första stycket* anges att Skatteverket har personuppgiftsansvar för den behandling av personuppgifter som myndigheten utför i databasen.

I *andra stycket* anges Polisens personuppgiftsansvar som täcker behandlingen av personuppgifter i ärendehanteringen när det gäller kopplingar mellan utländska eID-handlingar och svenska identitetsbegrepp. Polisen är också personuppgiftsansvarig för allt införande av uppgifter och handlingar i databasen som Polisen utför.

I *tredje stycket* regleras DIGG:s personuppgiftsansvar som omfattar den behandling av personuppgifter som DIGG utför för att kontrollera om koppling finns samt för att förmedla information om identitet till andra myndigheter.

Bestämmelsen behandlas i avsnitt 6.6.11.

Ansökan och registrering

7 §

I *första stycket* anges att en ansökan om registrering ska vara skriftlig och att den ska innehålla de uppgifter som behövs för prövningen. Vilka uppgifter som ska lämnas specificeras i förordningen. Att ansökan ska vara skriftlig inbegriper den elektroniska väg att lämna ansökan som har föreslagits.

I *andra stycket* anges förutsättningarna för att få en koppling registrerad. Ansökan ska vara gjord på rätt sätt samt den svenska identitetsbeteckningen och personens koppling till eID-handlingen ska vara styrkta.

Bestämmelsen behandlas i avsnitt 6.4.1 och 6.6.12.

8 §

Om en sökande inte har ansökt på rätt sätt eller inte har styrkt sin svenska identitetsbeteckning eller sitt innehav av eID-handlingen ska denne uppmanas att avhjälpa bristen. Om så inte sker inom förelagd tid ska ansökan avslås.

Bestämmelsen behandlas i avsnitt 6.6.12.

9 §

I *första stycket* anges att den registrerade kan ansöka om att en koppling tas bort. Ansökan ska vara skriftlig. Något annat krav ställs inte för att registreringen ska tas bort. Att kopplingen tas bort innebär att uppgifterna i 4 § inte längre kommer att finnas i databasens registerdel. Uppgifterna i handläggningsdelen kommer dock att finnas kvar. En fråga till databasen om det finns en registrerad koppling kommer att besvaras nekande.

Andra stycket behandlar borttagande av registrering på myndighetens initiativ. Om det framkommer att eID-handlingen upphört att gälla eller om den inte längre ska erkännas enligt eIDAS-förordningen, ska registreringen tas bort av myndigheten. Likaså ska registreringen tas bort av myndigheten om det finns skäl att anta att eID-handlingen inte hör till den person vars svenska identitetsbeteckning är registrerad. Bevisgraden är lågt satt så att bestämmelsen ska kunna används snabbt vid en misstanke om en eventuell identitetskapning.

Bestämmelsen behandlas i avsnitt 6.6.12.

10 §
I paragrafen ges en upplysning om att regeringen eller den myndighet som regeringen bestämmer med stöd av 8 kap. 7 § regeringsformen kan meddela ytterligare föreskrifter om ansökan och registrering.

Bestämmelsen behandlas i avsnitt 6.6.12.

Digitalt utlämnande

11 §
I paragrafen behandlas digitalt utlämnande.

I *första stycket* behandlas utlämnande till DIGG genom direktåtkomst för förmedling av uppgift om koppling och svensk identitetsbeteckning, till en svensk myndighet, via den svenska noden, i samband med att en användare vill logga in med stöd av en eID-handling, mot en digital tjänst som tillhandahålls av den svenska myndigheten.

I *andra stycket* anges att utlämnande till Polisen får ske genom direktåtkomst om det behövs för Polisens ärendehandläggning av kopplingsärenden.

I *tredje stycket* anges att utlämnande till enskild avseende person- och ärendeuppgifter om sig själv får ske via direktåtkomst.

I *fjärde stycket* lämnas utrymme för utlämnande från databasen av Skatteverket till andra myndigheter, på medium för automatiserad databehandling.

I *femte stycket* regleras utlämnandet via den svenska noden till svenska myndigheter. Ansvarig myndighet för noden är DIGG. Utlämnandet får ses som ett utlämnande på medium för automatiserad behandling.

Bestämmelsen behandlas i avsnitt 6.6.4.

Sökbegrepp

12 §
I paragrafen regleras att känsliga personuppgifter inte får användas som sökbegrepp i databasen.

Bestämmelsen behandlas i avsnitt 6.6.6.

Gallring

13 §
I paragrafen anges att uppgifter och handlingar som finns i databasen ska gallras senast fem år efter att beslut om kopplingen mellan den utländska eID-handlingen och den svenska identitetsbeteckningen registrerades.

Regeln innebär att alla registrerade måste förnya sin koppling vart femte år. Gallringsbestämmelsen avser alla uppgifter och handlingar. Uppgifter och handlingar som hör till ett ärende där koppling inte kommit till stånd ska också omfattas av gallringsbestämmelsen.

Bestämmelsen behandlas i avsnitt 6.6.7.

Överklagande

14 §
Av *första stycket* framgår att ett beslut får överklagas till Förvaltningsrätten i Stockholm. Skatteverkets säte är i Solna och Polisens i Stockholm.

Av *andra stycket* framgår att prövningstillstånd krävs vid överklagande till kammarrätten.

Bestämmelsen behandlas i avsnitt 6.6.1.

Ikraftträdandebestämmelse

Lagen ska träda i kraft den 1 juli 2020.

Bestämmelsen behandlas i avsnitt 6.7.2.

9.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

22 kap.

1 §

I paragrafens *första stycke* föreslås en ny tredje punkt. För uppgifter om en enskilds personliga förhållanden som, enligt lagen om behandling av koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar, registreras i kopplingsregistret ska sekretess gälla om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs.

Uppgifterna ska omfattas av sekretess med s.k. rakt skaderekvisit liksom uppgifter i folkbokföringen och sjömansregistret.

Bestämmelsen behandlas i avsnitt 6.6.13.

Bilaga 1 – Uppdraget

Regeringen

Regeringsbeslut

2018-05-17
Fi2018/02044/S3

Finansdepartementet

Skatteverket
171 94 Solna

Uppdrag om fördjupad utredning rörande koppling mellan utländsk e-legitimation och svenskt personnummer eller samordningsnummer

Regeringens beslut

Regeringen ger Skatteverket i uppdrag att vidareutveckla myndighetens promemoria Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer och lämna förslag som syftar till att möjliggöra ökad gränsöverskridande åtkomst till svenska digitala myndighetstjänster.

Uppdraget ska redovisas till regeringen (Finansdepartementet) senast den 31 januari 2019.

Skatteverket får för uppdraget rekvirera högst 3 000 000 kronor 2018. Kostnaderna ska belasta anslaget 1:18 Digitaliseringsmyndigheten, anslagsposten 7 Nationell digital infrastruktur, under utgiftsområde 2 Samhällsekonomi och förvaltning. Medlen utbetalas engångsvis efter rekvisition ställd till Kammarkollegiet senast den 15 september 2018. Medel som inte utnyttjats ska återbetalas till Kammarkollegiet senast den 15 mars 2019. Vid samma tidpunkt ska Skatteverket lämna en ekonomisk redovisning över använda medel till Kammarkollegiet med kopia till Regeringskansliet (Finansdepartementet). Rekvisitionen, eventuell återbetalning och redovisning ska hänvisa till det diarienummer som detta beslut har.

Bakgrund

I september 2014 publicerades 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 (eIDAS-förordningen). Förordningen medför bl.a. krav på svenska myndigheter som har e-tjänster där personer kan använda sig av nationell e-legitimation att fr.o.m. den 29 september 2018 även erkänna europeiska e-legitimationer som anmälts enligt eIDAS-förordningen. Detaljerna regleras i genomförandeakter som tagits fram i eIDAS expertgrupp där samtliga EU:s medlemsländer deltar. I skäl 14 till eIDAS-förordningen anges att principen om ömsesidigt erkännande endast bör avse autentisering för en nättjänst. Vidare framgår av samma skäl att åtkomsten till nättjänsten och dess slutliga leverans till användaren bör vara nära kopplad till rätten att ta emot sådana tjänster enligt villkoren i nationell lagstiftning.

I promemorian Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer (Fi2016/03889/DF) har Skatteverket lämnat förslag till en kopplingstjänst i form av ett register för att hantera kopplingar mellan europeiska eID-handlingar och svenska identitetsbeteckningar (nedan kopplingsregister) och till en ny lag och förordning om behandling av koppling mellan europeiska eID-handlingar och svenska identitetsbeteckningar.

I promemorian har Skatteverket även identifierat ett antal frågor som behöver eller kan utredas vidare. Vidare har Myndigheten för samhällsskydd och beredskap lyft fram vissa frågeställningar som kräver en fördjupad utredning. Därtill har det efter att promemorian lämnats skett förändringar av rättsläget i form av att lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:218) träder i kraft den 25 maj 2018. Det finns därmed behov av en vidareutveckling av den ovan nämnda promemorian.

I slutbetänkandet Reboot – omstart för den digitala förvaltningen (SOU 2017:114) gjordes bedömningen att målsättningen bör vara att erkännande av utländska elektroniska identitetshandlingar i svenska digitala myndighetstjänster innebär att användaren ska ges tillgång till de tjänster hon eller han har behov av. En förutsättning för att erbjuda denna tillgång är dock att avsteg inte görs från säkerhetsmässiga hänsynstaganden. Utredningen framförde med anledning av brister som finns i samordningsnummersystemet att ett kopplingsregister till att börja med endast borde omfatta kopplingar mellan utländska elektroniska identitetshandlingar och svenska personnummer.

Närmare om uppdraget

Skatteverket ska analysera riskerna för att det föreslagna kopplingsregistret kan angripas och nyttjas i missbrukssyfte och lämna förslag på hur sådana eventuella risker ska hanteras för att förhindra missbruk av identitetshandlingar och därigenom förebygga bedrägerier och brott mot välfärden. Vidare ska Skatteverket analysera och bedöma vilka åtgärder som bör vidtas för att säkerställa en god informationssäkerhet i det föreslagna kopplingsregistret.

Skatteverket ska även överväga om det för närvarande kan anses lämpligt att skapa en koppling mellan en utländsk e-legitimation och en individs styrkta samordningsnummer.

I uppdraget ingår att överväga om det finns behov av sekretessbestämmelser och sekretessbrytande bestämmelser för hantering av uppgifter i kopplingsregistret som är skyddade i andra länder eller som rör personer med skyddade personuppgifter samt utföra en förnyad och fördjupad bedömning av personuppgiftsbehandlingen i det föreslagna kopplingsregistret.

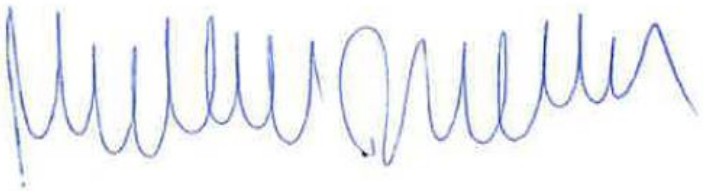
Skatteverket ska också överväga om registrering av koppling mellan en europeisk eID-handling och ett svenskt identitetsbegrepp som sker vid en personlig inställelse bör utföras vid vissa svenska utlandsmyndigheter som även är passmyndigheter. Därutöver ska Skatteverket utföra en fördjupad utredning om de tekniska förutsättningarna för ett kopplingsregister.

I uppdraget ingår även att bedöma kostnader och konsekvenser som förslaget kan komma att medföra. Vidare ska Skatteverket lämna förslag till nödvändiga författningsändringar. Skatteverket ska även redovisa konsekvenserna av eventuella författningsförslag i enlighet med 6–8 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Uppdraget ska utföras i samverkan med E-legitimationsnämnden, till dess myndigheten har avvecklats, och med Myndigheten för digital förvaltning, när myndigheten har inlett sin verksamhet. Rörande frågan om registrering av koppling vid en personlig inställelse ska synpunkter inhämtas från Regeringskansliet (Utrikesdepartementet), 2017 års ID-kortsutredning (Ju 2017:12) och Polismyndigheten. Polismyndigheten ska därutöver ges tillfälle att lämna synpunkter i fråga om riskerna för att kopplingsregistret

nyttjas i missbrukssyfte. De myndigheter och organisationer som medverkade vid framtagandet av den ursprungliga promemorian ska även ges möjlighet att lämna kompletterande synpunkter.

På regeringens vägnar



Magdalena Andersson

Cecilia Eriksson

Kopia till

Statsrådsberedningen/SAM
Justitiedepartementet/DOM, KRIM, L4, L6, PO, SIM, SSK och Å
Utrikesdepartementet/HI, KC och PLAN
Socialdepartementet/FS och SF
Finansdepartementet/BA, K, SFÖ och S3
Utbildningsdepartementet/GV och UH
Näringsdepartementet/D och SUBT
Arbetsmarknadsdepartementet/A
2017 års ID-kortsutredning (Ju 2017:12)
Arbetsförmedlingen
Centrala studiestödsnämnden
Datainspektionen
E-hälsomyndigheten
Försäkringskassan
Migrationsverket
Myndigheten för samhällsskydd och beredskap
Pensionsmyndigheten
Polismyndigheten
Transportstyrelsen
Tullverket
Universitets- och högskolerådet
Sveriges Kommuner och Landsting