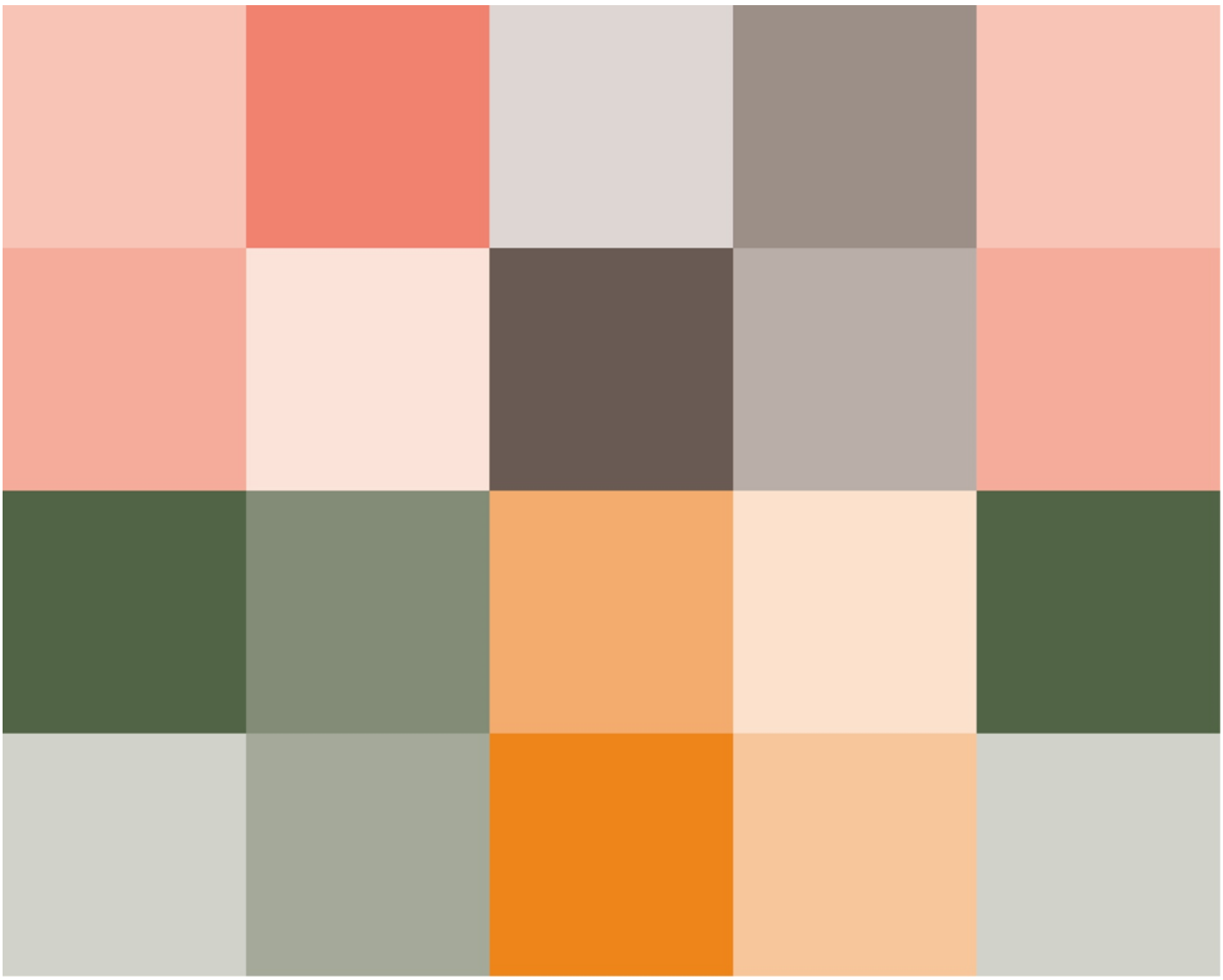


En sammanhållen infrastruktur för identitets- och behörighetshantering

Diarienummer: 2025–04363

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Myndigheten för digital förvaltning (Digg) har i uppdrag att ta fram en sammanhållen infrastruktur för identitets- och behörighetshantering inom ramen för Ena – Sveriges digitala infrastruktur. Infrastrukturen har fått namnet Samordnad identitet och behörighet. Uppdraget har bedrivits i nära samverkan med E-hälsomyndigheten, Inera AB, Sveriges Kommuner och Regioner (SKR), Stiftelsen för internetinfrastruktur (Internetstiftelsen), Skolverket, Vetenskapsrådet och två regioner. Arbetet har lagt grunden för en federationsbaserad modell som ska möjliggöra säker och effektiv digital samverkan mellan offentliga och privata aktörer.

Syftet är att skapa en gemensam grund för identitets- och behörighetskontroll i hela den offentliga sektorn och på sikt även inom andra delar av samhället. Infrastrukturen ska komplettera det befintliga systemet för elektronisk identifiering och möjliggöra digitalt stöd för att avgöra både vem en användare är och vilken behörighet denne har att agera i olika roller eller på annans vägnar.

Arbetet har omfattat juridiska analyser, teknisk arkitektur, principer för styrning och förvaltning samt bedömningar av nyttor, finansiering och beredskap. Analysen visar att en gemensam infrastruktur är nödvändig för att motverka dagens fragmentering, där olika sektorer utvecklat egna lösningar. En sammanhållen modell stärker rättssäkerhet, informationssäkerhet och effektivitet samt skapar förutsättningar för interoperabilitet med europeiska regelverk såsom det för den europeiska digitala identitetsplånboken (EUDIW)[1] och Single Digital Gateway (SDG)[2].

Den föreslagna lösningen bygger på öppna standarder, tydliga juridiska ramar och gemensamma tekniska specifikationer, och är utformad för att vara flexibel, skalbar och möjlig att tillämpa i flera sektorer.

Samtidigt kräver etableringen betydande samordning, resurser och förtroende. Det är avgörande att tidigare investeringar i befintliga system kan återanvändas och integreras, annars riskerar införandet att upplevas som kostsamt och resurskrävande. Om inte tillräckligt många aktörer ansluter i ett tidigt skede finns en risk för fortsatt fragmentering och begränsad nytta.

Digg föreslår att infrastrukturen regleras genom en kombination av författningsändringar och avtal mellan anslutna parter. Förslagen innebär att Digg ges rättsligt stöd för att utveckla, reglera och tillhandahålla infrastrukturen i samverkan med andra aktörer. Regeringen behöver därefter ta ställning till juridiskt mandat, finansiering och långsiktig styrning, så att infrastrukturen kan förvaltas stabilt och skalas upp över tid.

Det fortsatta arbetet med att etablera en sammanhållen infrastruktur innebär bland annat att genomföra tekniska tester i bredare skala, utveckla regelverk, fastställa styrnings- och

[1] Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet.
[2] Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012.

förvaltningsmodell, utveckla finansieringsmodellen, stärka kommunikation och förankring samt säkerställa beredskap, kontinuitet och resiliens.

Digg anser att den föreslagna modellen ger förutsättningar för en säker, effektiv och rättssäker digital samverkan över sektorsgränser, men kräver fortsatt målmedvetet arbete, gemensamt ansvarstagande och tydlig politisk förankring för att nå sin fulla potential.

Innehållsförteckning

Begreppslista

Begrepp	Förklaring
Aktörs- och funktionsregister	Samlingsbeteckning för de digitala kataloger som finns på olika nivåer över aktörer och funktioner inom behörighetsinfrastrukturen.
Behörighetshandling	En digitalt stämplad eller underskriven handling med uppgifter som används för juridisk behörighetskontroll.
Behörighetsinfrastruktur	En gemensam, förvaltningsövergripande struktur som möjliggör digital samverkan mellan självständiga aktörer genom gemensamma tekniska specifikationer och regelverk för utfärdande, förmedling och verifiering av behörighetshandlingar i digitala tjänster.
Digital aktör	En teknisk funktion som automatiserat utför åtgärder eller rättshandlingar i en huvudmans eller medarbetares ställe.
Digital samverkan	Digital samverkan är förmågan hos organisationer att interagera i en gemensam riktning mot ömsesidigt fördelaktiga och överenskomna gemensamma mål. När begreppet används i denna rapport så inkluderar det även den praktiska tillämpningen – där två eller flera aktörer utbyter information digitalt med stöd av gemensamma lösningsmönster och etablerade standarder. Fokus ligger i det avseendet på att möjliggöra säker och interoperabel informationsdelning mellan olika organisationer
Digital tjänst	En webbtjänst, ett programmeringsgränssnitt (API) eller en liknande funktion där behörighetshandlingar används för att granska medarbetares juridiska behörighet.
Egenskapsintyg	Ett digitalt stämplat intyg som beskriver egenskaper hos en aktör eller dennes tekniska komponenter.

Begrepp	Förklaring
Federation	En samverkansmodell där självständiga organisationer samarbetar enligt gemensamma regler, standarder och specifikationer men behåller ansvar för sina egna system.
Federationsmedlem	En utfärdare av behörighetshandlingar eller en förlitande part.
Federationsområde	En avgränsad tillämpning inom behörighetsinfrastrukturen med gemensamma regler för informationsutbytet.
Federationsområdesansvarig	Part som administrerar, samordnar och ansluter en grupp av utfärdare av behörighetshandlingar och förlitande parter, tillhandahåller gemensamma stödfunktioner, möjlighet att registrera tjänster och agerar som fullmäktig vid avtalsslut mellan parter inom det federationsområde där denne verkar, allt i enlighet med gällande anslutningsavtal och tekniska specifikationer.
Förlitande part	Part inom behörighetsinfrastrukturen som använder behörighetshandlingar för juridiska behörighetskontroller i enlighet med gällande anslutningsavtal och tekniska specifikationer.
Huvudman	En arbetsgivare, en uppdragsgivare eller någon annan som driver verksamhet för vars räkning medarbetare utför åtgärder, företar rättshandlingar eller agerar på annat sätt i relevanta roller.
Identitetsintyg	Stämplat intyg i elektronisk form med uppgift om användares identitet.
Identitetskontroll	Kontroll av vem en fysisk person är, normalt genom elektronisk identifiering (t.ex. e-legitimation).

Begrepp	Förklaring
Juridisk behörighetskontroll	En granskning av om en medarbetare, i juridisk mening är a) behörig att agera för angiven huvudmans räkning, b) har en yrkesroll som innefattar en rätt att agera på det sätt som sker, eller c) deltar i verksamhet hos angiven huvudman där medarbetaren behöver vidta en åtgärd eller agera på annat sätt.
Komponent	En avgränsad teknisk eller organisatorisk del av federationsinfrastrukturen som utför en definierad funktion, exempelvis autentisering, validering, registerhållning eller förmedling av behörighetsinformation.
Ledningsansvarig	Den som styr, reglerar, samordnar och utvecklar behörighetsinfrastrukturen, ansluter federationsområdesansvariga och agerar som fullmäktig vid avtalsslut mellan parter samt tillhandahåller gemensamma funktioner såsom den ledningsansvariges aktörs- och funktionsregister.
Medarbetare	Den som är anställd, uppdragstagare eller på annat sätt deltar i en huvudmans verksamhet och utför åtgärder, företar rättshandlingar eller agerar inom verksamheten med stöd av en viss roll, befattning, fullmakt eller reglerad yrkesroll. Medarbetare är inte parter i avtal om behörighetsinfrastrukturen utan har i regel ett anställnings- eller uppdragsavtal med huvudmannen.
Metadata	Strukturerad information om information som beskriver tekniska komponenter och deras egenskaper, adresser, nycklar och förmågor och används för att möjliggöra interoperabilitet och säker kommunikation mellan parter.
Områdesspecifika anpassningar	De kompletterande tekniska och administrativa funktioner och tjänster, samt de ytterligare regler, rutiner och kontrollmekanismer som en federationsområdesansvarig inför för att säkerställa en effektiv, ändamålsenlig och rättssäker juridisk behörighetskontroll inom det område där denne verkar.

Begrepp	Förklaring
Part	Var och en av ledningsansvarig, federationsområdesansvariga, utfärdare av behörighetshandlingar och förlitande parter.
Sedvanlig behörighetskontroll	En juridisk behörighetskontroll i enlighet med allmänna regler där uppgifter inte lämnas genom direktåtkomst.
Tekniskt ramverk för behörighetsinfrastrukturen	De tekniska specifikationer som den ledningsansvariga från tid till annan bestämmer för parterna (bilaga till regelverket).
Utfärdare av behörighetshandlingar	En huvudman eller tredje part som ställer ut och levererar behörighetshandlingar i enlighet med gällande avtal och tekniska specifikationer.

Författningsförslag

Förslag till ändring i förordningen (2018:1486) med instruktion för myndigheten för digital förvaltning

Härigenom föreskrivs att 3 § i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 §[3]
Myndigheten ska **1.** ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift, **2.** främja användningen av elektronisk identifiering och underskrift, **3.** ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med 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 (e-IDAS-förordningen) samt rättsakter som har meddelats med stöd av förordningen, **4.** tillhandahålla en förvaltningsgemensam infrastruktur för säker digital kommunikation till verksamheter inom välfärdsområdet som helt eller delvis är offentligt finansierade, **5.** ansvara för tillhandahållandet av en europeisk digital identitetsplånbok i enlighet med eIDAS-förordningen samt, i fråga om fysiska personer, även tillhandahålla sådana uppgifter för personidentifiering som avses i artikel 3 i eIDAS-förordningen vilka ska kunna kopplas till den europeiska digitala identitetsplånboken, och	
	6. ansvara för tillgången till infrastruktur och tjänster för elektronisk behörighetskontroll i **1.** verksamheter inom välfärdsområdet som helt eller delvis är offentligt finansierade, **2.** verksamheter inom välfärdsområdet som utan att vara offentligt finansierade omfattas av hälso- och sjukvårdslagen (2017:30), tandvårdslagen (1985:125), lagen (2001:499) om omskärelse av pojkar, lagen (2018:744) om försäkringsmedicinska utredningar, lagen (2019:1297) om koordineringsinsatser för sjukskrivna patienter, lagen (2021:363) om estetiska kirurgiska ingrepp och estetiska injektionsbehandlingar och **3.** verksamheter inom detaljhandel med läkemedel enligt lagen (2009:366) om handel med läkemedel.
Ansvaret enligt första stycket 4 omfattar drift, förvaltning och utveckling av infrastrukturen.	
	Ansvaret enligt första stycket 6 omfattar ledning, drift, förvaltning och utveckling av infrastrukturen.

[3] Lydelsen återges utifrån förslag i SOU 2024:45, som bl.a. omfattar en ny femte punkt i första stycket

1 Bakgrund

1.1 Uppdrag

Regeringen har gett Myndigheten för digital förvaltning (Digg) och E-hälsomyndigheten varsitt uppdrag att utveckla en sammanhållen infrastruktur för identitets- och behörighetshantering. I denna rapport redovisas Diggs uppdrag.

1.1.1. Uppdrag till Digg

Digg har i regleringsbrevet för 2025 (Fi2024/00591 och Fi2024/02483 [delvis]) fått i uppdrag att utveckla en sammanhållen infrastruktur för identitets- och behörighetshantering, som ska kunna tillhandahållas inom ramen för Ena – Sveriges digitala infrastruktur. Uppdraget ska utföras i nära samverkan med E-hälsomyndigheten för att möta behovet av att införa en nationell digital infrastruktur i hälso- och sjukvården, bland annat den nationella läkemedelslistan. Digg ska inom ramen för uppdraget analysera behovet av och lämna förslag på författningsändringar samt föreslå hur infrastrukturen fortsatt ska förvaltas och drivas, även i kris och krig.

1.1.2. Uppdrag till E-hälsomyndigheten

E-hälsomyndigheten har i regleringsbrevet för 2025 (S2024/02156 [delvis]) fått i uppdrag att ta fram och tillgängliggöra en sammanhållen infrastruktur för identitets- och behörighetshantering inom hälso- och sjukvården. Arbetet ska ske i samverkan med Digg och det förvaltningsgemensamma arbetet inom ramen för Ena – Sveriges digitala infrastruktur.

1.1.3. Uppdragets omfattning

Arbetet handlar om att etablera en nationell, skalbar och effektiv områdes- eller sektorsövergripande modell för identitets- och behörighetshantering. I enlighet med uppdraget sker arbetet både inom hälso- och sjukvårdssektorn i samverkan med E-hälsomyndigheten, och tillsammans med andra sektorer i samhället. Lösningen som ska tas fram ska kunna användas av människor, men även vid kommunikation mellan olika enheter i automatiserade processer (även kallat maskin-till-maskin-kommunikation eller tekniska gränssnitt).

Systemet för elektronisk identifiering (se 2.1.1) löser frågan om vem en person är, det vill säga själva identifieringen. Däremot saknas en motsvarande nationell lösning för att förlitande parter digitalt ska kunna få underlag för att bedöma om en person är behörig att agera för annans räkning eller inom ramen för en yrkesroll. Digg ska därför utveckla en sammanhållen infrastruktur för identitets- och behörighetshantering som kompletterar det befintliga systemet för elektronisk identifiering. Tillsammans skapar dessa infrastrukturer en robust grund för identifiering och behörighetskontroll inom Ena – Sveriges digitala infrastruktur. Den sammanhållna infrastrukturen har fått namnet Samordnad identitet och behörighet.

För att utveckla infrastrukturen Samordnad identitet och behörighet, har Digg tagit fram tekniska komponenter, föreslagit nödvändiga författningsändringar, påbörjat etablering av organisatoriska

modeller för styrning och förvaltning, påbörjat framtagande av avtalslösning samt skapat förutsättningar för förankring och kommunikation.

1.1.4. Avgränsningar

Digg har gjort följande avgränsningar i arbetet med uppdraget:

- Vi gör inga faktiska anslutningar av enskilda aktörer.
- Vi fastställer inga behörighetsregler. Exempelvis fastställs inte vilken personal som får åtkomst till vissa data inom vård eller skola. Sådana regler finns delvis i lag och förordning och behöver i övrigt även fortsättningsvis utformas inom respektive verksamhetsområde, men infrastrukturen ska ge en gemensam grund för att sådana regler kan tillämpas automatiserat.

1.2 Samverkan och förankring

Inom uppdraget har Digg samverkat med E-hälsomyndigheten och andra aktörer. Under året har det därför varit centralt att etablera effektiva samverkansstrukturer. Digg har prioriterat nedanstående delar eftersom de varit viktiga för genomförandet av uppdraget.

- Gemensamt strukturerat arbetssätt. Genom att etablera forum på både strategisk/taktisk nivå (utskottet) och operativ nivå (arbetsgrupper för teknik, juridik och verksamhet) har komplexa frågor kunnat hanteras samordnat. Deltagande aktörer har varit Digg, E-hälsomyndigheten, Inera AB, Sveriges kommuner och regioner (SKR), Skolverket, Stiftelsen för internetinfrastruktur (Internetstiftelsen), Vetenskapsrådet, Region Stockholm och Västra Götalandsregionen.
- Gemensam inriktning och säkerställande av samsyn. Aktörer i utskottet har enats i en avsiktsförklaring (bilaga 1) om att aktivt delta i arbetet och följa gemensamma principer.
- Tidigt fokus på juridik och säkerhet. Digg har tidigt i processen identifierat juridiska frågor och därefter löpande tagit upp sådana frågor i det taktiska utskottet. Möten har genomförts med Nationellt cybersäkerhetscenter för att samordna säkerhetsperspektiven.
- Bred förankring. Genom forum, konferenser och leverantörsmöten har Digg och E-hälsomyndigheten fått inspel från både offentliga och privata aktörer, vilket har gett bättre underlag för vidare utveckling och kommunikation. Samverkans- och förankringsarbetet beskrivs mer utförligt i bilaga 2.
- Förankring inom de samverkansstrukturer som finns för Ena - Sveriges digitala infrastruktur.

Digg har löpande informerat Regeringskansliet (Finansdepartementet och Socialdepartementet) om hur arbetet med uppdraget fortskridit.

1.3 Ena – Sveriges digitala infrastruktur

Den sammanhållna infrastrukturen för identitets- och behörighetshantering ska kunna etableras inom ramen för Ena – Sveriges digitala infrastruktur. Ena är en nationell resurs som möjliggör smartare digitalisering av offentlig sektor, underlättar för offentlig sektor att dela data och att bygga digitala lösningar som fungerar bättre för invånare och företag, samtidigt som kostnaderna för

digitalisering minskar. De olika lösningarna har tagits fram och förvaltas av olika myndigheter, där Digg idag ansvarar för flertalet. Digg har också ansvar för samordningen av Ena.

Flera av lösningarna inom Ena är inte synliga för användaren eftersom de utgör en underliggande digital infrastruktur som andra aktörer nyttjar för att skapa bättre digitala tjänster för användare. På så sätt bidrar Ena till bättre samhällsservice hos myndigheter, samt främjar innovation och tillväxt. Samordnad identitet och behörighet är en sådan underliggande infrastruktur som ska säkerställa att rätt person eller organisation får tillgång till rätt information vid rätt tillfälle och kan agera digitalt inom ramen för sitt mandat. Genom att erbjuda denna infrastruktur inom Ena, kan aktörer ta i bruk gemensamma standarder och komponenter för hantering av identitet och behörighet. Detta möjliggör bättre interoperabilitet både inom och mellan olika verksamhetsområden.

Av budgetpropositionen 2026[4] framgår att Regeringen ser behov av att stärka den strategiska styrningen och uppföljningen av den offentliga förvaltningens digitalisering genom att prioritera utveckling, förvaltning och användning av den nationella digitala infrastrukturen Ena. Syftet med att stärka styrningen och uppföljningen är att säkerställa en långsiktigt hållbar, säker, behovsanpassad och sammanhållen digital infrastruktur.

Arbetet med Ena fortsätter planerat och koordinerat. Genom att bygga ut den nya infrastrukturen Samordnad identitet och behörighet successivt, skapas en stabil grund för allt fler aktörer att ansluta sig så att hela den offentliga sektorn på sikt kan ges bättre förutsättningar att utveckla trygga och ändamålsenliga digitala tjänster.

[4] Prop. 2025/26:1, Utgiftsområde 22, sidan 123.

2 Nuläge, utmaningar och nyttor

Detta kapitel beskriver nuläget för identitets- och behörighetshantering i Sverige, de byggstenar som redan finns, samt de utmaningar och nyttor som ligger till grund för behovet av en sammanhållen infrastruktur.

2.1 Befintliga byggstenar

2.1.1. Systemet för elektronisk identifiering, grunden för identitetshanteringen

Arbetet med en sammanhållen infrastruktur för identitets- och behörighetshantering tar sin utgångspunkt i den nationella infrastrukturen för elektronisk identifiering. Den utgör redan idag en central byggsten i Sveriges digitala infrastruktur och lägger grunden för hur individer säkert kan identifieras digitalt.

Systemet regleras både genom EU-rätt och svensk författning, samt genom avtal och överenskommelser mellan anslutna parter. Det används i stor utsträckning inom statliga myndigheter, regioner och kommuner och är en förutsättning för att invånare och företag ska kunna få tillgång till digital service på ett tillräckligt säkert sätt. Systemet möjliggör även Sveriges deltagande i det europeiska samarbetet enligt eIDAS-förordningen, vilket innebär att svenska e-legitimationer kan användas gränsöverskridande i andra EU-länder.

Systemet för elektronisk identifiering består av flera delar, bland annat följande:

- Granskning av utfärdare av e-legitimationer.

Digg granskar och bedömer om en aktör som vill utfärda svenska e-legitimationer inom systemet för elektronisk identifiering uppfyller de krav som ställs i Tillitsramverket för svensk e-legitimation. Tillitsramverket innehåller omfattande krav inom bland annat organisation och styrning, ledningssystem för informationssäkerhet, fysisk, administrativ och personorienterad säkerhet, teknisk säkerhet samt processer för ansökan, identifiering och registrering. Om Digg finner att utfärdaren uppfyller dessa krav godkänns aktören för anslutning. På så sätt säkerställs att e-legitimationerna kan användas brett inom offentlig sektor och att både invånare och myndigheter kan ha förtroende för systemet och dess hantering. Årlig uppföljning av kravefterlevnad genomförs också av Digg.

- Den tekniska federationen som kallas Sweden Connect.

Sweden Connect är den infrastruktur som förmedlar elektronisk identifiering mellan utfärdare av e-legitimationer och de tjänster (förlitande parter) som behöver säker identifiering av användare. Genom Sweden Connect kan offentliga aktörer erbjuda invånare och företag säker inloggning med svenska e-legitimationer, via anslutna identitetsintygsutgivare.

2.1.2. Existerande federationer

I Sverige finns redan flera etablerade federationer som har utvecklats inom olika sektorer för att möta specifika behov som finns där. Sweden Connect används för elektronisk identifiering med e-legitimation, Sambi inom hälso- och sjukvården för identitets- och behörighetskontroll, bland annat kopplat till den nationella läkemedelslistan, och Skolfederation inom utbildningssektorn, bland annat för åtkomst till digitala läromedel. I bilaga 3 beskrivs några befintliga federationer närmare.

Ovanstående federationer har bidragit till standardisering inom sina respektive delområden och erbjuder tekniska funktioner för exempelvis autentisering, metadatautbyte och kataloghantering. De bygger emellertid på olika avtal och olika funktioner, vilket gör att helheten blir splittrad så att exempelvis en kommun eller region behöver ansluta sig till olika federationer för att kunna agera inom de olika områden där de är verksamma.

2.2 Utmaningar med dagens fragmenterade hantering av identitet och behörighet

Inom offentlig sektor hanteras idag identitet och behörighet i flera separata lösningar. Det beror på att myndigheter, regioner och kommuner över tid har utvecklat egna lösningar, ofta utifrån egna, lokala behov och juridiska förutsättningar. Därför finns inom offentlig sektor en splittrad struktur där tekniska standarder, avtal och regelverk skiljer sig åt mellan olika aktörer. Systemen är inte interoperabla, de kan inte enkelt samverka eller utbyta information på ett säkert och effektivt sätt. Detta försvårar i sin tur välfärdssystemets digitalisering och möjligheter till datadriven utveckling. Nedan beskrivs utmaningarna och deras konsekvenser kortfattat.

2.2.1. Konsekvenser av bristande interoperabilitet

När de olika systemen för identitet och behörighetshantering löses på olika sätt inom offentlig sektor ger den bristande interoperabiliteten en rad konkreta utmaningar.

Effektivitet och kostnader

- Dubbelarbete och höga kostnader, eftersom varje aktör utvecklar, förvaltar och uppdaterar egna lösningar.
- Onödig inloggningstid tar tid från kärnverksamheten.
- Stödfunktioner belastas, då it-tekniker och administratörer lägger mycket tid på att hantera system som inte är anpassade till varandra.
    - För it-tekniker handlar det bland annat om hantering av certifikat, synkronisering av konton och felsökningar.
    - För administratörer om manuell hantering av användarkonton för anställda, nyanställda och vikarier.

Arbetsmiljö och användarupplevelse

- Dålig arbetsmiljö i form av stress, frustration och en upplevelse av splittrade system för personal inom välfärden som behöver lägga mycket tid på att logga in i olika system.

Säkerhet, kvalitet och rättssäkerhet

- Manuell hantering ökar risken för fel, till exempel att en behörighet ligger kvar fast den borde vara borttagen, att någon inte får tillgång i tid eller att man slarvar med utloggning för att spara tid. Sådana misstag kan påverka både säkerheten och verksamheten.
- Oklarheter i ansvarsfördelning, påverkar rättssäkerhet och spårbarhet när flera system hanterar samma individs uppgifter på olika sätt.

Samverkan och informationsdelning

- Försvårad och ineffektiv samverkan mellan aktörer inom och med offentlig sektor, eftersom olika tekniska och juridiska förutsättningar hindrar ett effektivt informationsutbyte. Detta förhindrar exempelvis förbättringar inom vården.
- Avsaknad av säker och effektiv informationsdelning, detta minskar potentialen att använda data för kvalitetsutveckling, forskning och innovation.

Digital utveckling och samhällsmål

- Minskad förmåga att tillvarata digitaliseringens möjligheter.
- Försvårar välfärdssystemets förmåga att förebygga organiserad brottslighet.
- Begränsar effektivitet och säkerhet då bristen i informations- och datadelning försvårar arbete med att motverka arbetslivskriminalitet, bekämpa välfärdsbrottslighet och förenkla för företag.

2.2.2. Särskilt om utmaningar inom verksamhetsområde hälso- och sjukvård

Inom hälso- och sjukvården är behovet av en sammanhållen infrastruktur för identitets- och behörighetshantering särskilt tydligt. E-hälsomyndigheten beskriver i sin rapport *Hantering av digitala identiteter och styrning av behörigheter inom hälso- och sjukvård i Sverige* (E-hälsomyndigheten dnr. 2025–00348) bland annat hur hantering av digitala identiteter och styrning av behörigheter har byggts upp organiskt. Då de olika lösningarna är framtagna utifrån en organisations eller tjänsts behov så har det lett till bristande interoperabilitet och ökade kostnader, vilket i sin tur förhindrar förbättringar inom vården.

2.3 Nyttor med en sammanhållen nationell infrastruktur

Mot bakgrund av vad som beskrivs ovan finns ett tydligt behov av en sammanhållen nationell infrastruktur för identitets- och behörighetshantering. En sådan infrastruktur bidrar till ökad säkerhet, effektivitet och samverkan inom och med offentlig sektor. De beskrivna nyttorna förutsätter dock att infrastrukturen tas i aktivt bruk och används på avsett sätt av berörda aktörer, nyttorealisering sker inte enbart genom att infrastrukturen finns på plats. Nedan beskrivs övergripande nyttor för offentlig sektor.

2.3.1. Övergripande samhällsnyttor

Den gemensamma infrastrukturen är en viktig möjliggörare för digitalisering som skapar nytta för både medborgare, företag och offentlig sektor. Den bidrar till ökad säkerhet, effektivitet och

samverkan, i linje med målen för Sveriges digitala omställning om medborgarnytta, bättre välfärd och stärkt konkurrenskraft.

- Medborgarnytta och bättre välfärd. Gemensamma standarder och regler skapar förutsättningar för att offentlig sektor ska kunna dela information och samarbeta över organisationsgränser. Det gör att invånare och företag möter en mer sammanhållen och tillgänglig service, vilket stärker både välfärden och förtroendet för den offentliga förvaltningen som helhet.

- Ekonomisk effektivitet. En gemensam infrastruktur minskar behovet av att varje aktör utvecklar och förvaltar egna lösningar för identitet och behörighet. Genom att återanvända gemensamma komponenter och standarder kan resurser användas mer effektivt, vilket sänker kostnaderna för både offentlig sektor och dess leverantörer och frigör medel till kärnverksamhet och välfärd.

- Förvaltning och styrningsnytta. En gemensam ram för ansvar, regler och uppföljning gör det enklare för staten att styra och följa upp den digitala utvecklingen. Den skapar också tydlighet för de aktörer som ansluter, vilket underlättar efterlevnad, minskar risken för felaktig tolkning och bidrar till en mer enhetlig tillämpning i hela den offentliga sektorn.

- Robusthet och beredskap. Gemensamma säkerhetsprinciper och tekniska skyddsmekanismer stärker samhällets motståndskraft och förmåga att upprätthålla digitala tjänster vid störningar, kris eller krig. En samlad infrastruktur med inbyggd redundans och tydliga krav på kontinuitet bidrar till ökad resiliens i den offentliga sektorns digitala ekosystem. Det gör det möjligt att snabbt återställa funktioner, skydda samhällsviktig information och bibehålla tillit även under påfrestande förhållanden.

- Juridisk tydlighet. Ett gemensamt regelverk skapar trygghet och förutsägbarhet för både offentliga och privata aktörer. När ansvar och krav är tydligt definierade minskar risken för olika tolkningar, vilket effektiviserar samverkan och stärker rättssäkerheten. Den juridiska tydligheten gör det enklare att ansluta, minskar den administrativa bördan och ökar förtroendet för den digitala förvaltningen som helhet.

- EU och internationell anpassning. En gemensam infrastruktur gör det möjligt för Sverige att fullt ut delta i europeiska initiativ som den digitala identitetsplånboken (EUDIW)[5] och Single Digital Gateway (SDG) – en gemensam digital ingång till Europa[6]. Den säkerställer att svenska lösningar följer gemensamma standarder och regelverk för gränsöverskridande

[5] EUDIW står för EU Digital identity wallet, på svenska: Digital identitetsplånbok - en tjänst, i form av en app, som gör det möjligt för användare att identifiera sig, dela information och signera digitalt. Mer information finns på Diggs webbplats www.digg.se.

[6] SDG - Singel digital gateway, på svenska: en gemensam digital ingång till Europa, den ska göra det lättare för privatpersoner och företag att använda digitala tjänster i andra EU-länder. Mer information finns på Diggs webbplats www.digg.se.

digitala tjänster, vilket stärker interoperabiliteten och gör det enklare för både invånare och företag att verka i hela EU.

2.3.2. Nyttor inom hälso- och sjukvårdssektorn

E-hälsomyndigheten beskriver i sin rapport vilka effekter man ser förutsättningar för att nå inom hälso- och sjukvården med en sammanhållen infrastruktur för identitets- och behörighetshantering. Digg bedömer, utifrån dialog med aktörer i andra sektorer, att motsvarande nyttor kan möjliggöras även i andra delar av offentlig sektor där identitets- och behörighetshanteringen idag är parallell och fragmenterad. För att uppnå dessa nyttor krävs att aktörer ansluter sig till och tillämpar infrastrukturen.

- Högre tillit till den digitala infrastrukturen. Öka tilliten hos aktörer att implementera en robust och transparent lösning för identitets- och behörighetshantering.

- Ökad nationell interoperabilitet. Bidrar till att öka förutsättningarna för interoperabilitet mellan olika system, oavsett om en huvudman är offentligt finansierad eller inte.

- Effektiv datadelning. En gemensam identitets- och behörighetshantering bidrar till att möjliggöra effektiv delning av data mellan olika system och organisationer, både offentliga och privata aktörer.

- Förbättrad säkerhet. Bidrar till att säkerställa att endast behörig personal har tillgång till känslig information och system.

- Ökad effektivitet. Skapar förutsättningar för att minska onödig tid som medarbetare behöver lägga på till exempel inloggning i olika system, samt minskar den administrativa bördan både för medarbetare och IT-personal.

3 Nyläge - En svensk sammanhållen federationsinfrastruktur för identitets- och behörighetshantering

3.1 En federationsinfrastruktur för flexibilitet och skalbarhet

Digg förordar en infrastruktur för identitets- och behörighetshantering som byggs upp enligt en federativ modell. En federation är en samverkansmodell där självständiga stater eller organisationer samarbetar enligt gemensamma lagar, regler eller standarder, men behåller ansvar för egna system. I kapitel två har vi beskrivit att dagens lösningar för identitet och behörighet är uppdelade mellan flera aktörer och system. Vi har skillnader i teknik, avtal och regelverk som skapar hinder för digital samverkan.

För att en federation ska fungera krävs en infrastruktur, det vill säga en praktisk uppsättning av komponenter som gör samverkan möjlig. Infrastrukturen omfattar tekniska system, kataloger, register, roller, regler och avtal som tillsammans ger förutsättningar för en säker och effektiv samverkan. Federationen ger alltså gemensamma spelregler och verktyg. En samordnad federationsinfrastruktur ger en gemensam grund och etablerar interoperabilitet för informationsutbyten inom och med offentlig sektor.

Syftet med en federativ infrastruktur är att:

- göra det möjligt för självständiga organisationer att samverka digitalt och samtidigt behålla sitt eget ansvar.
- skapa en gemensam och enhetlig grund för hur identitets- och behörighetsinformation hanteras.
- genom gemensamma regler och specifikationer möjliggöra förtroende mellan aktörer så att information kan delas på ett säkert och rättssäkert sätt.
- säkerställa att aktörer samverkar enligt gemensamma spelregler men förblir självständiga i sina uppdrag.

Modellen gör det också möjligt att bygga ut infrastrukturen stegvis i takt med att fler aktörer ansluter.

3.2 Utgångspunkter och målsättning

För att den federativa modellen ska fungera i praktiken behövs en gemensam struktur för samverkan. Federationsinfrastrukturen utgör denna struktur och består av de komponenter, roller och regler som tillsammans gör samverkan möjlig. Den förenar två perspektiv:

Det juridiska perspektivet beskriver roller, ansvar och avtal som styr hur aktörer får använda infrastrukturen. I de juridiska kapitlen 4 – 6 beskrivs detta närmare.

Det tjänsteorienterade perspektivet beskriver hur systemen kopplas ihop och hur informationsflöden hanteras. Rapporten behandlar endast det juridiska perspektivet.
Målet är att etablera en sammanhållen infrastruktur som både är juridiskt hållbar och tekniskt interoperabel. Den ska kunna användas i olika verksamheter och stödja både mänskliga och automatiserade processer. Digg föreslår därför en gemensam, förvaltningsövergripande infrastruktur (behörighetsinfrastrukturen) som avser möjliggöra digital samverkan mellan självständiga aktörer med stöd av gemensamma tekniska specifikationer och regelverk för utfärdande, förmedling och användning av digitala behörighetshandlingar. Med stöd av denna infrastruktur ska medarbetares juridiska behörighet kunna kontrolleras automatiserat av förlitande parter som tillhandahåller digitala tjänster.

3.3 Federationsinfrastrukturens utformning

Federationsinfrastrukturen består inledningsvis av en behörighets- och en identitetsinfrastruktur. Varje aktör deltar med egna komponenter och tjänster, men följer gemensamma tekniska standarder och regler som säkerställer att allt fungerar tillsammans som en helhet.

Infrastrukturen är utformad för att vara decentraliserad, skalbar och robust, vilket gör att den kan växa och förändras över tid utan att förlora stabilitet eller förutsägbarhet. Genom en decentraliserad modell kan ansvar och funktioner fördelas mellan flera parter. Styrningen sker genom gemensamma specifikationer och överenskomna processer. Detta skapar en flexibel struktur som kan anpassas till olika verksamheters behov. Nya tjänster, komponenter eller federationsområden kan läggas till stegvis och integreras med befintliga delar.

Federationsinfrastrukturen bygger på den öppna internationella specifikationen OpenID Federation som beskriver hur olika protokoll för identitets- och behörighetskontroll (såsom OpenID Connect, OAuth 2.0 och med utökning skulle kunna omfatta SAML) ska användas för att skapa interoperabilitet. Dessa internationella specifikationer är generella och lämnar stort utrymme för tolkning. De utgör därför en gemensam grund som behöver profileras och kompletteras för att skapa en fungerande federationsinfrastruktur för svenska förhållanden. Inom denna kontext används specifikationerna för att reglera hur digital samverkan etableras och upprätthålls, till exempel hur metadata, nycklar och säkerhetskrav hanteras, hur ansvar fördelas och hur aktörer ansluts till federationen. Inom federationsinfrastrukturen kan det finnas flera federationsområden med egna krav och regler men med gemensamma grunder för interoperabilitet. På så sätt kan varje område anpassa lösningen efter sina behov men ändå vara en utgå från den nationella federationsinfrastrukturen.

Sammanfattningsvis, för att federationsinfrastrukturen ska kunna användas i praktiken delas ansvaret mellan flera roller som tillsammans möjliggör både den tekniska driften och användningen inom olika verksamhetsområden. Federationsinfrastrukturen utformas så att ett gemensamt ramverk möjliggör interoperabilitet, medan områdesspecifika policyer och behov fortsatt kan tillämpas. Infrastrukturen ska stödja variation, inte standardisera bort den. Det betyder i praktiken att det inom federationsinfrastrukturen, ur ett tekniskt perspektiv, initialt finns två områden, behörighetsinfrastruktur och identitetsinfrastruktur. Dessa avser att hantera den tekniska interoperabiliteten, vid behov kan ytterligare tekniska områden skapas.

4 Juridiska utgångspunkter

4.1 Behörighetsinfrastrukturens övergripande utformning

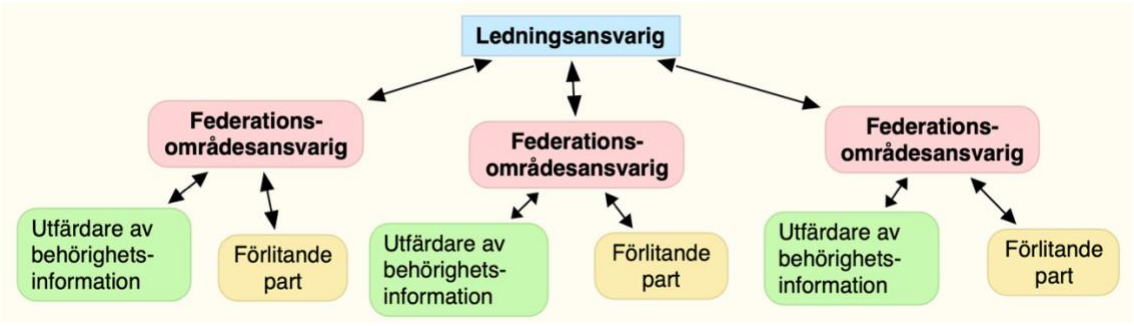
I detta kapitel och i de två följande beskrivs federationsinfrastrukturen ur ett juridiskt och delvis konceptuellt perspektiv. En beskrivning från ett tekniskt eller verksamhetsmässigt perspektiv skulle sannolikt behöva vara mer detaljerad och delvis behandla andra frågor, men är alltså inte syftet med texten. Detta innebär bl.a. att federationsområden definieras ur ett juridiskt perspektiv oberoende av eventuella tekniska domäner, tekniska roller eller organisatoriska tillämpningsområden.

4.1.1 Roller och ansvar

När en federationsinfrastruktur för behörighetskontroll ska beskrivas från ett juridiskt perspektiv kan det vara lämpligt att utgå från hur infrastrukturen för elektronisk identifiering fungerar. Där finns tre kategorier av aktörer: en ledningsaktör, leverantörer av identitetsintyg och förlitande parter. Inom en federationsinfrastruktur för juridisk behörighetskontroll behövs ytterligare en kategori – federationsområdesansvariga – som har till uppgift att administrera, samordna och ansvara för anslutning av utfärdare av behörighetshandlingar och förlitande parter. Juridiskt finns det alltså fyra roller med huvudsakligen följande uppgifter inom infrastrukturen:

En *ledningsansvarig* som styr, reglerar, samordnar och utvecklar behörighetsinfrastrukturen, ansluter federationsområdesansvariga och agerar som fullmäktig vid avtalsslut mellan parter samt tillhanda-håller gemensamma funktioner såsom en digital katalog över aktörer och funktioner inom behörighetsinfrastrukturen (ledningsansvarigs aktörs- och funktionsregister).

För varje federationsområde finns vidare en *federationsområdesansvarig* som administrerar, samordnar och ansluter en grupp av utfärdare av behörighetshandlingar och förlitande parter samt tillhandahåller gemensamma stödfunktioner såsom en digital katalog över de aktörer och funktioner som denne anslutit (federationsområdesansvarigs aktörs- och funktionsregister). En federations-områdesansvarig ska dessutom registrera tjänster och agera som fullmäktig vid avtalsslut mellan parter inom det federationsområde där denne verkar, allt i enlighet med gällande anslutningsavtal och tekniska specifikationer. Den federationsområdesansvarige ansluter härvid, dels *utfärdare av behörighetshandlingar,* som ställer ut digitalt stämplade eller underskrivna handlingar (*behörighetshandlingar*), dels *förlitande parter* som använder dessa handlingar för juridiska behörighetskontroller i digitala tjänster, se följande figur.



I kommande avsnitt fördjupas denna beskrivning från juridiska utgångspunkter.

4.1.2 Olika ”skikt” av funktioner måste hållas isär juridiskt

Det behöver tydligt framgå vilka delar som ingår respektive inte ingår i den behörighetsinfrastruktur som föreslås. De kan från juridiska utgångspunkter beskrivas som olika ”skikt” av funktioner där vissa ingår medan andra faller utanför behörighetsinfrastrukturen.

Det finns ett skikt med gemensamma funktioner, regler och rutiner för alla aktörer som är anslutna till behörighetsinfrastrukturen. Detta kan beskrivas som infrastrukturens fundament. Nästa skikt består av kompletterande funktioner, regler och rutiner som respektive federationsområdesansvarig behöver inom sitt område och som kan beskrivas som områdesspecifika tillägg. Infrastrukturen för elektronisk identifiering är ytterligare ett skikt som redan används, men behöver nyttjas på sätt som anpassats till behörighetsinfrastrukturen. Till detta kommer funktioner och tjänster via vilka aktörerna utbyter information. Fundamentet och de områdesspecifika funktionerna ingår i behörighetsinfrastrukturen medan hanteringen i övrigt stöds av behörighetsinfrastrukturen.

En digital tjänst som ger tillgång till sekretessreglerad information, eller som gör rättshandlingar möjliga, kräver vanligtvis säker identifiering med stöd av e-legitimation. Användningen av e-legitimation och digital tjänst ingår emellertid inte i behörighetsinfrastrukturen. Det som äger rum i den digitala tjänsten regleras genom författning eller villkor i avtal som är kopplade till respektive digital tjänst. Vid elektronisk identifiering för att få tillgång till en digital tjänst eller att skriva under elektroniskt tillämpas på motsvarande sätt föreskrifter i författning och avtal för elektronisk identifiering för hanteringen av metadata och användningen av e-legitimation. De flesta får antas ha tillgång till ändamålsenliga e-legitimationer eller andra former för elektronisk identifiering som godtas inom den sektor där medarbetaren är verksam. Dessutom är användningen av identitetsintyg, som har begärts och mottagits av förlitande part, reglerad i annan ordning och ingår inte i behörighetsinfrastrukturen.

Efter att en förlitande part beställt och mottagit en behörighetshandling ska den användas för att kontrollera medarbetarens juridiska behörighet. Denna användning sker emellertid inte inom behörighetsinfrastrukturen och regleras inte heller där. På motsvarande sätt som en förlitande part använder ett mottaget identitetsintyg kan den förlitande parten använda en behörighetshandling för att fatta beslut om åtkomst till dennes digitala tjänst. Beställning och mottagning av behörighetshandling sker alltså utanför behörighetsinfrastrukturen liksom den kontroll som förlitande part gör av en medarbetares identitet. Trots att mycket av hanteringen av identiteter och juridiska behörigheter översiktligt kan beskrivas som verksamhet inom ramen för ett och samma tekniska ramverk för autentisering och auktorisation, regleras således digitala tjänster, identitetskontroller och behörighetskontroller var för sig i juridisk mening. Olika regelverk gäller därmed för en förlitande parts kontroller av vilken medarbetare som agerar (identitetskontroll) respektive vilken behörighet en medarbetare har (behörighetskontroll).

Det fortsatta informationsutbytet efter att en identitets- och behörighetskontroll genomförts sker inte inom behörighetsinfrastrukturen eller system och funktioner som den ledningsansvarige eller en federationsområdesansvarig tillhandahåller för anslutna aktörer.

Det är av avgörande betydelse för den fortsatta analysen att inte blanda samman dessa olika ”skikt” av funktioner och den reglering som gäller för var och en av dem.

4.1.3 Vad innebär rollen som ledningsansvarig?

I it-standardiseringssammanhang har en federationsområdesansvarig en central roll. Utöver vad som föreskrivs om Diggs ansvar i förslaget till ändring i Diggs instruktion bör Digg ges möjlighet att i avtal och överenskommelser mellan anslutna parter ges ett ansvar som ledningsansvarig. Den ledningsansvarige svarar för regelverk och juridisk styrning. Hit hör utformning och förvaltning av tekniskt ramverk, inklusive specifikationer för interoperabilitet samt fastställandet av uppförandekoder, gemensamma format m.m. och övergripande regler för samverkan mellan parterna. Den ledningsansvarige ska vidare svara för administrationen av avtal och överens-kommelser genom att teckna sådana med en federationsområdesansvarig inom respektive federationsområde och med andra centrala aktörer som ansluts till federationsinfrastrukturen. Här ingår att fastställa och reglera krav på säker informationshantering och ansvarsfördelning vid fel eller avvikelser. Vidare ingår incident- och avvikelsehantering genom att den ledningsansvarige svarar för att etablera funktioner för hantering av incidenter och rapportering av avvikelser inom infrastrukturen, såväl tekniska fel som bristande efterlevnad av regler. Den ledningsansvarige har samtidigt ett övergripande ansvar för styrning och samordning så att infrastrukturen utvecklas enhetligt och ändamålsenligt över tid, vilket innebär att fungera som strategisk koordinator, föra dialog med ansvariga inom federationsområden, samt bevaka och anpassa infrastrukturen till nya juridiska, tekniska och samhälleliga krav. Genom att samla dessa funktioner hos den ledningsansvarige skapas förutsättningar för en likformig, säker och rättsligt hållbar tillgång till uppgifter för juridisk behörighetskontroll som kan användas inom hela den offentliga sektorn och för kontakter med andra anslutna aktörer.

Den ledningsansvarige bör vidare ansvara för att aktörs- och funktionsregister och andra tekniska funktioner inrättas och drivs på ändamålsenligt sätt, så att uppgifter tillgängliggörs om alla federationsområdesansvariga som är anslutna till behörighetsinfrastrukturen, inklusive uppgifter om digital adress och kryptografiskt nyckelmaterial till varje funktion som en federationsområdesansvarig tillhandahåller. Det faktiska informationsutbytet mellan den ledningsansvarige och en utfärdare av behörighetshandlingar eller en förlitande part sker emellertid, som framgått, inte inom behörighetsinfrastrukturen. Den ledningsansvarige samordnar huvudsakligen endast tillgängliggörandet av kvalitetssäkrade uppgifter för digital samverkan.

4.1.4 Vad innebär rollen som federationsområdesansvarig?

För att behörighetsinfrastrukturen ska fungera på ändamålsenligt sätt behövs som framgått inom respektive federationsområde en aktör på mellannivå, under den ledningsansvarige, som ges ett övergripande ansvar för att tillhandahålla, dels funktioner som ska vara enhetliga inom hela infrastrukturen (del av fundamentet), dels de kompletterande funktioner som behövs för att anpassa användningen av behörighetsinfrastrukturen till de särskilda behov och förutsättningar som finns inom den federationsområdesansvariges verksamhetsområde. Den federationsområdesansvarige bör därmed handha vissa administrativa uppgifter, bland annat att ansluta de utfärdare av behörighets-handlingar och förlitande parter som hör hemma inom dennes verksamhetsområde, och ansvara för att:

1. de gemensamma tekniska och administrativa funktioner och tjänster införs som behövs inom den federationsområdesansvariges federationsområde, att de styrs på ett ändamålsenligt sätt och att erforderliga beslut fattas,
2. kompletterande regler införs inom den federationsområdesansvariges federationsområde om det behövs, (allmänna villkor etc.) och att de följs upp och anpassas till utvecklingen,
3. den federationsområdesansvariges aktörs- och funktionsregister och andra nödvändiga tekniska funktioner inom den federationsområdesansvariges federationsområde inrättas, drivs och tillgängliggörs, med uppgifter om

    a) parter som är anslutna till den federationsområdesansvariges federationsområde,
    b) respektive parts digitala adress och kryptografiska nyckelmaterial, och
    c) respektive utfärdare av behörighetshandlingars förmåga att utfärda behörighetshandlingar och uppfyllelse av tekniska och administrativa krav,

4. uppgifter lämnas till den ledningsansvarige för att införas i dennes aktörs- och funktionsregister,
5. incidenter rapporteras till den federationsområdesansvarige, och
6. utfärdare av behörighetshandlingar och förlitande parter ansluts juridiskt och tekniskt till den federationsområdesansvarige och med stöd av fullmakter till övriga parter.

Varje federationsområdesansvarig svarar därmed för att införa sin del av fundamentet (som kompletterar den del av fundamentet som den ledningsansvarige tillhandahåller) samt de federationsområdesspecifika tekniska funktioner, regler och kontrollfunktioner som behövs för att behörighetsinfrastrukturen ska fungera inom dennes federationsområde.

Den federationsområdesansvarige svarar dessutom för den tekniska anslutningen av utfärdare av behörighetshandlingar och förlitande parter inom sitt federationsområde. Dessa funktioner och tjänster ska vara identiska i sin funktionalitet och regleras på samma sätt oberoende av inom vilket federationsområde en federationsområdesansvarig verkar. Funktionerna får således inte avvika från det som den ledningsansvarige har fastställt för federationsinfrastrukturens fundament. Det är nödvändigt för att varje federationsområdesansvarig ska kunna samverka med övriga anslutna parter på ett enhetligt, säkert och förutsägbart sätt. Funktionerna bör alltså inte vara valfria utan utgöra en obligatorisk bas som samtliga federationsområdesansvariga ska införa oberoende av vilket verksamhetsområde de tillhör. Funktionerna ska följa den struktur, de gränssnitt och de specifikationer som fastställts av den federationsområdesansvarige. Detta bör regleras genom avtal.

Även beträffande det som den federationsområdesansvarige tillhandahåller inom infrastrukturen gäller att informationsutbytet, i form av meddelanden och handlingar, mellan en utfärdare av behörighetshandlingar och en förlitande part inte hanteras inom federationsinfrastrukturen. Den federationsområdesansvarige samordnar och tillgängliggör i huvudsak kvalitetssäkrade uppgifter om adresser till parter och kryptografiskt nyckelmaterial för säker kommunikation.

4.1.5 Förmedling av behörighetshandlingar

Utfärdare av behörighetshandlingar, anslutna till respektive federationsområdesansvarig, svarar för att leverera behörighetshandlingar för medarbetare eller digitala aktörer. Varje utfärdare ansluter sig tekniskt till och tecknar avtal med en federationsområdesansvarig.

På liknande sätt som en utfärdare av identitetsintyg kontrollerar vem som har legitimerat sig och intygar användarens identitet, bör en roll som utfärdare av behörighetshandlingar införas för de aktörer som lämnar uppgifter om bland annat medarbetares eller digitala aktörers behörighet genom att ställa ut behörighetshandlingar. Skillnaden i förhållande till identitetsintyg är främst från vilken källa uppgifterna är hämtade. Uppgifter i behörighetshandlingar kommer inte från en identitetskontroll där identitetsuppgifterna stämts av mot Skatteverkets folkbokföringsuppgifter utan vanligtvis från en uppgiftssamling som knutits till behörighetsinfrastrukturen och där det har registrerats vilken behörighet vissa anslutna medarbetare eller digitala aktörer har. En myndighet eller annan organisation som för det register där behörigheten finns dokumenterad tilldelas normalt rollen som utfärdare av behörighetshandlingar (jfr den av myndigheter tillämpade principen att hämta uppgifter från källan). Detta innebär exempelvis att uppgifter om firmatecknare hämtas från bolagsregistret. Alternativt kan behörighetshandlingar, när de ställs ut av medarbetarens eller den digitala aktörens huvudman, ha getts formen av en fullmakt för denne eller ett utdrag ur ett protokoll eller liknande där det finns uppgifter om medarbetarens eller den digitala aktörens behörighet. Någon annan källa än själva behörighetshandlingen finns inte när det är fråga om en fullmakt. Innehållet får bedömas utifrån avtalslagens fullmaktsregler och om den som utfärdat fullmakten har den behörighet som krävs för att utfärda fullmakten. Utgör behörighetshandlingen istället ett utdrag ur ett protokoll eller liknande får medarbetarens eller den digitala aktörens behörighet bedömas utifrån vad som gäller inom berört område. Olika behörighetshandlingar kan således ha ett likartat innehåll men ändå juridiskt behöva bedömas på olika sätt eftersom olika regler om vem som är behörig behöver tillämpas.

För behörighetshandlingar som innehåller uppgifter från en uppgiftssamling som knutits till behörighetsinfrastrukturen blir främst två typer av ”behörighetsattributkällor” aktuella, dels publicitetsregister som vissa myndigheter för, till exempel Bolagsverket för aktiebolag m.fl. juridiska personer med uppgifter om firmatecknare och Lantmäteriet för uppgifter om fastighetsägare, dels register som upprättas för särskilda behov inom ett verksamhetsområde där vissa individer och deras roller finns förtecknade, exempelvis Hälso- och sjukvårdens register över personer och organisationer inom vård och omsorg i Sverige (HSA-registret). Inom federationsinfrastrukturen behöver alltså inte bara de roller innefattas som förenklat kan beskrivas som strikt juridiska, exempelvis ställföreträdare, befullmäktigade ombud och reglerade yrkesroller. Även andra roller kan vara av betydelse för förlitande aktörer, såsom för elever vid en skola.

Till detta kommer att en organisations ställföreträdare, exempelvis generaldirektör eller VD, sällan själv använder de funktioner och tjänster där den föreslagna behörighetsinfrastrukturen förväntas bli av särskild betydelse. De nyttjas istället av medarbetare som fått arbetsuppgiften delegerad till sig. På detta stadium i utvecklingsarbetet räcker det att konstatera att förenklade digitala rutiner för olika typer av behörighetskontroller är nödvändiga. Den närmare utformningen av dessa förfaranden får genomlysas i det fortsatta utvecklingsarbetet inom respektive federationsområde, både när det gäller typer av behörighetshandlingar och vilka som bör vara utfärdare.

Utfärdare av behörighetshandlingar bör ansluta sig till och teckna avtal med en federationsområdesansvarig för att leverera behörighetshandlingar på beställning av förlitande parter, oberoende av om den förlitande parten är ansluten till samma federationsområdesansvarig. Avtalen för anslutning till federationsinfrastrukturen behöver således utformas så att behörighetshandlingar ska kunna användas även inom ett annat federationsområde än det som utfärdaren av behörighetshandlingen är ansluten till. Möjligheten att få tillgång till behörighetshandlingar vidgas därmed. Förlitande parter bör således anslutas till och teckna avtal med en federationsområdesansvarig för att kunna beställa behörighetshandlingar.

4.1.6 Funktioner för att informera om en federationsmedlems förmåga

Det kommer att behövas tekniska funktioner för att informera om vilka aktörer som är anslutna till federationsinfrastrukturen och vilken förmåga en viss aktör har. Varje utfärdare av behörighetshandlingar, som ansluter sig till federationsinfrastrukturen genom att teckna avtal eller ingå en överenskommelse bör vara skyldig att redogöra för vissa uppgifter. Av avtal för federationsinfrastrukturen bör därmed följa att anslutna aktörer, själva eller genom en annan ansluten aktör, ska redogöra för vissa uppgifter i form av en deklaration av förmåga.

Under den inledande fas när en behörighetsinfrastruktur införs kommer emellertid endast ett begränsat antal federationsområden, federationsområdesansvariga, utfärdare av behörighetshandlingar och förlitande parter att delta. Anslutna parter bör då enkelt kunna få kännedom om vem som kan leverera den typ av behörighetshandling som efterfrågas och vilka förlitande parter som kommer i fråga för leverans av behörighetshandlingar. En och samma aktör kan emellertid verka i flera sammanhang, exempelvis när en kommun bedriver såväl skola och socialtjänst som vård och omsorg. Viss information krävs därmed, inte bara om vilka aktörer som är anslutna utan även om tillhandahållna aktörers och tjänsters förmåga, såsom vilka behörighets-handlingar som kan tillgängliggöras, vilken tjänst som är anpassad till det kontrollbehov som föreligger i det enskilda fallet och vilka tekniska krav som gäller beträffande exempelvis format och protokoll. I avtal för federationsinfrastrukturen bör därmed anges att anslutna aktörer, själva eller genom en annan ansluten aktör, ska redogöra för vissa uppgifter i form av en deklaration av förmåga.

Eftersom det handlar om detaljerade tekniska uppgifter som förändras över tid bör regleringen av bland annat vad som ska deklareras och i vilket format vara reglerat i en teknisk bilaga till de avtal som parterna tecknar och redan från start bör avtalen innehålla regler om en skyldighet för part att redogöra för vissa uppgifter i form av en deklaration av förmåga. Vilka förmågor som ska deklareras framgår alltså av avtalet eller av en bilaga till detta. Det behöver emellertid, från såväl juridiskt som praktiskt perspektiv, genomlysas hur dessa uppgifter ska tillhandahålls och av vem eller vilka. En tänkbar hantering för att tekniskt informera om en förmåga eller om uppfyllda villkor kan vara att använda stämplade metadata i form av egenskapsintyg, se vidare avsnitt 6.3.

4.2 Förhållandet mellan identitetskontroll och behörighetskontroll

4.2.1 Existerande funktioner för identitetskontroll bör återanvändas

Huvuddelen av de organisationer som berörs av federationsinfrastrukturen har redan anskaffat e-legitimationer till sina medarbetare, exempelvis SITHS inom hälso- och sjukvården. Det finns också utarbetade arbetssätt för identitetskontroll. Den del av uppdraget som består i att etablera en (sammanhållen) identitetshantering bör därmed kunna genomföras genom att existerande funktioner för elektronisk identitetskontroll integreras med den behörighetsinfrastruktur som föreslås. Kontroller som förlitande part gör av vilken medarbetare som agerar regleras därmed genom redan existerande avtal för elektronisk identifiering med tillägg av vissa åtgärder för att uppnå en fullgod elektronisk identitetskontroll.

De avtal som finns för elektronisk identifiering bör delvis kunna tillämpas även när denna hantering samordnas med elektroniska behörighetskontroller. En anpassning behövs dock till de särskilda förutsättningar som följer av att ett större antal aktörer ansluts som utfärdare av behörighetshandlingar, att ytterligare aktörer (federationsområdesansvariga) tillkommer för att stödja och styra respektive federationsområde och att de skydd och kontroller som behövs skiljer sig åt mellan olika områden.

Trots att mycket av hanteringen av identiteter och juridiska behörigheter översiktligt kan beskrivas som verksamhet inom ramen för ett och samma tekniska ramverk för autentisering och auktorisation, regleras digitala tjänster, identitetskontroller och behörighetskontroller var för sig i juridisk mening. Olika regelverk gäller därmed för en förlitande parts kontroll av vilken medarbetare som agerar (identitetskontroll) respektive kontrollen av om en medarbetare eller en digital aktör har juridisk behörighet att agera på det sätt som sker (behörighetskontroll). Den del av en identitetskontroll som omfattar elektronisk identifiering regleras redan idag genom etablerade och väl fungerande avtal och regelverk. Denna befintliga regleringen av elektronisk identifiering kan och bör användas även i fortsättningen, samordnad med den nya behörighetsinfrastrukturen. För identifieringsdelen ser det därmed inte ut att behövas några nya avtal eller särskilda regelverk. Skulle det visa sig att ytterligare regler behövs kan de införas genom exempelvis ett tilläggsavtal rörande identifiering.

Behörighetsinfrastrukturen bör således utformas så att den på ett effektivt och ändamålsenligt sätt kan integrera och dra nytta av befintliga lösningar för elektronisk identitetskontroll. Därmed begränsas behovet av nya avtal och regelverk till infrastrukturen för juridisk behörighetskontroll, inklusive de anpassningar som behövs för att möta särskilda behov inom vissa verksamhetsområden. Genom en sådan avgränsning kan en effektiv och flexibel infrastruktur etableras för juridisk behörighetskontroll där befintliga resurser nyttjas optimalt samtidigt som behovet av nya regelverk, administrativa rutiner och avtal minimeras.

4.2.2 Alternativ identifiering som komplement inom behörighetsinfrastrukturen

Digitala identitetskontroller kommer även fortsättningsvis att i första hand bygga på etablerade och förvaltningsgemensamma lösningar för elektronisk identifiering. Inom flera sektorer, särskilt i välfärdsverksamheter med varierande tekniska förutsättningar, förekommer dock situationer där en Medarbetare saknar tillgång till e-legitimation eller där sådana funktioner inte är tillgängliga i den konkreta användningen.

För att möjliggöra rättssäkra och praktiskt genomförbara kontroller i dessa fall bör funktioner för *alternativ identifiering* övervägas. Förfarandet bygger på att Förlitande part eller behörig administrativ funktion använder identitetsuppgifter från egna personaladministrativa system eller motsvarande interna datakällor för att fastställa Medarbetarens identitet.

Alternativ identifiering kan även aktualiseras när en Utfärdare av behörighetshandlingar mottar ett identitetsintyg, kontrollerar dess riktighet och därefter för över identitetsuppgifterna till en behörighetshandling. I sådana fall fungerar behörighetshandlingar inte enbart som bevis om juridisk behörighet utan även som bevis om identitet vid användning av en Digital tjänst. Ett sådant förfarande medför emellertid ett större kontrollansvar för en Förlitande part eftersom identitetsuppgifterna hämtas från lokala system eller annan alternativ källa. Genom att Alternativ identifiering införs som ett komplement inom behörighetsinfrastrukturen kan dock samtliga identifieringsförfaranden genomföras med enhetliga krav på dokumentation, spårbarhet och ansvarsfördelning, vilket minskar risken för felaktigheter och möjliggör en rättsenlig användning i de fall där Alternativ identifiering är det enda praktiskt möjliga alternativet.

4.3 Vad som menas med behörighetskontroll

Digg har i uppdrag att utveckla en sammanhållen infrastruktur för identitets- och behörighetshantering för Ena – Sveriges digitala infrastruktur (se avsnitt 1.1.1), medan E-hälsomyndigheten har i uppdrag är att ta fram en sådan infrastruktur för hälso- och sjukvårdsområdet (se avsnitt 1.1.2). Digg ska således utveckla en infrastruktur för *samhället som helhet* medan E-hälsomyndighetens uppdrag är *begränsat* till hälso- och sjukvårdsområdet. Den sammanhållna infrastrukturen ska vidare stödja *juridisk* kontroll av behörighet. Det är alltså inte fråga om ett behörighetskontrollsystem (BKS) *i teknisk mening,* utan om att digitalt tillgängliggöra de identitetsintyg och behörighetshandlingar som behövs vid en juridisk kontroll av identitet och behörighet. Digg har för detta ändamål definierat juridisk behörighetskontroll *som* en granskning av om en medarbetare *i juridisk mening* är behörig att agera för en angiven huvudmans räkning eller har en yrkesroll som innefattar en rätt att agera på det sätt som sker.

I definitionen har tillagts att den dessutom innefattar den som deltar i verksamhet hos en huvudman där medarbetaren behöver vidta en åtgärd eller agera på annat sätt, för att även andra kontrollbehov ska kunna tillgodoses inom infrastrukturen, exempelvis inom hälso- och sjukvården där medarbetare har direktåtkomst till uppgifter eller inom området för skola även om en kontroll som avser en elev inte tar sikte på en juridisk behörighet i egentlig mening, att agera för annans räkning eller med stöd av en yrkesroll.

4.3.1 När under handläggningen avgörs en fråga om juridisk behörighet

När en federationsinfrastruktur utvecklas behöver det beaktas att det finns, dels *materiella* regler som föreskriver under vilka förutsättningar en aktör anses vara behörig, dels *processuella* regler av två slag, dels de som föreskriver i vilken omfattning prövning av juridisk behörighet krävs i ett mål eller ett ärende, dels de som reglerar i vilken fas av en ärendehandläggning som denna prövning ska äga rum. Den som ska kontrollera juridisk behörighet behöver således ha klart för sig

1. *vad som gäller materiellt* för att en aktör ska anses vara behörig (exempelvis vad som krävs för att ha juridisk rätt att agera för en viss myndighets eller för ett företags räkning),

2. *hur omfattande* behörighetskontroller som behöver göras i ett ärende eller vid en transaktion (exempelvis kräver rättegångsbalken kontroll av fullmakt medan förvaltningslagen och den civilrättsliga regleringen lämnar över till den som handlägger ärendet eller transaktionen att bedöma om en fullmakt ska krävas i det enskilda fallet), och

3. *på vilket stadium* i ett rättsligt förfarande som sådana *preliminära frågor* som medarbetares identitet och behörighet ska hanteras.

Preliminära frågor ska avgöras innan en prövning i sak sker, exempelvis om det verkligen är angiven person som agerar och om denne är juridiskt behörig att företräda angiven huvudman eller har en yrkesroll som ger rätt att agera på det sätt som sker. Om det visar sig att det är en annan individ än den som anges eller att denne inte är juridiskt behörig ska målet eller ärendet *avvisas* enligt regler i bland annat rättegångsbalken och förvaltningslagen. En prövning *i sak,* det vill säga av den fråga som målet eller ärendet gäller aktualiseras först efter att de preliminära frågorna är avklarade. På samma sätt behöver identifiering och behörighetskontroll ske innan en rättshandling företas vid en civilrättslig transaktion. Detta gäller även för digital miljö och när digitala aktörer agerar för en myndighet eller ett företag. Vid direktåtkomst fungerar detta på annat sätt.

4.3.2 Diggs uppdrag

Diggs uppdrag omfattar inte själva behörighetskontrollen utan avser det stöd som ges genom federationer, för att inhämta underlag i form av identitetsintyg för säker identifiering och behörighetshandlingar för juridiska behörighetskontroller. Dessa digitala handlingar behövs för att avgöra

1. vem det är som agerar (identifiering),

2. om en medarbetare som agerar för en viss huvudmans räkning eller med stöd av en yrkesroll har juridisk rätt att göra på det sätt som sker (behörighetskontroll), och

3. om en digital aktör, exempelvis en robot som utför motsvarande åtgärder automatiserat, har satts i funktion på sådant sätt att den organisation som använder sig av den digitala aktören blir juridiskt bunden av de automatiserade åtgärderna (behörighetskontroll).

I traditionell fysisk miljö förväntas att den som agerar (t.ex. en befattningshavare vid en myndighet eller en företrädare för ett aktiebolag) tillhandahåller de behörighetshandlingar som krävs och eftersom förlitande parten normalt står risken för bristande behörighet är det den förlitande part som gör behörighetskontrollen. Vid en sådan kontroll används exempelvis protokollsutdrag (där det

framgår att en arbetsuppgift har delegerats), registreringsbevis från Bolagsverket (där det framgår vem som är ställföreträdare), en fullmakt eller annan liknande behörighetshandling (där det framgår att en viss individ har rätt att agera för en huvudmans räkning) eller ett skriftligt bevis om en yrkesroll som innefattar viss behörighet.

Allt fler digitala källor har emellertid tillkommit för att inhämta uppgifter om behörighet. Det har fört med sig att myndigheter, domstolar och företag allt oftare, i egenskap av förlitande part, beställer behörighetshandlingar. För detta behövs emellertid avtal med olika leverantörer och olika tekniska och administrativa funktioner som inte är samordnade. Det har fört med sig administrativa kostnader och tidsutdräkt. Samtidigt bygger de digitala tjänster som numera etableras ofta på att åtkomst kan ges i realtid. Behovet av de funktioner och tjänster som Digg och E-hälsomyndigheten har i uppdrag att ta fram är därmed starkt uttalat.

4.3.3 Sedvanliga behörighetskontroller

Diggs uppdrag är begränsat till att ta fram stöd för en sammanhållen infrastruktur för identitets- och behörighetshantering. Det innefattar inte att utföra själva behörighetskontrollerna. Vi kan emellertid inte bortse från hur en behörighetskontroll går till eftersom de funktioner som utvecklas måste fungera på ett ändamålsenligt sätt. Det blir därför av betydelse vilken part som ska samla in underlag för en behörighetskontroll – förlitande part eller den part som begär en behörighetshandling – och vilken part som ska göra kontrollen av om behörighet föreligger. En juridisk behörighetskontroll bygger på följande förfarande.

Den fråga som ställs	Hur den bedöms
a. Vilken fysisk person har agerat?	Här används underskrifter, legitimationshandlingar, m.m. – inom Infrastrukturen för e-legitimering
b. För egen eller för annans räkning?	I vems namn har personen agerat? Här används t.ex. firmateckning för att klargöra att åtgärden vidtagits i egenskap av företrädare för annan – inom infrastrukturen identifieras huvudmannen
c. Är den som agerar behörig att agera för annans räkning?	Här används protokollsutdrag, registreringsbevis som visar firmateckningsrätt, fullmakter, bevis om viss yrkesroll och liknande behörighetshandlingar – inom Infrastrukturen digitala behörighetshandlingar

Tabell 1: Beskrivning av juridisk behörighetskontroll.

Förfarandets utformning har sin grund i att förlitande part står risken i förhållande till angiven huvudman för om annan agerat än den individ som angivits (bristande identifiering) och om den som agerat saknat juridisk behörighet att utföra åtgärden (bristande juridisk behörighet). Funktioner för identitets- och behörighetskontroller behöver utformas i enlighet med rättsordningen, inom vedertagna juridiska ramar så som de tillämpas av jurister.

Frågan blir därmed hur en sammanhållen digital infrastruktur för identitets- och behörighetshantering kan anpassas till dessa förutsättningar. När ett mål eller ett ärende kommer in till en myndighet ska som framgått först en formell prövning ske, bland annat av om den som agerar

är behörig att vidta åtgärden. Saknas juridisk behörighet avvisas ärendet efter att tillfälle getts att styrka behörigheten. En handläggning i sak (t.ex. sekretessprövning, ändamålsprövning enligt en registerförfattning eller beslutsfattande) sker först efter att de formella frågorna prövats. Samma mönster bör i princip följas när en digital aktör, exempelvis en robot, ska använda en digital tjänst.

Dessa materiella och formella krav och bedömningen av om de uppfyllts innehåller inte någon prövning av tillåtna ändamål för behandling av personuppgifter eller någon sekretessprövning eller liknande eftersom en sådan prövning äger rum först efter att de preliminära frågorna har blivit klarlagda. Denna syn på juridiska behörighetskontroller är allmänt accepterad och grundad på allmänna regler. En annan utgångspunkt för den som handlägger en behörighetsfråga är att varje myndighet ansvarar för sin informationssäkerhet, om inte annat följer av särreglering inom ett område, och att ett informationsutbyte sker genom utlämnande på medium för automatiserad behandling efter att den myndighet som förfogar över uppgifterna först prövat om uppgifterna får lämnas ut.

En nationell infrastruktur för kontroll av juridisk behörighet behöver ta sin utgångspunkt i de materiella rättsreglerna om ställföreträdar- och ombudsskap, fullmakter, delegationsordningar och yrkesroller och den processuella regleringen av vilka kontroller som behöver göras i ett ärende. Infrastrukturen behöver vidare bygga på att förlitande part kontrollerar medarbetares identitet och behörighet och att informationsutbytet sker så att den myndighet som förfogar över behörighets-uppgifterna i varje enskilt fall prövar om uppgifterna får lämnas ut innan en mottagare ges tillgång till dem.

4.3.4 E-hälsomyndighetens uppdrag och behörighetskontroller inom hälso- och sjukvården

För vissa behörighetskontroller inom hälso- och sjukvårdssektorn är situationen den omvända mot det som beskrivits ovan. Regleringen för dessa behörighetskontroller är istället utformad så att det är den begärande parten själv som ska säkerställa identifiering och behörighet för den individ som begär åtkomst till uppgifterna. Förlitande part ska bedöma om vissa förutsättningar för utlämnande är uppfyllda. Förlitande part står i dessa fall risken inte gentemot den vårdgivare som begärt åtkomst till uppgifterna, utan gentemot den patient vars uppgifter begärande part vill ta del av.

För dessa tillämpningar inom hälso- och sjukvårdssektorn tar E-hälsomyndighetens uppdrag därmed inte sikte på själva identifieringen och behörighetskontrollen utan på det stöd som behövs genom federationer för att kunna utbyta uppgifter på ett kontrollerat och säkert sätt. Eftersom Diggs respektive E-hälsomyndighetens uppdrag nära knutits till varandra har Digg inledningsvis antagit att behörighetskontroller inom hälso- och sjukvården skulle vara ett typfall för hur juridisk behörighet regleras och kontrolleras inom övriga samhälls- och rättsområden. Det har emellertid visat sig att utbytet av information inom hälso- och sjukvårdsområdet i vissa fall är *särreglerat* och att de utmaningar som finns inom det området är präglat av det sätt att utbyta uppgifter som betecknas *direktåtkomst,* trots att de informationssystem som numera används tekniskt är utformade som fråga- och svarsfunktioner och i andra sammanhang används för utlämnande på medium för automatiserad behandling. Utöver detta beror utmaningarna på att åtkomst endast får ske om vissa förutsättningar är uppfyllda. Det kan sägas vara en kombination av juridisk behörighetskontroll och

i vissa delar en handläggning i sak (sekretessprövning eller ändamålsprövning enligt en register-författning).

Den myndighet som lämnar uppgifter får, vid ett utlämnande på medium för automatiserad behandling, en begäran om att lämna ut uppgifter och gör i varje enskilt fall en prövning av om uppgifterna eller handlingarna ska lämnas ut eller inte, innan något tillgängliggörs för annan (se HFD 2015 ref 61). Förutsättningarna är andra när patientdatalagen (2008:355; PDL) och lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation (SVOD) samt anknytande regler i förordning och myndighetsföreskrifter är tillämpliga. För det första är det inte den förlitande parten, i betydelsen den part som mottar en begäran om att få tillgång till hälso- och sjukvårdsdata, som beställer intyg om identitet och behörighet och med detta underlag gör de kontroller som behövs innan några handlingar lämnas ut. Istället ska viss bedömning och kontroll ha gjorts på förhand av bland annat den begärande organisationens regelefterlevnad. Den begärande organisationen får därefter antingen direktåtkomst eller åtkomst för att hämta uppgifter på medium för automatiserad behandling för sin personal eller sina digitala aktörer, till den utlämnande organisationens informationssystem och kan hämta uppgifter därifrån utan att den utlämnande organisationen gör en kontroll i det enskilda fallet. E-hälsomyndigheten har berört frågor om behörighetskontroller inom hälso- och sjukvården i sin rapport om genomförandet av en nationell digital infrastruktur för hälso- och sjukvård och EHDS primäranvändning.[7]

Viss tillämpning inom hälso- och sjukvården utgår ifrån att den vårdgivare som begär åtkomst (vårdgivare A) anskaffar de identitets- och behörighetshandlingar som behövs och sänder med dem till den utlämnande organisationen (vårdgivare B). Vårdgivare B ska visserligen logga transaktionen, men istället för att göra en egen identifiering och kontroll av behörighet kontrollerar vårdgivare B från vilken annan vårdgivare anropet kommer. Efter att denna kontroll gjorts litar vårdgivare B på att den enskilde användaren är identifierad av vårdgivare A och av A har tilldelats rätt behörighet. Vårdgivare B kontrollerar istället exempelvis att begäran gäller ett tillåtet ändamål för att behandla uppgifterna och att den individ som berörs av direktåtkomsten inte har spärrat sina uppgifter, jämför ovan om en prövning i sak. I övrigt gör vårdgivare B viss föreskriven granskning av sådan åtkomst i efterhand, utöver den förhandskontroll hos vårdgivare A som föreskrivs genom områdesspecifik reglering. Behörighetskontroller enligt lagen (2018:1212) om nationell läkemedelslista (NLL) följer en liknande struktur. Inom hälso- och sjukvården är dessutom dataskyddet särreglerat genom områdesspecifika bestämmelser i lag och annan författning. Kraven på informationssäkerhet inom andra områden följer istället normalt av särskilda författningar om informationssäkerhet.

Vad gäller tillgång till NLL har E-hälsomyndigheten också en lagreglerad skyldighet att på förhand göra en bedömning av om behörighets- och säkerhetsfrågorna är lösta på ett sätt som är tillfredsställande ur integritetssynpunkt och att behörigheten hos den som ska få direktåtkomst är begränsad till att endast gälla sådana uppgifter som denne har rätt att få ut (jfr. 8 kap. 2 § NLL).

---

[7] Se främst avsnitt 4.3 i Rättsliga förutsättningar för att realisera en nationell digital infrastruktur för hälso- och sjukvård Bilaga 1 till rapporten Genomförandet av en nationell digital infrastruktur för hälso- och sjukvård och EHDS primäranvändning Slutredovisning av regeringsuppdrag (S2023/02108 (delvis), S2024/01201(delvis) och S2024/02156 (delvis)) Dnr 2024/03223.

Inom hälso- och sjukvårdssektorn förekommer det även digitala tjänster där sedvanliga behörighetskontroller sker. Ett exempel på en sådan tjänst är Förskrivningskollen om tillhandahålls av E-hälsomyndigheten och där behörigheten avgörs utifrån bl.a. innehavande av yrkeslegitimation innan användaren kan ta del av information. Inloggning sker med e-legitimation.

4.4 Återanvändning och anpassning

Den befintliga förvaltningsgemensamma infrastrukturen för elektronisk identifiering har en utformning som liknar den infrastruktur som behövs för juridiska behörighetskontroller i digital miljö. Existerande tekniska funktioner, tjänster och regler för elektronisk identifiering och elektronisk identitetskontroll kan återanvändas och anpassas till behörighetskontroller. Detta innebär att en federationsinfrastruktur för behörighetshantering kan utformas på liknande sätt som den infrastruktur som redan finns för elektronisk identifiering eftersom det i allt väsentligt är samma tekniska standarder och behov av skydd för informationssäkerhet som aktualiseras. De administrativa och juridiska utmaningarna är också likartade. Behörighetskontroller kräver dock som framgått ytterligare en nivå av aktörer – federationsområdesansvariga – som kan samordna och anpassa hanteringen inom ett federationsområde.

Identitetskontroller och behörighetskontroller behöver samordnas så att de kan användas på ett ändamålsenligt sätt inom olika områden i samhället. Federationsinfrastrukturen behöver vara flexibel så att olika federationsområden kan nyttja funktionerna utifrån sina särskilda förutsättningar. De kontroller som förlitande parter behöver göra omfattar både vilken medarbetare eller digital aktör som agerar och om denne i juridisk mening är behörig att agera på ett visst sätt. Frågan om identitetskontroll kan därmed juridiskt inte separeras från frågan om behörighetskontroll, trots att det tekniskt delvis är olika infrastrukturer som används. Identitets- och behörighetskontroller behöver samordnas så att de kan nyttjas på ett ändamålsenligt sätt inom respektive verksamhetsområde. En ny federationsinfrastruktur behöver också utformas så att olika verksamhetsområden kan nyttja funktionerna utifrån sina särskilda förutsättningar.

4.5 En reglering genom avtal

Diggs bedömning är att behörighetsinfrastrukturen i huvudsak bör regleras genom avtal mellan anslutna parter. Ett skäl för att reglera genom avtal är att behovet av att använda e-legitimationer, nationellt och över organisationsgränser, hittills tillgodosetts huvudsakligen genom avtal och överenskommelser. Förslag som lagts fram om en reglering i lag och förordning av elektronisk identifiering har inte lett till lagstiftning (SOU 2017:114). En författningsreglering av en infrastruktur för behörighetskontroller framstår i nuläget inte som ett alternativ då funktioner för juridisk behörighetskontroll behövs i närtid. En infrastruktur för säker elektronisk identifiering finns redan på plats.

Avtalsarbetet

Arbetet med att ta fram en avtalsmodell som beskriver de legala förhållandena mellan parter med olika roller inom infrastrukturen är inte avslutat. Det är därför inte lämpligt att i detta skede redogöra för den närmare utformningen. Redan nu kan dock konstateras att utformningen av

avtalen förenklas genom att de regler som utvecklats för elektronisk identifiering delvis kan återanvändas. Dessutom kan erfarenheter från tidigare arbete tas tillvara vid den anpassning som behövs till de särskilda förutsättningar som gäller inom området för behörighetskontroll.

Är utfärdare av behörighetshandlingar eller förlitande part en statlig myndighet och därmed en del av samma juridiska person som den ledningsansvarige kan en överenskommelse tas fram för behörighetsinfrastrukturen, efter förebild av den reglering som införts genom avtal för förbetald e-legitimering. Det är också tänkbart att myndigheter som ingår i infrastrukturen kommer att ha uttryckliga uppdrag som regleras i myndighetens instruktion eller liknande (se avsnitt 5.6 och 5.7). Dessutom kan vissa av de uppgifter som myndigheter som agerar inom infrastrukturen kommer att tilldelas omfatta myndighetsutövning. Dessa uppgifter är inte möjliga att delegera till en privat aktör utan stöd i lag.

5 Bedömningar och förslag

5.1 Lösningar för vissa tillämpningar inom hälso- och sjukvården

Bedömning: En nationell digital infrastruktur kan inte utarbetas och regleras baserat på särlösningar som används för vissa tillämpningar inom hälso- och sjukvården. Hälso- och sjukvårdens användning av infrastrukturen bör i dessa fall betraktas som en områdesspecifik anpassning.

När en behandling av personuppgifter äger rum i enlighet med patientdatalagen (2008:355; PDL) eller lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation (SVOD) och till viss del även enligt lagen (2018:1212) om nationell läkemedelslista (NLL) sker informationsutbytet vanligtvis genom direktåtkomst, medan behörighetskontroll i andra sammanhang brukar ha formen av utlämnande på medium för automatiserad behandling där system för fråga och svar används. Den aktör som mottar en begäran om tillträde till en digital tjänst eller om att få ut vissa uppgifter (förlitande part) mottar därvid, eller samlar in, de behörighetshandlingar som behövs och avgör om behörighet föreligger, innan tillträde ges eller uppgifter lämnas ut. Inom hälso- och sjukvården utförs däremot kontroller av den *begärande* parten för att uppfylla lagstadgade krav för att få ta del av uppgifterna. Vidare finns föreskrifter om förhandsgranskning av en aktörs dataskydd. Detta innebär inte att *förlitande* part i varje enskilt fall ska kontrollera vem som agerar och om denne är juridiskt behörig att agera på det sätt som sker. Det är en annan sak att hälso- och sjukvården också använder sig av utlämnande på medium för automatiserad behandling så att den förlitande parten i varje enskilt fall kontrollerar vem som agerar och om denne är juridiskt behörig att agera på det sätt som sker.

Den hantering enligt PDL eller SVOD som baseras på direktåtkomst kan därmed inte läggas till grund för en generell modell för juridisk behörighetskontroll. Det som då i PDL och SVOD betecknas behörighetskontroll framstår i stället som en särskild tillämpning av bland annat dataskydds- och sekretessrätten – inte som en modell för prövning av juridisk behörighet i allmän mening. Direktåtkomst kan något förenklat sägas innebära att en medarbetare eller en digital aktör hos en annan vårdgivare släpps in i den utlämnande aktörens system för att själv söka fram och hämta uppgifter. Behörighetskontrollen liknar därmed mera en hantering för att bedöma om en aktör får i logga in i ett informationssystem för att vidta åtgärder i systemet, till skillnad från en sedvanlig juridisk behörighetskontroll som syftar till att kontrollera om en medarbetare eller en digitala aktör äger rätt att agera på det sätt som sker för en angiven huvudman eller med stöd av en yrkesroll, exempelvis genom att göra en framställning i ett förvaltningsärende eller begära en prövning av om att en viss handling ska lämnas ut.

En nationell infrastruktur för kontroll av juridisk behörighet behöver istället ta sin utgångspunkt i de materiella rättsreglerna om ställföreträdar- och ombudsskap, fullmakter, delegationsordningar och yrkesroller och de processuella regler som anger vilka kontroller som behöver göras i ett ärende och på vilket stadium i förfarandet. Infrastrukturen behöver vidare ta sin utgångspunkt i att

förlitande part kontrollerar identitet och behörighet, att informationen *utbyts på medium* för automatiserad behandling och att *behörighetskontroll sker innan* uppgifter lämnas ut.

Utifrån ovanstående ställningstagande gör Digg bedömningen att det behöver utredas ytterligare i vilken mån den rättsliga reglering som gäller för direktåtkomst och för kontroller av regelefterlevnad inom hälso- och sjukvården behöver ses över och anpassas till dagens praktiska verklighet där huvudregeln är att varje organisation ska ansvara för sin informationssäkerhet (jfr avsnitt 5.11). Hälso- och sjukvårdens skyldigheter att – innan direktåtkomst beviljas – kontrollera om en andra aktörer uppfyller sina lagstadgade krav på bl.a. dataskydd behöver utredas i annan ordning och bedömas med särskilda kunskaper om de förutsättningar som gäller inom hälso- och sjukvården. En sådan genomlysning bör ske i nära samverkan med vårdgivare och andra som genomför kontroller för att uppfylla författningsreglerade krav i gällande rätt beträffande bland annat förhandsgranskning och dataskydd.

Det är en annan sak att den behörighetsinfrastruktur som Digg föreslår avses få en så generell utformning att den ska kunna nyttjas även om områdesspecifika avvikelser behövs från det sedvanliga förfarandet vid en juridisk behörighetskontroll. Det blir med andra ord sannolikt väl fungerande att använda federationsinfrastrukturens tekniska funktionalitet för att förmedla den information som behövs för att bedöma om en viss aktör får i logga in i ett informationssystem för att vidta åtgärder i systemet, förutsatt att det först har gjorts en rättslig bedömning av att aktören uppfyller vissa uppställda villkor för direktåtkomst. Tekniska förutsättningar för användning av infrastrukturen även för hälso- och sjukvårdens specifika behov kan alltså finnas på plats redan när infrastrukturen tas i bruk. Dessutom bör det fundament och det regelverk som Digg föreslår för användning inom hela samhället kunna nyttjas också inom området för hälso- och sjukvård även när det sedvanliga förfarandet inte tillämpas. Den juridiska utformningen av federationsinfrastrukturen kan emellertid inte ta sin utgångspunkt i ett särreglerat område med en för sedvanliga behörighetskontroller avvikande reglering och hantering.

5.2 Kontroll av behörighet – inte av befogenhet

Bedömning: Alltför finmaskiga kontroller kan inte genomföras. Administration av befogenheter på detaljnivå blir alltför omfattande och kostnadsdrivande.

En juridisk gränsdragning av praktisk betydelse för behörighetsinfrastrukturens användning

Inom civilrätten finns en skillnad mellan medarbetares behörighet, det vill säga gränsen utåt för dennes handlingsförmåga, och medarbetarens befogenhet som är de interna instruktionerna för hur denna behörighet får utövas. Denna skillnad är grundläggande för omsättningens säkerhet. En fullmakt har i princip verkan enligt sitt innehåll gentemot tredje man medan inskränkande instruktioner som huvudmannen därutöver meddelat fullmäktigen endast gäller internt. Överskrider fullmäktigen sin befogenhet men håller sig inom behörigheten, blir rättshandlingen ändå bindande för huvudmannen, såvida inte tredje man insåg eller bort inse avvikelsen. Interna begränsningar får däremot ingen verkan mot tredje man. Enkelhet och förutsebarhet prioriteras således framför interna kontrollbehov. Detsamma gäller inom associationsrätten. I aktiebolagslagen

(2005:551), lagen (2018:672) om ekonomiska föreningar, handelsbolagslagen (1980:1102) och stiftelselagen (1994:1220) finns bestämmelser som föreskriver att en utsedd firmatecknares behörighet gäller utan inskränkning mot tredje man, även om interna begränsningar föreligger. Endast begränsningar som framgår av det offentliga registret – exempelvis att firmateckning endast får ske av två personer i förening, får verkan gentemot tredje man. En förlitande part som är i god tro ska inte behöva undersöka interna delegationsordningar, utan ska kunna förlita sig på den behörighet som framgår av register (i praktiken ett registerutdrag). Hanteringen får inte bli för krånglig och kostnadsdrivande.

Även inom den offentliga rätten upprätthålls en distinktion mellan behörighet och befogenhet, men med vissa särdrag jämfört med civilrätten. Myndigheters behörighet grundas ytterst på lag eller annan författning. Det innebär att åtgärder som vidtas utanför denna behörighet saknar rättsverkan. Befogenheterna anger däremot hur den tilldelade behörigheten får utövas i det enskilda fallet. Ett överskridande av befogenhet kan i förvaltningsrättsliga sammanhang leda till att ett beslut betraktas som en nullitet, dvs. utan rättsverkningar, eftersom det saknar stöd i gällande ordning. Praxis visar att beslut som fattas av organ eller befattningshavare som överskrider sina befogenheter inte får rättsverkan gentemot enskilda. Till detta kommer det straffrättsliga ansvaret. Enligt 20 kap. 1 § brottsbalken kan en befattningshavare som vid myndighetsutövning åsidosätter sina befogenheter dömas för tjänstefel. Bestämmelsen syftar till att upprätthålla förtroendet för att myndighetsutövning sker inom givna ramar och på ett rättssäkert sätt. Behörighetsinfrastrukturen bör när så kan ske renodlas till att avse den yttre och rättsligt bindande behörigheten. Befogenheterna hanteras bäst inom respektive myndighets interna styrning. Samtidigt bör det göras tydligt för tjänstemännen vilket ansvar som följer vid överskridande av befogenhet.

Slutsatser för en nationell behörighetsinfrastruktur

Vid utformning och användning av en nationell behörighetsinfrastruktur bör samma princip tillämpas som inom civilrätten och associationsrätten. De digitala behörighetshandlingarna bör i princip avse det som är offentligt, synbart och utåt förutsebart. Behörighetshandlingarna bör vara tydliga och entydiga, på liknande sätt som ett bevis från Bolagsverket om en registrerad firmateckningsrätt. Begränsningar på detaljnivå bör hanteras internt inom respektive organisation istället för att bygga in sådan komplexitet i den föreslagna nationella behörighetsinfrastrukturen. En inriktning mot att renodla behörighetsinfrastrukturen till en ordning som avser just behörighet – och motsvarande förordnanden inom offentlig förvaltning – är inte bara en juridiskt konsekvent lösning, utan också en tekniskt och organisatoriskt robust väg framåt. En sådan ordning stärker också rättssäkerheten och förutsebarheten. Förlitande part bör kunna utgå från att den behörighet som framgår av en behörighetshandling är gällande, utan att behöva beakta interna instruktioner som inte är kända utåt. I vilken mån detta synsätt kan genomföras rättsenligt får dock genomlysas område för område i takt med att nya federationsområden etableras.

5.3 Ett visst juridiskt risktagande kan inte undgås

Bedömning: Fullständiga kontroller av behörighet bör inte och kan inte alltid genomföras. Vissa juridiska risker måste accepteras för att digitala förfaranden inte ska bli för betungande.

I den juridiska litteraturen har framhållits att praktiskt taget alla transaktioner förutsätter att aktörerna tar vissa risker för att allt inte har gått rätt till. Att helt eliminera dessa risker är knappast möjligt; rigorösa försök i denna riktning skulle sannolikt leda till att verksamheten blir tungrodd och ineffektiv. Denna iakttagelse gör sig gällande också inom en digital behörighetsinfrastruktur. En förlitande aktör kan där i många fall bygga sin hantering på så kallad organisationstillit, dvs. antagandet att en korrekt identifierad huvudman eller myndighet också har tillsett att dess medarbetare är rätt person att agera i det enskilda fallet. Detta förhållningssätt har stöd i praxis och medför att särskilda, fördjupade kontroller inte krävs annat än när det finns skäl att misstänka felaktigheter.

Det beskrivna synsättet stärks här av att medarbetares identitet normalt kontrolleras med stöd av e-legitimation och att utfärdare av identitetsintyg och behörighetshandlingar har ett rättsligt ansvar för sin hantering. Här kan en jämförelse med traditionell pappersmiljö vara av intresse. Där har det vanligtvis ansetts tillräckligt att en handling har inkommit i original med logotyp och underskrift. Mottagande myndighet har sällan kontrollerat underskriftens äkthet och undertecknarens behörighet. I digital miljö är situationen den omvända. Här sker regelmässigt automatiserade kontroller av identitet genom e-legitimation, spärrlistor kontrolleras i realtid och digitala stämplar eller underskrifter kontrolleras maskinellt. Den föreslagna behörighetsinfrastrukturen erbjuder därmed en högre tillförlitlighet än traditionell pappershantering.

De risker som sällan kan elimineras hänför sig typiskt sett till tre kategorier, (1) brottsliga angrepp, exempelvis manipulation av behörighetsuppgifter eller användning av stulna identitetshandlingar, (2) administrativa brister, såsom att en delegation inte dokumenterats, att registeruppgifter inte uppdaterats eller att en behörighet inte återkallats i tid, och (3) systemtekniska fel (där ett åtkomstkontrollsystem eller en integrationslösning inte fungerar som avsett). Sammanblandningar av juridiska risker och informationssäkerhetsrisker bidrar ofta till orimligt komplexa krav på juridiska behörighetskontroller. För att infrastrukturen ska bli ändamålsenligt utformad och praktiskt användbar behöver dessa risker hålls isär och hanteras med olika medel: juridiska regler respektive tekniska skyddsåtgärder.

Att risker kvarstår innebär inte att rättsordningen står utan skydd. När obehöriga åtgärder ändå inträffar finns flera juridiska mekanismer för att korrigera eller sanktionera dem. På det förvaltningsrättsliga området kan beslut fattade av obehöriga överklagas och undanröjas. Om fel upptäcks efter att ett beslut vunnit laga kraft kan rättsinstitutet resning användas för att rätta till detta. Inom det civilrättsliga området finns regler om avtals ogiltighet om den som undertecknat eller på annat sätt rättshandlat, inte varit behörig att företräda sin huvudman. Den som åberopar en falsk eller obehörigen tillkommen handling kan bli skadeståndsskyldig. Dessutom finns regler om straffrättsligt ansvar som kan bli tillämpliga även på elektroniska behörighetshandlingar eftersom de kommer att förses med digital stämpel och därmed får urkundskvalitet. Riskerna bör alltså hanteras på ett rättssäkert och proportionerligt sätt genom kombinationer av tekniska skydd, organisatoriskt ansvar, ett tydligt regelverk för riskfördelning mellan utfärdare och förlitande aktör och ett straffrättsligt ansvar för en gärningsperson. På så sätt kan digitala kontroller både vara mer effektiva och ge ett starkare skydd än traditionella förfaranden, samtidigt som de bevarar en rimlig balans mellan så kallad organisationstillit och juridiska behörighetskontroller.

5.4 Behörighetshandlingar för digitala aktörer

Bedömning: Behörighetshandlingar för digitala aktörer bör utfärdas på funktionsnivå för att möjliggöra en otvetydig koppling mellan den juridiskt relevanta åtgärden och den process som faktiskt utfört åtgärden. Det kan därmed i efterhand klarläggas vilken digital aktör som utfört åtgärden och på vems uppdrag det skett, vilket minskar risken för obehöriga dispositioner och underlättar en tydlig ansvarsfördelning.

Med digital aktör avses här en automatiserad process som kan utföra uppgifter i ett informationssystem utan direkt mänsklig inblandning. Begreppet omfattar såväl robotiserad processautomation (RPA) som imiterar en fysisk användares interaktion i ett grafiskt användargränssnitt, som API-baserade automationsalgoritmer som kommunicerar direkt mellan system via programmeringsgränssnitt. Denna distinktion har praktisk betydelse för hur identitet och behörighet fastställs, styrks och hanteras inom behörighetsinfrastrukturen. I båda fallen är det nödvändigt att behörigheten kan knytas till den specifika funktion eller process som agerat, och inte enbart till det överordnade system där funktionen ingår. Därigenom kan spårbarhet och ansvarsfördelning säkerställas även vid helt automatiserade förfaranden.

En juridisk person saknar egen vilja och handlingsförmåga i praktisk mening och därför måste agera genom organ eller företrädare. Behörig företrädare tar emellertid ställning till om en digital aktör ska utvecklas och införas och beslutar om vad den får utföra. På liknande sätt som för en fysisk person som tilldelats viss behörighet att agera för en huvudmans räkning behöver en förlitande part förvissa sig om att en digital aktör som utför en uppgift för en myndighet eller ett privaträttsligt subjekt i juridisk mening är behörig att agera på det sätt som sker. När behörighetsinfrastrukturen nyttjas förutsätter detta att behörigheten styrks genom en behörighetshandling som entydigt identifierar den specifika funktion eller process som agerat. Digital aktör bör därmed definieras som en teknisk funktion som automatiserat utför åtgärder eller företar rättshandlingar i en huvudmans eller medarbetares ställe.

En sådan ordning ligger i linje med de principer om spårbarhet, ansvarsfördelning och åtkomstbegränsning som följer av allmänna förvaltningsrättsliga principer, dataskyddsreglering och grundläggande krav på informationssäkerhet. Genom att tilldela den digitala aktören en avgränsad behörighet, kopplad till ett visst ändamål och en viss uppgift, undviks överskottsbehörigheter och risken för missbruk av infrastrukturen begränsas. Detta gör det också möjligt att återkalla en behörighet eller ändra behörigheten för just den aktör som omfattas utan att det påverkar övriga funktioner inom samma system. Därigenom skapas en flexibel och rättssäker ordning som gör det möjligt att tillämpa samma juridiska bedömningsgrunder för manuell och automatiserad hantering.

En reglering av digitala aktörers behörighet i anslutning till behörighetsinfrastrukturen är av betydelse eftersom sådana automatiserade processer kan genomföra rättsligt relevanta åtgärder med samma rättsverkningar som om de hade utförts av en fysisk företrädare. Utan en tydlig ordning för hur sådan behörighet fastställs och styrks uppstår risker för rättsförluster, obehöriga dispositioner och bristande spårbarhet. En reglering i regelverket för federationsinfrastrukturen ger både förlitande parter och huvudmän rättslig förutsägbarhet och minskar risken för tvister om ansvar och behörighet vid automatiserat beslutsfattande och informationsutbyte.

När det gäller vilket bevisvärde en behörighetshandling för en digital aktör har får det antas att den ges samma rättsliga verkan som motsvarande handling för en fysisk företrädare. Handlingen utgör, rätt utformad, ett skriftligt bevis om att den aktuella funktionen eller processen haft behörighet vid tidpunkten för åtgärden och får därmed antas bli bedömd enligt de regler som gäller för fullmakter, protokollsutdrag eller registerutdrag, beroende på handlingens form och rättsliga grund. Genom att behörighetshandlingen är elektroniskt stämplad kan den dessutom fungera som bevis vid en rättslig prövning av såväl äkthet som innehåll. Detta är avgörande både vid tvister om ansvar eller giltighet av åtgärder som utförts automatiserat av en digital aktör och när straffrättsligt ansvar aktualiseras.

5.5 Digg behöver stöd i författning för uppdrag som ledningsansvarig

Förslag: Digg bör utses till ledningsansvarig. I myndighetens instruktion bör föreskrivas att Digg ska ansvara för tillgången till infrastruktur och tjänster för elektronisk behörighetskontroll i verksamheter inom välfärdsområdet som helt eller delvis är offentligt finansierade och verksamheter som utan att vara offentligt finansierade är att betrakta som vårdgivare enligt vissa utpekade lagar. Dessutom bör verksamhet inom detaljhandel med läkemedel enligt lagen (2009:366) om handel med läkemedel omfattas.

Digg har enligt förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning uppdrag som anknyter till en behörighetsinfrastruktur. Enligt 3 § ska Digg ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift, främja användningen därav, ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering samt tillhandahålla en förvaltningsgemensam infrastruktur för säker digital kommunikation till verksamheter inom välfärdsområdet som helt eller delvis är offentligt finansierade. Digg tillhandahåller således i enlighet med sin instruktion en federation för identifiering och för säker digital kommunikation som – beskrivet med en metafor – fungerar som den räls på vilken användningen av e-legitimationer, identitetsintyg och säker digital kommunikation vilar. Det är Digg som förvaltar och utvecklar dessa infrastrukturer. Digg har också, i regleringsbrevet för 2025, fått i uppdrag att utveckla en sammanhållen infrastruktur för identitets- och behörighetshantering, som ska kunna tillhandahållas inom ramen för Ena – Sveriges digitala infrastruktur.

En förvaltningsmyndighet under regeringen får agera endast inom ramen för sitt uppdrag. Detta gäller oavsett om det är fråga om myndighetsutövning, ärendehandläggning eller faktiskt handlande. I 5 § första stycket förvaltningslagen (2017:900) föreskrivs att en myndighet endast får vidta åtgärder som har stöd i rättsordningen. Bestämmelsen ger uttryck för legalitetsprincipen (1 kap. 1 § 3 st. RF) och tar sikte på de källor som tillsammans bildar rättsordningen i vidsträckt mening. Bestämmelsen innebär att det måste finnas någon form av normmässig förankring för all typ av verksamhet som en myndighet bedriver. Exempel på sådant författningsstöd kan vara allmänna bestämmelser i lag eller detaljerade regler i tillämplig speciallagstiftning. Det kan också vara fråga om allmänna eller särskilda bestämmelser i myndighetens instruktion eller myndighetsförordningen eller i någon annan förordning som regeringen har beslutat. Legalitetskravet kan även vara uppfyllt genom ett förvaltningsbeslut, exempelvis om åtgärden har stöd i myndighetens regleringsbrev.

Digg saknar idag ett uttryckligt rättsligt stöd för att tillhandahålla en sådan infrastruktur som omfattas av myndighetens uppdrag i regleringsbrevet för 2025. För att Digg ska kunna tillhandahålla infrastrukturen är det ändamålsenligt att stöd ges i författning. Det finns också andra fördelar med en uttrycklig författningsreglering. En författningsregel som säger att Digg ska tillhandahålla förvaltningsgemensamma lösningar kan även främja finansieringen av Diggs tillhandahållande eftersom regeringen, om Digg ges ett uppdrag att tillhandahålla en förvaltningsgemensam lösning, också behöver erbjuda rimliga förutsättningar för att kunna utföra arbetsuppgiften.

Uppdraget att ansvara för att tillhandahålla ytterligare en federation av liknande slag som de redan existerande bör, av bland annat kompetens- och effektivitetsskäl, anförtros Digg som har motsvarande funktioner i drift. Om Digg utses till ledningsansvarig bör Digg dessutom ges ett uttryckligt uppdrag i förordning att tillhanda en behörighetsinfrastruktur. Med hänsyn till den korta tid inom vilken den föreslagna infrastrukturen kan behöva tas i drift har vi valt att föreslå en ändring i Diggs instruktion, efter förebild av vad som föreskrivs där beträffande elektronisk identifiering och underskrift. I sammanhanget bör emellertid påpekas att motsvarande regler även skulle kunna tas in i en myndighetsövergripande förordning om nationell digital infrastruktur eller i en ny instruktion för en nybildad myndighet. Uttrycket juridisk behörighetskontroll har valts för att inte riskera en sammanblandning med det som i tekniska sammanhang brukar kallas behörighetskontrollsystem (BKS).

Diggs ansvar för tillgången till infrastruktur och tjänster för elektronisk behörighetskontroll i verksamheter inom välfärdsområdet bör inte vara inskränkt till verksamheter som är helt eller delvis är offentligt finansierade. Även andra som är att betrakta som vårdgivare enligt vissa utpekade lagar bör innefattas. Hit hör verksamheter som utan att vara offentligt finansierade omfattas av hälso- och sjukvårdslagen (2017:30), tandvårdslagen (1985:125), lagen (2001:499) om omskärelse av pojkar, lagen (2018:744) om försäkringsmedicinska utredningar, lagen (2019:1297) om koordineringsinsatser för sjukskrivna patienter, lagen (2021:363) om estetiska kirurgiska ingrepp och estetiska injektionsbehandlingar. Dessutom bör verksamhet inom detaljhandel med läkemedel enligt lagen (2009:366) om handel med läkemedel omfattas.

5.6 En rätt för Digg att meddela föreskrifter

Bedömning: Digg bör ges rätt att meddela de föreskrifter som behövs för infrastruktur och tjänster för kontroll av juridisk behörighet. En närmare reglering bör beträffande såväl Digg som övriga offentlig- eller privaträttsliga aktörer följa av avtal och överenskommelser.

De aktörer som ansluts till behörighetsinfrastrukturen behöver uppfylla vissa krav för att den ska fungera på ett säkert och effektivt sätt. Dessa krav måste kunna anpassas till den tekniska utvecklingen och ändrade förhållanden i övrigt. I den mån sådana krav inte bör regleras genom avtal och endast kan regleras i lag eller förordning finns det en risk för stelbenthet och bristande aktualitet. Digg bör därför, i egenskap av ledningsansvarig, ges en rätt att meddela föreskrifter. Denna rätt bör begränsas till det som är nödvändigt för administrationen, informationssäkerheten, interoperabiliteten, tillgängligheten och spårbarheten och bör bland annat kunna avse frågor som format och standarder för informationsutbyte, skyddsnivåer och loggning, krav på

anslutningstjänster, äkthetsskydd, incidentrapportering samt rutiner och krav för anslutning. Eftersom även enskilda – i detta fall privaträttsliga juridiska personer – avses anslutas till behörighetsinfrastrukturen och föreskrifterna inte alltid kan ses som rent tekniska bör ett sådant bemyndigande ha sin grund i 8 kap. 3 och 7 §§ regeringsformen.

Det går inte att på detta stadium bedöma den exakta utformningen av ett bemyndigande, eftersom detta bl.a. påverkas av avtalsarbetet samt av vilka myndigheter etc. som kommer att ta olika roller i federationsinfrastrukturen. I det fortsatta arbetet behöver även de förslag som redan tagits fram t.ex. inom arbetet med Ena och i betänkandet En reform för datadelning (SOU 2023:96), som för närvarande bereds i regeringskansliet, beaktas. Det kan också bli aktuellt att utreda föreskriftsrätt för andra myndigheter.

5.7 Stöd i rättsordningen för uppdrag som federationsområdesansvarig

Bedömning: När en myndighet utses till federationsområdesansvarig behöver det följa av rättsordningen att myndigheten ska ansvara för tillgången till vissa funktioner. Det bör övervägas om andra än myndigheter ska kunna utses till federationsområdesansvariga. Om en privaträttslig aktör ska ansvara för en viss funktion bör det följa av avtal att aktören ska ansvara för en sådan funktion. Den närmare regleringen bör beträffande såväl myndigheter som privaträttsliga aktörer följa av avtal.

Det behöver klargöras vilka som ska utses till federationsområdesansvariga inom behörighets-infrastrukturen. Anförtros denna roll till en myndighet medför legalitetsprincipen – på samma sätt som för den ledningsansvarige – att det behöver följa av rättsordningen att myndigheten ska ansvara för tillgången till en sådan funktion. Under en inledande fas när behörighetsinfrastrukturen är under uppbyggnad kan det visserligen vara ändamålsenligt att uppdrag som federationsområdesansvarig ges i den aktuella myndighetens regleringsbrev eller genom särskilt regeringsbeslut, men på sikt bör ett tydligt uppdrag följa av förordning.

Här kan utvecklingen av behörighetsinfrastrukturen i vissa skeden bli snabb och kräva anslutning av flera nya federationsområdesansvariga. Det är ändamålsenligt att regeringen får ta ställning till dessa, för infrastrukturens utveckling och inriktning centrala frågor. Ett uppdrag som federationsområdesansvarig kan för statliga myndigheter regleras i förordning. Det skulle då vara möjligt att föreskriva att vissa myndigheter utses till federationsområdesansvariga inom behörighetsinfrastrukturen med ansvar för tillgången till kompletterande infrastruktur och tjänster inom ett visst område. För att underlätta en reglering, om ett betydande antal myndigheter över tid kan antas komma att utses till federationsområdesansvariga, kan dessa anges i en bilaga till förordningen. I sammanhanget bör också förslag som Digg lämnat inom ramen för uppdraget att föreslå en långsiktig utveckling och förvaltning av Ena beaktas (Fi2024/01455). Detta innehåller bl.a. förslag till en ny förordning om nationell digital infrastruktur, som reglerar ett ramverk för styrningen av nationell digital infrastruktur.

Det bör övervägas om andra än myndigheter ska kunna utses till federationsområdesansvariga eller om privaträttsliga aktörer istället som underleverantör ska tillhandahålla vissa funktioner som en

federationsområdesansvarig ansvarar för. För en privaträttslig aktör som utses till federationsområdesansvarig kräver rättsordningen inte att uppdraget följer av lag, förordning eller beslut av regeringen i annan ordning. Det bör istället följa av avtal. Ska andra än myndigheter kunna utses måste det säkerställas att villkoren i avtal endast medger att den utses till federationsområdesansvarig som agerar lagligt och uppfyller höga ställda krav på verksamheten och dess ledning. I detta sammanhang behöver också beaktas hur den förslagna federationsinfrastrukturen ska förvaltas och drivas i kris och krig.

Närmare regler bör beträffande såväl myndigheter som privaträttsliga aktörer följa av avtal.

5.8 Stöd i rättsordningen för uppdrag som utfärdare av behörighetshandlingar

Bedömning: Ska en myndighet anslutas som utfärdare av behörighetshandlingar behöver det från fall till fall analyseras om myndighetens nuvarande uppdrag omfattar även den verksamheten eller om det behöver ges ytterligare stöd i rättsordningen. Ansluts en privaträttslig aktör som utfärdare av behörighetshandlingar bör det följa av avtal att utfärdaren ska ansvara för den funktionen. En närmare regleringen bör för såväl myndigheter som privaträttsliga aktörer följa av avtal eller överenskommelser.

Enligt förvaltningslagen (2017:900) och förvaltningsprocesslagen (1971:291) är det en grundläggande princip att myndigheter ska ha kännedom om vem de kommunicerar med i förvaltningsärenden. En myndighet har dessutom en skyldighet att kontrollera att den som företräder en annan i ett ärende är behörig ställföreträdare eller har en giltig fullmakt, se 15 § förvaltningslagen (2017:900) som ger myndigheten rätt att begära styrkande av behörighet genom en fullmakt och att förelägga om detta ifall det behövs. Juridisk litteratur ger ytterligare stöd för att myndigheter måste göra en noggrann bedömning av ombuds behörighet och att detta är en viktig del av att säkerställa rättssäkerhet och effektiv handläggning. En begäran från en förlitande part om en behörighetshandling har alltså stöd i författning samtidigt som en medarbetare respektive en digital aktör endast får agera inom den ram som dennes uppdrag respektive uppgift att agera automatiserat tillåter.

Av motiven till förvaltningslagen följer att det inte bör ställas krav på att varje enskild åtgärd som en myndighet vidtar kan kopplas till ett specifikt bemyndigande och att kravet på legalitet inte heller bör uppfattas så att en myndighets åtgärd måste ha uttryckligt stöd i en viss lagbestämmelse eller i andra föreskrifter som har meddelats i enlighet med 8 kap. RF.[8] Att en myndighet på begäran i pappersmiljö utfärdar en fullmakt för en medarbetare och skickar handlingen till en förlitande myndighet via vanlig post anses falla inom myndighetens uppdrag. Detsamma gäller om myndigheten istället skickar en vidimerad kopia av ett protokoll eller en liknande handling där det framgår att medarbetaren är behörig. Det behövs inte heller ytterligare stöd i författning när en myndighet digitaliserar denna hantering genom att ansluta sig till behörighetsinfrastrukturen som utfärdare av sådana behörighetshandlingar. För privaträttsliga förlitande parter som tillhandahåller digitala tjänster finns också anledning att kontrollera medarbetares respektive digitala aktörers

[8] Prop. 2016/17:180 s. 59.

behörighet för att undgå rättsförluster, exempelvis genom att uppgiftslämnande sker till en obehörig i strid mot gällande rätt.

Frågan blir mer komplex när innehållet i behörighetshandlingar istället hämtas ur ett register över juridisk behörighet för medarbetare eller digitala aktörer hos andra huvudmän än den som ställer ut behörighetshandlingen. Det kan vara fråga om ett publicitetsregister (exempelvis över firmatecknare) eller ett register över individer med specifika yrkesroller (exempelvis HOSP-registret), men det kan också handla om fullmaktsregister såsom Mina ombud (Bolagsverket/Digg), apoteks- och läkemedelsfullmakter (E-hälsomyndigheten) och register för patent- och bolagsärenden (PRV). För vissa av dessa uppgiftssamlingar gäller särskilda registerförfattningar där hanteringen regleras, bland annat när det gäller sättet för att lämna uppgifter. Andra register införs med stöd av avtal och överenskommelser där ansvarsfördelningen och den närmare hanteringen är reglerad. Vill en myndighet under sådana förutsättningar anslutas som utfärdare av behörighetshandlingar behöver det från fall till fall analyseras om myndighetens nuvarande uppdrag omfattar den verksamheten eller om legalitetsprincipen innebär att ett särskilt stöd behövs i rättsordningen. Ansluts en privaträttslig aktör som utfärdare av behörighetshandlingar bör det följa av avtal att utfärdaren ansvarar för en sådan funktion. Den närmare regleringen kan i många fall, för såväl myndigheter som privaträttsliga aktörer, följa av avtal.

Här bör samtidigt uppmärksammas att registerhållningen och informationsutbytet mellan utfärdare av behörighetshandlingar och förlitande part, som beskrivits, kommer att äga rum utanför behörighetsinfrastrukturen. Det är således utfärdare av behörighetshandlingar och förlitande part som ska säkerställa att beställning och utfärdande respektive mottagning och kontroll av juridisk behörighet sker författningsenligt.

5.9 Den ledningsansvariges personuppgiftsbehandling

Bedömning: Det finns inte något behov av att införa särskilda bestämmelser om den ledningsansvariges behandling av personuppgifter med anledning av ett införande av den föreslagna behörighetsinfrastrukturen.

Som redovisats i föregående avsnitt består behörighetsinfrastrukturen av funktioner och regler, dels gemensamma för alla (fundamentet), dels sådana som används och tillämpas inom respektive verksamhetsområde (verksamhetsområdesspecifika tillägg). Det föreslås att Digg ska föra ett centralt register över uppgifter om parter inom identitetsfederationen – ledningsansvarigs aktörs- och funktionsregister. Registret ska emellertid inte innehålla personuppgifter. Sådana uppgifter behandlas bara för att administrera behörighetsinfrastrukturen, exempelvis när det ska säkerställas vem som gör en ändring i registret och att denne är behörig att utföra åtgärden.

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/EG (allmän dataskyddsförordning), nedan kallad EU:s dataskyddsförordning, utgör den generella regleringen av personuppgiftsbehandling inom unionen. Till denna hör lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Det uppdrag som Digg bör utföra och myndighetens befogenheter som ledningsansvarig föreslås följa av en uttrycklig bestämmelse i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning. Det kan därmed knappast föreligga någon osäkerhet i fråga om vem som har personuppgiftsansvaret för eventuella behandlingar av personuppgifter som Diggs tillhandahållande av grundläggande funktioner och roll som ledningsansvarig kan föra med sig. Det finns därmed inte något behov av att införa särskilda bestämmelser om vem som har personuppgiftsansvaret. I den mån Digg behöver behandla personuppgifter inom ramen för sitt övergripande ansvar för behörighetsinfrastrukturen sker detta för att utföra uppgifter av allmänt intresse (artikel 6.1 e) som följer av lag eller annan författning. I dataskyddslagen tydliggörs att en uppgift av allmänt intresse utgör en rättslig grund för behandling av personuppgifter enligt artikel 6.1 e i dataskyddsförordningen om uppgiften följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning eller är ett led i den personuppgiftsansvariges myndighetsutövning om myndighetsutövningen sker enligt lag eller annan författning (2 kap. 2 §). En rättslig grund finns därmed för Diggs behandling av personuppgifter för behörighetsinfrastrukturen.

I artikel 5 i EU:s dataskyddsförordning ställs det vidare upp ett antal allmänna principer för behandlingen. Personuppgifterna ska bl.a. behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål. De får inte senare behandlas på ett sätt som är oförenligt med dessa ursprungliga ändamål. Uppgifterna ska vidare vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. De ska vara korrekta och, om nödvändigt, uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål. Vidare får personuppgifter inte förvaras under en längre tid än vad som är nödvändigt och de måste behandlas på ett sätt som säkerställer lämplig säkerhet. Artiklarna 5 och 6 är kumulativa. Det innebär att en personuppgiftsbehandling måste ha stöd i någon av de rättsliga grunderna i artikel 6 och alla principer i artikel 5 ska följas.

Någon omfattande samling av personuppgifter blir det inte fråga om och det föreslås inte att några känsliga personuppgifter ska behandlas. Det finns därmed inte behov av att införa särskilda bestämmelser om Diggs behandling av personuppgifter som ledningsansvarig inom behörighetsinfrastrukturen. De ändringar i förordning som föreslås beträffande Diggs instruktion och, i förekommande fall, andra berörda aktörers uppdrag innebär att myndigheterna får ett uttryckligt ansvar att tillhandahålla funktioner inom behörighetsinfrastrukturen.

Ett sådant uppdrag innebär samtidigt att den behandling av personuppgifter som är nödvändig för att utföra uppdraget har rättslig grund i artikel 6.1 e i EU:s dataskyddsförordning. Enligt 2 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning gäller att en uppgift av allmänt intresse som följer av lag eller annan författning utgör en rättslig grund för personuppgiftsbehandling. Därigenom blir det tydligt att Digg kan behandla personuppgifter i den utsträckning som är nödvändigt för att fullgöra sitt författningsenliga uppdrag inom behörighetsinfrastrukturen. Något behov av särskilda bestämmelser om rättslig grund eller personuppgiftsansvar föreligger därmed inte.

5.10 Federationsområdesansvarigas personuppgiftsbehandling

Bedömning: Det finns inte behov av att införa särskilda bestämmelser om en federations-områdesansvarigs behandling av personuppgifter med anledning av behörighetsinfrastrukturen.

Som beskrivits ovan innefattar behörighetsinfrastrukturen också funktioner som federations-områdesansvariga ansvarar för, dels sådana som är lika för alla inom behörighetsinfrastrukturen, dels funktioner som är verksamhetsområdesspecifika. Varje federationsområdesansvarig ska hålla en lokal katalog över utfärdare av behörighetshandlingar och förlitande parter som är anslutna. Som samlingsbeteckning för de register som en federationsområdesansvarig för över aktörer och funktioner inom den federationsområdesansvariges verksamhetsområde används federationsområdesansvarigs aktörs- och funktionsregister. Dessa kataloger ska inte heller innehålla personuppgifter. Sådana uppgifter behandlas bara för att administrera själva behörighetsinfrastrukturen. Det blir alltså inte heller här fråga om någon omfattande samling av personuppgifter och det föreslås inte att några känsliga personuppgifter ska behandlas. Några särskilda bestämmelser för federationsområdesansvariga om behandling av personuppgifter behövs därmed inte.

Som framgått sker själva informationsutbytet mellan utfärdare av behörighetshandlingar och förlitande part utanför behörighetsinfrastrukturen. Det bör därmed genomlysas i annan ordning utifrån de särskilda förutsättningar som gäller för varje federationsområdesansvarig. Vad som sagts i föregående avsnitt om följderna från dataskyddssynpunkt av de ändringar i förordning som föreslås beträffande berörda aktörers uppdrag gäller även här.

5.11 Direktåtkomst bör inte användas

Bedömning: Uppgifter för juridisk behörighetskontroll bör inte lämnas ut genom direktåtkomst. Det är en annan sak om en part, exempelvis inom hälso- och sjukvården, använder direktåtkomst för behandlingar som äger rum utanför behörighetsinfrastrukturen.

Förslag: Behörighetsinfrastrukturen bör utformas så att direktåtkomst inte används inom den. Krav på att ha system för direktåtkomst bör fasas ut.

Det finns inte någon legaldefinition av begreppet direktåtkomst. Regeringen har emellertid uttalat att det med sådan åtkomst vanligtvis avses att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen.[9] I begreppet ligger också att den som är personuppgiftsansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av.[10] Om en myndighet gör uppgifter tillgängliga för en annan myndighet genom direktåtkomst blir, något förenklat, varje uppgiftskonstellation (s.k. upptagning) som den andra

[9] Prop. 2009/10:85, s. 168
[10] Prop. 2011/12:45, s. 133

myndigheten kan nå genom direktåtkomst allmän handling även hos den andra myndigheten. Högsta förvaltningsdomstolen har i målet HFD 2015 ref. 61 funnit att vad som är direktåtkomst ska bedömas utifrån om den aktuella uppgiften kan anses förvarad hos den mottagande myndigheten enligt 2 kap. 3 § andra stycket tryckfrihetsförordningen, TF (numera 2 kap. 6 § TF). Avgörande är om uppgiften är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i uppfattbar form (en bedömning som har generell tillämplighet). Den tekniska utformningen av en myndighets system för utlämnande av uppgifter kan alltså bli avgörande för om det blir fråga om direktåtkomst eller annat utlämnande i elektronisk form (s.k. utlämnande på medium för automatiserad behandling).

Genom Högsta förvaltningsdomstolens avgörande klargjordes även de gränsdragningsfrågor kring begreppen direktåtkomst och utlämnande på medium för automatiserad behandling som informationshanteringsutredningen närmare redovisat i sitt betänkande Myndighetsdatalag (SOU 2015:39). Utredningen förklarade att Direktåtkomst innebär rättsligt att gränsen mellan de uppgiftsutbytande myndigheterna i viss omfattning tas bort, vilket inte är en konsekvens av annat elektroniskt utlämnande. Hur den mottagande myndigheten väljer att använda direktåtkomsten har den utlämnande myndigheten inte någon befogenhet att påverka, eftersom de handlingar som omfattas av åtkomsten redan har lämnats ut.[11]

Samverkan mellan myndigheter får inte heller förvaltningsrättsligt ta sig sådana former att de medverkande myndigheternas olika funktioner blandas samman och inte klart kan urskiljas (se JO 1993/94 s. 458). Dessa bedömningar har bekräftats i ett senare lagstiftningsärende där regeringen uttalat att IT-utvecklingen gått framåt så att det nu är möjligt att ta fram elektroniska lösningar som på annat sätt än genom direktåtkomst tillgodoser myndigheternas behov av att snabbt kunna ta del av aktuella uppgifter från andra myndigheter och att direktåtkomst bör tillåtas endast när det inte finns andra fullgoda alternativ som kan lösa behovet av informationsförsörjning.[12] I samma lagstiftningsärende utmönstrades en regel i 114 kap. 22 § socialförsäkringsbalken om att inte medge direktåtkomst förrän myndigheten försäkrat sig om att mottagaren uppfyller vissa informationssäkerhetskrav.

Behörighetsinfrastrukturen bör utformas så att direktåtkomst inte tillåts inom den. Sådan åtkomst leder ofta till att mottagaren får tillgång till överskottsinformation eftersom denne i regel har tillgång till fler uppgifter än vad denne behöver och kommer att nyttja. Enligt Diggs regelverk för förbetald e-legitimering får direktåtkomst inte användas då uppgifter lämnas ut i samband med utställande av identitetsintyg. Detsamma föreslås gälla för behörighetsinfrastrukturen, där utbyte av uppgifter avses ske på medium för automatiserad behandling genom att återanvända den tekniska och administrativa hantering och den juridiska reglering som gäller inom infrastrukturen för elektronisk identifiering.

Hanteringen bör utformas med utgångspunkt i Högsta förvaltningsdomstolens bedömning i HFD 2015 ref. 61. Närmare beskrivningar av hur direktåtkomst förknippas med föråldrad teknik och att

[11] SOU 2015:19, s. 135
[12] Prop. 2023/24:29, s. 74 och 77 ff

myndighetssystem numera utformas för utlämnande på medium för automatiserad behandling ges i eSam:s vägledning Elektroniskt informationsutbyte.[13]

Den tekniska utvecklingen har därefter tagit ytterligare snabba steg bort från direktåtkomst. Frågor om direktåtkomst kan bli aktuella i alla de beskrivna skikt av informationshantering som rör behörighetsinfrastrukturen. Som konstaterats i avsnitt 6.1 bör direktåtkomst inte äga rum inom ramen för den föreslagna behörighetsinfrastrukturen. Det är en annan sak om en part, exempelvis inom hälso- och sjukvården, använder direktåtkomst för behandlingar som äger rum utanför behörighetsinfrastrukturen, jfr avsnitt 4.1.2 och första stycket i avsnitt 6.1.

5.12 Myndighetsutövning bör inte delegeras

Bedömning: Behörighetsinfrastrukturen bör utformas så att det inte blir fråga om överlämnande av förvaltningsuppgifter vid exempelvis kontroll av en aktörs juridiska behörighet.

En behörighetskontroll kan ske som en del i handläggningen av ett ärende som innefattar myndighetsutövning. Ett exempel är att handläggningen av utlämnande av allmänna handlingar innefattar myndighetsutövning. Sådana förvaltningsuppgifter får enligt grundlag (12 kap. 4 § andra stycket RF) inte överlämnas till enskild utan stöd i lag. Detta förbud mot att lämna över skötseln av en angelägenhet som innefattar myndighetsutövning, tar sikte på hela handläggningen av ärendet. Beredningen av och beslutet i ett ärende anses utgöra oskiljaktiga delar av en och samma förvaltningsuppgift (JO 2019/20 s 279). En myndighet kan därmed inte heller delegera, t.ex. till en driftleverantör, att för myndighetens räkning bereda ärenden om sekretessprövning.

Att en tjänst som en utfärdare av behörighetshandlingar tillhandahåller blir använd med stöd av den planerade infrastrukturen innebär inte att en förvaltningsuppgift överlämnas till annan, utan endast att uppgifter om behörighet beställs och överlämnas i form av behörighetshandlingar. Den förlitande parten får på eget ansvar använda mottagna handlingar för att bedöma om den behörighet föreligger som krävs i det enskilda ärendet. Den föreslagna behörighetsinfrastrukturen bör således utformas så att det inte blir fråga om något överlämnande av förvaltningsuppgifter i strid mot regeringsformen. Det framstår dessutom som främmande att en myndighet som handlägger ett ärende skulle överlämna till en annan myndighet att pröva en fråga om behörighet i ett ärende hos den första myndigheten där ärendet ska handläggas.

Denna bedömning hindrar inte att en part lägger ut (outsourcar) automatiserad behandling av information till annan på ett rättsenligt sätt, förutsatt att ansvaret för beredningen och bedömningen av frågor om juridisk behörighet alltjämt vilar på den förlitande part som handlägger ärendet.

---

[13] https://www.esamverka.se/download/18.1d126bc174ad1e6c39ca4e/1464274317741/Elektroniskt%20informationsutbyte%2020en%20v%C3%A4gledning%20f%C3%B6r%20utl%C3%A4mnande%20i%20elektronisk%20form.pdf

6 Anpassningar för ett federationsområde

6.1 Behörighetshandlingarnas utformning

Bedömning: För att säkerställa interoperabilitet och återanvändbarhet inom behörighetsinfrastrukturen bör krav fastställas på format och informationsinnehåll för olika typer av behörighetshandlingar. Varje federationsområdesansvarig bör, i samråd med berörda aktörer, ansvara för utformningen av sådana handlingar. Den ledningsansvarige bör kunna ingripa mot olämpliga utformningar för att säkerställa att den gemensamma grunden inte undergrävs.

Som framgått av avsnitt 4.1.2 består behörighetsinfrastrukturen av ett skikt med gemensamma funktioner, regler och rutiner för alla parter inom behörighetsinfrastrukturen (infrastrukturens fundament) och ett kompletterande skikt med funktioner, regler och rutiner som respektive federationsområdesansvarig inför inom sitt område (områdesspecifika tillägg). Båda skikten är delar av behörighetsinfrastrukturen. Utfärdandet av behörighetshandlingarna och användningen av dem sker emellertid utanför de funktioner som inrättas för själva behörighetsinfrastrukturen. Detta innebär dock inte att krav på hur behörighetshandlingar ska vara utformade kan lämnas oreglerade. För varje typ av behörighetshandling behöver utfärdare och mottagare ha samma uppfattning om vilka uppgifter (attribut) som en behörighetshandling ska innehålla. Det kan vara fråga om exempelvis intyg från Bolagsverket om firmatecknare, från Lantmäteriet om fastighetsägare och från Socialstyrelsen om yrkesroll. För varje sådan typ av behörighetshandling behöver det bestämmas en minimiuppsättning av uppgifter som alltid ska finnas med samt en bruttolista över ytterligare uppgifter som får föras in i en behörighetshandling av den aktuella typen.

När en förlitande part därefter behöver en behörighetshandling innebär de standarder och närmare förfaranden som föreslås att den som beställer en behörighetshandling kan ange vilka uppgifter som denne behöver utöver angiven minimiuppsättning. På så sätt begränsas innehållet till de uppgifter som behövs för att göra en juridisk behörighetskontroll i det enskilda fallet, jämför reglerna i EU:s dataskyddsförordning om uppgiftsminimering. Dessutom behöver varje typ av behörighetshandling vara indelad i fält med en rubrik för varje fält så att den som ska göra en behörighetskontroll med stöd av behörighetshandlingen kan automatisera detta förfarande.

Här finns emellertid en risk för att det brister i samordning av vilka uppgifter som ska vara obligatoriska, vilka som därutöver får tas med i en viss typ av behörighetshandling samt hur den ska vara indelad i fält och annars strukturerad. Skulle sådana parallella lösningar byggas kan parterna hamna i en situation där olika standarder, avtal och tekniska varianter hindrar användningen av behörighetshandlingar mellan de olika områden där behörighetsinfrastrukturen införs. I ett regelverk för behörighetsinfrastrukturen behöver därför nödvändiga krav på behörighetshandlingarnas format och informationsinnehåll anges. Det blir fråga om krav för ett visst federationsområde. Varje federationsområdesansvarig bör därför ansvara för en samordning av de olika typer av behörighetshandlingar som ställs ut av de utfärdare av behörighetshandlingar som är anslutna till den federationsansvarige. Denne bör i samråd med berörda utfärdare av behörighetshandlingar och förlitande parter ta fram förslag som granskas av berörda parter innan den federationsansvarige bestämmer utformningen av aktuella typ av behörighetshandlingar.

Utformningen bör vidare granskas av den ledningsansvarige, som bör kunna förbjuda en utformning som är olämplig. På så sätt säkerställs att behörighetsinfrastrukturen förblir generisk och återanvändbar samtidigt som den ger en tillräcklig flexibilitet för de behov som är verksamhetsspecifika, utan att den gemensamma grunden undergrävs.

När en minimiuppsättning och de ytterligare uppgifter som tillåts ska bestämmas för en viss typ av behörighetshandling behöver det beaktas att materiella regler om juridisk behörighet blir avgörande för vad en behörighetshandling för ett visst område behöver innehålla. Kan en juridisk behörighetskontroll inte genomföras utan att först samla in kompletterande uppgifter utöver uppgifterna i föreliggande behörighetshandlingar kan momentana automatiserade kontroller av juridisk behörighet inte genomföras. Den närmare utformningen av varje typ av behörighetshandling behöver således ha sin grund i analyser av såväl uppgiftsbehoven som de juridiska förutsättningarna inom det område där en typ av behörighetshandling ska användas, jfr de analyser som kan behövas inom ett federationsområde av egenskapsintyg (avsnitt 6.3).

6.2 Tillämpning inom hälso- och sjukvården

Syftet med kapitel 6 är att beskriva de behov av anpassningar som Digg identifierat för federationsområdet hälso- och sjukvård. I följande avsnitt beskrivs situationer inom hälso- och sjukvården där uppgifter hämtas genom direktåtkomst, eftersom det främst är vid tillämpningen av sådana regler som behov av anpassningar har identifierats. I sammanhanget bör dock nämnas att även andra former av elektroniskt utlämnande i vissa fall är möjligt.

6.2.1 Användning av behörighetsinfrastrukturen inom hälso- och sjukvården

Bedömning: Behörighetsinfrastrukturens fundament bör utformas så att det kan användas även för särreglerade behörighetskontroller inom exempelvis hälso- och sjukvården, utan att de ges normerande verkan för infrastrukturen som helhet. Den grundläggande infrastrukturen för sedvanliga juridiska behörighetskontroller behöver därför kompletteras, men utan att det leder till påverkan eller fragmentering av den grundläggande strukturen.

Digg har som framgått i uppdrag att utveckla en infrastruktur för hela samhället, i enlighet med allmänna regler för juridisk behörighetskontroll, där uppgifter lämnas ut på medium för automatiserad behandling (här kallat sedvanliga behörighetskontroller). E-hälsomyndighetens uppdrag är däremot begränsat till informationsutbytet inom hälso- och sjukvården där uppgifter ofta hämtas genom direktåtkomst i enlighet med den särreglering som föreskrivs i patientdatalagen (2008:355; PDL), lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation (SVOD), lagen (2018:1212) om nationell läkemedelslista (NLL) och tillhörande föreskrifter i förordning och myndighetsföreskrifter (här kallat särreglerade behörighetskontroller). För behörighetskontroller inom hälso- och sjukvården tillämpas även ett annat mönster än vid sedvanliga behörighetskontroller, se följande sammanställning.

Område	**Sedvanlig juridisk behörighetskontroll** (fråga/svar, utlämnande på medium för automatiserad behandling)	**Vissa särreglerade kontroller inom hälso- och sjukvården där särskilda kriterier kan behöva vara uppfyllda** (PDL, SVOD, NLL – direktåtkomst, i vissa fall annat elektroniskt utlämnande)
Syfte med kontrollen	Fastställa om en viss fysisk eller digital aktör är behörig att agera för huvudman/med yrkesroll i det enskilda fallet innan utlämnande/åtgärd.	På förhand kontrollera och säkerställa att begärande vårdgivare uppfyller vissa krav på behörighetstilldelning och dataskydd m.m. och fastställa vid varje begäran om förfrågan kommer från angiven vårdgivare.
Beställare	Förlitande part beställer/mottar identitetsintyg och behörighetshandling (t.ex. registerutdrag, fullmakt) per ärende.	Begärande vårdgivare (A) tar fram och bifogar identitets- och behörighetsuppgifter; mottagande vårdgivare (B) kontrollerar avsändande organisation, ändamål och tillämpar spärrar – vanligtvis inte behörighet per individ för varje enskilt fall.
När i processen?	Före sakprövning/åtkomst; prövas som preliminär fråga (identitet + behörighet).	Före anslutning: förhandsbedömning/överenskommelser Vid åtkomst: kontroll av ändamål och tillämpning av spärr, inte återkommande individbaserad behörighetsprövning per transaktion.
Teknisk åtkomstmodell	Transaktionsvis fråga–svar (API/meddelande); utlämnande prövas per begäran.	Direktåtkomst till system hos vårdgivare B för användare/digital aktör hos A; loggning och efterhandsgranskning. Vid annat än direktåtkomst – fråga och svar
Rättslig grund	Allmänna materiella regler om ställföreträdarskap/ ombud, fullmakter, delegationsordningar, yrkesroller + processuella regler om när/var prövning sker.	PDL, SVOD, NLL och Socialstyrelsens föreskrifter om behörighetstilldelning (befogenhetstilldelning) krav avseende patientrelation, dataskydds-, sekretess- och säkerhetsreglering. I vissa fall särskilda förhandskrav beträffande behörighetstilldelning och dataskydd.
Identitetskontroll	E-legitimation + identitetsintyg; regleras i existerande avtal/ramverk.	Samma identitetsmekanismer kan användas; vårdgivare B litar på att vårdgivare A identifierat användaren korrekt.

Utförare av behörighetskontroll	Förlitande part gör en juridisk prövning i varje ärende/transaktion före utlämnande/åtgärd.	Förhandsbedömning av A (och E-hälsomyndigheten där NLL gäller); B kontrollerar ändamål/tillämpar spärrar och loggar.
Bevismedel	Behörighetshandlingar (registerutdrag, fullmakt, protokoll, yrkesrollsintyg); för digital aktör: funktionsnivå-intyg.	Organisationsnivåns styrning och behörighetstilldelning kontrolleras i förväg; enligt NLL även E-hälsomyndighetens prövning av behörighets- och säkerhetsfrågorna.
Roller i federationen	Ledningsansvarig (regelverk/ramverk), federationsområdesansvarig (sektorsanpassning), utfärdare av behörighetshandlingar, förlitande part.	Samma rollmodell kan användas som bärare av metadata/handlingar, men prövningslogiken är avvikande (förhandsbedömning).
Avtalsbehov	Huvudsakligen avtalsreglering (återanvänder e-ID-mönster) + tekniska bilagor/metadata.	Avtal + områdesspecifika krav/överenskommelser; beakta att delar kan behöva författningsregleras.
Loggning/uppföljning	Spårbarhet per utlämnande/transaktion.	Omfattande åtkomstloggning hos vårdgivare B och efterhandskontroller; spärrhantering för patient.
Konsekvens för nationell infrastruktur	Basmodell för sedvanlig juridisk kontroll och återanvändning av e-ID-infrastruktur.	Direktåtkomst ej lämplig som generell norm; ska hanteras som områdesspecifik anpassning ovanpå samma tekniska fundament.

Tabell 2: Mönster för sedvanliga- respektive sådana särreglerade behörighetskontroller som finns inom hälso- och sjukvården.

Dessa skillnader innebär inte att behörighetsinfrastrukturens fundament måste utformas så att en användning inom hälso- och sjukvården hindras. Fundamentet bör istället inrättas så att det efter områdesspecifika anpassningar kan nyttjas även när hanteringen omsätts i en IT-arkitektur med åtkomstmodeller, metadata och loggning för särreglerade behörighetskontroller. Avgörande för en reglering av en behörighetsinfrastruktur är dock att regler och IT-arkitekturer med åtkomstmodeller för särreglerade behörighetskontroller inte tillåts lägga grunden för, och därmed komplicera, den infrastruktur som föreslås för sedvanlig juridisk behörighetskontroll.

6.2.2 Kontroller vid direktåtkomst

Som framgått av avsnitt 5.1 kan en nationell infrastruktur inte utarbetas och regleras baserat på särlösningar för hälso- och sjukvården. Den behörighetsinfrastruktur som föreslås bör emellertid ges en så generell utformning att den kan nyttjas även när områdesspecifika avvikelser krävs från

förfarandet vid sedvanliga behörighetskontroller. Det finns situationer då det inte anses praktiskt möjligt att kontrollera att den som begär åtkomst verkligen har den rätt att agera som krävs. Detta kan illustreras med exempel från hälso- och sjukvården. Hälso- och sjukvårdspersonal har rätt att agera för sin arbetsgivares räkning vid förfrågningar om att ta del av patientuppgifter. Befogenheten för personalen att ta del av uppgifter skiljer sig åt. För att tillgodose den utlämnande aktörens behov av att kontrollera om en person har rätt att få tillgång till uppgifter räcker det inte med en kontroll av identitet eller att personen får företräda den organisation som den säger sig agera för. Personen behöver också ha rätt att se den efterfrågade informationen. En sedvanlig juridisk behörighetskontroll har då inte ansetts räcka samtidigt som det i dessa fall inte är praktiskt möjligt att kontrollera varje enskild befogenhet vid varje enskilt frågetillfälle. Dessa särskilda förutsättningar har samband med att direktåtkomst används för att ge tillgång till uppgiftssamlingar inom vården.

För att möjliggöra automatiserade informationsutbyten krävs i dessa fall att det är säkerställt mellan organisationerna att de personer som agerar för organisationens räkning inte har fått för vida befogenheter. I vissa fall, så som i hälso- och sjukvården, styrs dessa befogenheter till viss del av rättsliga regleringar som behöver följas. Den utlämnande parten har i dessa fall inte praktisk möjlighet att säkerställa att den person som efterfrågar informationen har av sin organisation fått sin befogenhet tilldelad på korrekt sätt vid varje givet tillfälle som personen efterfrågar åtkomst. Oftast hanteras detta genom att den utlämnande parten i förväg kontrollerar att den efterfrågande parten lever upp till de krav, i vissa fall rättsliga regelverk rörande säkerhetskrav, som finns för tilldelning av behörigheter till personal. Efter att erforderliga kontroller gjorts förlitar sig den part som ger tillgång till uppgifter på att de personer som efterfrågar åtkomst från den kontrollerade organisation har korrekta behörigheter så länge anropen kan verifieras komma från den organisationen. I detta fall har en tillit uppstått organisationerna emellan. Detta förtar inte den utlämnande partens ansvar för att uppgifter tillgängliggörs för rätt person med rätt. Den förlitande parten har emellertid gjort bedömningen att den kan förlita sig på att det är rätt person med rätt behörighet, givet de kontroller som har gjorts av organisationen.

6.2.3 Krav på granskning av annan parts informationssäkerhet och dataskydd

Bedömning: Ansvaret för informationssäkerhet och dataskydd är individuellt och kan inte delegeras. De särskilda reglerna om direktåtkomst inom hälso- och sjukvården skapar otydlighet i ansvarsfördelningen och bör ses över. I avvaktan på en sådan utredning bör behörighetsinfrastrukturen utformas för att stödja ändamålsenliga juridiska behörighetskontroller även vid områdesspecifika anpassningar inom hälso- och sjukvården, utan att det gemensamma fundamentet påverkas av särregleringen.

Ansvaret för en myndighets eller ett företags informationssäkerhet är individuellt. Det finns inte heller någon generell skyldighet för myndigheter eller företag att kontrollera andras informationssäkerhet. Huvudregeln är att varje organisation ansvarar för sin informationssäkerhet. På motsvarande sätt ansvarar varje personuppgiftsansvarig för att all dennes behandling av personuppgifter sker i enlighet med gällande lagstiftning, att den registrerades rättigheter skyddas och att uppgifter lämnas ut först efter att det i varje enskilt fall bedömts att ett utlämnande får ske.

Detta ansvar omfattar såväl tekniska som organisatoriska åtgärder och är inte möjligt att delegera till en annan myndighet eller ett företag.

Inom hälso- och sjukvården gäller emellertid särskilda regler för behandling av personuppgifter. Av särskilt intresse är 8 kap. 2 § NLL där det föreskrivs att direktåtkomst till uppgifter i den nationella läkemedelslistan får ges först sedan E-hälsomyndigheten *försäkrat sig om* att *behörighets- och säkerhetsfrågorna* är lösta på ett sätt som är tillfredsställande ur integritetssynpunkt och att behörigheten hos den som ska få direktåtkomst är begränsad till att endast gälla sådana uppgifter som denne har rätt att få ut enligt NLL.

Frågan är vad som menas med att direktåtkomst till uppgifter får ges först sedan E-hälsomyndigheten "försäkrat sig om" att angivna säkerhetsfrågor är lösta på tillfredsställande sätt och att behörigheterna är korrekt hanterade. I lagstiftningsärendet invände flera remissinstanser att det behövdes ett förtydligande kring ansvarsförhållandena rörande behörighet, åtkomstkontroll och tillsyn och Myndigheten för vård- och omsorgsanalys anförde att hälso- och sjukvårdens svårigheter med att leva upp till den aktuella lagstiftningen om behörighetsstyrning och åtkomstkontroll måste lösas. Myndigheten för samhällsskydd och beredskap hävdade att föreslagen reglering inte borde genomföras utan att föregås av en analys av vilka informations- och cybersäkerhetskrav som måste ställas. Regleringen genomfördes emellertid utan närmare förtydliganden i lagmotiven. Regeringen anförde istället att E-hälsomyndigheten borde ta fram rutiner för vilka krav som ska ställas på de aktörer som kommer i fråga för direktåtkomst och att det ankommer på E-hälsomyndigheten att säkerställa att risken för obehörig åtkomst och obefogad spridning minimeras.[14] Lagmotiven ger således uttryck för att ett betydande ansvar vilar på E-hälsomyndigheten att säkerställa berörda säkerhets- och behörighetsfrågor.

I 14 kap. 22 § socialförsäkringsbalken föreskrevs att en socialnämnd får ha direktåtkomst först sedan Försäkringskassan eller Pensionsmyndigheten har försäkrat sig om att handläggare hos socialnämnd bara kan ta del av uppgifter om personer som är aktuella i ärenden hos nämnden. I samband med att regleringen anpassades till att uppgifter numera kan lämnas på annat sätt än genom direktåtkomst utmönstrades denna regel utan närmare motivering av regeringen. I den framställning om författningsändringar som låg till grund för propositionen anfördes emellertid att kommunernas socialnämnder i dagsläget numera får uppgifterna på annat sätt än genom direktåtkomst.

Någon direkt motsvarighet till bestämmelsen i 8 kap. 2 § NLL, om att först försäkra sig om att behörighets- och säkerhetsfrågorna är lösta, finns inte i PDL. Liknande krav finns emellertid, särskilt i 5 kap. 4 §, där det föreskrivs att direktåtkomst endast är tillåten i den utsträckning som anges i lag eller förordning. Digg och E-hälsomyndigheten har översiktligt förhört sig om hur vårdgivare idag säkerställer att behörighets- och säkerhetsfrågorna är lösta och att åtkomsten är begränsad till behöriga personer och nödvändiga uppgifter. Därvid har bland annat framkommit att den åtkomst till patientuppgifter som ges kan vara genom NPÖ, där parterna har förbundit sig till att följa de tjänstekontrakt som finns till tjänsten. Därutöver finns det även delning som baseras på att vårdgivarna använder sig av samma vårdinformationssystem. Då handlar det oftast om att de vårdgivare som en region i egenskap av huvudman har upphandlat för att tillhandhålla vård även

[14] Prop. 2017/18:223, s. 178.

ska använda det vårdinformationssystem som regionen anvisar. Kontrollen av vårdgivaren kan där sägas ske genom de krav inom upphandlingen som ställs på vårdgivarna. Detta behöver dock fortsatt utredas för att få en tydlig bild av vilka olika krav och lösningsmönster som finns.

Vad som framkommit ger stöd för Diggs bedömning (se avsnitt 5.11) att direktåtkomst bör utmönstras eller i vart fall minimeras inom hälso- och sjukvårdsområdet, så som skett inom socialförsäkringens administration. En hantering som utgår från sedvanliga behörighetskontroller där vedertagna myndighetsgränser upprätthålls bör kunna stärka informationssäkerheten, sekretessen och dataskyddet eftersom en identitets- och behörighetskontroll skulle utföras i varje enskilt fall av den som lämnar ut uppgifter innan några uppgifter blir tillgängliga för annan. Samtidigt skulle regleringen och fördelningen av ansvaret för informationssäkerhetsfrågorna förenklas och förtydligas. Digitalt stämplade delar av metadata för en part (inom infrastrukturen använd standard kallad "trust mark") läker inte beskrivna svagheter utan väcker ytterligare frågor om vem eller vilka som ansvarar för de granskningar och kontroller som skulle krävas för att tilldela digitalt stämplade metadata en roll inom området när det gäller parters säkerhetsarbete (jfr avsnitt 6.3). Frågor skulle också uppkomma om hur sådana digitalt stämplade metadata förhåller sig till den författningsreglering som gäller generellt inom området för informationssäkerhet och vilket ansvar en granskare har om felaktiga metadata stämplas av denne. Är det granskaren som får ett juridiskt ansvar för den digitalt stämplade handlingen eller står den begärande eller utlämnande vårdgivaren denna risk?

En närmare genomlysning bör genomföras i annan ordning av de utmaningar som direktåtkomst, förhandskontroller av andras informationssäkerhet och så kallade trust marks för med sig inom hälso- och sjukvårdsområdet. I avvaktan på en sådan utredning bör den föreslagna behörighetsinfrastrukturen ta höjd för att kunna stödja ändamålsenliga kontroller av juridisk behörighet även inom ramen för behovet av områdesspecifika anpassningar för hälso- och sjukvården. Det är en annan sak att regler och IT-arkitekturer med åtkomstmodeller för särreglerade behörighetskontroller inte bör tillåtas lägga grunden för, och därmed komplicera, det fundament som föreslås för sedvanliga behörighetskontroller med stöd av behörighetshandlingar som lämnas ut på medium för automatiserad behandling för sedvanliga behörighetskontroller.

6.2.4 Personuppgiftsansvaret vid direktåtkomst

Bedömning: För att undvika otydliga eller överlappande ansvarsförhållanden bör behörighetsinfrastrukturen möjliggöra en tydlig och rättsenlig ansvarsfördelning, utan att särreglerade förfaranden tillåts påverka det gemensamma förfarandet.

En annan fråga som särregleringen inom hälso- och sjukvården aktualiserar är hur personuppgiftsansvaret ska anses vara fördelat när personuppgifter görs tillgängliga genom direktåtkomst. Enligt 2 kap. 6 § patientdatalagen (2008:355), PDL, ansvarar varje vårdgivare inte bara för den behandling av personuppgifter som sker inom den egna verksamheten, utan också för den behandling som uppstår när vårdgivaren i ett enskilt fall genom direktåtkomst tar del av patientuppgifter som finns hos en annan vårdgivare eller hos en annan myndighet inom samma region eller kommun. Motsvarande princip gäller enligt 4 kap. 1 § lagen (2023:480) om sammanhållen vård- och omsorgsdokumentation, SVOD, där det föreskrivs att personuppgiftsansvaret även

omfattar sådan behandling av personuppgifter som utförs när någon genom direktåtkomst eller annat elektroniskt utlämnande i ett enskilt fall bereder sig tillgång till personuppgifter hos en annan vårdgivare eller omsorgsgivare. Även där omfattar personuppgiftsansvaret den behandling som sker när en vårdgivare eller omsorgsgivare genom direktåtkomst eller annat elektroniskt utlämnande får tillgång till uppgifter hos en annan vård- eller omsorgsgivare. Sammantaget innebär detta att en vårdgivare- eller omsorgsgivare som använder direktåtkomst för att söka, läsa eller på annat sätt behandla personuppgifter hos en annan vårdgivare själv är personuppgiftsansvarig för den behandling som sker vid direktåtkomsten.

Frågan är därmed hur regleringen av personuppgiftsansvaret i lagen (2018:1212) om nationell läkemedelslista, NLL, ska förstås – om det avviker det från den ordning som gäller enligt PDL och SVOD. E-hälsomyndigheten är enligt 3 kap. 1 § NLL personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför i den nationella läkemedelslistan. Vid remissbehandlingen ifrågasatte Datainspektionen (numera IMY) att E-hälsomyndigheten skulle ges i uppdrag att som personuppgiftsansvarig behandla uppgifter som inte behövs inom myndighetens egen verksamhet utan för andra verksamheters behov och hävdade att detta skapar en gränsdragningsproblematik och oklarhet i fråga om både ansvar och roller mellan E-hälsomyndigheten, vårdgivare och apotek, ytterst också i förhållande till de registrerade.

Regeringen, som inte delade detta synsätt, angav som skäl för att E-hälsomyndigheten måste få behandla personuppgifter att myndigheten behöver kunna erbjuda en konkurrensneutral samt ur integritetssynpunkt säker överföring av personuppgifter mellan olika aktörer och att denna överföring är grundläggande för öppenvårdsapotekens funktion.[15] Samtidigt klargjorde regeringen att de behandlingar av personuppgifter som sker när öppenvårdsapotek eller hälso- och sjukvården genom direktåtkomst tar del av uppgifter i den nationella läkemedelslistan redan omfattas av respektive sektorslagstiftning – apoteksdatalagen och PDL. För öppenvårdsapoteken gäller att tillståndshavaren enligt 7 § apoteksdatalagen är personuppgiftsansvarig för all behandling som utförs på apoteket och den behandling som sker när apotekspersonal genom direktåtkomst tar del av uppgifter hos E-hälsomyndigheten är därför en behandling som faller under apoteksdatalagen. På motsvarande sätt gäller för hälso- och sjukvården, som framgått ovan, att den behandling som sker vid direktåtkomst till uppgifter i läkemedelslistan omfattas av PDL, där det i 2 kap. 6 § PDL föreskrivs att varje vårdgivare är personuppgiftsansvarig för den behandling av personuppgifter som denne utför. Mot denna bakgrund fann regeringen att det inte fanns behov av att särskilt reglera vårdgivarnas eller apotekens personuppgiftsansvar i lagen om nationell läkemedelslista och att ett sådant tillägg snarare skulle riskera att skapa otydlighet. Den myndighet, juridiska person eller enskilda näringsidkare som använder sin direktåtkomst och bereder sig tillgång till andra vårdgivares och omsorgsgivares uppgifter för att söka efter och läsa eller annars behandla personuppgifter är därmed personuppgiftsansvarig för den behandling av personuppgifter som detta innebär. Det rättsliga ansvaret för behandling vid direktåtkomst kvarstår alltså hos respektive aktör enligt såväl PDL och SVOD som NLL. E-hälsomyndighetens ansvar NLL är enligt lagmotiven begränsat till den behandling som myndigheten själv utför i sin roll som infrastrukturförvaltare.

[15] Prop 2017/18:223, s. 81.

Sker informationsutbytet istället på medium för automatiserad behandling med hjälp av sådana funktioner för fråga och svar som det var fråga om i HFD 2015 ref. 61 fattar den utlämnande myndigheten ett uttryckligt beslut om utlämnande så att ansvarsfördelningen för dessa behandlingar blir tydlig. Den utlämnande myndigheten synes därmed ansvara för behandlingen fram till dess att uppgifterna lämnats ut, vilket innefattar bedömningen av rättslig grund, tillämpningen av sekretessbestämmelser och det faktiska utlämnandet. Mottagaren (t.ex. en vårdgivare) blir personuppgiftsansvarig först efter att denne fått uppgifterna. Ansvaret övergår därmed efter utlämnandet, inte vid åtkomstögonblicket såsom vid direktåtkomst.

En regel som delvis inte förefaller passa in i denna struktur är 4 kap. 1 § andra stycket SVOD där det anges att personuppgiftsansvaret även omfattar sådan behandling av personuppgifter som utförs när någon genom *annat elektroniskt utlämnande i ett enskilt fall bereder sig tillgång* till personuppgifter hos en annan vårdgivare eller omsorgsgivare. Efter det klargörande avgörandet i HFD 2015 ref. 61 ges inte tillgång till annans uppgiftssamling genom utlämnande på medium för automatiserad behandling. Dessutom kvarstår vid sammanhållen vård- och omsorgsdokumentation, så som IMY gett uttryck för, att personuppgiftsansvaret fördunklas eller bli otydligt när flera vårdgivare respektive omsorgsgivare enas om gemensamma tjänster för drift, förvaltning eller säkerhet. En ordning som t.ex. innebär att varje myndighet eller privat vårdgivare som samverkar i sammanhållen journalföring har ett solidariskt ansvar för all personuppgiftsbehandling som förekommer eller en ordning som innebär att en viss på förhand utsedd vårdgivare ges ett ensamt ansvar skulle enligt regeringen undanröja risken för att en enskild behöver vända sig till mer än en vårdgivare med klagomål. Regeringen fann det emellertid olämpligt att peka ut vem som ska vara personuppgiftsansvarig för tekniska och organisatoriska säkerhetsåtgärder och överlämnade åt de privata vårdgivarna, regionerna och kommunerna att inom lagens ramar närmare bestämma detta vid sammanhållen journalföring och träffa avtal vari de närmare formerna för samarbetet preciseras.[16]

För att undgå risken för otydliga och överlappande ansvarsförhållanden framstår utlämnande på medium för automatiserad behandling som en ändamålsenlig väg framåt, i förening med en tydlig ansvarsfördelning genom avtal när flera aktörer enas om gemensamma tjänster för drift, förvaltning eller säkerhet inom en infrastruktur för juridisk behörighetskontroll. I avvaktan på att dessa frågor blir föremål för en närmare utredning bör den föreslagna behörighetsinfrastrukturen ta höjd för att stödja en ändamålsenlig fördelning av personuppgiftsansvaret genom områdesspecifika anpassningar inom ramen för gällande rätt. Det är en annan sak att de regler som gäller vid särreglerade behörighetskontroller inte bör tillåtas lägga grunden för, och därmed komplicera, den ansvarsfördelning som föreslås för sedvanliga behörighetskontroller med stöd av behörighetshandlingar som lämnas ut på medium för automatiserad behandling.

[16] Prop. 2007/08:126 s. 135.

6.2.5 Vilken aktör som kontrollerar behörighet och i vilket skede

Bedömning: Sedvanliga juridiska behörighetskontroller där varje aktör ansvarar för sin egen prövning och informationssäkerhet bör ge stöd för att förmedla information om motparten. Områdesspecifika anpassningar bör kunna stödjas av behörighetsinfrastrukturen utan att vara en del av dess fundament.

En sedvanlig juridisk behörighetskontroll innebär som framgått att den som förfogar över en uppgift gör en självständig prövning av den förfrågandes identitet och rätt att agera i det enskilda fallet innan en uppgift lämnas ut. Prövningen sker då som en preliminär fråga inom ramen för den utlämnande aktörens eget rättsliga ansvar. Den tekniska hanteringen utgår från ett fråge- och svarsförfarande, där uppgifter tillhandahålls på medium för automatiserad behandling först efter att identitet, behörighet och övriga rättsliga förutsättningar för ett utlämnande har konstaterats av den utlämnande aktören. Varje aktör ansvarar i denna modell för sin egen informationssäkerhet, sitt dataskydd och sina beslut om utlämnande. Någon generell skyldighet att granska eller godkänna andra aktörers säkerhetsarbete föreligger inte.

När åtkomst däremot sker genom direktåtkomst enligt de särreglerade modellerna inom hälso- och sjukvården förutsätts att en part – ofta E-hälsomyndigheten eller den mottagande vårdgivaren – i förväg varit aktiv med avseende på den andra partens informationssäkerhet och behörighets-tilldelning. Dessa förhandsvisa åtgärder ersätter – i förening med bland annat andra kontroller i efterhand – den transaktionsvisa prövning som sker av bland annat identitet och behörighet vid annat elektroniskt utlämnande än direktåtkomst. Hanteringen vid direktåtkomst innebär en principiell avvikelse från den allmänna rättsordningens uppdelning av ansvar, eftersom en myndighet eller organisation därmed kan behöva bedöma en annan parts efterlevnad av dataskydds- och säkerhetskrav och att den från vilken uppgifter hämtas inte gör en behörighetskontroll vid transaktionstillfället.

För att en nationell behörighetsinfrastruktur ska kunna tillämpas även för sådana särreglerade åtkomstmodeller krävs att infrastrukturen medger att uppgifter om genomförda granskningar, säkerhetsnivåer och behörighetsförtilldelning kan representeras som verifierbara attribut i intyg. På så sätt kan även denna typ av kontroll formaliseras med stöd av behörighetsinfrastrukturen. En reglering som utgår från sedvanliga juridiska behörighetskontroller – där prövningen sker vid utlämnande och ansvaret förblir hos den utlämnande aktören – bör dock läggas till grund för ett fundament för behörighetsinfrastrukturen. De särreglerade modellerna bör endast betraktas som områdesspecifika tillägg så att granskningen av en annan parts säkerhets- och dataskyddsarbete, där det förekommer, kan stödjas av behörighetsinfrastrukturen utan att utgöra en del av dess grundläggande funktioner inom fundamentet.

6.2.6 Sammanfattande bedömning och förslag

Bedömning: Behörighetsinfrastrukturen bör ta sin utgångspunkt i sedvanliga juridiska behörighetskontroller, där utlämnande sker på medium för automatiserad behandling och förlitande part prövar identitet och behörighet. Direktåtkomst och liknande särlösningar med otydlig ansvarsfördelning bör inte utgöra norm.

Förslag: Behörighetsinfrastrukturen utformas så generiskt att dess funktioner kan användas även där särreglerade åtkomstmodeller förekommer. Nödvändiga anpassningar utarbetas inom respektive federationsområde och införas genom avtal, utan att det gemensamma fundamentet påverkas.

Diggs grundläggande bedömning är som framgått att direktåtkomst bör utmönstras eller att regleringen i vart fall bör anpassas till dagens användning av informationssystem, så som skett inom socialförsäkringens administration där regeringen funnit att IT-utvecklingen gått framåt så att det nu är möjligt att ta fram elektroniska lösningar som på annat sätt än genom direktåtkomst tillgodoser myndigheternas behov av att snabbt kunna ta del av aktuella uppgifter från andra myndigheter. Regeringen anförde därvid att direktåtkomst bör tillåtas endast när det inte finns andra fullgoda alternativ som kan lösa behovet av informationsförsörjning.[17] Med beaktande av den korta tid som står till bud innan en behörighetsinfrastruktur behöver tas i bruk kan en sådan översyn dock inte nu läggas till grund för det förslag som Digg lägger fram. Istället föreslås att behörighetsinfrastrukturen ska utformas så *generiskt* att dess grundläggande funktioner kan användas även när författningsregleringen och den praktiska tillämpningen bygger på särlösningar såsom direktåtkomst.

Utöver de tekniska anpassningar av behörighetsinfrastrukturen som detta kräver blir det av betydelse för utformningen av det regelverk som Digg föreslår ska införas genom avtal mellan parter som anslut till behörighetsinfrastrukturen. Regelverket bör ta sin utgångspunkt i att behörighetsinfrastrukturen inrättas för sedvanliga behörighetskontroller. Det behöver emellertid också ges utrymme för nödvändiga områdesspecifika anpassningar. Som exempel på de regelfrågor som aktualiseras vid en anpassning för vissa tillämpningar inom hälso- och sjukvården kan nämnas hur en utlämnande parts rättigheter och skyldigheter bör regleras vid tillgång till uppgifter genom direktåtkomst. Identitets- och behörighetskontrollen utförs då, som framgått, av den organisation som hämtar uppgifter. Den utlämnande parten (jfr förlitande part) har istället vissa skyldigheter att göra vissa kontroller i efterhand. Dessa kontroller sker inom ramen för en form av organisationstillit, där den utlämnande parten, vid åtkomstögonblicket, kontrollerar från vilken myndighet eller annan organisation som anropet kommer (samt vissa andra uppgifter såsom ändamålet för behandling och om uppgifterna har spärrats), inte vilken individ det är och om denne är juridiskt behörig. En behörighetshandling (som även innehåller uppgifter om kontrollerad identitet) sänds visserligen över och loggas för eventuell framtida uppföljning men används inte vid åtkomstögonblicket av den utlämnande parten (jfr förlitande part).

[17] Prop. 2023/24:29, s. 74 och 77 ff.

Behörighetsinfrastrukturen bör således enligt Diggs bedömning utformas för reella kontroller av juridisk behörighet i enlighet med de processuella och materiella regler (se avsnitt 5.2.1) som en förlitande part har att tillämpa vid en sedvanliga behörighetskontroller innan uppgifter lämnas ut. Dessa materiella och formella krav och bedömningen av om de uppfyllts innehåller inte någon prövning av tillåtna ändamål för behandling av personuppgifter eller någon sekretessprövning. En sådan prövning äger rum först efter att de preliminära frågorna har blivit klarlagda som en bedömning i sak av själva ärendet. Denna syn på juridiska behörighetskontroller är som framgått allmänt accepterad och grundad på allmänna regler samtidigt som varje myndighet ansvarar för sin informationssäkerhet, till skillnad från den delvis oklara ansvarsfördelning som uppkommer vid direktåtkomst. Vid direktåtkomst enligt PDL, SVOD och NLL bryts dessutom vedertagna gränser igenom mellan sådana preliminärfrågor i ett ärende hos en myndighet som leder till avvisning (när behörighet inte föreligger) till skillnad från sådana frågor som är en del av själva ärendet och som avgörs genom en dom eller ett slutligt beslut av myndigheten (se avsnitt 4.3.1).

Ett regelverk för en nationell infrastruktur för kontroll av juridisk behörighet behöver således ta sin utgångspunkt i de materiella rättsreglerna om ställföreträdar- och ombudsskap, fullmakter, delegationsordningar och yrkesroller och den processuella regleringen av vilka kontroller som behöver göras i ett ärende. Infrastrukturen behöver vidare bygga på att förlitande part kontrollerar medarbetares identitet och behörighet och att informationsutbytet sker så att den myndighet som förfogar över behörighetsuppgifterna i varje enskilt fall prövar om uppgifterna får lämnas ut innan en mottagare ges tillgång till dem.

Den särreglering som behövs för bland annat direktåtkomst bör inom respektive område där särreglering krävs utarbetas av berörda federationsområdesansvariga och införas genom avtal när utfärdare av behörighetshandlingar och förlitande parter ansluts till en federationsområdesansvarig. Hur detta närmare bör utformas får genomlysas i samband med att ett regelverk tas fram för behörighetsinfrastrukturen.

6.2.7 Särskilt om förhandskontroller

Bedömning: E-hälsomyndigheten ska enligt lagen om nationell läkemedelslista försäkra sig om att behörighets- och säkerhetsfrågorna är tillfredsställande lösta innan direktåtkomst medges. Skyldigheten innebär inte något uttryckligt lagstöd för platsbesök eller andra ingripande kontroller, utan får anses omfatta mindre åtgärder såsom att begära och granska dokumentation samt att undantagsvis genomföra stickprovskontroller. Myndigheten kan därigenom med rimlig tillförlitlighet förvissa sig om att gällande krav är uppfyllda.

Som framgått får direktåtkomst till uppgifter i den nationella läkemedelslistan ges först sedan E-hälsomyndigheten försäkrat sig om att behörighets- och säkerhetsfrågorna är lösta på ett sätt som är tillfredsställande ur integritetssynpunkt och att behörigheten hos den som ska få direktåtkomst är begränsad till att endast gälla sådana uppgifter som denne har rätt att få ut enligt NLL. Denna bestämmelse innebär att E-hälsomyndigheten ska vidta vissa åtgärder innan direktåtkomst beviljas men den innefattar inget uttryckligt lagstöd för E-hälsomyndigheten att genomföra platsbesök hos externa aktörer. E-hälsomyndigheten har emellertid, enligt 2 § förordningen (2013:1031) med instruktion för E-hälsomyndigheten, rätt att vid behov genomföra kontroller av elektroniska system

för direktåtkomst till uppgifter hos myndigheten vilket innebär att EHM ges möjlighet att vidta mindre ingripande åtgärder som innebär konkreta kontroller. Exempel på sådana åtgärder kan vara att begära att anslutna aktörer tillhandahåller dokumentation som visar hur säkerhets- och behörighetsfrågor hanteras. Detta kan inkludera riskanalyser, riktlinjer för informationssäkerhet och loggar över åtkomst till NLL. E-hälsomyndigheten kan dessutom genomföra revisioner och stickprov för att kontrollera att aktörerna följer de fastställda säkerhetskraven.

Skyldigheten för E-hälsomyndigheten att försäkra sig om att behörighets- och säkerhetsfrågorna är lösta får därmed – så vitt avser förhandskontroller av anslutande aktörer – anses vara begränsad till mindre ingripande åtgärder som att begära och granska dokumentation på distans för att kontrollera att säkerhetskraven efterlevs. Som redovisats i avsnitt 6.2.2 invände flera remissinstanser att det behövdes ett förtydligande kring ansvarsförhållandena rörande behörighet, åtkomstkontroll och tillsyn, medan regeringen menade att E-hälsomyndigheten borde ta fram rutiner för vilka krav som ska ställas på de aktörer som kommer i fråga för direktåtkomst och att det ankommer på E-hälsomyndigheten att säkerställa att risken för obehörig åtkomst och obefogad spridning minimeras.[18]

E-hälsomyndigheten har tagit fram rutiner och krav för behörighet och åtkomstkontroll. Frågan blir därmed i vilken omfattning myndigheten har inrättat verksamhetsövergripande funktioner för att kontrollera att aktörerna följer de fastställda säkerhetskraven och hur omfattande åtgärder som krävs enligt 8 kap. 2 § NLL. E-hälsomyndigheten kan inte utföra kontroller i vidare omfattning än vad som följer av författningsregleringen. E-hälsomyndigheten bör därmed kunna försäkra sig om att behörighets- och säkerhetsfrågorna är lösta genom att begära in underlag, exempelvis i form av självdeklarationer av vidtagna åtgärder för dataskydd och informationssäkerhet där det framgår att kraven i övrigt är uppfyllda samt att granska detta material. Genom avtal eller överenskommelser kan ytterligare förfaranden för kontroll aktualiseras.

Om mera långtgående åtgärder skulle behövas kan E-hälsomyndigheten göra en anmälan till IVO eller IMY eller vidta åtgärder med stöd av ett avtal eller en överenskommelse mellan parterna.

6.2.8 En möjlighet att övergå till utlämnande på medium för automatiserad behandling

Bedömning: En övergång till utlämnande på medium för automatiserad behandling bör delvis vara möjlig redan enligt gällande rätt och kan minska integritetsrisker genom en prövning i varje enskilt fall. Ansvarsfördelningen tydliggörs därmed eftersom ett utlämnande prövas av den som innehar uppgifterna innan de görs tillgängliga för annan. Dagens särreglering behöver därför inte hindra en sådan anpassning till den användning av informationssystem som numera anses ändamålsenligt.

Lagstiftaren har, på liknande sätt som i exempelvis PDL, ansett att det i NLL behövs särskilda bestämmelser som reglerar i vilka fall direktåtkomst är tillåten till uppgifter i den nationella läkemedelslistan. Med direktåtkomst avses vanligtvis att någon har direkt tillgång till någon annans

[18] Prop. 2017/18:223, s. 178.

register eller databas och på egen hand kan söka efter information, dock utan möjlighet att påverka innehållet i registret eller databasen. I begreppet ligger också att den som är personuppgiftsansvarig för registret eller databasen – här E-hälsomyndigheten – inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av. Gränsdragningen mellan vad som är direktåtkomst och annat utlämnande på medium för automatiserad behandling avgörs av om den aktuella uppgiften kan anses förvarad hos den mottagande myndigheten enligt 2 kap. 3 § andra stycket tryckfrihetsförordningen. Avgörande är således om uppgiften är tillgänglig för mottagaren med tekniskt hjälpmedel som mottagaren själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas.[19] I regeringens ursprungliga förslag till registerförfattning för läkemedelslistan fanns en paragraf (motsvarande 10 § lagen om receptregister) som uttryckligen angav att uppgifter från läkemedelslistan får lämnas ut på medium för automatiserad behandling. Bestämmelsen utmönstrades efter att lagrådet konstaterat att den inte behövdes.

I lagmotiven till NLL anförde regeringen vidare att Högsta förvaltningsdomstolens dom kan tolkas så att den tekniska utformningen av en myndighets system för utlämnande av uppgifter kan bli avgörande och att det är E-hälsomyndigheten som kommer att utforma den tekniska lösningen för utlämnade av uppgifter från registret. Regeringen fann att NLL bör vara så teknikneutral och flexibel som möjligt så att den inte behöver förändras i takt med den tekniska utvecklingen eller till följd av förändringar av myndigheternas behov av att behandla personuppgifter. För det fall att den tekniska lösningen för den nationella läkemedelslistan utformas på så sätt att den är att beteckna som direktåtkomst ansåg regeringen emellertid att det behövs särskilda bestämmelser om att direktåtkomst i sådana fall är tillåten.[20] Av lagmotiven följer därmed att utlämnande även kan ske på medium för automatiserad behandling, exempelvis om den tekniska utvecklingen föranleder sådana rutiner.

I ett senare lagstiftningsärende samma år, rörande socialförsäkringens administration, har regeringen uttalat att IT-utvecklingen gått framåt så att det nu är möjligt att ta fram elektroniska lösningar som på annat sätt än genom direktåtkomst tillgodoser myndigheternas behov av att snabbt kunna ta del av aktuella uppgifter från andra myndigheter och att direktåtkomst bör tillåtas endast när det inte finns andra fullgoda alternativ som kan lösa behovet av informationsförsörjning. Tekniska experter har upplyst att myndigheters informationssystem redan är tekniskt utformade för fråga och svar och att en övergång juridiskt till denna verklighet är ändamålsenlig. I remissvar efterfrågade Integritetsskyddsmyndigheten en fullständig integritetsanalys som belyser de risker för den personliga integriteten som förslaget att gå över till annat utlämnande än direktåtkomst ger upphov till. Regeringen konstaterade emellertid att utlämnande genom direktåtkomst medför generellt sett större integritetsrisker än annat utlämnande, eftersom den utlämnande myndigheten vid direktåtkomst saknar kontroll över vilka uppgifter som lämnas ut vid varje enskilt utlämnande och dessutom kan orsaka problem med överskottsinformation, samt att minskad direktåtkomst därmed bör minska riskerna för den personliga integriteten.[21]

---

[19] HFD 2015 ref. 61 och prop. 2017/18:223, s. 143.
[20] Prop. 2017/18:223 s. 144.
[21] Prop. 2023/24:29, s. 74 och 77 ff..

E-hälsomyndigheten har redan infört utlämnande av uppgifter i den nationella läkemedelslistan genom utlämnande på medium för automatiserad behandling, exempelvis när en privatperson eller ett ombud för denne tar del av sådana uppgifter via en digital tjänst som E-hälsomyndigheten tillhandahåller. Därmed torde viss teknisk funktionalitet redan finnas för en sådan hantering. Genom att redan nu gå vidare på den vägen kan, som regeringen uttalat, riskerna för den personliga integriteten minskas samtidigt som bestämmelsen i 8 kap. 2 § NLL inte är tillämplig vid utlämnande på medium för automatiserad behandling (att E-hälsomyndigheten ska ha försäkrat sig om att behörighets- och säkerhetsfrågorna är lösta). Kontroller sker i varje enskilt fall, till skillnad från direktåtkomst där den som ges sådan åtkomst själv kan söka och hämta uppgifter och en felaktig åtkomst upptäcks först vid punktvisa kontroller i efterhand.

Även när PDL och SVOD gäller för ett informationsutbyte bör en sådan övergång vara möjlig. Här kan emellertid frågor uppkomma kring personuppgiftsansvaret så som det reglerats i 4 kap. 1 § andra stycket SVOD. Där föreskrivs att det även omfattar sådan behandling av personuppgifter som utförs när någon genom *annat elektroniskt utlämnande* i ett enskilt fall *bereder sig tillgång till personuppgifter hos* en annan vårdgivare eller omsorgsgivare". Efter att Högsta förvaltningsdomstolen genom HFD 2015 ref. 61 klargjort vad som menas med annat utlämnande än direktåtkomst kan det dock inte hävdas att någon som begär ett utlämnande på medium för automatiserad behandling bereder sig tillgång till personuppgifter *hos* en annan vårdgivare. Det är endast den vårdgivare som motar begäran om utlämnande som har uppgifterna hos sig. Den begärande myndigheten får tillgång till uppgifterna först efter att de avsänts från den utlämnande vårdgivaren.

6.3 Egenskapsintyg

Bedömning: Inom behörighetsinfrastrukturen bör egenskapsintyg kunna användas för att på ett standardiserat sätt ange att en aktörs tekniska komponenter har vissa egenskaper, exempelvis att ett visst avtal tecknats. Regleringen av egenskapsintyg bör främst ske inom det tekniska ramverket och – i förekommande fall – genom områdesspecifika villkor. Digg bör emellertid enligt regelverket för behörighetsinfrastrukturen ges rätt att ingripa om en områdesspecifik användning av egenskapsintyg skulle innebära rättsliga eller praktiska risker för infrastrukturen som helhet.

I vissa tekniska standarder som används vid elektronisk identifiering och behörighetskontroll förekommer så kallade *trust marks*. De är emellertid inte märken i traditionell juridisk mening, det vill säga kännetecken som är avsedda att uppfattas av en användare i ett visuellt gränssnitt. I stället avses digitalt stämplade metadata som behandlas automatiserat och som beskriver egenskaper hos tekniska komponenter i en infrastruktur. Dessa metadata, i det följande benämnda egenskapsintyg, är att anse som urkunder enligt 14 kap. 1 § brottsbalken och omfattas därför, på samma sätt som identitetsintyg och behörighetshandlingar, av straffansvar för urkundsförfalskning och osant intygande.

Inom infrastrukturen för elektronisk identifiering planerar Digg att använda egenskapsintyg för att informera förlitande parter om vilken tillitsnivå som tillämpas i det enskilda fallet enligt Tillitsramverket för Svensk e-legitimation. Digg planerar också att med egenskapsintyg informera om att en part tecknat ett visst anslutningsavtal, t.ex. Diggs Anslutningsavtal för Förbetald e-legitimering. Medan identitetsintyg innehåller uppgifter om vem en individ är och behörighetshandlingar innehåller uppgifter om en individs eller en digital aktörs juridiska

behörighet, ska egenskapsintyg innehålla uppgifter om egenskaper hos tekniska komponenter inom infrastrukturen i syfte att underlätta en ändamålsenlig användning av behörighetsinfrastrukturen. Alla de nämnda typerna av intyg består således av digitala data som en aktör har skrivit under eller stämplat digitalt.

Egenskapsintyg kan nyttjas även inom behörighetsinfrastrukturen. De är emellertid, som framgått, inte till för att förse med uppgifter om en medarbetares eller en digital aktörs juridiska behörighet (till exempel firmateckningsrätt, fullmakt, visst förordnande eller reglerad yrkesroll). Sådana uppgifter lämnas i behörighetshandlingar och för dem bör andra regler och rutiner gälla än för egenskapsintyg.

På nuvarande stadium i arbetet är det delvis oklart i vilka sammanhang och för vilka syften det kan vara ändamålsenligt att införa egenskapsintyg. Frågan kan emellertid belysas genom exempel. På samma sätt som Digg avser att använda egenskapsintyg inom infrastrukturen för elektronisk identifiering för att ange om anslutningsavtal för exempelvis Förbetald e-legitimering tecknats för en viss aktörs komponenter, så bör egenskapskapsintyg kunna ge besked om med vilken federationsområdesansvarig som avtal tecknats för behörighetsinfrastrukturen. Eftersom det är respektive federationsområdesansvarig som ansluter utfärdare av behörighetshandlingar och förlitande parter kan det visa sig lämpligt att dessa egenskapsintyg ställs ut av dem. Med utgångspunkt från vad som framkommer vid en närmare analys får det visa sig om denna hantering behöver regleras i regelverket för behörighetsinfrastrukturen, exempelvis när det gäller hur de får utfärdas och vilket ansvar det innebär att ställa ut ett sådant intyg. Det kan emellertid visa sig vara tillräckligt att bara reglera egenskapsintyg i den tekniska bilagan till regelverket för behörighetsinfrastrukturen och att falla tillbaka på det straffansvar som kan inträda vid exempelvis ett osant intygande.

Ett annat exempel skulle kunna vara att Inspektionen för vård och omsorg (IVO) stämplar metadata (ställer ut egenskapsintyg) som anger att en aktör enligt IVO:s vårdgivarregister är en vårdgivare som har en viss angiven kod enligt registret. IVO skulle kunna tilldelas en sådan uppgift genom förordning eller – efter delegation – en myndighetsföreskrift, så att det inte behöver införas någon ytterligare part i avtal för behörighetsinfrastrukturen. Sådana uppgifter om en ansluten aktör lämnas som framgått inte i behörighetshandling eftersom uppgiften inte rör en medarbetares eller en digital aktörs juridiska behörighet. Det är fråga om en uppgift som rör en part såsom utfärdare av behörighetshandlingar eller förlitande part och därmed dennes tekniska komponenter – vad som ibland kallas organisationsattribut. Eftersom vårdgivare och öppenvårdsapotek ansluts till en federationsområdesansvarig inom området för hälso- och sjukvård och en uppgift av detta slag sannolikt inte efterfrågas inom andra områden kan det visa sig ändamålsenligt att dessa egenskapsintyg ställs ut av den federationsområdesansvarige och blir föremål för reglering där om ytterligare regler krävs än vad som följer av tekniskt ramverk.

E-hälsomyndigheten genomför, enligt 8 kap. 2 § lagen (2018:1212) om nationell läkemedelslista, åtgärder för att försäkra sig bland annat om att behörighets- och säkerhetsfrågorna är lösta på tillfredsställande sätt. Det bör vara möjligt för myndigheten att, efter genomförda åtgärder, utfärda ett egenskapsintyg som anger att åtgärder vidtagits. Ett sådant intyg kan därefter användas av E-hälsomyndigheten själv vid direktåtkomst. Om intyget används enbart internt kan regleringen i tekniskt ramverk anses tillräcklig, men om andra aktörer ska använda intyget kan ytterligare

reglering behövas, exempelvis om hur ansvaret fördelas om en felaktig uppgift finns i intyget. Är bara E-hälsomyndigheten användare av dessa egenskapsintyg behövs sannolikt ingen särskild reglering utöver vad som följer av tekniskt ramverk. Krävs särskild reglering bör detta ses som en fråga om områdesspecifik reglering.

Ska egenskapsintyg istället nyttjas av andra vårdgivare kan det visa sig att det inte räcker med regler i tekniskt ramverk utan att det också behövs vissa regler exempelvis för att fördela ansvar. En områdesspecifik tillämpning av detta slag bör emellertid inte regleras i regelverket för behörighetsinfrastrukturen på annat sätt än att Digg bör ha rätt att ingripa om hanteringen skulle visa sig skadlig för behörighetsinfrastrukturen, praktiskt eller juridiskt.

Används en behörighetshandling, som utfärdats av en aktör som anslutit sig till en federationsansvarig för hälso- och sjukvårdsområdet, inom ett annat federationsområde krävs sannolikt inte egenskapsintyg för hälso- och sjukvården. Istället nyttjas själva behörighetshandlingen för att genomföra en sedvanlig behörighetskontroll, innan en medarbetare eller en digital aktör ges tillträde eller får ut uppgifter.

Egenskapsintyg av beskrivna områdesspecifika slag bör således inte regleras i regelverket för behörighetsinfrastrukturen, utöver det som kan komma att följa av tekniskt ramverk. Det bör istället vara en uppgift för den federationsområdesansvarige, dock att Digg bör ha rätt att ingripa om en områdesspecifik hantering visar sig vara skadlig för behörighetsinfrastrukturen.

Utöver denna användning av intyg för att ange egenskaper hos tekniska komponenter inom infrastrukturen har frågan väckts om egenskapsintyg ska kunna införas även som bevis för att kraven på informationssäkerhet och dataskydd är uppfyllda. Till skillnad från området för elektronisk identifiering, där tillitsramverket för Svensk e-legitimation möjliggör en enhetlig användning, varierar förutsättningarna för juridisk och organisatorisk behörighet i hög grad mellan olika verksamheter och användningsområden. Mot denna bakgrund är det inte ändamålsenligt att försöka utforma motsvarande ramverk för behörighetsinfrastrukturen.

Det finns som framgått av avsnitt 6.2.3 inte någon generell skyldighet för myndigheter eller företag att kontrollera andras informationssäkerhet. Varje organisation ansvarar för sin informationssäkerhet. När direktåtkomst tillämpas såsom inom hälso- och sjukvården bryts emellertid denna gräns delvis igenom, se bland annat 8 kap. 2 § NLL där det föreskrivs att direktåtkomst till uppgifter i den nationella läkemedelslistan får ges först sedan E-hälsomyndigheten försäkrat sig om att behörighets- och säkerhetsfrågorna är lösta på ett sätt som är tillfredsställande och att behörigheten är begränsad för den som ska få direktåtkomst. För att underlätta sådana kontroller har E-hälsomyndigheten och Inera fört fram att det behöver utarbetas gemensamma krav på informationssäkerhet och dataskydd för att få hantera behörighetsinformation inom behörighetsinfrastrukturen. I stället för ett tillitsramverk av det slag som införts för elektronisk identifiering skulle gemensamma krav och principer för informationssäkerhet och dataskydd kunna utarbetas med olika skyddsnivåer för olika behov. Dessa krav skulle normera hur behörighetsinformation skapas, förvaltas och förmedlas på enhetligt sätt.

Som framgått av avsnitt 6.2 bör fundamentet inte påverkas av områdesspecifik särreglering. Fördelningen av ansvaret för informationssäkerhet och dataskydd bryts normalt inte igenom där

sedvanliga behörighetskontroller sker. På samma sätt som för infrastrukturen för elektronisk identifiering bör det därmed vara tillräckligt med den reglering som följer av ett regelverk för behörighetsinfrastrukturen och gällande rätt. Digg föreslår därför inte att det ska utarbetas något nytt ramverk för informationssäkerhet och dataskydd och inte heller att egenskapsintyg ska införas som bevisa för en viss nivå av informationssäkerhet och dataskydd hos en aktörs tekniska komponenter. Finner en federationsområdesansvarig att en sådan ytterligare användning av egenskapsintyg är nödvändig inom det området finns det emellertid inte hinder mot att ta tillvara behörighetsinfrastrukturens tekniska funktionalitet, bara det inte innebär rättsliga eller praktiska risker för infrastrukturen som helhet. En sådan användning av egenskapsintyg får emellertid den federationsområdesansvarige och anslutna parter till denna, hantera själva och reglera specifikt om det krävs.

Sammanfattningsvis utgör egenskapsintyg en teknisk och rättslig konstruktion för att på ett standardiserat sätt ange vissa egenskaper hos tekniska komponenter som används av en ansluten part. Egenskapsintygen kan bidra till ökad interoperabilitet och transparens inom behörighetsinfrastrukturen. Användningen bör dock begränsas till uppgifter om tekniska och organisatoriska egenskaper, inte om juridisk behörighet. Egenskapsintyg bör som huvudregel utfärdas av federationsområdesansvarig, men även andra aktörer kan ges uppdrag att utfärda sådana intyg genom författning eller uppdrag (exempelvis IVO för vårdgivare). Regleringen bör i huvudsak ske inom det tekniska ramverket eller genom områdesspecifika bestämmelser, men Digg bör enligt regelverket ha rätt att ingripa om en områdesspecifik hantering skulle motverka infrastrukturen eller medföra rättsliga eller praktiska risker.

6.4 Fördelning av juridiskt ansvar – en nyckel till en balanserad lösning

Fördelningen av ansvar inom den föreslagna behörighetsinfrastrukturen behöver bedömas utifrån flera rättsliga utgångspunkter när parterna ska samverka inom ett tekniskt och rättsligt ekosystem. Ansvar kan uppkomma enligt såväl offentligrättsliga och civilrättsliga som dataskyddsrättsliga, och processrättsliga regler. Samma händelseförlopp kan därmed ge upphov till olika former av ansvar, samtidigt som infrastrukturen måste fungera som en sammanhängande helhet. Vid bedömningen härav blir det vanligtvis avgörande vilken aktör som faktiskt haft kontroll över den behörighetshandling, den tekniska komponent eller det händelseförlopp där ett fel eller en brist uppstått.

Behörighetsinfrastrukturen kan härvid, något förenklat, beskrivas som tre skikt. Det första skiktet avser den materiella behörigheten, det vill säga den bakomliggande rättsliga grund som avgör om en medarbetare eller digital aktör är behörig att vidta en viss åtgärd. Det andra skiktet avser själva behörighetshandlingen, dess äkthet, giltighet och informationsinnehåll som på ett standardiserat sätt ska förmedla information om juridisk behörighet. Det tredje skiktet utgörs av den digitala infrastruktur som införs för att etablera en behörighetsinfrastruktur, dvs. den tekniska och organisatoriska ram som måste utformas tillräckligt säkert och på ett ömsesidigt fungerande sätt. Fördelningen av ansvar kan därmed delvis avvika från vad som brukar gälla i mera traditionella sammanhang.

I behörighetsinfrastrukturen kan en metod vara att ge en aktör ansvar för *det sätt* på vilket denne upprättar behörighetshandlingar eller kontrollerar sådana, utan att samtidigt garantera eller annars bära ett närmast strikt ansvar för att alla uppgifter om behörighet som lämnas i ett intyg är korrekta och aktuella. Detta kan något förenklat beskrivas som ett ansvar för metoden, dvs. att uppfylla vissa strikt angivna krav på hantering. Som exempel på ett sådant metodansvar kan nämnas det som en e-legitimationsutfärdare bär enligt eIDAS-förordningen. Fastställda rutiner, kontroller och standarder måste ha följts. Blir det fel av annat skäl uppkommer normalt inte en skadeståndsskyldighet för utfärdaren av e-legitimationen. I andra sammanhang kan en aktör bär det fulla ansvaret för resultatet, här uppgifter som lämnats i en behörighetshandling. Som exempel kan nämnas att en fullmaktsgivare normalt får stå för den fullmaktsförklaring en fullmakt innehåller, oberoende av bakomliggande register eller liknande.

För administrationen av den digitala infrastrukturen kan Federationsområdesansvarig åläggas ett ansvar för metoden att på ett säkert sätt administrera det metadata som deltagarna i federationen behöver för att kommunicera. För detta kan ett enhetligt regelverk utformas som varje Federationsområdesansvarig inom infrastrukturen är skyldig att efterleva. Brister i denna hantering kan leda till ansvar, se följande tabell över frågor som aktualiseras inom behörighetsinfrastrukturen och hur ansvaret kan komma att fördelas och regleras inom ramen för befintlig rätt eller avtal mellan parterna.

Ansvarstyp	Utfärdare av behörighetshandlingar	Förlitande part	Federations-områdesansvarig
Civilrättsligt	Kan ansvara för oaktsamhet alternativt för resultatet beroende på hur ansvaret utformas i regelverket.	Kontrollerar intygets äkthet, att det ställts ut av behörig och att materiella behörighetsregler uppfylls.	Ansvarar för att tillhandahålla grundläggande tjänster och att följa de regler som ställts upp för administration av metadata.
Offentlig-rättsligt	Myndighet: ansvar enligt förvaltningslag och skadeståndslag samt regelverk för behörighetsinfrastrukturen Privat: kan omfattas av offentlig reglering genom avtal och regelverket.	Myndighet: ansvar vid myndighetsutövning som grundas på intyget. Privat: ansvar enligt områdesspecifika krav.	Ansvarar för att tillhandahålla grundläggande tjänster och att följa de regler som ställts upp för administration av metadata.

Ansvarstyp	Utfärdare av behörighetshandlingar	Förlitande part	Federations-områdesansvarig
Dataskydds-rättsligt	Personuppgiftsansvarig för behandling av personuppgifter för. Ska säkerställa laglighet, korrekthet och säkerhet (kan vara särreglerat i registerförfattning)	Personuppgiftsansvarig för behandling vid verifiering och användning (kan vara särreglerat i registerförfattning)	Personuppgiftsansvarig för de grundläggande funktioner och tjänster denne tillhandahåller
Bevisrättsligt	Svarar för att intyget utfärdats korrekt och enligt gällande krav	Står själv risken för fel i denna hantering	Svarar för att funktioner och tjänster som denne tillhandahåller sköts enligt regelverket.

Tabell 3: Frågor som aktualiseras inom behörighetsinfrastrukturen och hur ansvaret kan komma att fördelas och regleras inom ramen för befintlig rätt eller avtal mellan parterna.

Civilrättsligt ansvar inom behörighetsinfrastrukturen kan således bestå antingen i ansvar för oaktsamhet eller ansvar för resultat. Detta är förenligt med principerna i svensk civilrätt, där ansvar för oaktsamhet ofta är kopplat till att en aktör inte har följt fastställda rutiner eller standarder, medan ansvar för resultat innebär att en aktör är skyldig att garantera att en viss prestation eller ett visst resultat uppnås. Offentligrättsligt ansvar följer av förvaltningslagen och skadeståndslagen, samt områdesspecifika regelverk. Dataskyddsrättsligt ansvar regleras av GDPR och registerförfattningar. Aktörer inom behörighetsinfrastrukturen är personuppgiftsansvariga för den behandling av personuppgifter som sker inom ramen för deras verksamhet. Informationssäkerhetsrättsligt ansvar följer av flera olika lagar och andra författningar, bland annat av lagen (2018:1174) om informations-säkerhet för samhällsviktiga och digitala tjänster. Samtliga aktörer inom behörighetsinfrastrukturen måste vidta de tekniska och organisatoriska åtgärder som får anses nödvändiga för att hantera de egna risker som annars hotar säkerheten i nätverk och informationssystem. Ansvaret för en myndighet att processuellt agera korrekt följer av bland annat förvaltningslagen och anknytande områdesspecifik särreglering.

För frågan om hur ansvaret bör fördelas är det dessutom av betydelse om den som utfärdar en behörighetshandling ska lämna uppgifter om egna medarbetare, exempelvis i form av en fullmakt eller ett förordnande, eller om utfärdaren ska tillhandahålla behörighetshandlingar för andra aktörers medarbetare, exempelvis i form av utdrag ur publicitetsregler med behörighetsuppgifter eller register över lämnade fullmakter som en aktör för med stöd av författning eller avtal mellan berörda parter. Det kan framstå som naturligt att bära ett närmast strikt ansvar för uppgifter som lämnas om egna medarbetare medan kontrollen över behörighetshanteringen blir mera begränsad för den som lämnar utdrag ur publicitetsregister, fullmaktsregister eller liknande. I de senare fallen

kan det vara naturligt med ett mera begränsat ansvar där det är tillräckligt att ha följt regler i författning eller avtal om metoden för kontroller med mera (jfr eIDAS-förordningen).

När aktörer av vitt skilda slag ska anslutas, bland annat som utfärdare av behörighetshandlingar, behöver det vidare beaktas att högre krav kan ställas på en aktör som har en betydande Kompetens inom teknik och informationssäkerhet, betydande resurser och redan åtnjuter ett högt förtroende men att samma krav inte kan ställas på exempelvis en liten kommun utan egna jurister och IT-experter. För att balansera dessa aktörers olika förutsättningar att möta krav inom en behörighetsinfrastruktur kan det juridiska ansvaret behöva anpassas till praktiska realiteter. Har en aktör begränsade förutsättningar att uppfylla rigorösa krav på informationssäkerhet bör denne kanske bara utfärda behörighetshandlingar för egna medarbetare baserat på ett närmast strikt ansvar för uppgifterna (jfr fullmakt), medan redan betrodda aktörer som har betydande resurser och kompetens inom berörda områden kan utfärda behörighetshandlingar för andras medarbetare, på liknande sätt som utfärdare av e-legitimationer. Närmare överväganden av dessa frågor behöver göras beträffande varje aktör och varje konkret tillämpning för sig eftersom förutsättningarna kan variera kraftigt.

Att infrastrukturen bör ta sikte på stöd för annat utlämnande än genom direktåtkomst kan enklast beskrivas genom en jämförelse med ett arkiv i traditionell fysisk miljö. Om någon enstaka känd, särskilt betrodd medarbetare hos en annan aktör vill ha uppgifter ur arkivet kan den som ansvarar för det ha så god kännedom om medarbetaren och så grundmurat förtroende för denne att han eller hon själv får gå in i arkivet och hämta handlingar istället för att be en arkivarie om att få vissa handlingar utlämnade och vänta på att arkivarien hämtar handlingarna och bedömer om de kan lämnas ut. I takt med att allt fler vill ha uppgifter ur arkivet blir det emellertid tydligt att det inte är lämpligt att släppa in andras medarbetare så att de själva får hämta de handlingar de behöver. Eventuella kontroller sker då först i efterhand och hindrar således inte ett missbruk. De möjliggör endast att oegentligheter kan uppdagas och beivras när skadan redan skett. En sådan oönskad utveckling blir följden om allt fler ges direktåtkomst till känsliga samlingar med personuppgifter, såsom när fler vårdgivare ges direktåtkomst.

7 En ändamålsenlig försöksverksamhet

Utformningen av en nationell behörighetsinfrastruktur bör grundas på praktiskt genomförbara och rättsligt förankrade pilotfall inom användningsområden där det redan finns en etablerad rättslig normering, ett brett behov av förenklade behörighetskontroller och ett tekniskt kunnande som lämpar sig för en stegvis digitalisering. Syftet bör vara att visa hur manuella behörighetskontroller kan ersättas med digitala, maskinläsbara och standardiserade behörighetshandlingar och automatiserade kontroller, utan avkall på rättsverkan, ansvarsfördelning eller informationssäkerhet.

En ändamålsenlig försöksverksamhet bör således kännetecknas av att det finns en entydig och rättsligt bindande källa eller rättslig reglering som fastställer behörigheten, att kontrollmomentet motsvarar ett redan välkänt och frekvent förekommande rättsligt förfarande och att pilotfall är av sådan praktisk betydelse att en digitalisering leder till påtagliga effektivitets- och tillförlitlighetsvinster för både myndigheter och enskilda. Mot denna bakgrund kan kontrollen av ställföreträdare för juridiska personer, särskilt aktiebolag, vara ett lämpligt pilotfall. Här föreligger ett tydligt, lagreglerat förhållande mellan registrerad uppgift och rättsföljd, förlitande parter med långtgående behov av korrekt information och en befintlig myndighetsinfrastruktur – Bolagsverkets aktiebolagsregister – som redan i dag bär upp rättsverkningarna av de uppgifter som kontrolleras. Andra exempel kan vara behörighetshandlingar beträffande rektorer inom skolväsendet och vårdgivare och den vård de tillhandahåller.

De exempel som redovisas i detta kapitel är emellertid principiella och illustrativa. De redovisar inte överenskomna eller planerade pilotprojekt hos någon av de berörda aktörerna, utan syftar endast till att visa hur den föreslagna behörighetsinfrastrukturen skulle kunna tillämpas i praktiken inom vissa typer av verksamheter. Beskrivningarna innebär inte att utredningen tar ställning i sektorsspecifika tolkningsfrågor eller föregriper kommande ställningstaganden från ansvariga myndigheter. En faktisk försöksverksamhet behöver utformas och förankras i fortsatt dialog med berörda aktörer och utgå från fördjupade analyser inom respektive rättsområde.

7.1 Ställföreträdare för juridiska personer

7.1.1 Ett renodlat exempel på sedvanliga behörighetskontroller

Frågan om vem eller vilka som är legala ställföreträdare för ett aktiebolag, och därmed kan teckna aktiebolagets firma, är ett klassiskt och renodlat exempel på juridisk behörighetskontroll. Behörigheten för en ställföreträdare omfattar inte bara att skriva under handlingar utan även muntliga rättshandlingar och att få tillträde till digitala tjänster för att ta del av uppgifter och att agera för aktiebolagets räkning.

Uppgifter om bland annat styrelse, särskilda firmatecknare och hur firman tecknas finns i det aktiebolagsregister som förs av Bolagsverket. Uppgifterna är normalt rättsligt bindande i förhållande till en förlitande part och utgör läroboksexemplet för hur tredje man ska kunna få korrekta och aktuella uppgifter om en medarbetares rätt att agera för en huvudmans räkning. Inom en behörighetsinfrastruktur utgör detta ett rättsligt väl avgränsat fall av sedvanlig behörighetskontroll. Här finns en normativ grund, en offentlig registrering och ett tydligt behov av att göra

behörighetskontroller automatiserat med hög tillförlitlighet. Därför är kontroller av om en individ är behörig att, själv eller i förening med annan, företräda ett aktiebolag i egenskap av ställföreträdare ett ändamålsenligt pilotfall för en behörighetsinfrastruktur. Bolagsverket har dessutom en hög mognadsgrad för en sådan hantering och har redan idag vissa funktioner för att digitalt leverera intyg som man kan hanteras automatiserat.

En samordnad hantering inom hela samhället av behörighetshandlingar för ställföreträdare innebär att motsvarande rättsliga underlag som i pappersmiljö används manuellt kan nyttjas helt automatiserat. Här skapas således en direkt motsvarighet mellan den analoga och den digitala världen. De som är registrerade som ställföreträdare får, genom en maskinläsbar och stämplad eller underskriven behörighetshandling, möjlighet att visa sin behörighet utan manuella slagningar.

7.1.2 Frågor som behöver genomlysas

För att juridiska behörighetskontroller beträffande ställföreträdare för aktiebolag ska bli möjliga med stöd av den föreslagna behörighetsinfrastrukturen behöver emellertid ett antal frågor genomlysas, bland annat den rättsliga grunden, intygens utformning, den tekniska representationen av ställföreträdarskap och hur regler för firmateckningsrätt ska uttryckas, ansvarsfördelningen mellan parter, de krav som ska gälla för verifiering, säkerhet och integritet samt hur omvandlingen från analoga till digitala kontrollmetoder ska genomföras.

När det gäller den rättsliga grunden finns en tydlig reglering i aktiebolagslagen (2005:551) och annan associationsrättslig registreringslagstiftning samt förordningen (2007:1110) med instruktion för Bolagsverket. Ett bolags registrerade uppgifter om firmateckningsrätt och ställföreträdare ska anmälas av bolaget självt och registreras efter sedvanlig kontroll av formella förutsättningar. Den centrala principen — som utvecklats genom såväl lag som praxis — är att det är de registrerade uppgifterna som är rättsligt bindande i förhållande till tredje man. Bolagsverket har således ett myndighetsansvar att föra register som är korrekta i den meningen att de återspeglar de uppgifter som lagligen ska registreras och som bolaget själv har att underrätta myndigheten om. Detta ansvar omfattar korrekt registrering, riktiga beslut, materiell och formell handläggning samt att uppdateringar sker utan dröjsmål.

Registrerade uppgifter om ställföreträdare har rättsverkan. Den förlitande parten ska kunna utgå från att uppgiften är korrekt, under förutsättning att inte ond tro föreligger. Denna reglering innebär inte att Bolagsverket bär ett civilrättsligt garantiansvar för att uppgiften materiellt sett motsvarar verkliga interna förhållanden. Däremot har Bolagsverket ett offentligrättsligt ansvar för att registreringen sker korrekt och enligt gällande normer. För en behörighetsinfrastruktur innebär detta att behörighetshandlingarnas rättsverkan bärs upp av den underliggande registreringsordningen. Det är inte ett nytt intygsinstitut utan en digitaliserad tillämpning av gällande rätt. En stämplad behörighetshandling som utfärdas med stöd av behörighetsinfrastrukturen utgör ett strukturerat utlämnande av redan registrerade uppgifter som ska vara korrekta enligt registret vid tidpunkten för utlämnandet.

Bolagsverket ansvarar däremot inte för hur intyget används, tolkas eller integreras i mottagarens system. Denna uppgift vilar på mottagaren i enlighet med gällande civilrättsliga och offentligrättsliga principer. På samma sätt som underleverantörer till förlitande parter utvecklat

tjänster för att kontrollera individers identitet får det antas att ett införande av behörighetshandlingar för ställföreträdare också kommer att leda till tjänster med stöd av vilka förlitande parter normalt kan göra själva behörighetskontrollen helt automatiserat.

Denna hantering illustrerar väl den principiella modell som behörighetsinfrastrukturen bör bygga på när uppgifter om behörighet hämtas ur så kallade publicitetsregler som förs av myndigheter och där myndigheten ansvarar för att ha agerat i enlighet med föreskrivna metoder eller förfaranden. Dessa behörighetshandlingar kan därmed fungera som exempel på hur behörighetshandlingar från publicitetregister bör standardiseras och tillhandahållas strukturerat så att de ger det stöd som behövs för att kunna göra en juridisk behörighetskontroll.

7.2 Rektors behörighet inom skolväsendet

7.2.1 Ytterligare exempel på sedvanliga behörighetskontroller

Frågan om vem som är rektor för en skolenhet är ett tydligt och renodlat exempel på sedvanlig behörighetskontroll inom offentlig verksamhet. Rektor företräder huvudmannen vid en skolenhet och har ett långtgående ansvar enligt skollagen, däribland beslutanderätt i pedagogiska frågor, elevärenden, ordningsfrågor och förvaltning av vissa resurser. Rektors behörighet omfattar därför även tillträde till digitala tjänster, administrativa system och möjligheten att föra talan eller fatta beslut å huvudmannens vägnar inom sitt ansvarsområde.

Skolverkets allmänna skolenhetsregister regleras genom förordningen (2020:833) om skolenhetsregister, som utgör en officiell och normerande informationskälla avsedd att ge en samlad och enhetlig bild av landets skolhuvudmän, skolenheter och vissa centrala roller inom dessa, bland annat vem som är rektor för en skolenhet.

Enligt 6 § i förordningen får Skolverket behandla personuppgifter i registret bl.a. när det är nödvändigt för att kontrollera verksamhetsföreträdares identitet och behörighet. En rektor är enligt skollagen en sådan verksamhetsföreträdare och är den funktion som har det yttersta ansvaret för den pedagogiska ledningen vid en skolenhet. Registret har således ett uttryckligt ändamål kopplat till identitets- och behörighetskontroll av just de roller som utgör bärande moment i en skolhuvudmans rättsliga och organisatoriska struktur.

Uppgifterna i registret lämnas normalt av huvudmännen själva genom obligatoriska rapporteringsrutiner medan registret förs av en statlig myndighet i enlighet med författning och är föremål för offentlig kontroll, administrativa rutiner och rättsligt reglerade ändamål. Detta ger registret en tyngd, även om det formellt inte har samma rättsverkan som exempelvis aktiebolagsregistret. Vid bedömningen av om registret kan ge en tillräckligt säker grund för behörighetshandlingar inom ramen för behörighetsinfrastrukturen är bland annat följande av intresse. Registret innehåller uppgift om vem som är utsedd till rektor för en viss skolenhet, och uppgiften är knuten till en definierad organisatorisk enhet och beslutad av huvudmannen. Rollen har ett rättsligt reglerat innehåll av samma typ som information vilken inom andra sektorer betraktas som en grund för formell behörighet. Rektor utses genom ett formellt beslut hos huvudmannen och uppgiftsskyldigheten innebär att huvudmännen fortlöpande ska rapportera

förändringar. Återstående risk är främst fördröjning i rapportering, men denna risk förekommer i alla register där ansvariga aktörer ska rapportera förändringar.

Skolverket ansvarar för registerhållning, medan skolhuvudmannen ansvarar för att uppgifterna är korrekta och aktuella. Denna ansvarsfördelning motsvarar strukturen i flera andra offentliga register som traditionellt används som källa för juridiska behörighetskontroller. Uppgifterna kan göras tillgängliga i maskinläsbar form. För en modern behörighetsinfrastruktur är möjligheten att tillhandahålla strukturerad och automatiskt verifierbar information avgörande. Inga bestämmelser i förordningen hindrar ett sådant tillgängliggörande genom standardiserade gränssnitt. Jämför man registret med exempelvis Bolagsverkets aktiebolagsregister är rättsverkan inte identisk, men funktionellt är uppgiften om rektor en normerande och rättsligt styrande uppgift, som dessutom ofta utgör beslutsunderlag i myndighetsutövning. Det gör att registret, på en funktionsbaserad nivå, är en lämplig och legitim källa för behörighetshandlingar.

En digital hantering av dessa uppgifter innebär att exakt samma rättsliga underlag som tidigare funnits i analoga eller manuellt distribuerade register görs tillgängligt i maskinläsbar form. Rektor (vars identitet är känd genom e-legitimation) kan då, genom en stämplad och maskinläsbar behörighetshandling baserad på Skolverkets registeruppgifter, visa sin behörighet utan att den förlitande parten behöver begära utdrag eller manuella bekräftelser från huvudmannen. Detta möjliggör en direkt och säker motsvarighet mellan den analoga och digitala kontrollkedjan.

7.2.2 Frågor som behöver genomlysas

För att juridiska behörighetskontroller av rektors ställning och behörighet vid en skolenhet ska kunna genomföras med stöd av den föreslagna behörighetsinfrastrukturen behöver ett antal frågor analyseras närmare. Dessa omfattar bland annat den rättsliga grunden, utformningen av behörighetshandlingar, den tekniska representationen av rektorsrollen, ansvarsfördelningen mellan berörda aktörer, krav på verifiering, säkerhet och integritet samt hur övergången från analoga till digitala kontrollmetoder ska genomföras.

När det gäller den rättsliga grunden finns en tydlig reglering i skollagen (2010:800), förordningen (2020:833) om skolenhetsregister samt skolverkets föreskrifter och uppdrag. Av skollagen följer att varje skolenhet ska ledas av en rektor som utses av huvudmannen och som ansvarar för det pedagogiska arbetet samt för ett antal offentligrättsliga beslut. Huvudmannen ansvarar vidare för att skolenhetsregistret tillförs riktiga och aktuella uppgifter, inklusive uppgift om rektor. Den centrala principen — som framgår av både lag och registerförordning — är att uppgifter som huvudmannen anmält och som förts in i registret utgör den officiella uppgiften gentemot tredje part.

Skolverket har ett myndighetsansvar att föra ett korrekt register i den meningen att det ska avspegla de uppgifter som huvudmannen är rättsligt skyldig att lämna. Detta omfattar korrekt hantering, formell och materiell registrering samt uppdatering utan dröjsmål. Registret har offentlig rättsverkan i förhållande till de uppgifter som ska vara registrerade. Förlitande parter ska därmed kunna utgå från att uppgiften om rektor är korrekt, under förutsättning att inte särskilda skäl föreligger som gör att uppgiften bör ifrågasättas. Skolverket ansvarar dock inte för att uppgiften materiellt sett återspeglar interna organisatoriska förhållanden hos huvudmannen; det

offentligrättsliga ansvaret avser att registrering sker korrekt enligt gällande normer med de uppgifter som huvudmannen har lämnat.

För en behörighetsinfrastruktur innebär detta att behörighetshandlingarnas rättsverkan följer av den underliggande registreringsordningen. Intyget blir inte ett nytt rättsinstitut utan en digitaliserad, strukturerad återgivning av de uppgifter som finns registrerade vid tidpunkten för utlämnandet. En stämplad behörighetshandling avseende rektor vid en skolenhet utgör därmed ett kontrollerbart utlämnande av redan registrerade uppgifter som ska återges korrekt i enlighet med registrets innehåll.

Skolverket ansvarar däremot inte för hur mottagaren använder eller tolkar intyget eller hur det integreras i mottagarens system och processer. Dessa delar faller på den förlitande parten utifrån gällande offentligrättsliga och civilrättsliga principer. På samma sätt som tjänster utvecklats för automatiserad identitetskontroll kan det förväntas att införandet av behörighetshandlingar för rektorsstatus leder till tekniska tjänster som möjliggör automatiserad kontroll av behörighet gentemot skolenhetsregistret.

Denna ordning utgör ett tydligt exempel på hur behörighetshandlingar från offentliga register med publicitetsverkan bör struktureras och tillhandahållas inom behörighetsinfrastrukturen. Genom att registrens rättsverkan och myndigheternas ansvar bevaras kan digitala intyg användas som ett rättssäkert underlag vid juridiska behörighetskontroller.

7.3 Digitala aktörers behörighet vid administrering av kataloger

7.3.1 Exempel på behörighetskontroller beträffande digitala aktörer

Inom hälso- och sjukvården finns och utvecklas löpande digitala tjänster för informationshantering och uppgiftslämnande mellan vårdgivare, statliga myndigheter och andra aktörer. Exempel går att finna i de nationella kataloger och register där vårdgivare självständigt administrerar information om sin egen verksamhet. Sådana kataloger är avsedda att samla grundläggande uppgifter om vårdgivare och deras verksamheter så att dessa kan återanvändas i olika digitala tjänster. Uppgifter om vårdgivare kommer i en sådan ordning typiskt att lämnas eller uppdateras av de ansvariga aktörerna själva, inom ramen för de regler och tekniska lösningar som fastställs i respektive genomförande.

Sådana uppgifter kan administreras av vårdgivaren genom e-tjänster eller via tekniska gränssnitt. I en sådan modell agerar digitala aktörer, till exempel verksamhetssystem eller andra tekniska komponenter, för vårdgivarens räkning. Vårdgivaren står fortsatt som ansvarig för riktigheten i uppgifterna, men det uppstår ett behov av att på ett strukturerat sätt kunna visa att en viss digital aktör är behörig att lämna uppgifter för en viss vårdgivare.

En behörighetshandling för en digital aktör kan i detta sammanhang användas för att koppla samman vårdgivaren, en viss teknisk komponent och ett avgränsat uppdrag, till exempel att uppdatera vissa uppgifter i ett register. Behörighetshandlingen skulle då kunna användas av den

registerförande aktören som underlag för att kontrollera att uppgifterna lämnas genom en behörig digital aktör.

7.3.2 Frågor som behöver genomlysas när den digital aktören ska agera

För att juridiska behörighetskontroller av vårdgivares behörighet att låta digitala aktörer agera för deras räkning vid uppdatering av uppgifter i en nationell katalog ska kunna genomföras med stöd av en behörighetsinfrastruktur krävs en närmare analys av flera sammanhängande frågor. Det handlar bland annat om hur relationen mellan vårdgivare, fysisk person, digital aktör och teknisk komponent ska beskrivas i behörighetshandlingar, hur spårbarheten ska säkerställas över tid så att det går att klarlägga vem eller vad som faktiskt har agerat, hur ansvarsfördelningen mellan vårdgivare, registerförande aktören, systemleverantörer och andra inblandade parter ska regleras samt vilka säkerhetskrav som ska ställas på de tekniska lösningarna.

En grundläggande utgångspunkt är att vårdgivaren även i en automatiserad modell bär ansvaret för riktigheten i de uppgifter som lämnas, medan den registerförande aktören ansvarar för registret och de tekniska lösningar som används för att ta emot uppgifter. Behörighetshandlingarna bör utformas så att de tydligt uttrycker denna ordning, utan att skapa nya materiella ansvarsförhållanden eller ge intryck av att ansvar har flyttats från huvudmannen till en teknisk komponent.

Frågor om rättslig grund, ansvarsfördelning, säkerhet och spårbarhet behöver analyseras inom ramen för hälso- och sjukvårdens och socialtjänstens ordinarie styrning och regelutveckling. Ett pilotfall enligt denna modell bör därför utformas i nära dialog med berörda aktörer och med respekt för befintliga roller och uppdrag. Exemplen i detta avsnitt ska inte läsas som ställningstaganden i sakfrågor om hur nationella kataloger slutligt ska regleras eller användas, utan som en belysning av hur en behörighetsinfrastruktur kan integreras med redan planerade informationsflöden.

7.4 Övrig pilotverksamhet

Utöver de pilotfall som har behandlats finns ett brett behov av digitala behörighetshandlingar även för andra verksamheter där behörighetskontroller i dag huvudsakligen bygger på manuella rutiner och dokument som inte är utformade för maskinell prövning. Detta gäller bland annat för mindre offentliga och privata aktörer som saknar egna register att luta sig mot och som därför själva måste garantera riktigheten i uppgifter som styrker deras behörighet. I dessa fall fyller fullmakter, avskrifter av protokoll och motsvarande handlingar i dag funktionen som bevismedel. Här svarar utställaren av en fullmakt för den behörighet som ges till fullmäktigen och utställaren av en avskrift vid straffansvar för att avskriften överensstämmer med originalet. Digitala behörighetshandlingar behöver här i sin konstruktion beakta att verkan ytterst vilar på avsändarens ansvar – inte på ett publicitetsregister eller liknande.

Motsvarande behov återfinns i kommunal verksamhet där behörigheter följer av delegationsbeslut som dokumenteras i nämndprotokoll. Dessa protokoll och deras bestyrkta avskrifter utgör offentliga handlingar som enligt gällande rätt ska återges oförvanskat; den som bestyrker ett sådant utdrag kan bära straffansvar om innehållet återges felaktigt. En digital behörighetsinfrastruktur behöver kunna

stödja även dessa förutsättningar, samtidigt som den tekniska representationen gör automatiserade kontroller möjliga.

Gemensamt för dessa verksamheter är att det saknas etablerade förebilder för hur angivna behörigheter ska översättas till digitalt kontrollerbara behörighetshandlingar. Lösningar inom en nationell behörighetsinfrastruktur måste därför säkerställa att den digitala representationen återger den underliggande handlingen, samtidigt som den ger förlitande parter ett tekniskt tillförlitligt och spårbart underlag för sin bedömning. Detta är särskilt viktigt för mindre aktörer som inte kan uppfylla tillräckliga krav på registerförvaltning men som ändå måste kunna lämna behörighetsuppgifter som andra kan lita på.

Genom att även inkludera dessa typer av fall i den fortsatta utvecklingen skapas förutsättningar för en mer heltäckande och rättsligt robust behörighetsinfrastruktur som fungerar oberoende av verksamheternas storlek, organisatoriska mognad eller tekniska kapacitet. Detta är en förutsättning för att infrastrukturen långsiktigt ska kunna få en generell tillämpning inom såväl offentlig sektor som näringslivet.

8 Förvaltnings- och driftsmodell i fredstid, kris och krig

I enlighet med uppdraget tar Digg fram förslag på hur infrastrukturen ska förvaltas och drivas långsiktigt, både i fredstid och i kris och krig. Eftersom infrastrukturen som föreslås ska vara federativ, där flera aktörer är med och delar på ansvaret, så behöver vissa delar av förvaltningen byggas upp med det i åtanke. Ett exempel är incidenthantering. Här behöver Digg ta fram en process både för att upptäcka, analysera och åtgärda driftincidenter på egen hand, samt hur det ska ske i samverkan med aktörer. Ett annat exempel kan vara kommunikation och utbildning. Arbetet befinner sig i en utvecklingsfas, vilket innebär att vi just nu utvecklar lösningar för en robust och säker förvaltning.

Digg som ledningsansvarig i infrastrukturen behöver ha förmågor för att säkerställa drift, förvaltning och utveckling. Därför ligger Diggs fokus på att bygga de förmågor som krävs för att säkerställa att såväl Diggs verksamhet som infrastrukturen fungerar under alla förhållanden. Arbetet lägger grunden för en framtida förvaltningsmodell som är både flexibel och motståndskraftig. Omvärldsläget har succesivt försämrats under de senaste åren och detta måste spegla utvecklingen och förvaltningen av infrastrukturen. Detta innebär att vid utveckling och drift så ska totalförsvarets krav beaktas samt de krav som följer av NIS2-direktivet, CER-direktivet och säkerhetsskyddslagen.

8.1 Förmågor som krävs för att förvalta infrastrukturen

Förvaltning av infrastrukturen för Samordnad identitet och behörighet kan brytas ned i olika delar, eller förmågor. Det är de här förmågorna som tillsammans skapar förutsättningar för en organisation att utföra en uppgift. För att kunna säga att man har en förmåga så behöver ofta flera olika delar vara på plats:

- Processer – här finns beskrivningar av hur ett arbete ska utföras.
- Människor och kompetens – man behöver ha personal på plats som har de roller och färdigheter som krävs.
- Teknik och infrastruktur – man har de system och plattformar som möjliggör utförandet.
- Styrning och regelverk – man har de ramar på plats som anger vad som är rätt och tillåtet.

Nedan följer de huvudsakliga förmågorna som behövs.

Strategisk styrning	Förmåga att sätta mål, inriktning och prioriteringar för infrastrukturen.
Samordningsförmåga	Koordinering mellan myndigheter, kommuner, regioner och privata aktörer.
Regel- och avtalshantering	Förmåga att förvalta och utveckla regelverk, anslutningsavtal och villkor.

Förmåga att kontrollera efterlevnad	Förmåga att kontrollera att anslutna aktörer följer krav.
Risk- och kontinuitetshantering	Identifiera risker och säkerställa kontinuitet vid störningar och kriser.
Drift och övervakning	Upprätthålla stabil drift, övervaka prestanda, kapacitet och säkerhet.
Incidenthantering	Upptäcka, analysera och åtgärda incidenter på egen hand och i samverkan med aktörer.
Problem- och ändringshantering	Hantera grundorsaker till fel och driva tekniska/lösningsmässiga förbättringar.
Kapacitetshantering	Anpassa resurser och miljöer efter belastning och framtida behov
Tillgänglighetshantering (SLA)	Säkerställa att drift och svarstider uppfyller avtalade krav.
Konfigurations- och versionshantering	Förvalta mjukvaruversioner, certifikat, metadata och kataloger.
Informationssäkerhet i drift	Kryptering, loggning, nyckelhantering, samt krav enligt NIS2 och säkerhetsskydd.
Onboardingförmåga	Ta emot, tillhandahålla testmöjligheter och stötta nya aktörer som ansluter till infrastrukturen.
Utbildnings- och kommunikationsförmåga	Förklara krav, vägleda och skapa forum för erfarenhetsutbyte.
Kompetensförsörjning	Säkerställa kompetensförsörjning inom relevanta områden utifrån behov och situation som arbetet befinner sig i.
Ekonomi- och finansieringsförmåga	Hantera budget, avgiftsmodeller och nyttorealisering.
Analys- och uppföljningsförmåga	Mäta och analysera anslutningsgrad, incidenter, kostnader och nyttor.

Tabell 4: Förmågor som krävs för att förvalta infrastrukturen.

Digg kommer att behöva säkerställa att alla dessa förmågor finns i infrastrukturen. Den federativa utformning som Digg föreslår innebär emellertid att ansvaret fördelas på andra aktörer inom infrastrukturen.

8.2 Förvaltning i fredstida krissituationer och höjd beredskap och krig

I kris- och krigssituationer blir nationell digital samverkan inte bara en effektivitetsfråga utan en fråga av vikt för hela beredskapssystemet. En gemensam infrastruktur för identitets- och behörighetshantering möjliggör att samhällsviktiga funktioner kan fortsätta fungera över organisations- och landsgränser. Lösningar för bland annat identifiering, behörighetskontroll, bevisutbyte och datadelning skapar förutsättningar för snabb, säker och kontrollerad åtkomst till information, vilket underlättade exempelvis covid-bevishantering och utbetalningar av krisstöd under pandemin. Erfarenheterna från Ukraina visar också hur digitala nationella tjänster kan bli avgörande för både civila behov (evakueringar, gränsöverskridande ID-handlingar) och för mobilisering av resurser och lägesbild (insamling av data, stöd till försvarsmakten). Förmågan till interoperabilitet, både nationellt och med EU och NATO, bygger på att system kan dela data.

Dagens regelverk och hotbild ökar kraven på robusthet och cybersäkerhet; en väl utbyggd och sammanhållen digital infrastruktur gör det också möjligt att stödja mindre aktörer som saknar egna resurser, och att snabbt skala upp gemensamma skyddsåtgärder och redundans.

Nedan beskrivs hur infrastrukturen fortsatt ska kunna förvaltas och drivas även i fredstida krissituationer och höjd beredskap och krig.

8.2.1 Grundläggande principer

Planen vilar på följande nationella principerna för den civila beredskapen:

- Ansvarsprincipen: att den som har ansvar för en verksamhet i normala situationer också har motsvarande ansvar vid störningar i samhället.
- Likhetsprincipen: att aktörer inte ska göra större förändringar i organisationen än vad situationen kräver. Verksamheten under samhällsstörningar ska fungera som vid normala förhållanden, så långt det är möjligt.

Dessa principer är vägledande för de förmågor som beskrivs nedan även om förvaltning, teknik och processer ännu inte är fastställda.

8.2.2 Ansvarsfördelning utifrån roller

Beskrivning av roller utifrån ansvarsprincipen och likhetsprincipen

Ledningsansvarig

- Ansvar: Har det övergripande mandatet att samordna, hålla register och sätta ramar. Det ansvaret kvarstår även i kris och krig – det kan inte ”parkeras”.
- Likhet: Samma processer som i normala fall ska gälla, men förstärkta med krisledning och redundans. Skillnaden är inte hur ansvar fördelas, utan intensiteten och prioriteringen.

Federationsområdesansvarig

- Ansvar: Federationsområdesansvarig svarar alltid för sina egna områden och de operatörer som de anslutit. Federationsområdesansvarig måste kunna garantera funktion och avtal även i kris- och krigssituationer.
- Likhet: Federationsområdesansvarig fortsätter att vara länken mellan operatörer och Ledningsansvarig men kan behöva ta beslut snabbare, med förenklade rutiner. I grunden gör de samma saker, men i kortare cykler och ibland med förenklade kontroller.

Leverantörer av behörighetshandling

- Ansvar: Leverantören ansvarar för att intyg är korrekta och att de bygger på rätt register. Ansvarsprincipen gör att detta gäller lika mycket i krig och höjd beredskap som i fred.
- Likhet: Intygsutställandet ska ske enligt samma logik och juridiska ramar, men metoderna kan ändras och förenklas (t.ex. kortare giltighet, förenklade valideringar). Kärnan är att leverantören garanterar riktigheten.

Förlitande parter

- Ansvar: Förlitande part ansvarar för att kontrollera intyg innan tillgång ges till en tjänst. Om det inte fungerar korrekt är det förlitande part som äger risken. Detta gäller även i kris och höjd beredskap/krig.
- Likhet: Samma kontroll ska göras, men kan genomföras med förenklade processer (t.ex. acceptera intyg från fallback-listor). Principen är att tillträde aldrig blir ”fritt” – det är alltid en kontroll, även om den är enklare.

Huvudmän (arbetsgivare, skolor, vårdgivare m.fl.)

- Ansvar: Ansvarar för riktigheten i de underlag (anställning, roll, fullmakter) som intygen bygger på. Detta ansvar är oförändrat i alla lägen.
- Likhet: Processen för att lämna uppgifter är densamma, men i kris kan man acceptera enklare format (manuell lista, offline-rapport) tills normalt läge återställs.

8.2.3 Förmågeperspektiv

Nedan beskrivs de förmågor som i första hand berörs samt hur de behöver anpassas utifrån fredstida krissituationer samt höjd beredskap/krig.

8.2.4 Kritiska förmågor som måste etableras

Inledningen av varje förmåga beskrivs i generella ordalag vad förmågan avser att hantera, därefter följer en beskrivning av förmågorna utifrån situation.

Ledningsförmåga

Förmågan innebär att i både fred, fredstida krissituationer och höjd beredskap/krig kunna leda och samordna infrastrukturen (vem styr, vem beslutar, vem kommunicerar).

- fredstida krissituationer: Krisledning aktiveras, redundanta beslutsvägar används, snabbare kommunikation krävs. Ledningsansvarig samordnar men ansvarsprincipen gäller oförändrat.
- höjd beredskap/krig: Robust och decentraliserad ledning krävs. Beslut kan behöva fattas lokalt men ska följa samma grundprinciper som i fred (likhetsprincipen).

Kommunikationsförmåga

Förmågan innebär att säkert kunna dela incidentinformation och lägesbilder mellan aktörer, oavsett om ordinarie kanaler är nere.

- fredstida krissituationer: Alternativa kommunikationskanaler aktiveras (säker telefoni, Rakel, WIS, krypterad e-post). Lägesbilder delas tätare.
- höjd beredskap/krig: Informationsdelning sker redundansbaserat och ofta decentraliserat, men måste fortfarande vara spårbar. Prioritering sker utifrån samhällskritiska behov.

Kontinuitetsförmåga (resiliens)

Kontinuitetsförmåga innebär att infrastrukturen och organisationen kan fortsätta leverera sina mest kritiska funktioner även när delar av systemet eller omgivningen är störda, attackerade eller otillgängliga.

- fredstida krissituationer: Degraderade lägen aktiveras (förenklade funktioner, manuella processer). Målet är att hålla igång kärnverksamheten.
- höjd beredskap/krig: Endast den absolut viktigaste verksamheten kan fungera trots stora avbrott. Fokus ligger på de delar som är av vikt för totalförsvaret.

Återställningsförmåga

Förmågan innebär att kunna återgå till normalläge efter en störning, inklusive att hantera eftersläpande data, loggar och juridiska krav.

- fredstida krissituationer: Snabb återställning till normal drift efter incident, med dokumentation och lärande.
- höjd beredskap/krig: Gradvis återställning från reservlägen. Fokus på att återföra verksamheten till en fungerande normallinje när hotnivån sjunker.

Informationssäkerhet i drift

Förmågan innebär att upprätthålla konfidentialitet, riktighet och tillgänglighet även under störda förhållanden.

- fredstida krissituationer: Minimikrav på kryptering och integritet, reservnycklar och förenklade loggningsrutiner.
- höjd beredskap/krig: Endast grundläggande skydd mot intrång och manipulation kan garanteras. Fokus på att bibehålla samhällskritiska flöden.

Incidenthantering

Förmågan innebär att upptäcka, analysera och åtgärda störningar och attacker.

- fredstida krissituationer: Snabb mobilisering, alternativa rapporteringskanaler, tätare uppföljning.
- höjd beredskap/krig: Incidentrapportering sker med förenklade metoder. Fokus på snabb åtgärd för att återställa kritiska funktioner.

8.2.5 Arbete som återstår inom förvaltningsområdet

I nuvarande fas handlar arbetet om att:

- Fastställa hur förvaltningsansvar ska fördelas mellan Ledningsansvarig, Federationsområdesansvarig och operatörer.
- Identifiera vilka tekniska komponenter som är mest kritiska att realisera tidigt (t.ex. katalogtjänster, intygsfunktioner, säker kommunikation).

Det fortsatta arbetet definierar processer för incidenthantering och samordning. När dessa finns på plats kan förmågebeskrivningarna omsättas i konkreta rutiner, system och linjeras med juridiska förutsättningarna samt Diggs övergripande beredskapsplanering. Från år till år ska kontinuerlig bedömning av lösningen göras utifrån hur samhällsviktig verksamheten som bedrivs i och runt den är.

8.2.6 Hur infrastrukturen påverkar Digg

Etableringen av infrastrukturen innebär att Digg behöver en intern organisation som kan axla rollen som Ledningsansvarig inom federationen. Det kräver kompetens om hur federationer fungerar, samt utökat mandat för strategisk styrning, juridisk reglering, och teknisk samordning av federationen. Nya funktioner behöver inrättas för ledning och koordinering av federationsområdesansvariga och operatörer, förvaltning av registrerade aktörer, samt uppföljning. Förvaltningen och utvecklingen av infrastrukturen ska etableras som ordinarie verksamhet på Digg.

Rollen som Ledningsansvarig innebär både direkta kostnader för etablering och drift samt indirekta kostnader för styrning, samverkan och förvaltning. För att detta ska fungera krävs en säkerställd långsiktig finansiering av Diggs del av infrastrukturen. Vår bedömning är att en avgifts- eller ersättningsmodell som täcker både drift och utveckling kan behövas för att skapa möjligheter till finansiering av den del av infrastrukturen som operatör eller sektorsmyndigheter ansvarar för.

Förvaltningsmodellen behöver integreras med Diggs befintliga styrning med gemensamma processer för livscykelhantering, risk- och säkerhetshantering samt incidenthantering.

Infrastrukturen innebär en gradvis men strukturell förändring för Digg. Rollen som Ledningsansvarig placerar myndigheten i centrum för ett helt nytt ekosystem av digital samverkan men liknar roller som Digg redan har i andra infrastrukturer. Påverkan kommer att omfatta ekonomi, kompetensförsörjning, och externa relationer. För detta behöver Digg etablera en stabil förvaltningskapacitet som kan hantera ett nationellt långsiktigt ansvar.

9 Behov av finansieringsmodell för infrastrukturen

När det gäller finansieringen av infrastrukturen som helhet bör det ske enligt de förslag och modeller som finns beskrivet i rapporten *Förslag till långsiktig utveckling och förvaltning av Ena,* (Fi2024/01455) samt den tillhörande bilagan *Långsiktig finansiering av Ena,* (Fi2024/01455). De frågor som är specifika för denna infrastruktur handlar framför allt om hur olika former av aktörer ska kunna få finansiering för de uppgifter de utför inom infrastrukturen.

För att infrastrukturen för identitet och behörighetshantering ska bli långsiktigt hållbar och användbar för både offentliga och privata aktörer, behöver finansieringsmodellen vara flexibel, långsiktig och rättvis. Eftersom infrastrukturen är en kollektiv nyttighet som ska vara tillgänglig för många aktörer, är det avgörande att det finns incitament för användarna att ansluta sig. Samtidigt innebär en sådan lösning att aktörerna behöver göra anpassningar på sina egna system och processer för att kunna nyttja infrastrukturen fullt ut.

Det är därför viktigt att nyttorna med att ansluta till infrastrukturen, som tillgång till relevanta tjänster, ökad säkerhet och interoperabilitet, väger över kostnaderna på lång sikt. En sådan modell måste vara flexibel nog för att kunna utvecklas och anpassas efter nya behov och tekniska krav som uppstår. En viktig aspekt är att finansieringsmodellen inte ska skapa inlåsningseffekter eller hindra aktörer från att göra förändringar som är nödvändiga för att kunna använda infrastrukturen effektivt. Modellen måste säkerställa att aktörerna har förutsättningar att delta på lika villkor, oavsett om de är offentliga eller privata aktörer.

Finansieringsmodellen måste därför inte bara ta hänsyn till de kortsiktiga kostnaderna utan också skapa långsiktiga incitament för alla aktörer att engagera sig och fortsätta bidra till utvecklingen av infrastrukturen. I detta avsnitt återges de behov som uttryckts hos Internetstiftelsen och Inera, vilka är exempel på aktörer som kan ta tjänsteroller som operatörer i den federerade infrastrukturen, samt hos Sveriges Kommuner och Regioner vilka representerar användarperspektivet.

9.1 Förväntade kostnadsdrivande delar för operatörer

De centrala kostnadsdrivande faktorerna för operatörer innefattar både drift och administration av tjänster, samt säkerställande av att de uppfyller de nödvändiga tekniska och säkerhetsmässiga krav som en federerad infrastruktur ställer. För anslutningsoperatörer innebär detta ansvar för att upprätthålla en teknisk plattform som säkerställer interoperabilitet, hantera anslutningsprocesser inklusive onboarding och support, samt upprätthålla säkerhet och tillgänglighet.

9.2 Behov hos Inera

Inera uttrycker ett behov av en finansieringsmodell som både säkerställer kostnadstäckning och gör det möjligt för dem att uppnå sina vinstmål på 3%. För att kunna engagera sig i federationsinfrastrukturen på ett hållbart sätt behöver de en modell som täcker både driftkostnader och de investeringar som krävs för att utveckla och upprätthålla sina tjänster. Under hösten genomför Inera en förstudie för att bedöma business-caset för att engagera sig i federationen, vilket

bland annat innebär att de behöver investera i en server för att kunna ansluta sina tjänster till systemet. För att kunna motivera dessa initiala investeringar behöver de en finansieringsmodell som ger tydliga förutsättningar för hur de kan finansiera sina kostnader innan intäkterna från de anslutna aktörerna börjar strömma in.

Inera betonar också att för att de ska kunna skapa värde för sina ägare, som består av kommuner och regioner, måste finansieringsmodellen ge dem tillräcklig ekonomisk täckning. De behöver en långsiktig stabilitet som gör att de kan fortsätta tillhandahålla tjänster utan att riskera sin ekonomiska stabilitet. Därmed är det viktigt att modellen ger utrymme för långsiktig stabilitet och utveckling, och att de har en säker väg för att finansiera både de initiala investeringarna och löpande drift.

En annan viktig aspekt för Inera är att modellen måste vara transparent och rättvis i sin fördelning av kostnader. Större aktörer, som regioner, betalar ofta mer för de tjänster de använder, vilket innebär att det finns ett behov av att säkerställa att mindre aktörer, som kommuner, inte blir ekonomiskt utestängda från att delta på grund av höga avgifter. Inera behöver en flexibel modell som gör det möjligt att hantera olika betalningspreferenser beroende på aktörernas storlek och användning.

9.3 Behov hos Internetstiftelsen

Internetstiftelsen lyfter fram att den föreslagna federerade infrastrukturen ställer höga krav på långsiktighet, stabilitet och professionalitet. För att en infrastrukturbärande aktör ska kunna bidra uthålligt och med hög kvalitet behöver vissa grundläggande förutsättningar vara uppfyllda. Utveckling och förvaltning av digital infrastruktur kräver stabila och förutsägbara ramar – juridiskt, organisatoriskt och ekonomiskt – och kan inte baseras på kortsiktiga projektmedel eller tillfälliga satsningar. Internetstiftelsen betonar därför vikten av att finansieringsmodellen utformas med omsorg, så att inlåsningseffekter undviks och långsiktiga investeringar möjliggörs genom tydliga spelregler och hållbara samverkansformer mellan staten och de aktörer som bär upp infrastrukturen.

Vidare framhåller Internetstiftelsen att finansieringsmodellen måste vara flexibel och kunna anpassas till förändrade tekniska krav och samhällsbehov över tid. En infrastruktur av detta slag behöver utvecklas successivt och med uthållighet, och utan rimliga incitament och förutsättningar för långsiktig planering riskerar även etablerade aktörer att få svårt att bidra på ett hållbart sätt. Internetstiftelsens egen modell för självfinansierad, oberoende och professionell drift av gemensamma nyttigheter lyfts fram som ett exempel på hur en transparent och långsiktigt hållbar förvaltningsstruktur kan utformas.

Internetstiftelsen understryker också vikten av att infrastrukturen bygger på öppna standarder, fria och väldefinierade gränssnitt samt en tydlig separering mellan infrastruktur- och applikationslager. Starka beroenden till specifika tekniska lösningar, leverantörer eller operatörer riskerar att skapa inlåsningseffekter som hämmar innovation, minskar interoperabiliteten och begränsar förutsättningarna för ett konkurrensneutralt ekosystem. En nationell styrning bör därför aktivt främja öppenhet, flexibilitet och utbytbarhet och säkerställa att arkitekturen inte låses fast i applikationslagret eller bindas till enskilda implementationer.

Slutligen framhåller Internetstiftelsen att en tillitsbärande infrastruktur kräver hög grad av professionalisering. Det omfattar inte bara teknisk drift utan också etablerade processer för riskhantering, revision, säkerhetsgranskningar, incidentrespons och långsiktig planering av arkitektur och specifikationer. Roller och ansvar bör enligt Internetstiftelsen därför tilldelas aktörer med dokumenterad erfarenhet av stabil drift, hög tillgänglighet och robust governance. Det är denna operativa förmåga, snarare än formell myndighetsstatus, som långsiktigt bygger förtroende i infrastrukturen.

9.4 Behov hos kommuner och regioner

SKR betonar att kommunerna ser en federerad infrastruktur som ett positivt steg för att hantera identitet och behörighet på ett mer enhetligt sätt. SKR har tagit fram vägledning för att stödja framförallt kommuner med lägre mognadsgrad inom området. SKR rekommenderar att alla medarbetare inom kommunalverksamhet ska ha en e-tjänstelegitimation som är godkänd på minst tillitsnivå 3. Det stärker kommunernas förutsättningar att ansluta till federationen på sikt.

När det gäller finansiering betonar SKR att det är centralt med transparens och förutsägbarhet. Kommunerna föredrar fasta avgifter framför "tick"-avgifter, eftersom det blir svårt att budgetera för rörliga avgifter och dessa kan skapa incitamentsproblem. En stabil och enkel kostnadsstruktur underlättar långsiktigt engagemang och gör det möjligt för kommunerna att fatta välgrundade beslut om anslutning till infrastrukturen. SKR förespråkar en kostnadsmodell där avgifterna anpassas efter kommunernas behov, exempelvis genom kommunstorlek. Att anpassa fasta avgifter efter kommunernas behov (eller t.ex. storlek) möjliggör att finansieringsmodellen blir mer rättvis och förutsägbar för alla aktörer.

I detta sammanhang ser SKR gärna att finansieringsmodellen bygger på en "abonnemangsmodell", där kommunerna betalar en fast och förutsägbar årlig avgift för att få tillgång till alla eller flera delar av Ena:s tjänster. Denna modell skulle ge kommunerna möjlighet att använda de tjänster de behöver, utan att behöva oroa sig för variabla kostnader som kan hämma deras digitalisering och användning av Ena - Sveriges digitala infrastruktur.

9.5 Konsekvenser beroende av framtida vägval

Digg lämnar inget förslag på hur användningen av infrastrukturen ska finansieras (t.ex. avgifter eller statlig finansiering) och hur olika aktören ska ersättas (affärsmodell). I det fortsatta arbetet behöver dessa frågor lösas. Detta är en förutsättning för att infrastrukturen ska kunna användas i större skala och för att de nyttor som beskrivs i kapitel 2 ska realiseras. Det är även en förutsättning för att fullt ut kunna bedöma konsekvenserna av förslaget. Beroende på vilka beslut som fattas kan olika konsekvenser uppstå. Dessa beskrivs kortfattat nedan, men behöver analyseras vidare i arbetet med finansiering och affärsmodell.

9.5.1 Regelverket om offentlig upphandling kommer att aktualiseras

Upphandlingslagstiftningen aktualiseras i flera delar vid etablering och drift av en nationell behörighetsinfrastruktur. Modellen för upphandling bör fastställas tidigt, anslutningen utformas öppet och icke-diskriminerande och samtliga undantagsbedömningar dokumenteras.

Upphandlingslagstiftningen i Sverige syftar till att säkerställa konkurrens, transparens och likabehandling när myndigheter och offentligt styrda organ anskaffar varor, tjänster eller byggentreprenader. Det måste därför genomlysas i vilken mån en behörighetsinfrastruktur kan komma i konflikt med dessa regler, såväl vid etableringen som vid den löpande driften, särskilt i fråga om anskaffning av fundament och verksamhetsområdesspecifika anpassningar. En sådan genomlysning kan göras först när arbetet med infrastrukturen och avtalen kommit längre.

9.5.2 Statsstöd

En nationell behörighetsinfrastruktur som finansieras och drivs av staten kan omfattas av statsstödsreglerna, särskilt om vissa aktörer ges tillgång på förmånliga villkor eller om infrastrukturen i praktiken tränger undan konkurrerande kommersiella lösningar. Statsstödsriskerna kan hanteras genom att systemet tillhandahålls på icke-diskriminerande och marknadsmässiga villkor, genom att infrastrukturen ges en tydlig status som tjänst av allmänt ekonomiskt intresse med proportionell kompensation, samt – i förekommande fall – genom notifiering till och godkännande av Europeiska kommissionen.

10 Förslag till införandeplan

Planen för perioden 2026–2029 syftar till att stegvis ta infrastrukturen från koncept och tekniska prototyper till fungerande lösningar i praktisk användning. Arbetet ska bygga på tydliga användningsfall, ett nära samarbete mellan Digg och olika sektorer samt förberedelser för långsiktig robusthet och lagstiftningsanpassning. För att planen ska vara realiserbar krävs en långsiktig finansiering och juridiska förutsättningar.

Införandeplanen är beskriven utifrån faser med tillhörande tillstånd. Ett tillstånd är det förväntade läget efter att planerade insatser eller aktiviteter genomförts.

10.1 Introduktionsfas - 2026

Arbetet 2026 handlar om att ta infrastrukturen från prototyp till produktionsmiljö samt att kommunicera kring utrullningen för att anslutande aktörer ska kunna planera sitt införande.

Tillstånd att uppnå under året:

- Det finns en basnivå av den tekniska infrastrukturen i produktion i form av tekniska specifikationer och komponenter. Det skapar förutsättningar för en ensad tillämpning av teknisk kommunikation, identifiering av organisation samt förmedling och verifiering av behörighetsgrundande information.
- Det finns avtalsmodeller för infrastrukturen för de första implementationerna.
- En tillämpning i begränsad skala (pilot) i produktionsmiljö är genomförd. Arbetet är planerat att genomföras inom hälso- och sjukvårdsområdet och innehålla minst en federationsområdesansvarig med tillhörande operatörer
- Aktörer förstår nyttor som ett deltagande i infrastrukturen medför och det finns tydliga incitament för att ansluta.

Förutsättningsskapande arbete:

- Ett förslag till finansieringsmodell finns framtagen baserat på inriktning från politiken. Målsättningen är att hitta en modell som är välfungerande för infrastrukturens alla olika parter.
- Beslut om nödvändiga författningsändringar är fattade.
- Löpande dialog med de sektorer som har behov av infrastrukturen framåt.

2026 års arbete handlar också om att förbereda de sektorer som har stora behov av infrastrukturen på ett kommande införande. Det är centralt att lösningarna ses som nyttoskapande redan i detta tidiga skede för att underlätta det bredare införandet längre fram genom att skapa förutsättningar för interoperabilitet.

10.2 Etableringsfas - 2027

Under 2027 börjar infrastrukturen används i skarp drift och fler sektorer och nya operatörer tillkommer. Fokus ligger på att etablera stabil drift, stödja de första sektorsvisa införandena och säkerställa att förvaltning fungerar i praktiken.

Tillstånd att uppnå under året:

- Fler operatörer ansluter vilket skapar förutsättningar för att skala upp i både tillämpning av och anslutning till infrastrukturen.
- Fler tjänster/tillämpningar börjar nyttja infrastrukturen
- En fungerande styrning och ledningsstruktur finns för att styra, följa upp, förstå behov och omsätta insikter i styrning och förbättring.

Viktigt i denna fas är att fånga erfarenheterna som de olika tillämpningarna genererar in i det fortsatta arbetet. Målet är att säkerställa nytta i befintliga och nya områden, visa på interoperabilitet och kvalitetssäkra infrastrukturen. Existerande tjänster kan anslutas för att snabbt skapa värde.

10.3 Tillväxtfas - 2028

Under 2028 sker ett breddinförande där infrastrukturen används inom flera sektorer. Fokus ligger på att skapa en "kritisk massa" som möjliggör för mer omfattande effekthemtagningar samt att etablera stöd för samhällskritiska tillämpningar. Infrastrukturen ses som en gemensam resurs och är accepterad som standard för identitets- och behörighetshantering i offentlig sektor.

Tillstånd att uppnå under året:

- Befintliga federationer har påbörjat eller genomfört anpassning för att kunna ingå i infrastrukturen
- Infrastrukturen är accepterad och används som utgångspunkt inom det offentligas informationsutbyten.
- Reservlösningar för kris och krig är etablerade

10.4 Mognadsfas - 2029

Under 2029 är målet en fullt etablerad infrastruktur som kan användas för en bredd av verksamheter, även när det gäller samhällsviktiga sådana och där kraven på tillgänglighet är höga. I detta skede behöver Digg ha fått långsiktigt mandat samt långsiktig finansiering för sitt arbete och sin roll kopplat till infrastrukturen.

Tillstånd att uppnå under året:

- Infrastrukturen är fullt operativ och kan användas även av samhällsviktiga verksamheter.
- Infrastrukturen har hög redundans och tillgänglighet.
- Infrastrukturen har internationell interoperabilitet och kan hantera gränsöverskridande federering.

Förutsättningsskapande:

Författningsregleringen är klar och regler etablerat.

11 Risker och beroenden

Arbetet med att etablera en nationell infrastruktur för identitets- och behörighetshantering är komplicerat och påverkas av flera faktorer som ligger utanför Diggs direkta kontroll. För att lyckas krävs att juridiska, tekniska och organisatoriska delar utvecklas i nära samspel, samtidigt som aktörer på olika nivåer engageras och ansluter sig. Detta innebär att det finns risker och beroenden som kan fördröja, försvåra eller i värsta fall hindra införandet om de inte hanteras tidigt och systematiskt.

I detta kapitel tydliggör vi de mest betydande riskerna och beroendena som måste beaktas, så att arbetet kan planeras med rätt förutsättningar och åtgärder för att minimera konsekvenserna.

11.1 Fragmentering och områdesspecifika lösningar

En central risk är att den föreslagna modellen inte upplevs som tillräckligt gemensam och därför utvecklas olika inom olika sektorer, exempelvis vård, skola eller kommunal förvaltning. Om varje område bygger egna anpassningar eller parallella lösningar kommer offentlig förvaltning fortsatt vara fragmenterad med öar av olika standarder, avtal och tekniska varianter. Det skulle motverka syftet med en nationell infrastruktur, öka komplexiteten, öka kostnaderna och minska möjligheten till enkel anslutning för aktörer som verkar i flera områden.

En sådan fragmentering skulle också försvåra Sveriges möjligheter att uppfylla EU:s krav på interoperabilitet och gränsöverskridande informationsutbyte, exempelvis inom ramen för EHDS och SDG. På nationell nivå skulle det samtidigt försämra förutsättningarna att nå målen i den svenska digitaliseringsstrategin, särskilt de som rör datadriven innovation, en digitalt samverkande förvaltning och en effektivare välfärd.

För att hantera denna risk behöver förslagen om ett tydligt ledningsansvar som säkerställer att infrastrukturen förblir generisk och återanvändbar genomföras.

11.2 Svårigheter att få igång anslutningar initialt

En återkommande utmaning vid etablering av nationella infrastrukturer är att skapa en första kritisk massa av anslutna aktörer. Innan nyttorna är tydligt synliga kan kommuner, regioner, myndigheter och leverantörer tveka att prioritera resurser för anslutning. Detta riskerar att skapa en ond cirkel där begränsat deltagande leder till att värdet av infrastrukturen upplevs som lågt, vilket i sin tur minskar incitamenten att ansluta.

Om inte en tillräcklig bredd av aktörer ansluter tidigt riskerar införandet att stanna upp, med följden att infrastrukturen fastnar i pilotstadiet och tappar förtroende. Det kan också innebära att parallella lösningar fortsätter att utvecklas, vilket ökar risken för dubbelarbete, ineffektivitet och fragmentering.

För att hantera risken krävs samordnade insatser på flera nivåer: tydlig kommunikation om nyttor och långsiktiga vinster, riktade stödåtgärder för tidiga anslutare samt en finansieringsmodell som

gör det praktiskt möjligt att delta. Särskilt viktigt är att skapa förutsättningar för de första anslutningarna så att infrastrukturen snabbt kan börja leverera nytta och bygga förtroende för den gemensamma modellen.

På längre sikt kan någon form av obligatorisk anslutning behöva övervägas för särskilt centrala delar av den offentliga sektorn. Liknande resonemang har tidigare lyfts i Diggs rapport *Förslag till långsiktig utveckling och förvaltning av Ena*, där behovet av gemensamma åtaganden betonas för att skapa full effekt av investeringarna.

11.3 Bristande återanvändning av befintliga investeringar

Offentliga och privata aktörer har redan gjort omfattande investeringar i befintliga lösningar för identitet, behörighet och åtkomsthantering. Om den nya infrastrukturen inte utformas så att dessa investeringar kan återanvändas finns en risk att införandet blir alltför kostsamt och resurskrävande för aktörerna. Det kan leda till motstånd mot anslutning, fördröjt införande och i värsta fall utveckling av parallella lösningar.

Att inte ta tillvara befintliga lösningar innebär även en risk för minskat förtroende. Aktörer kan ifrågasätta om nyttan står i proportion till de kostnader som uppstår om behovet av anpassningar är för stora, vilket kan underminera viljan till samverkan och skapa praktiska problem i form av fragmenterade lösningar och bristande interoperabilitet.

För att hantera risken behöver infrastrukturen bygga på etablerade standarder och principer, stödja integration med befintliga system och tydligt visa hur investeringar i dagens lösningar kan återanvändas och förstärkas. Genom att bygga vidare på det som redan finns, i linje med Enas grundprinciper, skapas förtroende, kostnadseffektivitet och långsiktig stabilitet i hela det digitala ekosystemet.

11.4 Beroenden till andra initiativ och infrastrukturer

Arbetet med infrastrukturen för identitets- och behörighetshantering sker inte i ett vakuum. Det finns en rad parallella initiativ och befintliga infrastrukturer inom digitalisering, både nationellt och internationellt. Om samordningen med dessa inte fungerar riskerar lösningarna att krocka, överlappa eller skapa onödigt dubbelarbete.

Detta kan i sin tur leda till ineffektiv resursanvändning, ökade kostnader och bristande förtroende hos de aktörer som förväntas ansluta. En otydlig koppling till närliggande satsningar kan även resultera i tekniska hinder eller juridiska konflikter, där aktörerna tvingas välja mellan oförenliga lösningar.

För att minska denna risk krävs ett aktivt och kontinuerligt samarbete med andra pågående initiativ, både inom ramen för Ena och andra nationella eller internationella satsningar. Det innebär att följa gemensamma principer, tydligt definiera gränsytor och säkerställa återanvändning av befintliga komponenter där det är möjligt.

11.5 Bristande tillit i infrastrukturen

Tillit är den mest avgörande faktorn för att infrastrukturen ska fungera. Utan ett gemensamt och accepterat ramverk för tillit riskerar hela modellen att förlora sin bäring. Om aktörer inte känner sig trygga i att identiteter, behörigheter och intyg hanteras på ett tillförlitligt sätt kommer de tveka att ansluta eller välja att bygga egna lösningar.

Detta kan leda till fragmentering, minskad interoperabilitet och förlorade effektivitetsvinster. En bristande tillit gör också att de investeringar som krävs för infrastrukturen inte får önskad utväxling, eftersom nyttorna endast realiseras fullt ut när många aktörer deltar och använder infrastrukturen på lika villkor.

Att etablera tillit kräver tekniska, juridiska och organisatoriska mekanismer. Detta måste hanteras vid etablering av infrastrukturen för att inte riskera att infrastrukturen uppfattas som osäker, ofärdig eller irrelevant, vilket skulle allvarligt äventyra dess genomslag.

12 Slutsatser och rekommendationer

Arbetet med regeringsuppdraget har bedrivits intensivt och i bred samverkan. Vi har nått viktiga delmål och etablerat en stabil grund för en nationell infrastruktur för identitets- och behörighetshantering. Samtidigt har uppdragets komplexitet och bredd gjort att vissa delar ännu inte är fullt utvecklade. I detta kapitel sammanfattar vi de viktigaste slutsatserna och lämnar rekommendationer för hur de återstående frågorna bör hanteras i det fortsatta genomförandet.

12.1 Övergripande slutsatser

Arbetet med regeringsuppdraget har visat att en nationell infrastruktur för identitet och behörighet är både nödvändig och möjlig att etablera. Analysen och samverkan med centrala aktörer bekräftar att dagens situation präglas av fragmentering, dubbla lösningar och bristande interoperabilitet, vilket leder till ineffektivitet, ökade kostnader och risker för såväl rättssäkerhet som informationssäkerhet.

Vi kan konstatera att:

- Behovet är brett och tydligt. Både statliga myndigheter, kommuner, regioner och privata utförare efterfrågar en gemensam infrastruktur som kan stödja digital samverkan över organisationsgränser. Det gäller särskilt inom välfärdssektorn, där invånare ofta möter flera aktörer i samma ärende.
- Det finns en stark samsyn kring inriktningen. Genom arbetet inom Ena, i nära samverkan med myndigheter, SKR, regioner och leverantörer, har en gemensam förståelse vuxit fram för att lösningen behöver bygga på en federativ modell, öppna standarder och tydlig ansvarsfördelning.
- De första byggstenarna är på plats. Vi har tagit fram förslag till juridiska ramar, en arkitektur för federationen samt principer för styrning, förvaltning och finansiering. Tekniska tester har inletts i samarbete med centrala aktörer.
- Potentialen är stor. En sammanhållen infrastruktur för identitets- och behörighetshantering kan ge betydande samhällsnytta: ökad säkerhet, minskade kostnader, högre kvalitet i digitala tjänster, enklare digital samverkan och stärkt förtroende hos både invånare och verksamheter.
- Samordning är avgörande. För att infrastrukturen ska bli långsiktigt hållbar måste juridiska, tekniska och organisatoriska frågor utvecklas både gemensamt och inom varje aktörs eget ansvar. Det gemensamma ramverket behöver kompletteras med att varje aktör anpassar sina interna processer, system och styrformer så att de stödjer helheten. Detta förutsätter tydlig ledning, samverkan över sektorsgränser och långsiktig finansiering.

Slutsatsen är att vi står på en stabil grund men att det fortsatt krävs ett målmedvetet arbete för att realisera infrastrukturen fullt ut. Den föreslagna federationsmodellen har stark förankring och stöd hos berörda aktörer och kan utgöra en strategisk plattform för hela den offentliga sektorns digitalisering.

12.2 Vägen framåt i det fortsatta arbetet

12.2.1 Fokusområden för fortsatt utveckling

Det fortsatta arbetet behöver inriktas på att gå från analys till praktisk tillämpning. Nedan beskrivs de områden där fördjupning, testning och konkretisering krävs för att infrastrukturen ska kunna tas i bruk, skalas upp och förvaltas långsiktigt.

Juridiska ramar och avtal

Digg har identifierat och beskrivit författningsändringar som bedöms nödvändiga för att myndigheten ska kunna förvalta infrastrukturen och säkerställa dess långsiktiga funktion. Det juridiska arbetet behöver även fortsätta, särskilt vad gäller avtalsmodellen. I det fortsatta arbetet är det viktigt att juridiska frågor hanteras parallellt med den tekniska och organisatoriska utvecklingen, så att lösningarna kan stödja varandra och bygga en sammanhållen helhet.

Styrning, förvaltning och samordning

Arbetet med att ta fram en modell för styrning och förvaltning har inletts och lagt en grund för hur infrastrukturen ska ledas och utvecklas. Nästa steg är att fördjupa och konkretisera detta arbete, särskilt när det gäller ansvarsfördelning, beslutsprocesser och samordning mellan aktörer. De övergripande processerna för uppföljning, incidenthantering och gemensam vidareutveckling behöver nu omsättas i praktiken och etableras på ett enhetligt sätt. Det är avgörande för att skapa transparens, förtroende och långsiktig stabilitet. Arbetet ska ske parallellt med den tekniska och juridiska utvecklingen så att styrningen stödjer helheten och möjliggör en flexibel men sammanhållen förvaltning över tid.

Teknisk verifiering och utveckling

Tester av de tekniska komponenterna har påbörjats men hittills i begränsad omfattning tillsammans med ett fåtal aktörer. För att kunna bedöma lösningens funktion, interoperabilitet och användbarhet behövs bredare tester i praktiska miljöer.

Nästa steg är att genomföra teknisk verifiering i större skala och samla in erfarenheter från olika sektorer. Resultaten ska användas för att justera, förenkla och vidareutveckla lösningen inför kommande införande. Arbetet ska även ge underlag för hur infrastrukturen kan skalas upp stegvis och hur drift- och integrationsfrågor ska hanteras långsiktigt. Det bör samtidigt skapas särskilt stöd för tidiga anslutningar, exempelvis genom samordning, teknisk vägledning och praktiska incitament, så att de första aktörerna inte möter orimliga trösklar.

Kommunikation och förankring

Kommunikationen ska nu växla från introduktion till etablering. Fokus framåt är att skapa tydliga budskap om nyttor, ansvar och tidplaner, samt att bygga långsiktiga strukturer för dialog och

återkoppling. Arbetet ska bidra till förståelse, delaktighet och förtroende hos berörda aktörer i takt med att infrastrukturen konkretiseras.

Effekt- och nyttoanalys

För att ge beslutsfattare ett robust underlag behövs fördjupade analyser av kostnader, effektiviseringsvinster och samhällsnytta. Arbetet ska resultera i en samlad nyttokalkyl som kan användas för prioritering, finansieringsbeslut och uppföljning av resultat över tid.

Det behövs också inriktning från Regeringen rörande en långsiktigt hållbar finansieringsmodell, som skapar incitament för anslutning och en rättvis fördelning av kostnader och ansvar.

Beredskap och säkerhet

Givet det rådande omvärldsläget och de ökade krav som följer av detta kommer området fortsatt att vara i fokus. Ett fortsatt arbete krävs för att konkretisera hur infrastrukturen ska fungera under störda förhållanden, där totalförsvarets krav är dimensionerande. Fokus ligger på att ta fram krav och lösningar för cybersäkerhet, kontinuitetshantering, redundans och återställningsförmåga samt att tydliggöra roller och ansvar vid driftstörningar, kris eller krig. Syftet är att säkerställa att infrastrukturen bidrar till Sveriges digitala beredskap. Arbetet ska även beakta särskilda krav enligt NIS2-direktivet, CER-direktivet och säkerhetsskyddslagen.

12.2.2 Roller och ansvar i det fortsatta arbetet

Etableringen av infrastrukturen kräver samverkan mellan flera aktörer med olika roller och mandat. Digg har ett övergripande ansvar för att driva utvecklingen framåt, men genomförandet kan inte ske enbart inom myndighetens ramar. Flera andra aktörer behöver bidra aktivt, både strategiskt och operativt, för att skapa en fungerande helhet.

Regeringen

Regeringen behöver skapa långsiktiga förutsättningar för införandet genom att ge tydliga mandat och rättsligt stöd, exempelvis genom författningsändringar. Det är också viktigt att säkerställa stabil finansiering och styrning över tid, så att infrastrukturen kan utvecklas och förvaltas som en nationell tillgång.

Digg

Digg behöver fortsätta samordna utvecklingen av de gemensamma komponenterna, driva framtagandet av juridiska, tekniska och organisatoriska ramar samt stödja aktörer som vill ansluta. Myndigheten behöver även etablera processer för löpande uppföljning, vägledning och utveckling av infrastrukturen i takt med att fler aktörer ansluter.

Kommuner och regioner

Kommuner och regioner spelar en central roll i genomförandet, särskilt inom välfärdssektorn. Ett första steg är att börja planera för anslutning och se över interna processer för identitets- och behörighetshantering. På längre sikt behöver dessa aktörer bidra till förvaltning och vidareutveckling genom praktisk användning och återkoppling.

Myndigheter med särskilda uppdrag eller ansvarsområden

Myndigheter som ansvarar för tillitsramverk, register eller särskilda verksamhetsområden behöver bidra med expertis och delta i arbetet med att säkerställa att deras lösningar kan integreras i den gemensamma infrastrukturen. Detta gäller särskilt inom områden där interoperabilitet är avgörande, såsom hälso- och sjukvård och utbildning.

Branschorganisationer och leverantörer

Branschorganisationer och leverantörer är viktiga för att skapa bred anslutning och driva teknisk utveckling. De behöver successivt anpassa sina lösningar så att de kan fungera inom den föreslagna federationsinfrastrukturen och bidra till att marknaden utvecklas i enlighet med gemensamma standarder och principer.

Samspelet mellan aktörerna

För att arbetet ska lyckas krävs ett nära och strukturerat samspel mellan dessa roller. Det gemensamma ramverket måste balanseras med respektive aktörs ansvar, så att arbetet blir både samordnat och förankrat. En etablerad dialogstruktur och tydliga kontaktvägar mellan aktörerna är avgörande för framdrift, transparens och förtroende i genomförandet.

13 Konsekvensutredning

13.1 Problemställning, alternativa lösningar och konsekvenser om ingen förändring genomförs

Digg har fått ett uttryckligt uppdrag att ta fram och utveckla en sammanhållen infrastruktur för identitets- och behörighetshantering inom ramen för Ena – Sveriges digitala infrastruktur. Även om uppdraget kan genomföras på olika sätt förväntas Digg föreslå en lösning. Att inte lämna något förslag alls är därmed inte ett alternativ.

Digg har valt att föreslå en juridisk lösning som innebär att behörighetsinfrastrukturen i huvudsak regleras genom avtal mellan anslutna parter. Det skulle även vara möjligt att låta en större del av infrastrukturen regleras genom författning. Digg har dock bedömt att en sådan lösning, med hänsyn till bl.a. att utvecklingen på området är snabb och att ett regelverk behövs i närtid, inte är möjlig. Skälen för detta behandlas i avsnitt 4.4. och 4.5.

13.2 Beskrivning av vilka som berörs av förslagen

Den föreslagna federationslösningen kommer att i större eller mindre utsträckning beröra privatpersoner, företag, statliga, kommunala och regionala myndigheter samt organisationer av olika slag.

13.3 Kostnader för anslutning och anpassning

Den föreslagna infrastrukturen kommer på olika sätt att medföra kostnader för bland annat anslutning och anpassning av tekniska system för berörda företag, statliga, kommunala och regionala myndigheter samt organisationer av olika slag.

13.4 Konsekvenser för statliga myndigheter

Statliga myndigheter kan komma att ges uppdrag/roller inom infrastrukturen. Myndigheter som kommer att beröras av förslaget är bland annat. E-hälsomyndigheten, vars roll beskrivs närmare nedan, samt Skolverket och Vetenskapsrådet. Statliga myndigheter kan också beröras om de ansluter en digital tjänst till infrastrukturen. Digitala tjänster är en förutsättning för att lösningen ska bli relevant. Det är därför viktigt att statliga myndigheter på sikt ansluter digitala tjänster till infrastrukturen och blir utfärdare av behörighetshandlingar.

13.5 Konsekvenser för Digg

Förslaget innebär att Digg kommer att ansvara för att utveckla, reglera och tillhandahålla den förvaltningsgemensamma infrastrukturen – inklusive tekniska ramverk, kataloger, avtalsmodeller och centrala funktioner. Digg utvecklar och förvaltar generella funktioner som behövs för alla sektorer – exempelvis tekniska specifikationer, tillitsstrukturer, modeller för federationsområdesansvariga och incidenthantering. Sammantaget innebär detta ansvar för Digg

både på kort och lång sikt. De förmågor som Digg bedömt krävs för att förvalta infrastrukturen beskrivs i avsnitt 8.1.

13.6 Konsekvenser för E-hälsomyndigheten

E-hälsomyndigheten föreslår att myndigheten ska få fortsatt uppdrag med syfte att säkerställa att infrastrukturen kan användas inom hälso- och sjukvården. Fokus för fortsatt arbete kommer att ligga på tillämpning, förvaltning och vidareutveckling av infrastrukturen.

13.7 Konsekvenser för företag

Privata företag kommer att ha olika roller inom federationsinfrastrukturen. Detta kan t.ex. gälla för Inera AB (SKR:s digitaliseringsbolag) och Internetstiftelsen. Företag och andra icke-kommunala/regionala driftsformer (stiftelser, ekonomiska föreningar m.m.) som bedriver verksamhet inom t.ex. vård, omsorg och skola kommer att kunna ansluta till infrastrukturen. De kommer också att beröras i egenskap av arbetsgivare då deras anställda använder infrastrukturen. Företag som utvecklar olika former av systemstöd, appar osv. som används inom t.ex. vård och skola kan också komma att beröras.

13.8 Konsekvenser för andra organisationer

I takt med att användningen ökar kommer en stor mängd organisationer att indirekt vara berörda. Hit hör bland annat fackförbund, arbetsgivarorganisationer och branschorganisationer. Detta gäller exempelvis Vårdföretagarna, Sveriges företagshälsor, Vårdförbundet, Sveriges lärare, Sveriges läkarförbund, Svenska Kommunalarbetareförbundet, Friskolornas riksförbund och Idéburna skolors riksförbund.

13.9 Konsekvenser för enskilda

Enskilda påverkas inte direkt av infrastrukturen. De mål som finns i och med etablering av infrastrukturen syftar bland annat till att öka patientsäkerhet och patientintegritet samt förenkla delning av data mellan vårdgivare, vilket är till fördel för patienter.

13.10 Konsekvenser för kommuner och regioner

13.10.1 Konsekvenser för hälso- och sjukvården

Infrastrukturen som beskrivs i denna rapport är frivillig att använda. För vissa användningsområden kan det dock bli aktuellt att i praktiken göra anslutning till infrastrukturen obligatorisk. E-hälsomyndigheten gör bedömningen i sin rapport att aktörer inom hälso- och sjukvården kommer att behöva ansluta till identitet- och behörighetsinfrastrukturen för realisering av NDI inklusive införandet av EHDS. En ny konsekvensutredning behöver göras i fall infrastrukturen görs obligatorisk att använda, vilket dock inte är en del av detta uppdrag.

För en enskild organisation som, oavsett skäl, ska ansluta till infrastrukturen innebär det alltid att visst arbete krävs. Vårdgivare behöver ha system som är anpassade till de tekniska specifikationer som tagits fram. De leverantörer som tillverkar och säljer vårdinformationssystem och IAM-system behöver därmed anpassa sina system till dessa specifikationer. Kostnader för utveckling och anpassning av system lär i många fall belasta vårdgivare.

De organisationer som ansluter sina system behöver uppfylla de krav som ställs på t.ex. informationssäkerhetsarbete. Förutsättningar hos olika organisationer skiljer sig åt i dessa avseenden.

13.10.2 Offentlig upphandling

Den infrastruktur som Digg erbjuder kommuner och regioner kan omfattas av lagen (2016:1145) om offentlig upphandling (LOU). Om det däremot införs en reglering med innebörden att vårdgivare måste ansluta sig till tjänsten (obligatorisk anslutning) kan detta ses som en s.k. ensamrätt som faller utanför LOU. Det kan också spela roll om federationen är kostnadsfri, eftersom det då måste analyseras om det ändå är fråga om ett kontrakt i LOU:s mening. Om det inte är fråga om ett kontrakt behöver tjänsten inte upphandlas. En författningsreglering där Digg får ett uttalat uppdrag att kostnadsfritt tillhandahålla infrastrukturen skulle kunna medföra att tjänsten tas bort från det konkurrensutsatta området och blir en del av det offentliga åtagandet. En närmare analys av dessa frågor behöver göras i det fortsatta arbetet med finansieringslösning.

13.10.3 Konkurrensfrågor

I det fortsatta arbetet med finansiering kan även frågor om konkurrens behöva utredas närmare. Detta gäller bl.a. frågor om konkurrensbegränsade offentlig säljverksamhet, prissättning och tillåtligheten av säljverksamheten. I detta sammanhang behöver även förslagen i betänkandet Förbättrad konkurrens i offentlig och privat verksamhet (SOU 2025:22) analyseras.

13.10.4 Kostnader för kommuner och regioner

Kommuner och regioner kan också beröras om de ansluter en digital tjänst till infrastrukturen. Det är i dagsläget inte klarlagt hur finansierings- och prismodell kommer att se ut. Avgifter för anslutning och medlemskap i federationen kan därmed tillkomma. Frågan berörs i avsnitt 8.4.

13.11 Genomförande och ikraftträdande

Genomförandet av uppdraget kommer att behöva ske stegvis i takt med att infrastrukturen tas i bruk. Digg kommer löpande att informera berörda genom bl.a. information på myndighetens webbplats. De föreslagna ändringarna i Diggs instruktion bör träda i kraft så snart som möjligt.

13.12 Förslagens förenlighet med EU-rätten

De förslag till lösning som Digg lämnat överensstämmer enligt Diggs bedömning med de skyldigheter som följer av Sveriges anslutning till EU. I det fortsatta arbetet kommer EU-rättsliga

aspekter med koppling till bl.a. statsstöd, offentlig upphandling och tillämpningen av förordningen om det europeiska hälsodataområdet[22] att behöva beaktas.

[22] Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847

Bilaga 1

Diarienummer: 2025-04363

Klassificerings-ID:

Avsiktsförklaring för gemensamt arbete inom ramen för uppdrag att utveckla en sammanhållen infrastruktur för identitets- och behörighetshantering

Avsiktsförklaringen handlar om arbetsformer för samverkan och framtida användning av ekosystemet för identitets- och behörighetshantering inom ramen för Ena - Sveriges digitala infrastruktur.

Bakgrund och syfte

Regeringen har i regleringsbrev för budgetåret 2025 gett Myndigheten för digital förvaltning (Digg) i uppdrag att utveckla en sammanhållen infrastruktur för den identitets- och behörighetshantering som ska kunna tillhandahållas inom ramen för Ena – Sveriges digitala infrastruktur. Digg ska utföra uppdraget i nära samverkan med E-hälsomyndigheten för att möta behovet av att införa en nationell digital infrastruktur i hälso- och sjukvården, inklusive den nationella läkemedelslistan. Inom ramen för uppdraget ska Digg också analysera behovet av och lämna förslag på författningsändringar samt föreslå hur infrastrukturen fortsatt ska förvaltas och drivas, även i kris och krig.

På motsvarande sätt har E-hälsomyndigheten fått ett uppdrag i regleringsbrevet 2025 att ta fram och tillgängliggöra en sammanhållen infrastruktur för identitets- och behörighetshantering inom hälso- och sjukvården. Detta arbete ska ske i samverkan med Myndigheten för digital förvaltning och det förvaltningsgemensamma arbetet inom ramen för Ena – Sveriges digitala infrastruktur.

Uppdragen är viktiga steg i byggandet av ett nationellt ekosystem för identitets- och behörighetshantering. Det ska stärka digitaliseringen och underlätta samarbeten mellan offentliga och privata verksamheter.

Syftet med en gemensam avsiktsförklaring

Syftet med samarbetet är att lösa utmaningar om tillit och auktorisation vid informationsutbyte i offentlig sektor och med offentlig sektor. Lösningarna ska vara sektorsövergripande men lösa specifika problem. För att ha framgång i arbetet krävs ett gemensamt och samordnat arbete mellan fler aktörer än Digg och E-hälsomyndigheten. Denna avsiktsförklaring syftar till att formalisera alla deltagande parters gemensamma engagemang i att utveckla och att använda en sammanhållen infrastruktur för identitets- och behörighetshantering vid datautbyte.

Avsiktsförklaring

Parter

Denna avsiktsförklaring omfattar följande parter:

- E-hälsomyndigheten
- Inera AB
- Myndigheten för digital förvaltning (Digg)
- Skolverket
- Stiftelsen för Internetinfrastruktur (Internetstiftelsen)
- Sveriges kommuner och regioner (SKR)
- Vetenskapsrådet

Principer för fördelning av ansvar

Digg ansvarar för att leda och koordinera arbetet. Parterna har för avsikt att samarbeta enligt nedan under 2.3.

Samverkansformer

De ingående parterna beskriver genom detta dokument sin avsikt att:

- Aktivt delta i planering, utveckling och implementering av en sammanhållen infrastruktur för identitets- och behörighetshantering vid datautbyte.
- Identifiera och tillhandahålla relevanta resurser inom teknik och verksamhet för att bidra till effektiv utveckling av arbetet.
- Säkerställa nödvändig intern förankring inom det egna ansvarsområdet.
- Delta i regelbundna möten och avstämningar för att säkerställa transparens och samordning.
- Tydligt kommunicera sina respektive behov och krav inom ramen för samarbetet.
- Säkerställa att erforderliga resurser tillsätts för aktörens överenskomna åtaganden inom infrastrukturen.
- Eventuella meningsskiljaktigheter hanteras i det etablerade samarbetet mellan aktörerna.

Avsikt att följa ekosystemets principer

När ekosystemet för identitets- och behörighetshantering inom ramen för Ena är etablerat och dess principer är fastslagna är det parternas avsikt att följa dem för befintliga och kommande digitala tjänster.

Tid och kostnader

De parter som ingår i avsiktsförklaringen står för sin egen finansiering.

Giltighet och vidare arbete

Denna avsiktsförklaring börjar gälla när parter under 2.1 beslutat den. Avsiktsförklaringen ligger till grund för fortsatt samarbete och planering.

Anslutning

Parterna ansluter sig till arbetet efter att myndighetschefen eller motsvarande beslutat att ansluta till avsiktsförklaringen. När avsiktsförklaringen har trätt i kraft kan även nya aktörer ansluta sig förutsatt att de har för avsikt att följa denna avsiktsförklaring och att anslutningen godkänns av Digg.

Bilaga 2

Samverkan och förankring

Samverkan har varit en viktig arbetsmetod i arbetet med uppdraget eftersom den är en förutsättning för att vi ska kunna nå målen med infrastrukturen. Digg har bedrivit arbetet utforskande tillsammans med E-hälsomyndigheten och ett flertal aktörer. Under året har arbetet breddats från att initialt vara drivet av arkitekter med tekniskt fokus till att nu omfatta både fler kompetenser och fler organisationer. Syftet har inte bara varit att få fram konkreta leveranser, utan också ett förändrat samverkansklimat med tydliga strukturer och leveranser.

Digg och E-hälsomyndigheten har haft täta möten och workshops under året. I april 2025 anordnade Digg ett stormöte för att samla alla strategiska och operativa representanter, skapa en gemensam bild av uppdraget och starta ett strukturerat samarbete mellan alla delaktiga aktörer.

Strategisk och taktisk samverkan - ett utskott

Enas taktiska samverkansforum beslutade att det skulle bildas ett särskilt utskott för arbetet med infrastrukturen för identitets- och behörighetshantering. Utskottet bildades i januari 2025 med uppdrag att följa arbetet och fatta nödvändiga taktiska och strategiska beslut för att arbetet ska kunna fortskrida. Chefer för Digg, E-hälsomyndigheten, Inera AB, Skolverket, Internetstiftelsen, Vetenskapsrådet, SKR, Region Västra Götaland och Region Stockholm deltar i utskottet. Digg och E-hälsomyndigheten leder utskottsarbetet.

Aktörer i utskottet ingick en gemensam avsiktsförklaring (bilaga 1) i april 2025 om att aktivt delta i utveckling och införande av infrastrukturen, tillhandahålla tekniska och verksamhetsnära resurser, säkerställa intern förankring och långsiktig användning, samt följa gemensamma principer för en fungerande infrastruktur. Utskottet har haft månatliga möten.

Operativt arbete – arbetsgrupper

Det operativa arbetet har bedrivits inom teknik, verksamhet och juridik i arbetsgrupper där deltagande aktörer bjudits in att delta aktivt. Arbetsgrupperna har letts av Digg och E-hälsomyndigheten, med veckovisa möten för samordning mellan arbetsgrupperna.

Särskilt kring juridik och säkerhet

Digg har i det juridiska arbetet löpande tagit upp sådana frågor i det taktiska utskottet. Syftet har varit att tidigt väcka de juridiska frågorna och beskriva vad det juridiskt innebär att vara en deltagande aktör i lösningen för identitet och behörighet. Detta för att öppna upp för inspel och reflektioner.

I maj 2025 hade Digg möte med Nationellt cybersäkerhetscenter, NCSC, för att introducera vårt arbete och identifiera gemensamma säkerhetsperspektiv och samverkansmöjligheter. Digg och E-

hälsomyndigheten har genomfört en första workshop inom säkerhetsfrågor och detta arbete behöver fördjupas när infrastrukturen utvecklats vidare.

Förankringsarbete

Digg har löpande informerat, kommunicerat och samlat inspel i externa forum:

- Mars 2025: Forum för informationshantering inom skolväsendet – FFIS (anordnat av Skolverket).
- Maj 2025: Konferensen Vitalis (hälsa, vård och omsorg).
- September 2025: Leverantörsträff (anordnat av Digg).
- Oktober 2025: Konferensen Digitaliseringsforum (anordnat av Digg).
- November 2025: Webbinariet Digg forum med live-chatt (anordnat av Digg).
- Löpande: Träffar med privata aktörer tillsammans med E-hälsomyndigheten (anordnat av E-hälsomyndigheten).

Utöver detta har Digg publicerat information på digg.se, hänvisat via länkar till samverkansaktörer, och informerat om uppdraget även vid mindre sammankomster som till exempel anordnas av Sveriges kommuner och regioner. I informationen som Digg kommunicerar framgår det att uppdraget är en del av Ena – Sveriges digitala infrastruktur.

Dessa erfarenheter ger en grund för fortsatt kommunikation efter 2025, med ökat fokus på införandestöd och bred förankring i hela den offentliga sektorn och bland deras leverantörer.

Bilaga 3

Befintliga federationer

Federationer finns redan inom några samhällsområden. Denna bilaga ger en översikt av befintliga lösningar för identitets- och behörighetshantering inom olika verksamhetsområden. Beskrivningarna visar hur arbetet är organiserat, vilka aktörer som ansvarar för respektive område och vilka tekniska eller organisatoriska lösningar som används i dag. Syftet är att ge en samlad bild av nuläget och identifiera de erfarenheter och komponenter som kan vara relevanta för den fortsatta utvecklingen av en nationell infrastruktur. Begreppet federation används i dessa bakgrundsbeskrivningar i en vid mening, det kan avse både en ren teknisk federation och en federativ informationsstruktur.

Inledningsvis sammanställs de i följande tabell. Tabellen visar vad lösningarna heter och vilka delar som behöver vidareutvecklas för att de ska kunna samverka inom en gemensam nationell infrastruktur.

Samhälls-verksamhetsområde	Federation eller liknande lösning	Vad som saknas eller behöver utvecklas
Utbildning, skolväsendet **Utbildning, högre utbildning**	Skolfederation (SAML-baserad) Skolon (tjänsteplattform) Skolmyndighetsfederation (under etablering) Fidus (interfederation) Skolfederationens Moa (TLS-federation) Swamid	Interoperabilitet med andra verksamhetsområden
Kommunområdet **(ej vård och skola)**	Bilaterala avtal och säkerhetslösningar	Nationell federationsmodell, gemensam identitetsstruktur
Hälso- och sjukvård	Sambi (nationell, vård och omsorg)	Utvidgning till EHDS (Det europeiska hälsodataområdet) och privat sektor, rollharmonisering

Företagsregister (Bolagsverket)	Bilaterala avtal och säkerhetslösningar, Bolagsverket agerar ”avtalshub”	Attributstjänster för digitalt bruk i realtid, bredare anslutning
Fastighetsinformation (Lantmäteriet)	E-legitimering vid inloggning, ej federation	Federerad identitetslösning för aktörsintegration saknas
Folkbokföring och skatter (Skatteverket)	Navet (bilaterala avtal och säkerhetslösningar)	Modern federativ åtkomst med identitetskoppling och rollhantering
Energiområdet	Lokala och regionala digitala lösningar, ej enhetlig federation	Nationell federation för säker åtkomst och interoperabilitet mellan energibolag och nätoperatörer
Trafikområdet	Trafikverkets interna lösningar, ej verksamhetsövergripande federation	Federativ lösning för verksamhetsövergripande behörighetshantering mellan trafikmyndigheter och transportörer

Tabell 5: Visar lösningar som finns idag, vad de heter och vilka delar som behöver vidareutvecklas för att de ska kunna samverka inom en gemensam nationell infrastruktur.

Hälso- och sjukvårdsområdet

Hälso- och sjukvården är ett område där ansvaret delas mellan ett flertal aktörer. Regionerna har det övergripande ansvaret för att planera och tillhandahålla den allmänna hälso- och sjukvården för befolkningen, inklusive primärvård, specialistvård, akutsjukvård, psykiatri och tandvård inom folktandvården. Kommunerna ansvarar för viss hälso- och sjukvård inom särskilda boendeformer, hemsjukvård samt rehabilitering och habilitering inom äldre- och funktionshinderomsorgen. Därutöver finns privata och idéburna vårdgivare som bedriver vård i egen regi eller på uppdrag av regioner eller kommuner.

Verksamheten regleras genom bland annat hälso- och sjukvårdslagen (2017:30), patientdatalagen (2008:355), patientsäkerhetslagen (2010:659), dataskyddsförordningen (GDPR) samt i sekretessbestämmelser enligt offentlighets- och sekretesslagen (2009:400). Dessa regelverk ställer höga krav på sekretess, patientsäkerhet och spårbarhet, vilket gör säker identitets- och behörighetshantering helt avgörande. Åtkomst till vårdsystem måste alltid vara ändamålsbegränsad, rollstyrd och individuellt spårbar.

Ett stort antal aktörer är inblandade i hälso- och sjukvårdens digitala identitetshantering:

- E-hälsomyndigheten ansvarar för läkemedelsrelaterade system och e-hälsoutveckling, förvaltar den nationella läkemedelslistan och nationella åtkomsttjänster samt hanterar samverkan mellan apotek, vårdgivare och myndigheter.

- E-hälsomyndigheten ansvarar för läkemedelsrelaterade system och e-hälsoutveckling, förvaltar den nationella läkemedelslistan och nationella åtkomsttjänster samt hanterar samverkan mellan apotek, vårdgivare och myndigheter.
- Socialstyrelsen utfärdar yrkeslegitimationer och hanterar behörighetsfrågor, stödjer utvecklingen av e-hälsa, förvaltar nationella klassifikationer och koder (t.ex. ICD-10-SE, KVÅ) samt tar fram nationella riktlinjer som vägleder vård och socialtjänst. Myndigheten för register över legitimerad hälso- och sjukvårdspersonal (HOSP) enligt gällande förordning samt är sektorsansvarig myndighet för beredskapssektorn hälsa, vård och omsorg.[23]
- Inera driver HSA-katalogen (en elektronisk katalog med kvalitetsgranskade uppgifter om organisationer och personer inom vård och omsorg), Legitimeringstjänst IdP för medarbetare (verifierar användarens identitet och förser systemen med behörighetsgrundande information om användaren) samt plattformar som 1177, Journalen och NPÖ (Nationell patientöversikt, en tjänst som möjliggör att behörig vårdpersonal, med patientens samtycke, kan ta del av patientinformation från olika vårdgivare).[24]

Federerade lösningar används redan i viss mån. Sambi är en nationell infrastrukturlösning för identiteter och behörighetsstyrande attribut för den svenska vård- och omsorgssektorn.[25] Swamid används i vissa forsknings- och utbildningssammanhang, medan HSA-katalogen fungerar som adress- och attributkälla för federerad autentisering.[26] Samtidigt är inte alla vårdgivare anslutna, och parallella lösningar finns och detta försvårar samverkan.

Utbildningsområdet

Skolväsendet

Skolverket är sektorsmyndighet enligt skollagen (2010:800). Inom skolområdet finns identitetsfederationer som Skolfederation (drivs av Internetstiftelsen) och Skolon (som använder federativa standarder för inloggning men inte är en federation i formell mening) riktade till skolor, kommuner, fristående huvudmän och utbildningsrelaterade aktörer. Användarna är främst elever, lärare och administrativ personal inom de skolformer som omfattas av skollagen. För de fall som myndigheter, andra verksamhetsområden eller organisationer utanför skolväsendet vill kunna samverka över verksamhetsgränser har Skolverket tillsammans med Vetenskapsrådet, Sunet, startat en "interfederation".[27]

---

[23] https://www.socialstyrelsen.se/om-socialstyrelsen/det-har-ar-socialstyrelsen (2025-11-10).
[24] https://www.inera.se/tjanster/alla-tjanster-a-o (2025-11-10).
[25] https://sambi.se/medlem-i-sambi/vad-ar-sambi/ (2025-11-10).
[26] https://www.sunet.se/services/identifiering/swamid (2025-11-10).
[27] https://www.skolverket.se/prov-och-bedomning/provtjansten/tekniska-krav-och-vagledning/inloggningstjanst-och-e-legitimation/interfederationen-fidus (2025-11-10).

Högre utbildning

Universitetskanslersämbetet och Universitets- och högskolerådet ansvarar för tillsyn, kvalitetssäkring, antagning och statistik enligt högskolelagen, även om ingen formellt är sektorsmyndighet. Tillsammans utgör de statens institutionella infrastruktur för högre utbildning. Här finns identitetsfederationen Swamid, som drivs av Sunet inom Vetenskapsrådet, och används av studenter, forskare och personal inom universitet och forskningsinfrastruktur.

Federationer och samordning

Skolfederation och Swamid har vuxit fram genom intern samverkan och saknar uttryckliga regeringsuppdrag. De är separata med olika teknisk förvaltning, men kopplas samman genom Fidus, som gör det möjligt att använda Skolverkets digitala tjänster oavsett om medarbetarens organisation är ansluten till Skolfederation eller Swamid federationstillhörighet. Skolverket har inrättat Fidus, medan Sunet ansvarar för den tekniska infrastrukturen. Frågan om långsiktig förvaltning efter 2027 är ännu inte löst.[28]

Behörigheter

Identitetsintyg (SAML) från skolhuvudmän eller universitet innehåller uppgifter om identitet, organisationstillhörighet och roll (t.ex. student, forskare, rektor). Detta möjliggör styrning av åtkomst, licenstilldelning och samordning med e-legitimering.

Vård- och omsorgsverksamhet inom utbildningsområdet omfattas inte av Skolfederation eller Swamid, se ovan om hälso- och sjukvårdsområdet.

Kommunområdet

Kommunen är en offentligrättslig juridisk person med egen rättskapacitet och har ett brett uppdrag i enlighet med kommunallagen och särskild lagstiftning. Nämnder är organ inom kommunen och inte självständiga myndigheter – vilket får betydelse för informationsdelning och sekretess mellan olika verksamheter, till exempel mellan socialtjänst och bygglov.

Kommunen, eller i vissa fall respektive nämnd, är personuppgiftsansvarig för behandlingen av personuppgifter inom sina verksamheter och ansvarar för hanteringen av identiteter och behörigheter inom sina system.[29]

Vid sekretess mellan olika verksamhetsgrenar krävs tydliga organisatoriska och tekniska avgränsningar samt åtkomststyrning.

---

[28] https://www.skolverket.se/download/18.6a1930fe1999e2487adb2f2/1759476361247/pdf13326.pdf (2025-11-10).

[29] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/ (2025-11-10).

Socialtjänsten samverkar ofta med hälso- och sjukvården, men de utgör rättsligt skilda områden med egna lagstiftningar. Kommunerna ansvarar även för delar av hälso- och sjukvården, främst inom äldreomsorg, funktionsstöd och hemsjukvård.

Nationellt stöd ges av bl.a. av Myndigheten för samhällsskydd och beredskap (MSB), Boverket, Socialstyrelsen, Naturvårdsverket och Digg. SKR har en central roll i vägledning, samordning och intressebevakning, ofta i samarbete med myndigheter och Inera.

Det saknas en heltäckande kommunal federation för identitet och behörighetshantering. Istället används olika lokala lösningar, vilket skapar behov av integrationer. Fragmenteringen behöver ersättas av nationella federationsmodeller, anpassade för kommunala verksamheter men samordnade för effektiv digitalisering.

Trafikområdet

Inom trafik finns flera aktörer samt olika typer av identitetshantering för resenärer, personal och myndigheter. Transportstyrelsen anger till exempel att inloggning till deras digitala tjänster kan ske med e-legitimation (t.ex. BankID) eller via behörighetskod och registreringsnummer.[30]

Trafikverket beskriver i sin digitaliserings- och färdplansdokumentation att deras arbete sker i ett digitalt ekosystem med många aktörer och system.

Det innebär att:

- Myndigheter som Trafikverket och Transportstyrelsen använder e-legitimation och interna inloggningslösningar för att hantera behörighet och tjänster.
- Regioner och kommuner samt kollektiva trafiksystem i flera fall bygger egna digitala lösningar och portaler, ofta med lokala konton eller e-legitimation, men det finns inte tydliga offentliga uppgifter om en gemensam, övergripande federation för identitet och behörighet över alla transportslag. Studien "Digital självständighet – kollektivtrafikmyndigheter utvecklar egna digitala lösningar" pekar på att kollektivtrafikmyndigheter i vissa fall utvecklar egna lösningar.[31]
- Operatörer och leverantörer har egna system för personalåtkomst, åtkomststyrning och tekniska enheter – även om detaljerna kring identitet och behörighet för sådana interna system inte alltid är öppet redovisade.
- Digg har inte hittat uppgifter på att det i dagsläget finns någon fullskalig nationell federation för identitets- och behörighetshantering specifikt för trafiksektorn.

Nationella riktlinjer för identitetshantering inom trafiksektorn tycks saknas. Utvecklingen inom EU-regelverk (t.ex. eIDAS 2.0) och utvecklingen av digitala plånböcker kan särskilt komma att påverka hur identiteter för förare, passagerare och underleverantörer hanteras i framtiden. Samtidigt kvarstår behovet av nationell samordning och verksamhetsområdesövergripande

[30] https://www.transportstyrelsen.se/sv/om-oss/about-the-site/inloggning-till-vara-e-tjanster/ (2025-11-10).
[31] https://www.k2centrum.se/nyheter/digital-sjalvstandighet-kollektivtrafikmyndigheter-utvecklar-egna-digitala-losningar/ (2025-11-10).

principer för hur autentisering, behörighetstilldelning och ansvarsfördelning ska fungera i en distribuerad och komplex trafikmiljö.

Energiområdet

Svenska kraftnät är systemansvarig myndighet för Sveriges elöverföringssystem.[32] Energimarknadsinspektionen (EI) är tillsynsmyndighet för el- och energimarknaden enligt ellagen och förordningar.[33]

Inom energi- och elsystemet ställs höga krav på informationssäkerhet och ¬styrning för operatörer av samhällsviktiga tjänster — enligt t.ex. NIS2 direktivet och svensk lagstiftning om informationssäkerhet för samhällsviktiga och digitala tjänster.[34]

Det finns en bred rollfördelning med aktörer som nät- och stamnätsbolag, producenter, leverantörer, systemansvariga myndigheter och regulatorer. Dessa hanterar olika typer av identiteter — för personal och beteckningsmässiga roller, för tekniska enheter och åtkomster till styr- och driftssystem.

Även om specifik dokumentation kring gemensamma federerade identitetslösningar för energisektorn är begränsad, indikeras det att sektorn i hög grad består av organisations- och systemspecifika lösningar snarare än en sammanhållen nationell federation.

Utmaningar relaterade till säker informationshantering och autentisering blir tydliga i samband med digitalisering och integrering av elmarknadens system.[35]

Utvecklingen mot ett mer distribuerat energisystem — med lokala producenter, aggregatorer och nya tjänsteaktörer — ökar behovet av interoperabel identitetshantering, behörighetsstyrning och ansvarsfördelning för fjärråtkomst till känslig infrastruktur och tekniska gränssnitt.

Därtill är det klart att EU-regelverk som NIS2 kommer att påverka sektorn och sätta ökade krav på säkerhet, incidentrapportering och samverkan mellan aktörer.[36]

Bolagsverkets publicitetsregister

Vid juridisk behörighetskontroll är Bolagsverket en central aktör då myndigheten ansvarar för registrering av företag, föreningar och andra juridiska personer. Uppgifter om firmatecknare,

---

[32] https://www.svk.se/om-kraftsystemet/om-systemansvaret (2025-11-10).
[33] https://ei.se/om-oss (2025-11-10).
[34] https://www.energimyndigheten.se/en/cooperation/cybersecurity/network-and-information-security-nis (2025-11-10).
[35] https://embriq.no/en/news/enhancing-cyber-resilience-in-the-nordic-energy-sector-a-comprehensive-guide-to-nis2-compliance/ (2025-11-10).
[36] https://www.energimyndigheten.se/energiberedskap/informations--och-cybersakerhet/sakerhet-i-natverk-och-informationssystem/nis2 (2025-11-10).

styrelse, vd och andra med företrädanderätt registreras och har rättsverkan, vilket gör att tredje man kan förlita sig på informationen.[37]

Dessa uppgifter utgör ett centralt underlag för digitala identitets- och behörighetskontroller, där digitala identiteter kan kopplas till verifierbar information från Bolagsverkets register. Exempelvis vid åtkomst till tjänster eller digital signering av avtal.

Bolagsverket tillhandahåller flera digitala tjänster för åtkomst till uppgifter som är avgörande för juridisk behörighetskontroll. Ett registreringsbevis kan laddas ned som pdf med information om t.ex. firmatecknare, styrelse och bolagsform, och uppgifter om företag och deras företrädare kan hämtas direkt från näringslivsregistret.[38]

Särskilt viktiga är de maskin-till-maskin-tjänster som gör det möjligt att hämta företagsinformation i realtid via API:er. Här utmärker sig bastjänsten för grunddata om organisationer (SSBTGO), där Bolagsverket fungerar som operativt ansvarig myndighet i en lösning som bygger på federativa principer och ger myndigheter och offentliga aktörer säker och standardiserad åtkomst till grunddata om organisationer. Bolagsverket ansvarar för utveckling och förvaltning, medan andra aktörer som Skatteverket och SCB bidrar med data.[39]

Även verksamt.se, som drivs i samverkan mellan Bolagsverket, Skatteverket och Tillväxtverket, erbjuder tjänster för juridisk behörighetskontroll och kan integreras i digitala processer via API:er. Även om verksamt.se inte är en federation i sig, kan den ses som en del av en federerad modell genom att samla flera myndigheters tjänster under en gemensam inloggning.[40]

Lantmäteriet publicitetsregister

Lantmäteriet tillhandahåller uppgifter som har betydelse för behörighetsbedömningar när det gäller fastigheter. Lantmäteriet ansvarar för fastighetsregistret och för att registrera vem som äger respektive fastighet.[41]

Lantmäteriet tycks inte vara ansluten till någon identitetsfederation. Många offentliga aktörer behöver uppgifter från lantmäteriet, särskilt inom kommunal verksamhet, exempelvis vid bygglovshantering eller när en kommun inom sitt geografiska område övertagit ansvaret som lantmäterimyndighet från det statliga Lantmäteriet. Det finns därför behov av att kunna få tillgång till uppgifter om bland annat fastighetsägare på ett federerat sätt.

---

[37] https://bolagsverket.se/omoss.2047.html (2025-11-10).
[38] https://bolagsverket.se/sokforetagsinformation/registreringsbevis.5660.html?utm_source=chatgpt.com (2025-11-10).
[39] https://bolagsverket.se/omoss/utvecklingavdigitalatjanster/densammansattabastjanstenforgrunddataomorganisationerssbtgo/omssbtgo.5242.html (2025-11-10).
[40] https://verksamt.se/om-verksamt-se (2025-11-10).
[41] https://www.lantmateriet.se/sv/fastighet-och-mark/information-om-fastigheter/Min-fastighet/hjalp-och-tips-till-min-fastighet (2025-11-10).

Skatteverkets publicitetsregister

Skatteverket är inte direkt anslutet till någon specifik identitetsfederation. Det finns inslag av federativa principer i hur åtkomst till Skatteverkets informationssystem Navet hanteras, även om det inte är en traditionell identitetsfederation.[42] Denna federativa struktur används också för att ge tillgång till andra typer av information. Det är främst genom sin digitala tjänst Ombud och behörigheter som Skatteverket tillhandahåller behörighetsinformation. Där kan företag och privatpersoner utse ombud för att agera å deras vägnar i olika ärenden. Tjänsten möjliggör hantering av behörigheter för olika typer av ombud, såsom deklarationsombud, momsombud och registreringsombud.[43] För systemintegration erbjuder Skatteverket ett API för ombudshantering, vilket gör det möjligt för externa system att få information om vilka ombud som har en viss behörighet.[44]

---

42 https://skatteverket.se/offentligaaktorer/informationsutbyte/navethamtauppgifteromfolkbokforing.4.18e1b10334ebe8bc80001754.html?utm_source=chatgpt.com (2025-11-10).

43 https://www.skatteverket.se/privat/etjansterochblanketter/allaetjanster/tjanster/ombudochbehorigheter.106.74ada82d142bdcc36bb1bb.html?q=one+stop+shop&utm_source=chatgpt.com (2025-11-10).

44 https://www7.skatteverket.se/portal/apier-och-oppna-data/utvecklarportalen/api/ombudshantering/2.0.0/%C3%96versikt?utm_source=chatgpt.com (2025-11-10).