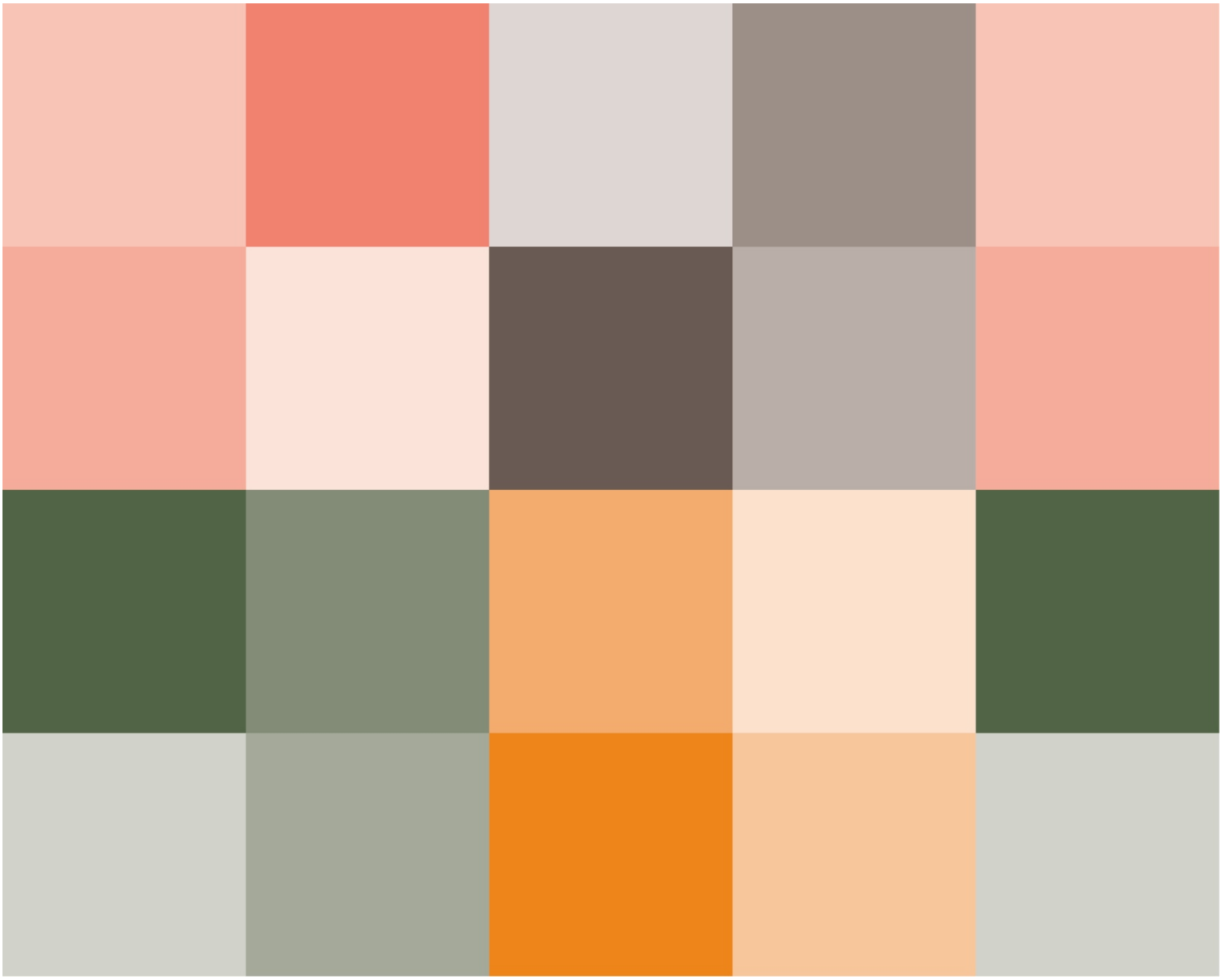


eID för medarbetare

Rapport inom Digital identitet

UTKAST 26 juni 2020. Får gärna spridas.

Skicka eventuella synpunkter eller anmäl intresse av att delta i proof-of-concept till eva.sartorius@digg.se senast 28 augusti 2020

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Det ska enkelt finnas tillgång till eID:n som kan användas av medarbetare i många externa tjänster. Behoven är stora enligt E-legitimationsenkäten 2019.

Det finns idag minst sex organisationer som erbjuder svenska eID:n som arbetsgivare kan anskaffa till sina medarbetare. Tre alternativ är offentliga och tre är privata. I tillägg till dessa alternativ finns det organisationer som har egna säkra eID-lösningar som personalen använder. Trots att det finns eID:n för medarbetare finns det inget eID-alternativ för medarbetare som idag är valbart i ett stort antal externa tjänster.

Vi föreslår därför att ett enkelt avtal tas fram som knyter ihop eID-utfärdare med förlitande parter. Avtalet ska erbjuda kostnadsfria transaktioner. Det kan fungera därför att anskaffning mot ersättning genomförs av arbetsgivaren. Kostnaden som arbetsgivare betalar eID-utfärdaren tar redan idag vanligen höjd för användning i interna och externa digitala tjänster.

Kvalitetsmärkning ska vara ett krav i avtalet eftersom det är viktigt att veta vilka eID:n som det går att lita på. Alla eID-utfärdare, även offentliga och de som har en intern lösning, har möjlighet att ansöka om kvalitetsmärkning hos DIGG. Två av de sex alternativen, Freja eID+ och SITHS, har redan sådan kvalitetsmärkning.

Avtalsparterna ska delta i den nationella digitala infrastrukturen Sweden Connect, som är den identitetsfederation som DIGG ansvarar för och där den svenska eIDAS-noden finns. Motivet är att elektronisk identifiering av medarbetare ska ske på ett standardiserat, effektivt och säkert sätt över organisationsgränserna.

Tillgång till aktuell behörighetsinformation om medarbetare är centralt för att rätt användare ska få rätt tillgång i en digital tjänst. Att det behövs nationell digital infrastruktur även för attributförsörjning råder det inga tvivel om. Förstudien belyser sex olika attributförsörjningsmönster som behöver utvärderas mer detaljerat och stämmas av med flera parter innan förslag om nationella digital infrastruktur tas fram.

Slutligen är medarbetares möjligheter till e-underskrift en mycket viktig funktion, såväl externt som internt. Huvudmönstret bör vara, precis som för privatpersoner, att medarbetaren skriver under i anslutning till den digitala tjänst som används, det vill säga med stöd av en till e-legitimationen fristående underskriftstjänst. Validering av inkommande underskrivna handlingar består av flera utmaningar som till viss del behöver lösas gemensamt, bland annat med valideringsintyg.

Innehållsförteckning

1 Inledning

Det saknas idag ett fullgott nationellt ekosystem för e-legitimation i tjänsten som täcker fallet när medarbetare som tillhör en organisation ska logga in i andra organisationers digitala tjänster. Det finns sektorsvisa lösningar och det finns e-legitimationer, men alla förutsättningar för att knyta ihop delarna till en nationell helhet har så här långt inte funnit på plats.

Ett nationellt ekosystem för e-legitimation i tjänsten har stor betydelse för förmågan till effektivt informationsutbyte i de fall informationsutbyte via API:er inte räcker utan behöver kompletteras med manuell åtkomst för interna eller externa medarbetare.

Medarbetares användning av e-legitimation (eID) har därför stått i fokus i detta förstudiearbete. Under arbetet har vi tagit sikte på att det nationella ekosystemet ska fungera för medarbetare och digitala tjänster i både offentlig och privat sektor, däribland inte minst offentligfinansierad privat verksamhet.

Frågorna vi har studerat är:

- Försörjning med eID för medarbetare
- Avtal som passar med medarbetares användning
- Informationssäkerhet, federationslösning, tillits- och policyfrågor
- Mönster för behörighetsgrundande information
- E-underskrift för medarbetare

Förstudiearbetet har bedrivits som en del av regeringsuppdraget om effektivt informationsutbyte, inom byggblocket Identitet.

2 Behov

Behovet av säkert informationsutbyte i det digitala ekosystemet handlar till stor del om hur organisationer kan fungera bättre tillsammans genom gränsöverskridande digitaliserade processer som utgår från privatpersoners och företagares behov i ett livshändelseperspektiv (både nationellt och internationellt). Sådana behov kan uppfyllas bäst genom **organisatorisk tillit** och ett säkert elektroniskt informationsutbyte mellan berörda organisationer (via API).

Ett av många exempel på externt informationsutbyte via API:er är polisens tillståndshandläggare för vapenlicenser som via det egna verksamhetssystemet kontrollerar godkänd jägarexamen i Naturvårdsverkets jägarregister genom API-

fråga på den sökandes personnummer.[1] Handläggaren har då identifierat sig mot polisens verksamhetssystem och Naturvårdsverket hyser tillit till den identifieringen.

2.1 Behov av eID för medarbetare

När möjligheter till direkt informationsutbyte (via API) inte finns kan det istället vara aktuellt att en medarbetare i en organisation loggar in och utför något i en digital tjänst som tillhör en annan organisation, exempelvis fakturahantering hos Statens servicecenter eller orosanmälan hos socialtjänsten i kommunen. I de fallen behöver medarbetaren ha tillgång till minst en i sammanhanget användbar e-legitimation (eID). Det finns således behov av att medarbetares e-legitimationer kan fungera både externt och internt.

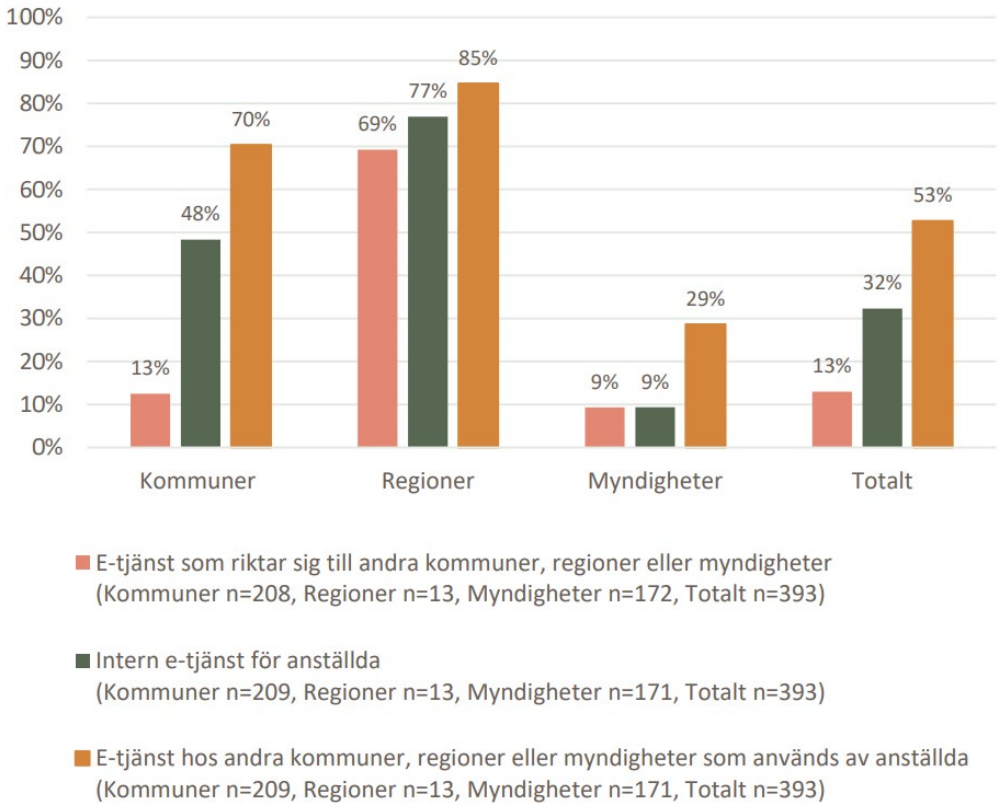
Om e-legitimationen är kvalitetsmärkt av myndigheten DIGG kan organisationen som ansvarar för den digitala tjänsten på goda grunder hysa samma tillit till en e-legitimation oavsett om den är anskaffad av medarbetaren som privatperson eller av arbetsgivaren för medarbetarens räkning.

Däremot kan villkoren vid användning skilja sig åt, exempelvis vad gäller ersättning till eID-utfärdaren. En medarbetare kan behöva använda sin e-legitimation många gånger under en arbetsdag. Det finns därför ett behov hos ansvariga för digitala tjänster av överskådliga kostnader för medarbetares användning av e-legitimation. Det kan även finnas arbetsrättsliga eller praktiska skäl för arbetsgivare att anskaffa e-legitimationer till sin personal.

2.2 E-legitimationsenkäten pekade på tydliga behov

Drygt hälften av de organisationer som besvarade E-legitimationsenkäten 2019 uppger att deras anställda använder e-legitimation för att logga in i tjänster hos andra kommuner, regioner eller myndigheter. Ungefär en tredjedel av organisationerna uppger att de har interna tjänster riktade till anställda där e-legitimation används.

[1] https://www.naturvardsverket.se/Nyheter-och-pressmeddelanden/Nyhetsarkiv/Nyheter-och-pressmeddelanden-2018/Forenklad-handlaggning-av-vapenlicens-till-jagare/



Figur 2: andel med e-tjänster för anställda inom offentlig förvaltning

Av de organisationer som erbjuder tjänster riktade till andra kommuner, regioner och myndigheter uppger knappt hälften att de även har tjänster som kräver e-underskrift. Motsvarande andel för interna tjänster riktade till anställda är knappt 40 procent. Av dem som anger att anställda använder e-legitimation för att logga in i tjänster som erbjuds av andra uppger 42 procent att de anställda även använder sig av e-underskrift i dessa tjänster.

2.3 Motsvarande behov finns även i privat sektor

Under förstudiearbetet har det i flera sammanhang påtalats att det är viktigt att försöka hitta ett ekosystem som fungerar även för medarbetare i privat sektor, exempelvis ordningsvakter. Ekosystemet ska om möjligt även inkludera möjlighet för digitala tjänster i privat sektor, exempelvis privata vårdgivares tjänster.

2.4 Behov av behörighetsgrundande information

Digitala tjänster erbjuder vanligen funktionalitet eller utökad information för vissa organisationer eller för vissa medarbetare. I det fallet behöver den digitala tjänsten ha tillgång till ytterligare behörighetsgrundande information (s.k. attribut) om medarbetaren än att bara veta vem det är. Uppgifterna kan exempelvis handla om vilket uppdrag eller vilka fullmakter medarbetaren har. Det finns ett stort behov av att denna information ska vara aktuell, och att den överförs på ett säkert och

automatiserat sätt, så att tillit till attributen kan säkerställas. Läs mer om attributförsörjning i avsnitt 6.

2.5 Informationsklassning och e-legitimationers tillitsnivå

Medarbetare som ska komma åt sekretessbelagd information kan behöva ha e-legitimation som uppfyller en högre tillitsnivå än övrig personal. Därför är det viktigt med informationsklassning för att avgöra vilken lägsta godtagbara tillitsnivå som ska gälla för e-legitimationer i en digital tjänst.

Informationsklassning innebär att man värderar sina informationstillgångar, som exempelvis kan nås via digitala tjänster, utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet. Informationsklassning kan även avse behörighetsgrundande attribut. Informationstillgångarna graderas i konsekvensnivåer.

Informationstillgångarna skyddas genom att koppla adekvata säkerhetsåtgärder till varje konsekvensnivå. Genom att man kopplar säkerhetsåtgärder till organisationens konsekvensnivåer får man så kallade **skyddsnivåer**.

När man kopplar säkerhetsåtgärder till konsekvensnivåerna är det viktigt att inte bara se till informationens värde och de oönskade konsekvenserna. Man behöver också väga in en riskbedömning. Hur stor är sannolikheten att information i en viss klass exponeras för en risk som innebär att den oönskade konsekvensen inträffar? Vilka säkerhetsåtgärder krävs för att minska just den risken? Det riskområde som kan orsaka störst skada vid felaktig identifiering av en användare ska ses som avgörande för vilken lägsta tillitsnivå på e-legitimation som tillåts.

E-legitimationer delas in i olika **tillitsnivåer**, där en tillitsnivå anger graden av skydd en e-legitimation på den nivån medför. Skyddsbehovet bedöms i förhållande till vilken grad av **skada** (begränsad, måttlig, betydlig, allvarlig) som kan uppstå. Skadorna delas in i följande typer

- Olägenhet, oro eller ryktesskada
- Finansiell skada eller skadeståndsansvar
- Röjande av känsliga uppgifter till obehöriga
- Brottsyttringar
- Skada på verksamhet och allmänintresse
- Personsäkerhet

Om exempelvis röjande av känsliga uppgifter till obehöriga skulle leda till betydande skada, bör tillitsnivå 3 enligt Tillitsramverket för Svensk e-legitimation väljas. Om det skulle leda till måttlig skada krävs eventuellt fortfarande stark

autentisering men då kan tillitsnivå 2 enligt samma tillitsramverk ge tillräckligt skydd. Läs mer om tillitsnivåer på DIGG:s webbplats.[2]

2.6 Övriga behov som identifierats

Utöver de behov som presenterats i de föregående delavsnitten har förstudien även identifierat följande behov:

- eID:n ska utformas så att de kan användas likvärdigt av alla medarbetare, oavsett kön och funktionsvariationer
- En medarbetare kan ha flera olika uppdrag hos en arbetsgivare och även ha uppdrag hos flera arbetsgivare
- Vanligen krävs det flera uppgifter om en användare än bara vem det är och vilken organisation som beställt e-legitimationen för att parten som är ansvarig för en digital tjänst ska kunna besluta om tillgång till tjänsten (auktorisation)
- Medarbetare kan vid användning av e-legitimation behöva ett ”digitalt omklädningsrum” till anställningsidentitet eller till annan pseudonym för personnummer, styrkt samordningsnummer eller utländskt personidentitetsbegrepp
- Medarbetare har behov av att informeras om vilka attribut som överförs om dem och det gäller såväl eID-utfärdare som andra intygsutfärdare. Bara för att ett exempelvis BankID används hos arbetsgivaren måste arbetsgivaren inte föra personnumret vidare till den digitala tjänst som medarbetare ska få åtkomst till
- Arbetsgivare behöver ha kontroll över behörighetsgrundande information om sina medarbetare så att den är korrekt och det är särskilt viktigt i samband med att en medarbetare avslutar sin anställning eller sitt uppdrag
- Det behövs reservlösningar till om en medarbetare har glömt sitt eID hemma eller om en ny medarbetare mycket snabbt måste ha tillgång till eID. Här kan så kallade id-växlingar från tillåta eID:n, underskrivna intyg från kollegor m.m. nyttjas bättre än idag.
- Det är viktigt för användbarheten med single sign-on (SSO) mellan tjänster i ett sammanhang, exempelvis interna tjänster eller inom ett visst verksamhetsområde. SSO för interna tjänster främjar även säkerhet och kostnadseffektivitet för minskad administration kring lösenordshantering.
- Typen av bärare av eID, exempelvis mobil lösning eller lösning på kort, samt om det är trådlös eller trådbunden kommunikation etc. kan vara viktiga krav i vissa yrkesgrupper
- Medarbetarens eID ska kunna användas både i Sverige och utomlands, åtminstone i tjänsten

[2] https://www.digg.se/digital-identitet/e-legitimering/offentlig-aktor/tillitsnivaer/

- Medarbetare med utländskt eID ska kunna använda sitt eID i Sverige (i enlighet med eIDAS-förordningen)
- Det behövs flera oberoende eID-lösningar så att det finns möjlighet till reservlösning exempelvis vid driftstörning eller allvarlig incident
- Kostnadsdrivande spretighet mellan sektorer ska undvikas och standardisering och enhetlighet eftersträvas
- Behoven är till viss del verksamhetsspecifika och därför bör arbetsgivare kunna ställa krav i samband med anskaffning av eID till sina medarbetare
- Det ska vara möjligt att internt eller bilateralt följa andra specifikationer än de nationella, där ett nu aktuellt exempel är OpenID Connect jämfört med SAML 2.0
- Icke nödvändig administration och felregistreringar ska undvikas
- Medarbetare har behov av att skriva under elektroniskt både externt och internt.
- Organisationer, och i vissa fall deras medarbetare, har behov av att validera elektroniska underskrifter både internt och över organisationsgränser

3 Försörjning med eID för medarbetare

eID för medarbetare skiljer sig inte från eID för privatpersoner på annat sätt än att arbetsgivaren är huvudansvarig för anskaffning och spärr av e-legitimationen. Rutinen för utfärdande av e-legitimationen kan underlättas av om arbetsgivare i förhållande till eID-utfärdaren kan ikläda sig delansvaret för att grundidentifiera användaren i samband med ansökan om utfärdande av eID.

I och med anskaffningen är eventuell upphandling redan genomförd och det finns en möjlighet för eID-utfärdaren att bidra med organisationsnummer och namn på den anskaffande arbetsgivaren i de identitetsintyg som ställs ut vid autentisering, samt en eventuell pseudonym till användarens personnummer eller styrkta samordningsnummer. Överföring av ytterligare behörighetsgrundande information kan göras antingen av med hjälp av eID-utfärdaren eller annan leverantör, läs mer i avsnitt 6.

3.1 Ekosystem där både privata och offentliga eID-utfärdare och förlitande parter är välkomna

I Sverige har vi en modell där både privat och offentligt utfärdade e-legitimationer är välkomna. På privatpersonssidan är BankID den helt dominerande lösningen, men även Freja eID+, AB Svenska Pass och Telia finns som alternativ. En statligt utfärdad e-legitimation är föreslagen (SOU 2901:14). I många fall används privat anskaffade e-legitimationer även i tjänsten, enligt E-legitimationsenkäten 2019.

Under förstudiearbetet gjorde vi en inventering av vilka eID:n för medarbetare som finns idag. Vi fann tre offentliga och tre privata alternativ som för närvarande kan anskaffas av arbetsgivare. Det är troligt att fler kan tillkomma.

Slutsatsen vi drar är att både offentliga och privata eID-utfärdare ska välkomnas i fallet med eID för medarbetare. Dessutom bör privat anskaffade e-legitimationer allmänt sett inte uteslutas från användning i tjänsten, däremot kan det finnas hinder mot sådan användning, exempelvis styrt av arbetsgivarens policy. I tillägg till detta finns interna eID-lösningar med potential att kunna användas externt.

De identifierade externa eID-alternativen och eID-utfärdarna är:

1. SITHS från Inera AB
2. EFOS från Försäkringskassan
3. eduID från SUNET
4. Freja Organisation eID från Verisec AB
5. Telia e-legitimation från Telia
6. Smart ID från Nexus

Dessa ska ses som exempel att utgå från, inte som en uttömmande lista.

3.2 SITHS

Identifieringstjänsten SITHS består bl.a. av en e-legitimation från Inera AB som kan användas av alla regioner, kommuner, privata vårdgivare och statliga myndigheter. SITHS gör det möjligt för användare att identifiera sig med stark autentisering vid inloggning i e-tjänster.

SITHS e-legitimation används i nuläget av ca 600 000 medarbetare inom vård och omsorg för att uppfylla kraven på stark autentisering vid åtkomst till information. SITHS är kvalitetsmärkt av DIGG på tillitsnivå 3.

Inera kommer att göra stora förändringar i SITHS-tjänsten under kommande år. Tjänsten moderniseras och utökas med stöd för bl.a. mobila lösningar.

3.3 EFOS

EFOS är ett statligt eID-alternativ som på frivillig grund har fokus på arbetsgivare i staten. Försäkringskassan är eID-utfärdare.

I skrivande stund är det 42 000 medarbetare som har EFOS och antalet är i växande. Försäkringskassan har ansökt hos DIGG om kvalitetsmärkning och arbete med detta pågår. EFOS har kompletterats med en mobil variant, kallad mobilt EFOS.

3.4 eduID

eduID är en digital identitet för organisationer inom utbildning och forskning. Med eduID kan studenter och anställda vid lärosäten komma åt sina digitala resurser.

En eduID identitet kan användas före, under och efter studietiden. Statliga SUNET ansvarar för eduID.

3.5 Privat sektors utbud för medarbetare

Freja eID+ från Verisec AB finns i en variant avsedd för medarbetare, Freja Organisation eID. Freja eID+ är kvalitetsmärkt av DIGG på tillitsnivå 3 och finns med i den nationella identitetsfederationen Sweden Connect, som drivs av DIGG.

Andra alternativ som kan upphandlas är Nexus SmartID och Telia, båda väletablerade aktörer på området, precis som ID06 inom exempelvis byggsektorn. De alternativen är dock ännu inte kvalitetsmärkta av DIGG.

3.6 Organisationens egen lösning

En del organisationer har byggt upp egen eID-lösning för medarbetare, t.ex. Polismyndigheten och Åklagarmyndigheten. Samma sak kan gälla arbetsgivare i privat sektor. Det finns möjlighet även för dem att bli kvalitetsmärkta av DIGG och de skulle därmed kunna ingå bland de eID:n som kan användas i många externa digitala tjänster.

3.7 Privat anskaffade svenska e-legitimationer

Även privat anskaffade eID:n kan tillåtas i digitala tjänster som riktar sig till medarbetare och tillitsnivåerna är desamma som för eID för medarbetare. Däremot kan det skilja sig vad gäller affärsvillkoren och beträffande möjligheten att i eID-utfärdarens identitetsintyg få tillgång till ett organisationsnummer kopplat till användaren. Andra mönster för överföring av organisationsnummer och andra uppgifter om medarbetare finns, läs mer i avsnitt 6.

3.8 Kvalitetsmärkning av eID är viktigt för tilliten

Vi föreslår att eID för privatpersoner och eID för medarbetare ska följa samma tillitsramverk: Tillitsramverket för Svensk e-legitimation (DIGG). eID-utfärdaren ansöker till DIGG om granskning mot tillitsramverket och efter godkänt resultat får eID-utfärdaren använda DIGG:s kvalitetsmärke för Svensk e-legitimation.

4 Avtal om medarbetares användning av svenska eID:n

I fallet med medarbetares användning av eID som är anskaffade av arbetsgivaren föreslår vi att ersättning för användning av e-legitimationen inkluderas i de avgifter som eID-utfärdaren enligt avtal får från arbetsgivaren som anskaffat e-legitimationerna.

Därmed blir det möjligt med ett avtal mellan eID-utfärdare och förlitande parter om användning utan ersättning, ett avtal som således inte innebär upphandling

eftersom anskaffningen redan är genomförd av arbetsgivaren. Därför kan avtalet vara öppet för både offentliga och privata förlitande parter. Andra godkända eID:n med kostnadsfria transaktioner än de för medarbetare kan också inkluderas.

4.1 Nytt avtal med kostnadsfria transaktioner inom Sverige

Vi föreslår att DIGG tar fram en avtalsreglering om ”elektronisk identifiering utan ersättning” som ett komplement till den reglering som redan finns eller är planerad.

Avtalsparterna är svenska **eID-utfärdare** i offentlig och privat sektor som har kvalitetsmärkning från DIGG och **förlitande parter** i offentlig och privat sektor i Sverige.

Funktionen består av elektronisk identifiering, det vill säga att eID-utfärdaren på begäran av förlitande part e-legitimerar användare och i anslutning till detta ställer ut identitetsintyg till förlitande part.

Översiktliga villkor för att nå tillit och standardisering:

- eID-utfärdaren ska vara godkänd av DIGG för de e-legitimationer som ansluts
- Båda parter ska a) ingå i aktörsregistret i den nationella identitetsfederationen Sweden Connect och b) följa Tekniskt ramverk för Sweden Connect
- eID-utfärdaren tillhandahåller funktionen utan ersättning.

Genom ett sådant avtal byggs ekosystemet ut på ett standardiserat och enhetligt sätt. Vi har sonderat möjligheten med de sex identifierade eID-utfärdarna och fått positiv respons.

Ett förberedande arbete med avtalsmodellen har därför inletts inom ramen för förstudiearbetet. En enkel avtalskonstruktion kan nå framgång på kort tid om möjligheten kommuniceras ut på ett bra sätt. Därmed kan kvalitetsmärkta eID:n för medarbetare börja användas på betydligt bredare front än hittills.

Att ingå detta avtal ska inte utesluta att andra avtal, om exempelvis att använda en annan teknisk metod internt, kan slutas och ”gå före” detta avtal.

4.2 Möjlighet till användning utomlands

Användning av svenska kvalitetsmärkta eID:n utomlands behöver regleras i anslutning till det pågående arbetet med anmälan av svenska eID:n enligt EU:s eIDAS-förordning.

4.3 Möjlighet till användning av övriga eID:n

Denna förstudie föreslår **inte** att andra eID:n eller inloggningslösningar än de som kommer att ingå enligt ovanstående avtalsförslag ska uteslutas som valbara alternativ för medarbetare i digitala tjänster. Exempel kan vara BankID och

Migrationsverkets kommande lösning. Valbarheten styrs i dessa fall av andra regler och avtal.

5 Användning av medarbetares utländska eID:n

5.1 Användning av eID enligt eIDAS-förordningen

Som stöd för identifiering (autentisering) av användare med eID från annat land finns EU:s eIDAS-förordning. Ett ökande antal länder har eID:n som fungerar över landsgränserna och det finns allmänt sett en skyldighet för offentliga organ att acceptera dessa. Det finns möjlighet för andra än EU:s medlemsstater att avtalas in i eIDAS. Norge, Island och Lichtenstein är exempel på det.

eIDAS tekniska specifikationer innehåller ett identitetsattribut för fysiska personer som sätts av eID-landet och unikt avser endast en person. Begreppet ska vara så stadigvarande (persistent) som möjligt. Däremot kan en fysisk person ha flera identitetsbegrepp i vissa länder. Det är även tillåtet för länderna att skicka pseudonym för det ordinarie personidentitetsbegreppet.

Den svenska eIDAS-noden (DIGG) underlättar för svenska digitala tjänster genom att konvertera de utländska identitetsintygen så att de följer Tekniskt ramverk för Sweden Connect och det finns en flagga för hur landet gör med sina personidentitetsbegrepp. Lösningen finns på plats och svenska förlitande parter ansluter sig löpande till Sweden Connect och den svenska eIDAS-noden.

Transaktionerna (”Foreign eID”) är lagstyrda och kostnadsfria för offentliga förlitande parter. Förlitande parter i svensk privat sektor får också ingå anslutningsavtalet hos DIGG. Det land som anmäler eID får enligt eIDAS-förordningens regler bestämma ersättningsvillkor för förlitande parter i privat sektor kopplat användning av dessa eID:n. Inget av de länder som har anmält sina eID har hittills gjort det.

Ett behov som skulle öka användningen är att nationellt, reglerat och med goda rutiner, bygga upp ett register som kopplar ihop en användares utländska personidentitetsbegrepp med användarens svenska personnummer eller styrkta samordningsnummer för att kunna ge medarbetare, företagare och privatpersoner god service genom tillgång till rätt digitala tjänster i Sverige.

5.2 Internationell användning av eID:n inom högskolesektorn

Inom den akademiska världen används redan eID:n över landsgränserna i stor utsträckning. Den svenska delen består av eduID (se avsnitt 3.4) och av identitetsfederationen för forskning och högre utbildning, SWAMID.

SWAMID har motsvarigheter i resten av världen som är kopplade till varandra. Förlitande parter får information om tillitsnivå och användarens tillhörighet som student eller anställd hos en akademisk organisation. Inom utbildningssektorn fungerar detta som tjänstelegitimationer som spänner över organisationsgränser och landsgränser.

6 Digitala tjänsters försörjning med behörighetsinformation

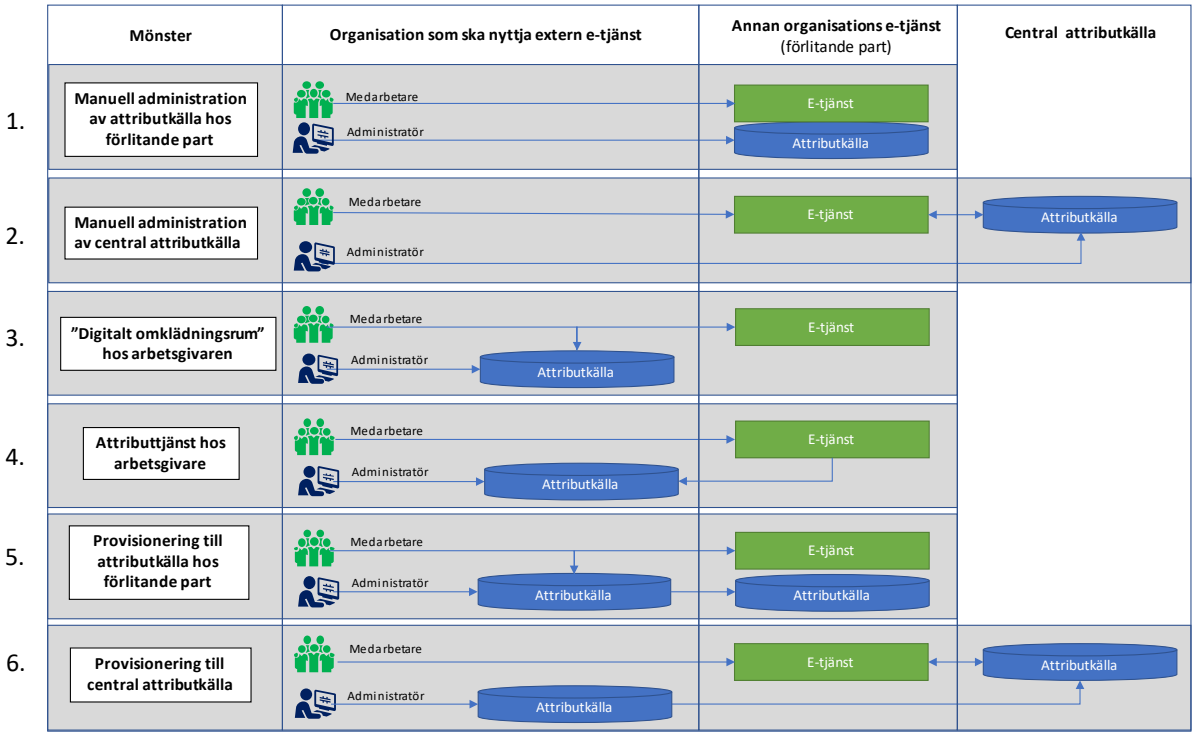
6.1 Stora behov och stora utmaningar

Den digitala tjänst som medarbetaren ska använda måste ha tillgång till relevanta uppgifter om medarbetaren för att kunna fatta korrekta beslut om medarbetarens tillgång till tjänsten (auktorisation). Uppgifternas konfidentialitet, riktighet, tillgänglighet och spårbarhet är centrala behov för att det ska bli rätt. Dessa behov är inte alltid lätta att uppfylla och det är viktigt att arbetsgivarna har genomtänkta lösningar så att ändrade uppgifter om en medarbetare skyndsamt får genomslag på alla nödvändiga ställen.

Den personliga integriteten ska värnas genom att inte överföra överskott av information och det är viktigt att den förlitande parten på ett korrekt sätt hanterar uppgifterna om medarbetare, däribland i enlighet med Dataskyddsförordningen. Endast uppgifter som både kan lämnas ut och efterfrågas, ska lämnas ut.

Vi har under förstudiearbetet identifierat sex olika huvudmönster för hur behörighetsgrundande attribut kan överföras från arbetsgivaren till en annan organisations digitala tjänst. I alla mönster förutsätter vi att de rättsliga förutsättningarna finns på plats. Varje mönster har sina för- och nackdelar.

Uppräkningen av mönster är sannolikt inte heltäckande, utan beskrivningen ska ses som ett första försök som därefter kan förädlas vidare. Här finns även beroenden till andra uppdrag och byggblock för nationell digital infrastruktur, exempelvis Mina ombud och Auktorisation.



Figur: översikt över mönster för överföring av behörighetsgrundande attribut om en medarbetare

6.2 Manuell administration av attributkälla hos förlitande part

Det första mönstret består av att en behörig person hos arbetsgivaren manuellt registrerar personalens information och behörigheter i en extern attributkälla hos den organisation som tillhandahåller en viss extern e-tjänst (förlitande part). E-tjänsten identifierar användaren och fattar beslut om tillträde (auktorisation) baserat på behörighetsgrundande attribut i e-tjänstens egen attributkälla.

På kort sikt förefaller detta mönster vara det enklaste, men över tid har mönstret stora nackdelar. Den stora nackdelen är att arbetsgivaren riskerar att tappa kontrollen över vilka medarbetare som finns registrerade var. En viktig nackdel är också att e-tjänsten riskerar att förlita sig på attribut som inte längre är aktuella. Dessutom finns det potentiella säkerhetsluckor vid upplägg av administratören, särskilt den första gången.

Att samla uppgifter om personal nära den digitala tjänsten kan i vissa fall ändå vara effektivt om det fungerar väl, men det måste samtidigt vägas mot att personuppgifter, som till en del kan vara känsliga eller sekretessbelagda, riskerar att bli tillgängliga på ett samlat sätt hos en annan ansvarig organisation. Denna nackdel löses bäst ett genom automatiserat informationsutbyte i stället för att ha manuella externa digitala tjänster.

6.3 Manuell administration av central attributkälla

En behörig person registrerar medarbetare manuellt i en extern central attributkälla, dit e-tjänster från olika organisationer vänder sig med förfrågan efter identifiering av användaren.

En central attributkälla med attribut av nationellt intresse, exempelvis receptförskrivare eller firmatecknare, är effektivt och betydelsefullt. Att lokala administratörer samlar uppgifter om personal centralt kan också vara effektivt men det måste vägas mot att personuppgifter, som till en del kan vara känsliga eller sekretessbelagda, kan bli tillgängliga på ett samlat sätt hos en annan ansvarig organisation. Skydd behövs för obehörig åtkomst till uppgifterna.

Det är i fallet med manuell registrering i central attributkälla viktigt med välfungerande rutiner för att föda tillbaka uppgifter från det centrala behörighetsregistret (”mastern”) till de egna systemen. Annars krävs manuell dubbelregistrering i det centrala registret och i minst ett internt register, vilket är ineffektivt och riskerar att leda till att fel uppstår.

Tjänsten som hämtar attribut från den centrala attributkällan tillhandahålls med fördel i federation.

6.4 ”Digitalt omklädningsrum” hos arbetsgivaren

I detta fall finns attributkällan med användarnas behörighetsgrundande information hos arbetsgivaren eller hos arbetsgivarens underleverantör. Attributen ingår i det intyg som den digitala tjänsten tar emot från arbetsgivaren och arbetsgivaren går i god för att användaren har identifierats tillräckligt säkert i ett tidigare steg.

Fördelen med detta mönster är att arbetsgivaren i varje stund rår över sitt behov av att behörighetsgrundande attribut som når externa e-tjänster är aktuella. Dessutom finns det en viktig möjlighet för arbetsgivaren att vid behov byta ut användarens personnummer (eller motsvarande personidentitetsbegrepp) mot användarens anställnings-id eller annan pseudonym (”omklädningsrum”), under förutsättning att den digitala tjänsten efterfrågar och kan hantera pseudonymen.

Arbetsgivaren ska i detta mönster, själv eller genom underleverantör, bygga upp förmågan att tillhandahålla behörighetsgrundande attribut om användaren i ett elektroniskt intyg till externa digitala tjänster efter genomförd identifiering hos arbetsgivaren. Spårbarhet tillbaka till vem som vid vilket tillfälle hade vilket anställnings-id eller pseudonym är också en viktig förmåga. Ansvarsfördelningen blir i omklädningsrumsmönstret delvis ett annat när det är arbetsgivaren som begär autentisering av användaren och går i god för detta inför den digitala tjänsten, jämfört med att den digitala tjänsten själv begär autentisering från eID-utfärdaren.

I detta mönster går således arbetsgivaren i god inte endast för den behörighetsgrundande informationen, utan även för att användarens identitet har

kontrollerats minst på den begärda tillitsnivån och bidrar med de attribut som efterfrågats och kan lämnas ut.

Intygen tillhandahålls med fördel i federation. Exempel på mönstret finns realiserade i identitets- och behörighetsfederationerna Sambi (e-hälsa), SWAMID (högskolor) och Skolfederation (skolor). Olika attributprofiler finns för de olika sektorerna.

Fördelen med denna variant är att arbetsgivaren är tydligt ansvarig för vilken behörighetsinformation som lämnas i samband med varje inloggning. Nackdelen är att varje arbetsgivare, vanligen med hjälp av underleverantör, behöver ha förmågan att identifiera sin personal, underhålla inblandade attributkällor och ställa ut identitets- och behörighetsintyg på ett sätt som skapar tillit hos den förlitande parten. Förmågorna liknar de som vanligen krävs för internt bruk.

6.5 Attributtjänst hos arbetsgivare

Attributkällan och attributtjänsten finns i detta fall hos arbetsgivaren, eller hos arbetsgivarens underleverantör. Den digitala tjänsten begär först identifiering av medarbetaren och ställer därefter en fråga till arbetsgivarens attributtjänst, eller till en samlad attributtjänst exempelvis kopplad till digitala fullmakter som har rätt att hämta attribut från arbetsgivaren, för att få kompletterande behörighetsgrundande information om medarbetaren.

Fördelen med detta mönster är att arbetsgivaren i varje stund rår över utmaningen att behörighetsinformation som når externa e-tjänster ska vara aktuell. Arbetsgivaren ges även god kontroll över vilka uppgifter som lämnas ut till vilken extern förlitande part.

Nackdelen med detta mönster är att det innebär utmaningar för användarupplevelsen när en medarbetare har många uppdrag. Digitala tjänster som använder detta mönster behöver också hantera åtkomst till flera olika arbetsgivares attributtjänster med rätt nivå av säkerhet och tillgänglighet (servicenivå) vilket påverkar skalbarheten i lösningar som baseras på mönstret. Det är viktigt att arbetsgivaren erbjuder rätt förmågor.

Arbetsgivarnas attributtjänster, alternativt den centrala attributtjänsten eller fullmaktstjänsten, tillhandahålls med fördel i federation.

6.6 Provisionering till attributkälla hos förlitande part

Attributkällan finns hos arbetsgivaren eller hos arbetsgivarens underleverantör. Beslutade attribut för medarbetare per extern part överförs automatiserat (ofta på begäran) till en attributkälla hos förlitande part, det vill säga externa parters speglade attributkällor, gärna med stöd av en federation för god säkerhet och effektivitet. Provisionering är ett lånat ord från engelskans ”provisioning”.

Ett exempel på detta mönster är Skolfederations digitala infrastruktur ”Kontosynk” för skolhuvudmäns provisionering (med stöd av standarden SS

12000) av uppgifter om skolpersonal och elever till skolhuvudmannens anskaffade digitala läromedel och till Skolverket.

Fördelen med detta mönster är att arbetsgivaren relativt väl, jämfört med manuell extern registrering, rår över att attributen som når externa e-tjänster är aktuella. Arbetsgivaren, exempelvis skolhuvudmannen, har även god kontroll över vilka uppgifter som lämnas ut till vilken extern förlitande part. Fördelen är också att identitetsintyg som skickas vid inloggning kan hållas begränsade till sitt innehåll, vilket är bra ur kapacitetssynvinkel. Dessutom kan det finnas möjlighet att hos den förlitande parten kvalitetssäkra attributen gentemot den förlitande partens strukturer innan användaren ska logga in, exempelvis att rätt elever finns med i en grupp som ska skriva ett visst prov.

Nackdelen är att lösningen är beroende av en mycket god livscykelhantering av behörighetsinformation, så att inte onödigt mycket personuppgifter finns spridda hos många parter eller att informationen blir inaktuell.

6.7 Provisionering till central attributkälla

I det sjätte mönstret finns attributkällan hos arbetsgivaren eller hos arbetsgivarens underleverantör. Beslutade attribut överförs automatiserat till en central katalog, det vill säga till en samlad, speglad attributkälla, som är kopplad till en central attributtjänst. Den centrala attributtjänsten kan med fördel ingå i federation för god säkerhet och effektivitet.

Fördelen med detta mönster är att arbetsgivaren relativt väl, jämfört med manuell extern registrering, rår över att behörighetsinformation är aktuell. Fördelen är också att identitetsintyg som skickas vid inloggning kan hållas begränsade till sitt innehåll, vilket är bra ur kapacitetssynvinkel.

Nackdelen är att lösningen är beroende av en mycket god livscykelhantering av attributen så att exempelvis borttag görs både internt och på ett automatiserat sätt externt centralt när medarbetare slutar. Att samla uppgifter om personal centralt kan vara effektivt men det måste vägas mot att personuppgifter, som till en del kan vara känsliga eller sekretessbelagda, riskerar att bli tillgängliga på ett samlat sätt hos en annan ansvarig organisation och behöver gott skydd. Det är viktigt för arbetsgivaren att rå över vilka uppgifter om den egna personalen som når vilken extern digital tjänst när de ställer attributfrågor till den centrala attributkällan. Det är därför i detta mönster särskilt viktigt med reglering och information.

6.8 Nästa steg beträffande nationellt ekosystem för attribut

Det är, utöver att följa regelverk, viktigt att väga in olika typer av behov för att säkrare kunna avgöra vilka attributmönster som passar när, samt avgöra vilka tekniska metoder som bör användas i de olika fallen och vilken digital infrastruktur som då behövs. Exempel på två behov är att en medarbetare kan ha flera olika uppdrag och att behov av single sign-on är stort.

Därför behöver ytterligare aktiviteter genomföras tillsammans med deluppdragen Mina ombud, Auktorisation och API-hantering, och med övriga som anmäler intresse (se avsnitt 8). Det är även viktigt att ta hänsyn till att alla mönster redan finns implementerade i olika sektorer.

Vi har identifierat att regelverksfrågor kopplat till digital infrastruktur för attributförsörjning behöver hanteras vidare i ett fortsatt eller nytt uppdrag, där ett första steg efter ovanstående aktiviteter bör vara att analysera vad som behöver regleras på en a) förvaltningsgemensam, b) nationell respektive 3) EU-gemensam nivå för att attributförsörjningen ska fungera väl, där hänsyn tas till bland annat verksamhetsbehov, informationssäkerhet, personlig integritet och effektivitet.

6.9 Utmaningar med överföring av attribut över landsgränser

Även internationellt är försörjning med behörighetsgrundande information en utmaning. Här följer några exempel.

Det finns ett identitetsattribut för juridiska personer i den tekniska eIDAS-specifikationen, men det finns ännu ingen gemensam tolkning mellan länderna av hur identitetsattribut för juridiska personer ska tolkas eller användas.

De nordisk-baltiska länderna (NOBID), med flera länder, för samtal om hur ett utländskt personidentitetsbegrepp kan kopplas ihop med befintliga nationella personidentitetsbegrepp, i Sverige personnummer eller styrkt samordningsnummer. Frågan har utretts flera gånger i Sverige utan att någon nationell lösning har beslutats. Behovet är nu åter högaktuellt inom arbetet med Single Digital Gateway.

Portugal, Nederländerna och Estland tillhör de pådrivande länderna i frågan om överföring av ytterligare uppgifter (attribut) om användare som behövs för auktorisation i digitala tjänster. Det finns olika uppfattningar om både regler och lösningar och det kan rimligen inte finnas så många e-tjänster som är konstruerade för att konsumera ett annat lands behörighetsattribut utan att man kommer överens om gemensam tolkning av attributen. Det finns en arbetsgrupp som arbetar med frågan och en slutsats de har dragit är att skillnaderna är för stora mellan medlemsstaternas sätt att hantera behörigheter för att det ska gå att finna ett gemensamt sätt att uttrycka behörigheter. Arbetsgruppens förslag är i stället att det via eIDAS-noderna ska gå att fråga om en person är behörig att utföra en viss operation. Detta förfarande innebär också utmaningar i vissa flöden, inte minst för Sverige.

En grupp av länder driver på för att kunna utnyttja eIDAS-infrastrukturen för att kunna lägga till ytterligare behörighetsattribut i identitetsintygen via eIDAS-noderna. Det är dock långt ifrån självklart att över landsgränsen börja hantera ytterligare behörighetsattribut i identitetsintygen eftersom SAML-standarden som är lagstiftad i eIDAS-förordningens genomförandeakt om interoperabilitet inte är konstruerad för detta. Sverige ser därför att ett alternativ som borde prövas över

landsgränsen är att utgå från ett ramverk som i grunden är gjort för auktorisation baserat på överföring av attribut via API:er.

7 Medarbetares möjlighet till e-underskrifter

Enligt E-legitimationsenkäten 2019 var även medarbetares underskriftsmöjligheter ett viktigt behov. En medarbetare kan exempelvis behöva 1) göra underskrift i en extern digital tjänst, 2) lokalt skriva under en PDF som ska skickas i väg eller 3) skriva under ett internt personalärende.

Det är alltid en användare, dvs. medarbetare i detta fall, som skapar en elektronisk underskrift. När en organisation gör motsvarande är det en elektronisk stämpel, se EU:s eIDAS-förordning för mer information.

Det första som den ansvariga verksamheten (och lagstiftaren) bör analysera är om underskrift verkligen behövs vid övergång från papper till digitalt alternativ. Ibland kan den digitala tjänsten som sådan eller elektronisk identifiering av användaren vara tillräcklig. I andra fall kan organisationens elektroniska stämpel vara ett effektivare alternativ än att medarbetare manuellt ska skriva under exempelvis beslut elektroniskt. Under förutsättning att medarbetaren verkligen behöver skriva under finns det två alternativa lösningar: fristående underskriftstjänst och så kallad lokal underskrift.

7.1 Huvudspår: fristående underskriftstjänst kopplad till den digitala tjänsten

När en medarbetare befinner sig i en digital tjänst där en underskrift ska göras är det mest effektivt att utföra underskriften med hjälp av en från e-legitimationen fristående underskriftstjänst (eng. remote signing service, ibland kallad central underskriftstjänst). En fristående underskriftstjänst kan upphandlas från marknaden av den organisation som är ansvarig för den digitala tjänsten baserat på den normativa specifikation och granskning som DIGG ansvarar för.

Ett viktigt krav vid upphandling är att ha klart för sig vilken säkerhetsnivå som underskrifterna ska nå upp till: kvalificerad, avancerad eller varken kvalificerad eller avancerad. Läs mer i EU:s eIDAS-förordning och i DIGG:s vägledande beskrivning, samt eventuella regleringar i registerlagstiftning eller motsvarande EU-lagstiftning, för mer information.

7.2 Validering av underskrifter som skapas hos förlitande part

Så fort underskriften har skapats med stöd av en fristående underskriftstjänst i anslutning till den digitala tjänsten kan underskriften enkelt valideras eftersom den förlitande parten rår över underskriftslösningen.

7.3 I vissa fall finns behov av lokal underskrift

När den på underskriften förlitande parten inte erbjuder någon fristående underskriftstjänst och inte heller medarbetarens egen organisation har någon fristående underskriftstjänst som kan användas, finns det behov av en så kallad lokal underskriftstjänst. Ett exempel på behov kan vara vid gränsöverskridande transaktioner.

Om arbetsgivaren inte har tillräckliga underskriftsvolymer för att anskaffa en fristående underskriftstjänst som även kan kopplas till medarbetares behov av att kunna skicka i väg underskrivna handlingar finns det därför skäl för arbetsgivaren att överväga anskaffning av lokal underskriftslösning exempelvis i samband med anskaffning av eID. Även i detta fall finns det skäl att överväga behov av att kunna skapa underskrifter på den kvalificerade, avancerade och varken kvalificerade eller avancerade nivån, beroende på vilken typ av ärenden och vilken lagstiftning som omfattas.

Här skulle man som en variant på lösning av behovet kunna tänka sig att en statlig myndighet hänvisar till eller erbjuder en för behovet förberedd fristående underskriftstjänst som kan användas mot självkostnadspris per underskrift, aktuell för exempelvis en kommun med mycket små underskriftsvolymer.

7.4 Validering av underskrift som har skapats hos annan part

När underskriften är skapad, skickas den tillsammans med den elektroniska handlingen till den på underskriften och handlingen förlitande parten, som vid behov validerar underskriften. Denna validering är inte okomplicerad på den avancerade nivån eller lägre, eftersom det saknas tydliga gemensamma regler att följa.

Det är därför av vikt att underskrivande parter ställer gemensamma krav på att vissa standarder ska följas vid skapande av underskrifter, vilket inte sker idag. Detta ställer till det för den förlitande parten. Bolagsverket och Skatteverket är två exempel på organisationer som ibland får in underskrifter som inte kan valideras och därför i många fall avvisas. I takt med ökad digitalisering kommer valideringsutredningar som görs hos många förlitande parter att totalt sett bli mycket kostsamma. Det finns därför ett stort behov av en förvaltningsgemensam funktion för validering. Den offentliga utredningen ”reboot” (SOU 2017:114) föreslog att DIGG ska ha ett sådant uppdrag. Dessutom måste regelverket utvecklas så att åtminstone avancerade underskrifter blir fullt valideringsbara.

7.5 Långtidvalidering med stöd av valideringsintyg

En annan fråga som det finns behov av att lösa är den komplexitet som uppstår vid försök att validera en elektronisk underskrift vid ett långt senare tillfälle än vid tidpunkten för underskriftens skapande, så kallad långtidsvalidering. Härvan av certifikat som har löpt ut och som ska analyseras, blir allt mer komplex vartefter tiden går. EU gör försök att standardisera detta på den kvalificerade underskriftsnivån, men det kan bli mycket kostnadskrävande rutiner.

Som vi ser det finns det två alternativa lösningar på problemet: 1) att validera direkt efter mottagandet och därefter förlita sig på att validering gjordes och 2) att validera direkt efter mottagandet, ställa ut ett stämplat valideringsintyg i klartext och sedan förlita sig på valideringsintyget. På detta område finns det också behov av ett förvaltningsgemensamt stöd.

8 Risker med rapportens förslag

I denna rapport föreslår vi att en ny avtalsmöjlighet om elektronisk identifiering utan transaktionskostnader tas fram. Med det förslaget ser vi följande risker:

1. För få eID-utfärdare ansluter sig
2. Svårt att kommunicera om ”ännu en avtalsmöjlighet” vilket riskerar att leda till långsamt införande hos förlitande parter
3. Om det skulle finnas en lösning genom lagstiftning som är enklare jämfört med avtalsreglering
4. Ett misslyckande eller lagstiftning leder till onödiga kostnader hos DIGG för avtalsadministration.

Risk 1 och 2 medför inga konsekvenser som förvärrar läget jämfört med hur det är idag. Risk 3 är att se som en möjlighet, där verksamhet inom befintlig rätt har pågått fram tills dess. Risk 4 kan lösas genom att göra avtalsadministrationen mycket enkel i förhållande till det redan erbjuder i avtalsväg, exempelvis anslutningsavtalet till Sweden Connect och den svenska eIDAS-noden.

I övrigt gör vi ställningstaganden som kan bearbetas vidare till konkreta förslag eller genomföras därför att de redan är föreslagna och bedömda av andra.

9 Plan för fortsatt arbete

Övergripande plan för fortsatt arbete:

September 2020 – januari 2021

1. Besluta om avtalsmodell och ta fram avtal om elektronisk identifiering utan ersättning.
2. Arbeta med PoC för överföring av behörighetsgrundande attribut.
3. Färdigställ förstudierapporten och bidra till rapportering av regeringsuppdraget-

Februari 2021 – december 2021

4. Komplettera Tekniskt ramverk för Sweden Connect åtminstone med profil som medger överföring av eID-anskaffande arbetsgivares

organisationsnummer, samt med vad som i övrigt beslutas efter utförd PoC.

5. Bidra med underlag till DIGG:s löpande uppdrag om vägledning och stöd inom området, samt vid behov till kompletteringar av regelverk.
6. Kommunicera om möjligheten ”eID för medarbetare”.

Bilaga 1 - Begrepp i förstudien

Användare	Här: en individ som innehar en elektronisk identitetshandling (**eID**, **e-legitimation)** och som vill identifiera sig med hjälp av denna, vanligen för att få åtkomst till en digital tjänst
API	Application Programming Interface, en specifikation och ett gränssnitt för hur program kan använda och kommunicera med en specifik programvara, datasystem eller tjänst.
Auktorisation	Beslut om att ge en **användare** a) tillträde eller b) rätten att utföra vissa åtgärder
Autentisering	En elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form (eIDAS-förordningen)
Attribut	Uppgifter, här: uppgifter om en medarbetare som vill få åtkomst till en digital tjänst
Attributintyg	Intyg med **attribut** om **användare** som stämplas och skickas till en **förlitande part**
Attributkälla	Register med **attribut**
Attribututfärdare	Aktör som ansvarar för uppgifter om en **användare** och ställer ut stämplade **attributintyg**
Behörighetsgrundande attribut	**Attribut** om en **användare** som krävs för **auktorisation**
eID	Elektronisk identitetshandling
eID-utfärdare	Aktör som utfärdar **eID** till **användare** och ställer ut **identitetsintyg** i samband med

	elektronisk identifiering av **användaren**
E-legitimation	Se **eID**
Elektronisk identifiering	En process inom vilken personidentifieringsuppgifter i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används (eIDAS-förordningen)
Förlitande part	Aktör som förlitar sig på **identitetsintyg** eller **attributintyg** och vanligen **auktoriserar användare (eng. Relying Party)**
Grundidentifiering	Syftar till att koppla ihop en individ med uppgifter i folkbokföringsregistret och resulterar i en identitetshandling (”reboot”, SOU 2017:114)
Identitet	Ett övergripande beskrivning av personidentitetsbegrepp, **eID** m.m.
Identitetsintyg	Intyg som efter kontroll av användarens identitet stämplas och skickas till **förlitande part**
Stark autentisering	**Autentisering** baserad på användning av flera unika faktorer kombinerad med en **grundidentifiering** som bekräftar **användarens** uppgifter i officiellt register
Tillitsnivå	Skyddsklass. Här: grad av skydd som **elektronisk identifiering** med en given **eID** innebär
Tillitsramverket för Svensk e-legitimation	Kravdokument med regler för att nå viss **tillitsnivå** för **eID.** Alla tillitsnivåer (2, 3 och 4) i kravdokumentet innebär **stark autentisering**
Medarbetare	Här: **användare** (exempelvis medarbetare, arbetstagare, konsult) vars **eID** har anskaffats på ett sådant

sätt att kostnad för **elektronisk identifiering** ingår

Bilaga 2 - Värdeerbjudanden

Business Model Canvas (BMC) för Byggblock Identitet

Business Model: Identitet

Datum: 2020-06-23
Version: 0.5

Nyckelpartners

Arbetsgivare (t.ex. Skatteverket, Statens Servicecenter)

Tillhandahållare av legitimeringstjänster:
- Privata aktörer

EU:s samarbetsforum för eIDAS

Nyckelaktiviteter

Nyttja tillitsramverk, tekniskt ramverk och infrastrukturella tjänster, som stödjer samverkanslösning med rätt säkerhetsnivå för att uppnå tillit och förtroende mellan parter.

Nyckelresurser

- Förvaltning, drift och support av identitetsfederationen Sweden Connect och tillitsramverket
- Juridisk kompetens för avtalshantering och attributförsörjning
- Informationssäkerhet inriktat mot tillitsramverk, certifikatsutfärdande och attributförsörjning
- Andra byggblock (Tillitsramverk, Auktorisation och Mina ombud)

Värdeerbjudande

- Enkel tillgång till elektronisk identifiering av privatpersoner
- **Enkel tillgång till elektronisk identifiering av medarbetare**
- Enkel tillgång till elektronisk underskrift för privatpersoner
- **Enkel tillgång till elektronisk underskrift för medarbetare**
- Enkelt att få reda på svenska eID:n som godkänts av DIGG
- **Kostnadsfritt avtal om elektronisk identifiering av medarbetare med svenskt eID**
- Digital infrastruktur för användning av eID inom Sverige och utomlands
- Möjlighet för svenska aktörer att identifiera medarbetare med utländskt eID
- **Vägledning om attributförsörjning vid elektronisk identifiering**

Kundrelation

- Anslutningsavtal Sweden Connect
- Avtal för Auktorisationssystem
- Avtal för kostnadsfria transaktioner för elektronisk identifiering
- Samarbetsforum
- Granskning (främst utfärdare av eID)

Kanaler

Webb - digg.se, swedenconnect.se
DIGG Kundtjänst
Sociala medier
Konferenser (t.ex. Offentliga rummet)
Forum (t.ex. Sweden Connect eller annat kundforum)

Kunder & Kundsegment

Förlitande parter (tillhandahållare av tjänster):
- Myndigheter
- Kommuner
- Regioner
- Företag

Utfärdare av eID:
- Offentliga aktörer (Inera, Försäkringskassan)
- Privata aktörer

Utfärdare av behörighetsgrundande attribut:
- Offentliga aktörer
- Privata aktörer

Slutanvändare (indirekt):
- Offentliga medarbetare
- Privata medarbetare
- Ombud (fullmakt)
- Privatpersoner

Kostnader

- Utveckling och förvaltning av federationen Sweden Connect
- Avtalsadministration
- Arbetsgivares kostnader för anskaffning av eID (inklusive kostnadsfria transaktioner) och tillhandahållande av attributtjänster med rätt skyddsnivå

Nytta

- Sektorsoberoende standard för e-legitimering av medarbetare över organisationsgränser
- Mindre behörighetsadministration
- Snabbare handläggning vid personalförändringar
- Avtals- och finansieringsmodell som främjar digital utveckling genom genom fast förutsägbar kostnad
- Tidsbesparande stöd till tjänsteutvecklare genom tydlig vägledning kring avtal och teknik

Value Proposition Canvas (VPC) - värdeerbjudandet ”Enkel tillgång till elektronisk identifiering av medarbetare”

Värdeerbjudande — Kundsegment

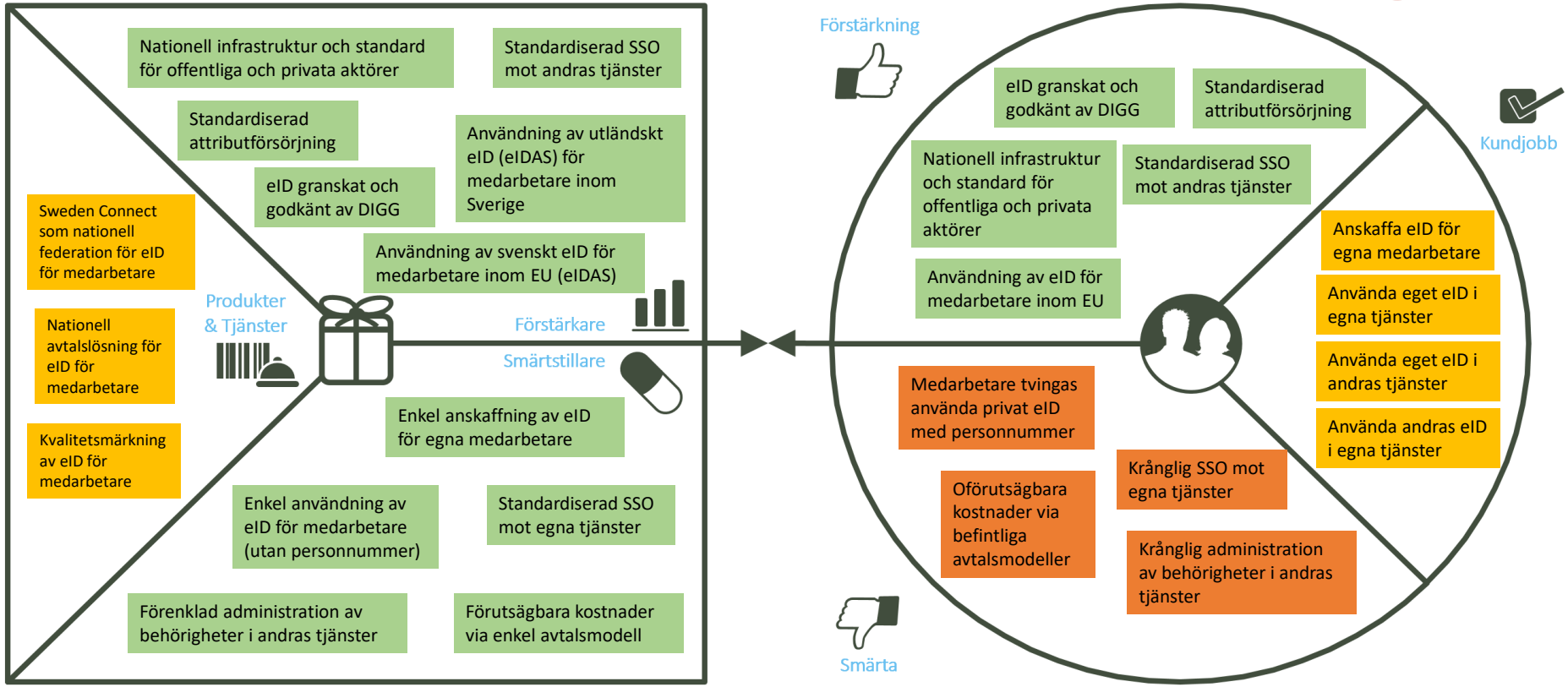
Datum: 2020-06-23

Version: 0.5

Utkast

Enkel tillgång till elektronisk identifiering av medarbetare

Förlitande parter



Bilaga 3 - Uppdragets utförande

Förstudiearbetet har bedrivits inom regeringsuppdraget om effektivt informationsutbyte, där medarbetares digitala identitet har visats sig vara viktigt för att nå framgång.

Som underlag för denna förstudierapport har veckovisa arbetsmöten på distans hållits under perioden 2020-05-11 och 2020-06-26. Bemanningen har bestått av:

- Eva Sartorius, DIGG, uppdragsledare
- Sven-Erik Ceedigh, DIGG
- Magnus Enmarker, Försäkringskassan
- Kristina Fenger-Krog, Sveriges Kommuner och Regioner
- Marie Furusten, Skatteverket
- Pedro León, Domstolsverket
- Robert Malm, Skatteverket
- Ulf Palmgren, Sveriges Kommuner och Regioner
- Joakim Sandberg, E-hälsomyndigheten
- Gustav Söderlind, Myndigheten för samhällsskydd och -beredskap

Behov av juridiska och tekniska resurser för att arbeta vidare med det föreslagna avtalet och PoC (proof of concept) för attributförsörjningsmönster tillkommer under hösten.