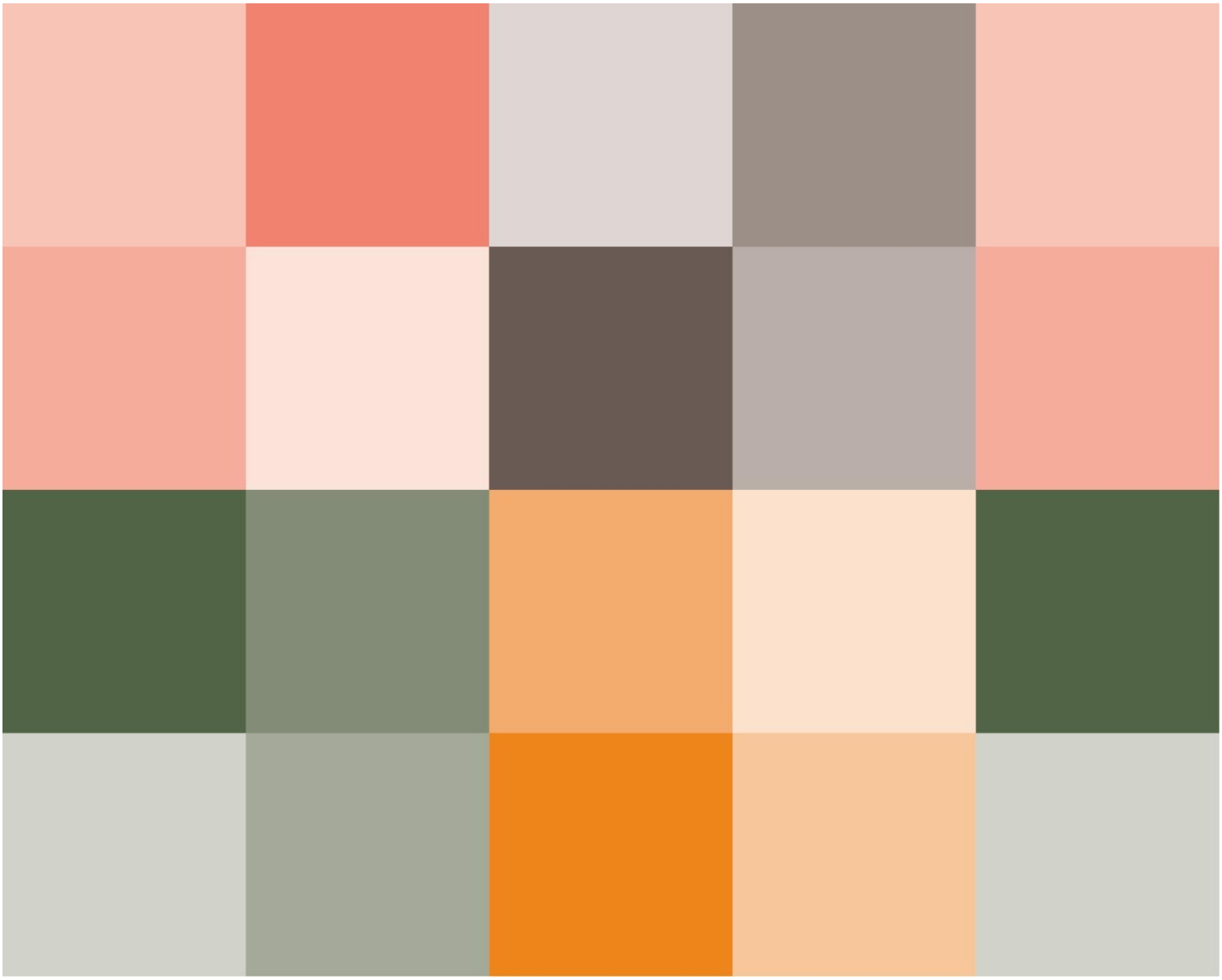


eID för medarbetare

Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte

Ärendenr: 2019-582

Datum: 2020-12-14

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Medarbetares e-legitimationer ska kunna användas i många externa tjänster. Behoven är stora enligt E-legitimationsenkäten 2019[1].

Det finns idag minst sex svenska eID-utfärdare som arbetsgivare kan anskaffa eID:n från till sina medarbetare och andra målgrupper. Tre alternativ är privata som kan upphandlas, och tre är offentliga. De offentliga riktar sig till vissa målgrupper. Trots att det redan finns eID-alternativ kan förstudiens arbetsgrupp konstatera att inte alla behov är fyllda. Som exempel kan nämnas att alla alternativ ännu inte är godkända av DIGG.

Anskaffande organisationer gör därför rätt i att framföra sina behov och krav till eID-utfärdare inför anskaffning av eID till sina medarbetare och andra målgrupper. Förstudierapporten kan användas som inspirationsunderlag för detta.

Den största användningen av eID i tjänsten finns idag internt inom organisationen eller inom sektorn, exempelvis inom e-hälsa. Det finns ännu inget eID-alternativ som arbetsgivare kan anskaffa och som för närvarande är valbart som inloggningsmetod i ett stort antal sektorsoberoende tjänster.

För att lösa detta behov föreslår denna rapport därför att ett enkelt civilrättsligt avtal tas fram, som i huvudfallet knyter ihop eID-utfärdare med förlitande aktörer. Det behövs även en variant av avtal mellan arbetsgivare och förlitande aktörer för de transaktioner som går via arbetsgivaren. Avtalen ska vara ersättningslösa[2]. Arbetsgruppen bedömer, baserad på en rättslig analys[3], att avtalsupplägget kan fungera därför att arbetsgivarens anskaffning av eID görs mot ersättning, exempelvis års- eller månadsavgifter.

Avtalsparterna rekommenderas i första hand att delta i den nationella digitala infrastrukturen för digital identitet, som DIGG ansvarar för. Motivet är att elektronisk identifiering av medarbetare bör ske på ett standardiserat, effektivt och säkert sätt över organisationsgränserna. Detta kan kräva viss teknisk anpassning hos eID-utfärdare. Förlitande offentliga myndigheter som kopplat upp sig mot

---

[1] Rapport enkät e-legitimationer (SKR 2019) https://webbutik.skr.se/sv/artiklar/rapport-enkat-e-legitimationer.html och E-legitimering inom den offentliga förvaltningen 2019 (DIGG 2019) https://www.digg.se/publicerat/publikationer/2019/e-legitimering-inom-den-offentliga-forvaltningen-2019

[2] De ska alltså vara benifika

[3] Rättslig promemoria om upphandlingsfrågor kopplade till eID för medarbetare", 2020-11-13, ärende 2019-582

eIDAS-noden (”Foreign eID”) eller använder Valfrihetssystem 2017 E-legitimering har redan anpassat sig tekniskt.

Leverantörer av intygsfunktioner kommer att tillitsgranskas för att behålla en säker kedja mellan eID-utfärdare och förlitande aktörer oavsett om intyget överförs direkt eller indirekt till förlitande aktör. De förslagna avtalen kan ses som en basnivå och andra tekniska varianter och profiler, som kan vara effektiva internt eller inom en sektor, ska inte förhindras.

Medarbetares möjligheter till e-underskrift är en mycket viktig funktion, såväl externt som internt. Huvudmönstret bör vara, precis som för privatpersoner, att medarbetaren skriver under med stöd av en till e-legitimationen fristående underskriftstjänst. Om en fristående underskriftstjänst inte finns, kan en lokal variant av underskriftstjänst vara aktuell som alternativ.

Validering av inkommande underskrivna handlingar består av flera kompetenskrävande utmaningar som behöver lösas gemensamt. Det finns behov av att öka DIGG:s stöd för detta genom en förvaltningsgemensam valideringstjänst som ställer ut valideringsintyg.

Innehållsförteckning

1 Inledning

Ett effektivt, säkert informationsutbyte mellan organisationer utförs bäst helt digitalt med hjälp av elektroniskt informationsutbyte. När sådana automatiserade rutiner saknas kan manuell åtkomst för medarbetare via digitala tjänster vara nödvändig. Då blir medarbetarens digitala identitet och elektronisk identifiering av medarbetaren över organisationsgränserna en viktig fråga.

Elektronisk identifiering har utretts flera gånger[4]. I de tidigare utredningarna har siktet främst varit inställt på elektronisk identifiering av privatpersoner och deras tillgång offentlig service. I denna förstudie är det däremot medarbetares användning av eID som står i fokus.

När medarbetare använder en e-legitimation inom en krets av aktörer med koppling till varandra kan tillit troligen nås även utan DIGG:s godkännande. Däremot kan DIGG:s godkännande vara viktigt för att nå tillit i bredare sammanhang.

Internt och sektorvis finns det i vissa fall fungerande sammanhållande funktioner för elektronisk identifiering av medarbetare, exempelvis inom hälso- och sjukvårdsområdet. Däremot saknas det idag en fullgod förvaltningsgemensam digital infrastruktur som täcker in fallet när medarbetare som tillhör en organisation ska logga in i andra organisationers digitala tjänster.

1.1 Både privat och offentligt utfärdade e-legitimationer

I offentlig förvaltnings digitala tjänster är både privat och offentligt utfärdade eID:n är välkomna. På privatpersonssidan är BankID den helt dominerande lösningen. Även Freja eID+, AB Svenska Pass och Telia finns som alternativ. En statligt utfärdad e-legitimation är föreslagen (SOU 2019:14) och förslaget bereds inom Regeringskansliet. På eID förlitande aktörer är antingen med i DIGG:s e-legitimeringsavtal (valfrihetssystem) eller upphandlar e-legitimering på annat sätt, vanligen via sina systemintegratörer.

För medarbetare finns exempelvis SITHS, EFOS och Freja OrganisationsID (se fler alternativ i avsnitt 3), men det saknas e-legitimeringsavtal som passar med frekvent användning över organisationsgränser. Alla eID-alternativ som används av medarbetare är ännu inte godkända av DIGG, vilket medför osäkerhet för de på eID förlitande aktörerna.

[4] SOU 2009:86 Strategi för myndigheternas arbete med e-förvaltning och SOU 2020:104 E-legitimationsnämnden och Svensk e-legitimation

Det är vanligt att den på eID förlitande arbetsgivaren integrerar ihop olika tekniska metoder i sin egen IdP, och i sin tur ställer ut identitetsintyg till de digitala tjänster medarbetaren har behov av.

1.2 Om förstudiearbetet

Detta förstudiearbete har bedrivits av DIGG i samarbete med flera andra myndigheter och med Sveriges Kommuner och Regioner (för deltagare i arbetsgruppen, se bilaga 4), inom byggblocket Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (I2019/03306/DF).

1.3 Omfattning i denna rapport

Arbetsgruppen har tagit sikte på att medarbetares e-legitimationer fungera i digitala tjänster i både offentlig och privat sektor, däribland inte minst offentligfinansierad privat verksamhet. Omfattningen i detta uppdrag och för DIGG är dock begränsad till digitala tjänster i offentlig förvaltning[5]. Därför gäller förslagen endast digitala tjänster i offentlig förvaltning.

Siktet har dessutom varit inställt på att elektronisk identifiering ska fungera både internt mot exempelvis upphandlade digitala tjänster och helt externt till andra organisationers digitala tjänster.

Frågor som arbetsgruppen har studerat är:

1. Försörjning med eID för medarbetare (se avsnitt 3)
2. Digital infrastruktur som är anpassad för eID för medarbetare (se avsnitt 4 och 5)
3. Avtal för elektronisk identifiering som passar med medarbetares användning (se avsnitt 5 och 6)
4. E-underskrift för medarbetare som kan knytas till juridisk person, samt funktion för validering av e-underskrifter (en översiktlig beskrivning finns i avsnitt 7).

I ett publikt utkast till denna rapport fanns skisserade flöden för behörighetsgrundande information med. Arbetsgruppen kunde baserat på synpunkterna som kom in konstatera att dessa behov och lösningar måste analyseras vidare inom deluppdrag Auktorisation inom regeringsuppdraget Att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (I2019/03306/DF).

Bedömningar och förslag kopplade till eID för medarbetare finns beskrivna i avsnitt 5.

[5] Dels för att regeringsuppdraget har denna omfattning, dels för att författningsstöd saknas

2 Behov

Behovet av säkert digitalt informationsutbyte handlar till stor del om hur organisationer kan fungera bättre tillsammans genom digitaliserade processer som utgår från privatpersoners och företagares behov exempelvis i ett livshändelseperspektiv (både nationellt och internationellt). Det finns även direkta behov av informationsutbyte för att organisationer ska klara sina uppdrag.

Informationsutbyten kan bäst uppfyllas genom organisatorisk tillit och ett säkert elektroniskt informationsutbyte mellan berörda organisationer. Vid organisatorisk tillit kan det i vissa fall vara viktigt att reglera krav på viss tillitsnivå vid elektronisk identifiering av användare, exempelvis ”minst tillitsnivå 3 enligt Tillitsramverket för Svensk e-legitimation”, när användare använder sin organisations verksamhetssystem.

Ett av många exempel på externt informationsutbyte är polisens tillståndshandläggare för vapenlicenser som via det egna verksamhetssystemet kontrollerar godkänd jägarexamen i Naturvårdsverkets jägarregister genom API-fråga på den sökandes personnummer.[6] 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 elektroniskt informationsutbyte inte finns kan det istället vara aktuellt att en medarbetare[7] i en organisation loggar in och utför något i en digital tjänst som tillhör en annan organisation, exempelvis fakturahantering hos Statens servicecenter eller när en elektronisk orosanmälan hos socialtjänsten i kommunen ska göras. I de fallen behöver medarbetaren ha tillgång till minst en i sammanhanget användbar e-legitimation (eID) och den måste fungera både externt och internt.

Behovet av elektronisk identifiering av medarbetare har visat sig vara stort enligt e-legitimationsenkäten 2019, och det gäller såväl inom en organisation som mellan organisationer[8]. Behoven är stora även enligt Ineras rapport (2020) om kommuners behov inom området identitet och åtkomst[9].

Det är möjligt att det i vissa fall räcker med att medarbetaren använder sin privat anskaffade eID. Behov som leder till att arbetsgivaren i stället anskaffar eID till

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

[7] Uttrycket ”medarbetare” och ”arbetsgivare” ska tolkas mycket brett. Med medarbetare avses även uppdragstagare, förtroendevalda, elever och andra som är knutna till en part (här: ”arbetsgivare”) som vill anskaffa eID för sina målgruppers räkning.

[8] Rapport enkät e-legitimationer (SKR 2019) https://webbutik.skr.se/sv/artiklar/rapport-enkat-e-legitimationer.html

[9] Ineras rapport finns här: https://www.inera.se/utveckling/utveckling-for-kommuner/arkitektur-och-infrastruktur/sektorsovergripande-identitetshantering-samt-standarder-och-strukturer-for-atkomsthantering/

sina medarbetare kan röra affärsvillkor, typ av bärare, funktionalitet, pseudonym, personlig integritet för medarbetaren och sekretessregler kring var medarbetaren loggar in i förhållande till privat utfärdad eID. Det måste därför finnas försörjning med eID för medarbetare som arbetsgivare kan anskaffa om de vill.

Ett exempel på behov av bärare eller funktionalitet är om verksamheten har särskilda behov av mobilitet eller behov av att en aktiv session avbryts om medarbetaren lämnar sin dator för att hämta något. Möjlighet att avtala med eID-utfärdaren om sekretess kan vara ytterligare ett behov. Att använda pseudonym för personnummer (och motsvarande personidentitetsbegrepp) kan också vara ett behov som en eID-utfärdare kanske kan hjälpa till med. För arbetsgivaren kan det även vara viktigt att eID-utfärdarens utbud täcker hela verksamhetens behov och inte bara medarbetare som arbetar inom en viss sektor.

Den digitala tjänsten har behov av att veta vilken tillit som kan hysas till medarbetarens eID. Om e-legitimationen är godkänd av myndigheten DIGG kan organisationen som ansvarar för den digitala tjänsten där e-legitimationen används på goda grunder hysa samma tillit till e-legitimationen oavsett om den är anskaffad av medarbetaren som privatperson eller av arbetsgivaren för medarbetarens räkning. Däremot kan det skilja sig åt beträffande vilken information, exempelvis pseudonym för personnummer, som kan skickas från eID-utfärdaren till den digitala tjänsten.

Andra villkor kan också skilja sig åt, exempelvis vad gäller så kallad tick-baserad (transaktionsbaserad) ersättning till eID-utfärdaren. En medarbetare kan behöva använda sin e-legitimation många gånger under en arbetsdag. Det finns därför ett särskilt behov hos ansvariga för digitala tjänster, och därmed även för arbetsgivare, av överskådliga kostnader för medarbetares användning av e-legitimation.

Även hos medarbetare kan det finnas behov av att arbetsgivaren anskaffar eID. Det kan exempelvis röra sig om att arbetsgivaren avtalar med eID-utfärdaren om särskilt skydd av personuppgifter vid användning i tjänsten. Det kan också röra medarbetare som har svårigheter att skaffa eller använda en e-legitimation som kan användas i tjänsten, exempelvis om svenskt personnummer saknas eller om särskild funktionsanpassning krävs.

2.2 Motsvarande behov finns i privat sektor

Under förstudiearbetet har det i flera sammanhang påtalats att det är viktigt att medarbetare kan identifiera sig i många olika digitala tjänster i både offentliga och privat sektor. Det står därför helt klart att det finns behov av att modellen i möjligaste mån inkluderar privat sektor, även om det för närvarande finns hinder.

Ett behov är att medarbetare inom offentlig förvaltning ska kunna logga in även i vissa tjänster i privat sektor, exempelvis kommunens HR-funktion hos KPA Pension. Ett annat skäl är att digital infrastruktur som är bra för offentlig förvaltnings digitalisering har potential att vara bra för hela Sveriges digitalisering.

Privata utförares verksamheter växer och får allt större betydelse i samhället. Därför blir detta behov med tiden allt viktigare.

Däremot finns det inte stöd i författning för att kunna inkludera digitala tjänster i privat sektor. Frågan ingår inte i detta regeringsuppdrag men har lyfts i andra sammanhang och utreds därför inte närmare här.

2.3 Behov av tillit till e-legitimationer

Medarbetare som ska komma åt sekretessbelagd eller känslig information kan behöva ha en e-legitimation som uppfyller en högre tillitsnivå än övrig personal. Därför är det viktigt att verksamheten som ansvarar för den digitala tjänsten genomför informationsklassning i syfte att avgöra vilken lägsta godtagbara tillitsnivå som ska gälla för e-legitimationer.

Informationsklassning innebär att man värderar sina informationstillgångar, som exempelvis kan nås via digitala tjänster, utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet. 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[10]. 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

[10] Dessutom kan sårbarhetsanalys och analys av tillgänglighetskrav vara viktiga att genomföra.

Om exempelvis röjande av känsliga uppgifter till obehöriga skulle leda till betydande skada, bör tillitsnivå 3 enligt Tillitsramverket för Svensk e-legitimation[11] väljas. Om det skulle leda till måttlig skada krävs eventuellt fortfarande stark autentisering men då kanske tillitsnivå 2 enligt samma tillitsramverk kan ge tillräckligt skydd. Tillitskrav avgörs av den ansvariga verksamheten och kan vara författningsreglerat.

Läs mer om e-legitimationers tillitsnivåer på DIGG:s webbplats[12] och om informationsklassning på Myndigheten för samhällsskydd och -beredskaps (MSB) webbplats Informationssäkerhet.se[13], samt på SKR:s webbplats KLASSA[14].

DIGG tillhandahåller digital infrastruktur för identitet, däribland ett metadataregister som beskriver aktörernas förmågor. För att tillit ska nås blir den digitala infrastrukturen säkerhetsgranskad av oberoende part. Den senaste granskningen gjordes 2018 och nästa granskning är planerad till 2021. Arbetsgruppen anser att det är viktigt att information om säkerhetsgranskningarna finns tillgänglig på ett transparent sätt.

2.4 Övriga behov kopplat till eID

Utöver de behov som presenterats i de föregående delavsnitten har arbetsgruppen identifierat följande behov kopplat till e-legitimation för medarbetare:

- Det ska finnas alternativ som medger att eID kan användas likvärdigt av alla medarbetare, oavsett funktionsvariationer
- Alla medarbetare har inte svenskt personnummer men ingår ändå i den grupp som behöver svenskt eID via arbetsgivaren
- En del medarbetare har ett utländskt eID som är godkänt i Sverige (enligt eIDAS-förordningen[15]), vilket kan ses som en extra möjlighet för den digitala tjänsten
- Det behövs reservlösning när en medarbetare ar glömt sitt eID hemma, eller om en ny medarbetare mycket snabbt måste ha tillgång till eID. Här kan så kallade id-växlingar från tillåtande eID-utfärdare, exempelvis den föreslagna statliga e-legitimationen till medborgare och folkbokförda, underskrivna intyg från kollegor, bevis i verksamhetssystem m.m. nyttjas bättre än idag av eID-utfärdare i kombination med arbetsgivare så att även reservlösningarna är tillräckligt säkra
- På övergripande nivå behövs flera oberoende eID-lösningar så att det finns möjlighet till alternativ lösning vid exempelvis större driftstörning, allvarlig

[11] Tillitsramverket för Svensk e-legitimation https://www.digg.se/digital-identitet/e-legitimering#kvalitetsmarket_svensk_e-legitimation (Under ”Så går granskningen till”)
[12] DIGG:s information om tillitsnivåer https://www.digg.se/digital-identitet/e-legitimering/offentlig-aktor/tillitsnivaer/
[13] MSB:s webbplats om informationssäkerhet https://www.informationssakerhet.se/
[14] KLASSA https://klassa-info.skl.se/page/start
[15] EU:s förordning 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 https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32014R0910&from=SV

incident eller täcka in alla behov. Detta är dock ingen ersättning till behovet att varje eID-utfärdare erbjuder god tillgänglighet till sina lösningar

- Medarbetarens eID ska helst kunna användas både i Sverige och utomlands, men det är inget tvingande krav på övergripande nivå
- Arbetsgivaren kan ha behov av att reglera i anställningsavtal eller motsvarande vilka eID:n medarbetaren använder, och var[16]
- Behoven är till viss del verksamhetsspecifika och därför bör arbetsgivare kunna ställa sina krav i samband med anskaffning av eID till sina medarbetare. Stöd till att formulera allmänna krav behövs också
- För att nå bred effektivitet är det viktigt med sektorsgemensamma tekniska specifikationer för elektronisk identifiering[17], men det ska även vara möjligt att, exempelvis inom en sektor eller vid intern användning, komma överens om att följa andra tekniska specifikationer[18]
- Det måste finnas svenska eID:n att anskaffa som fyller verksamhetens behov
- Det har under förstudiearbetets gång lyfts behov av att även inkludera eID:n som inte är godkända av DIGG, exempelvis interna eID:n, i modellen i den mån det är lämpligt. Detta behov bör lösas i annan ordning än förvaltningsgemensamt.
- En del arbetsgivare har behov av att få agera mellanhand mellan eID-utfärdaren och den digitala tjänsten, i syfte att förenkla för medarbetare, integrera olika tekniska metoder, komplettera viss information och skapa redundans. Samtidigt måste tillitskedjan förbli obruten, särskilt vid helt extern inloggning.

2.5 Behov kopplade till e-underskrifter

Arbetsgruppen har identifierat följande behov kopplat till e-underskrifter:

- Det finns behov av att medarbetare kan skriva under elektroniskt både externt och internt[19]. Så kallad kontrasignering är i vissa fall också ett behov
- Organisationer[20], och deras verksamhetssystem och medarbetare, har behov av att kunna validera elektroniska underskrifter, både internt och över organisationsgränser. Denna validering kan vara förknippad med mycket stora utmaningar som medför behov av gemensamt stöd
- Det finns i vissa fall behov av att kunna skriva under med stöd av en pseudonym till personnummer eller annat officiellt personidentitetsbegrepp (exempelvis anställnings-id) och kunna ange vilken organisation medarbetaren tillhör vid undertecknandet.

[16] Exempelvis reglera huruvida en eID som arbetsgivaren anskaffat får användas för privat bruk
[17] DIGG:s tekniska ramverk för Sweden Connect https://swedenconnect.se/tekniskt-ramverk.html
[18] Exempelvis Ineras referensarkitektur https://www.inera.se/digitalisering/infrastruktur/infrastruktur-for-identitet-och-atkomst/referensarkitektur-for-identitet-och-atkomst/ eller attributspecifikation inom e-hälsa
[19] Exempel: interna personalärenden och i externa e-tjänster.
[20] Detta behov gäller även privatpersoner men det ligger utanför denna förstudie

- Normalt sett finns det behov av att i en digital tjänst erbjuda underskriftsmöjlighet oberoende av vilken e-legitimation som används (under förutsättning att den når viss tillitsnivå), så kallad fristående underskriftstjänst, men det kan även finnas behov av att användaren har tillgång till lokal underskriftsfunktion[21].

2.6 Behov av behörighetsgrundande information

Digitala tjänster erbjuder vanligen funktionalitet eller utökad information för vissa organisationer eller för vissa medarbetare med utgångspunkt från deras uppdrag, roller eller fullmakter. Då behöver den digitala tjänsten ha tillgång till ytterligare uppgifter om medarbetaren utöver att bara veta vem det är som loggar in och vilken organisation som anskaffat användarens eID. Uppgifterna kan exempelvis handla om vilken eller vilka fullmakter medarbetaren har. Detta är ett mycket viktigt område för att helheten ska fungera. En fördjupad behovsanalys behöver göras inom detta område och arbetet med attributförsörjning tillhör närmast i tiden deluppdrag Auktorisation och deluppdrag Mina ombud, inom samma regeringsuppdrag.

[21] Exempel: om en elektronisk handling ska skrivas under och skickas i väg och det internt inte finns någon fristående underskriftstjänst

3 Försörjning med eID för medarbetare

För att svara på frågan om försörjning med eID för medarbetare gjorde arbetsgruppen en inventering av vilka eID:n för medarbetare som finns idag. Det finns tre offentliga och tre privata alternativ som för närvarande kan anskaffas av arbetsgivare och arbetsgruppen bedömer att det är troligt att fler alternativ kan tillkomma.

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

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

Dessa alternativ ska ses som exempel att utgå från och inte som en uttömmande lista. ID06, som är vanligt inom byggsektorn, bör också nämnas. I tillägg till listan finns det interna eID-lösningar med potential att kunna användas externt.

3.1 SITHS

Identifieringstjänsten SITHS består bl.a. av en e-legitimation från Inera AB som kan användas av 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 godkänt 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.

3.2 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 godkännande och arbete med detta pågår. EFOS har kompletterats med en mobil variant, kallad mobilt EFOS.

3.3 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. eduID är inriktat på tillitsnivå 2, inklusive möjlighet till flerfaktorsautentisering, och är i skrivande stund inte godkänt av DIGG.

3.4 Privat sektors utbud för medarbetare (punkt 4 – 6)

Freja eID+ från Verisec AB finns i en variant avsedd för medarbetare, Freja Organisation eID. Freja eID+ är godkänt av DIGG på tillitsnivå 3 och finns med i den nationella identitetsfederationen för elektronisk identifiering[22], som drivs av DIGG.

Andra alternativ som kan upphandlas är Nexus SmartID och Telia, båda väletablerade aktörer på området, samt ID06 inom exempelvis byggsektorn. Dessa alternativ är dock ännu inte granskade av DIGG.

3.5 Krav vid anskaffning av eID

Det finns således förutsättningar för organisationer att kunna anskaffa eID till sina medarbetare och andra målgrupper, samtidigt som det finns behov av alla eID:n som ska användas brett blir godkända av DIGG och att ytterligare möjligheter erbjuds av eID-utfärdare så att verksamheters alla behov kan fyllas.

Krav som kan vara viktiga för arbetsgivaren att överväga i samband med anskaffning av eID berörs i avsnitt 2 om behov. Arbetsgruppen vill särskilt lyfta fram möjligheten att överväga följande krav:

- eID:n som är godkända av DIGG och har tillräcklig tillitsnivå[23]
- bärare av eID och tillgänglighetskrav som passar med verksamhetens och användares behov
- affärsvillkoren ska täcka ersättningsfri[24] användning och eventuell egen intygsfunktion
- vid användning ska intygsfunktionen stödja DIGG:s tekniska ramverk (se avsnitt 4) och finnas med i DIGG:s identitetsfederation[25]
- eventuella andra tekniska specifikationer som också ska stödjas, exempelvis vid intern användning
- om det behövs eID:n till personer utan svenskt personnummer, a) men med svenskt samordningsnummer som bygger på den högsta nivån av

[22] https://www.swedenconnect.se/
[23] Inspiration kan hämtas från kraven i DIGG:s Tillitsramverk för Svensk e-legitimation och från de digitala tjänster där eID ska användas
[24] Ibland kallad ”tick-fri”, både i förhållande till eID-anskaffande organisation och i förhållande till den förlitande aktören
[25] Se https://swedenconnect.se/

styrkt identitet[26] eller b) personer helt utan koppling till den svenska folkbokföringen[27]

Det är betydelsefullt att ramavtal tas fram som täcker behoven i de fall upphandling från privata eID-utfärdare ska göras av arbetsgivare.

3.6 Organisationers egen eID-lösning

En del organisationer har byggt upp egen eID-lösning för sina medarbetare, exempelvis Polismyndigheten, Stockholms stad och Åklagarmyndigheten.

När användning sker inom en krets av aktörer med koppling till varandra kan tillit troligen nås även utan DIGG:s godkännande. De organisationer som vill ha med sin egen eID-lösning i den förvaltningsgemensamma modellen har möjlighet att ansöka hos DIGG om granskning och godkännande enligt Tillitsramverket för Svensk e-legitimation.

3.7 Privat anskaffade svenska e-legitimationer

Även privat anskaffade eID:n, exempelvis BankID, kan tillåtas i digitala tjänster som riktar sig till medarbetare. DIGG:s godkännande och tillitsnivåer för privat anskaffade eID:n motsvarar helt de regler som gäller för eID för medarbetare.

Däremot kan det skilja sig vad gäller affärsvillkor, exempelvis så kallade tick-kostnader (transaktionskostnader), vilket kan leda till att medarbetarens arbetsgivare har regler som motsätter sig användning av privat anskaffad eID i tjänsten. Möjligheten att i eID-utfärdarens identitetsintyg få tillgång till uppgift om anskaffande organisation eller användarens arbetsrelaterade pseudonym kan dessutom vara mer begränsad.

3.8 Slutsats om försörjningen med svenska e-legitimationer

Det finns en försörjning med eID som står aktörerna fritt att vidareutveckla i enlighet med anskaffande organisationers behov. Upphandlande organisationer kan formulera sina krav vid avrop eller egen upphandling. Som inspiration kan behov som finns uppräknade i avsnitt 2 och krav från avsnitt 4 och 5 användas vid kravställning. Denna rapport lägger därför inga förslag i fråga om försörjningen med eID.

3.9 Användning av eID enligt eIDAS-förordningen

Som stöd för identifiering (autentisering) av användare med eID från annat land finns EU:s eIDAS-förordning[28]. Ett ökande antal länder har eID:n som fungerar över landsgränserna. Sverige förbereder sin första anmälan av svenska e-

[26] Här väntas förändringar i samordningsnummerhanteringen och det är den högsta kvalitetsnivån som avses här

[27] I första hand rekommenderar arbetsgruppen att arbetsgivaren rekvirerar samordningsnummer från Skatteverket baserat på högsta nivån av styrkt identitet så att användarens eID ska kunna vara kvalitetsmärkt ”Svensk e-legitimation”. I andra hand får undantagshantering för tillitsnivåmarkering gälla enligt instruktioner från DIGG.

[28] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32014R0910&from=PL

legitimationer. Det finns möjlighet för andra än EU:s medlemsstater att avtalas in i eIDAS. Norge, Island och Liechtenstein är exempel på det. DIGG tillhandahåller den svenska eIDAS-noden för e-legitimering över landsgränsen och anslutningsavtal för detta[29].

Som komplement till eID-möjligheter som hittills nämnts i denna rapport kan möjligheter över den svenska landsgränsen därför också övervägas av aktörerna.

3.10 Internationell användning av eID:n inom högskolesektorn

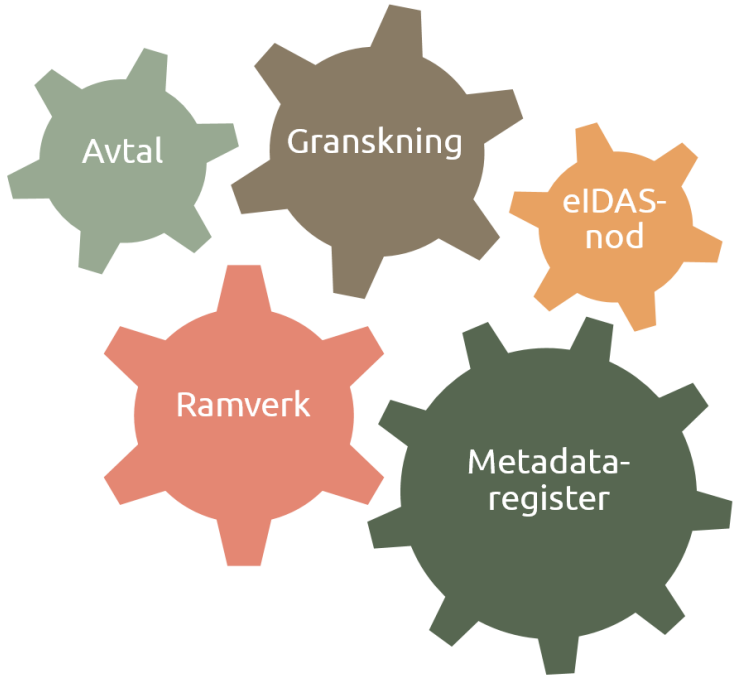
Inom den akademiska världen används redan eID:n över landsgränser i stor utsträckning. Den svenska delen består av eduID (se avsnitt 3.3) och av identitetsfederationen för forskning och högre utbildning, SWAMID, som Vetenskapsrådet/SUNET ansvarar för.

[29] Läs mer om anslutning till eIDAS-noden på DIGG:s webbplats https://www.digg.se/digital-identitet/e-legitimering/offentlig-aktor/internationell-e-legitimering

4 Befintlig digital infrastruktur

DIGG[30] tillhandahåller den förvaltningsgemensamma digitala infrastrukturen för digital identitet. Området består av infrastruktur för offentlig förvaltnings behov av e-legitimering och e-underskrift. Användare av e-legitimering och e-underskrift är fysiska individer som kan vara privatpersoner, medarbetare eller inneha andra roller.

Identitetsfederation[31] är ett samlingsbegrepp för metadataregister[32] och regler som stödjer säker elektronisk identifiering av användare. DIGG:s huvudsakliga områden kan sammanfattas i följande bild:



Figur 1: DIGG:s digitala infrastruktur för e-legitimering och e-underskrift

Den digitala infrastrukturen består i skrivande stund av:

a) Avtal om e-legitimering[33]
b) Granskning[34] av eID-utfärdare mot Tillitsramverket för Svensk e-legitimation och granskning av underskriftstjänster
c) Tillitsramverket för Svensk e-legitimation, normativ specifikation för underskriftstjänster och tekniskt ramverk

[30] Myndigheten DIGG:s information om infrastruktur för e-legitimering https://www.digg.se/digital-identitet/e-legitimering
[31] DIGG:s tekniska information om identitetsfederationen https://swedenconnect.se/
[32] Benämnt ”aktörsregister” i avtal
[33] Anslutningsavtal till Sweden Connect inklusive den svenska eIDAS-noden, samt valfrihetssystem för e-legitimering
[34] I granskningen kan även förlitande aktörer delta

d) Metadataregister[35], som tillsammans med avtal och tekniskt ramverk utgör DIGG:s identitetsfederation[36]
e) Den svenska eIDAS-noden för e-legitimering över landsgränsen

I metadataregistret deklarerar eID-utfärdare och på eID:n förlitande aktörer vilka adresser, nycklar och förmågor de har. Förmågorna handlar exempelvis om e-legitimationers tillitsnivåer och vilka tekniska profiler som stöds. Både eID-utfärdare och förlitande aktörer har rätt att anlita underleverantörer och delegera befogenhet till dem att sköta deltagandet i metadataregistret.

I metadataregistret ingår den svenska eIDAS-noden (som en IdP). Alla förlitande aktörer som har kopplat upp sig mot den svenska eIDAS-noden (”Foreign eID”) finns därför redan med i metadataregistret och har tecknat anslutningsavtalet, samt följer det tekniska ramverket åtminstone för ”Foreign eID”[37]. En förlitande aktör har även möjlighet att delegera befogenhet till sina leverantörer att i identitetsfederationens metadataregister deklarera den förlitande aktörens (arbetsgivarens) intygsfunktion och fristående underskriftstjänst.

[35] Även kallat aktörsregister, som då inkluderar även en administrativ lista över aktörerna
[36] Läs mer på DIGG:s webbplats https://swedenconnect.se/
[37] Motsvarande gäller även dem som tecknat Valfrihetssystem 2017 E-legitimering

5 Förslag och bedömningar

Bedömning: Endast e-legitimationer som är godkända av DIGG inkluderas i det nedan föreslagna avtalet

Digitala tjänster som medarbetare ska använda hanterar vanligen personuppgifter, som kan vara känsliga, och i vissa fall ingår sekretessbelagd information. Detta ställer krav på att medarbetaren är säkert identifierad innan tillträde till en digital tjänst ges.

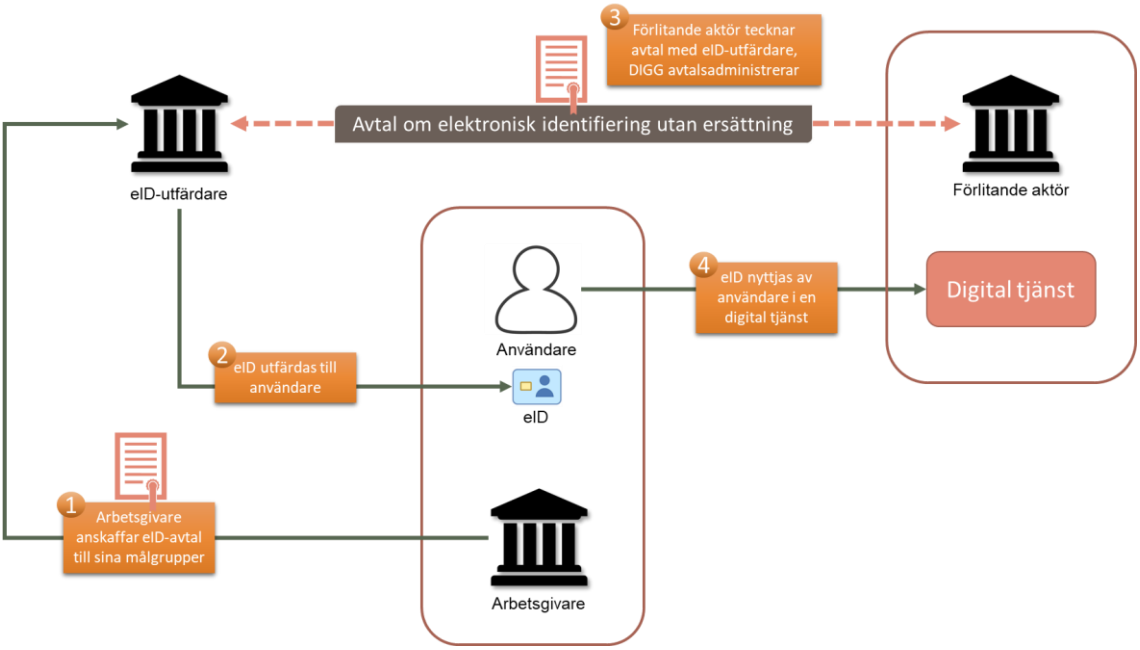
Det har kommit in önskemål om att få ansluta eID:n som inte är godkända av DIGG. Vår bedömning är att det i detta förvaltningsgemensamma sammanhang inte ska accepteras. De förlitande aktörerna väljer visserligen vilka tillitsnivåer de vill acceptera i en viss digital tjänst, men det kan uppstå tolkningsproblem eller misstag. Många timmar kan gå åt till att debattera vilken skyddsnivå lägre nivåer än de av DIGG godkända når upp till.

För en del förlitande aktörer är det dessutom väsentligt att alla eID:n är godkända av DIGG för att användaren ska ges tillgång till en tjänst, exempelvis den nationella läkemedelslistan hos E-hälsomyndigheten. Därför bör eID:n som ska stödjas i det önskade resultatet vara godkända av DIGG. Resultatet i stort ska heller inte hindra att medarbetare även fortsättningsvis kan få använda sitt godkända privata eID på arbetet[38].

Förslag: Ett kompletterande ersättningslöst e-legitimeringsavtal i två varianter tas fram och administreras av DIGG. I huvudvarianten är eID-utfärdaren leverantör, i tilläggsvarianten är arbetsgivaren leverantör.

Ett behov handlar om att den transaktionsbaserade ersättning som finns för privat anskaffade eID:n inte passar med medarbetares frekventa användning av eID i tjänsten. Vanligen har eID till medarbetare anskaffats inklusive villkor om fri användning mot att arbetsgivaren betalar en års- eller månadsavgift. Den svenska modellen för digital identitet kompletteras så att det fungerar översiktligt i enlighet med denna bild:

[38] Det är arbetsrättslig fråga och en fråga om hur attribut om medarbetaren hanteras



Figur 2 – Översiktsbild över huvudflödet i den önskade modellen

Flödet i den önskade modellen kopplat till ovanstående bild:

- Arbetsgivare anskaffar eID[39] (1.) till sina medarbetare från eID-utfärdare
- eID-utfärdare utfärdar[40] eID (2.) till användarna (medarbetarna).
- eID-utfärdare tecknar (det nya) avtalet med förlitande aktörer (3.).
- Användaren väljer som huvudalternativ sitt eID[41] (4.), eller sin arbetsgivare, i den digitala tjänstens lista över inloggningsalternativ[42]. Om användaren väljer sin arbetsgivare, görs valet av eID i stället i arbetsgivarens lista över valbara eID:n[43].

Den på eID förlitande aktören tar hjälp av sitt (sina) avtal om e-legitimering, beslutar om lägsta godtagbara tillitsnivå i sammanhanget och tar även stöd av DIGG:s metadataregister[44] för att veta vilka e-legitimationer som ska visas upp som valbara för användaren. Den förlitande aktören kan vara den helt externa

[39] En möjlighet är att avropa på Kammarkollegiets ramavtal ”Produkter och tjänster för identifiering och behörighetskontroll”
[40] I vissa fall med stöd av arbetsgivaren för identitetskontroll av medarbetaren och utgivning
[41] Kan vara en samlad inloggningspunkt för flera tjänster hos den förlitande aktören, ibland kallad den förlitande aktörens IdP
[42] Beroende på vilka intygsfunktioner som ingår och vilka visningsnamn de har
[43] Om det vid tillfället inte fungerar med single sign-on
[44] https://swedenconnect.se/

organisation som användaren vill få tillträde hos, eller arbetsgivarens centrala inloggningsfunktion (”IdP”).

eID-utfärdaren svarar på begäran från förlitande aktörer med ett i det externa huvudfallet krypterat identitetsintyg baserat på avtalsregler[45]. Den förlitande aktören dekrypterar identitetsintyget och avgör om ytterligare uppgifter om användaren ska hämtas in.

Identitetsintyg som skickas mellan eID-utfärdare och förlitande aktörer i Sverige passerar inte DIGG[46], utan går direkt mellan eID-utfärdaren och den förlitande aktören. Mönstret kallas i den juridiska vägledningen om e-legitimering[47] för ”direkt legitimering”. Både eID-utfärdaren och den förlitande aktören kan ha underleverantörer.

När den på eID förlitande aktören är arbetsgivaren, kan arbetsgivaren (själv eller med stöd av underleverantör) i sin tur ställa ut intyg med stöd av sin egen intygsfunktion (IdP). Syftet med detta kan vara att underlätta single sign-on, minska antalet interaktioner för användaren, konvertera från annan teknisk metod eller att komplettera med ytterligare attribut i förhållande till de förlitande aktörer som arbetsgivaren har avtal med. Arbetsgivaren får[48] registrera sin IdP i DIGG:s metadata och kan delegera till en underleverantör att bistå med teknisk kontaktperson. I denna variant blir eID-utfärdaren underleverantör till arbetsgivaren.

Bedömning: det är av central betydelse att även IdP-leverantörer tillitsgranskas och godkänns av DIGG.

DIGG tillitsgranskar eID-utfärdare och deras e-legitimationer mot Tillitsramverket för Svensk e-legitimation. DIGG utför tekniska tester för att kontrollera att IdP:er i DIGG:s identitetsfederation följer DIGG:s tekniska ramverk. DIGG kommer framledes, även av andra skäl än ”eID för medarbetare”, att tillitsgranska IdP-leverantörer mot relevanta delar av Tillitsramverket för Svensk e-legitimation. Därmed kan en större acceptans nås för den variant av e-legitimeringsavtal där arbetsgivare med godkänd IdP är leverantör. Mönstret kallas i den juridiska vägledningen om e-legitimering för ”indirekt legitimering”. Tillitsgranskning av IdP-leverantörerna är nödvändig för att skapa tillit hos förlitande aktörer, exempelvis E-hälsomyndigheten.

[45] Begreppet identitetsintyg ska vid användning av andra metoder än SAML tolkas på en logisk nivå, inte teknisk.
[46] Däremot hanterar DIGG de identitetsintyg som skickas över landsgränsen i enlighet med EU:s eIDAS-förordning
[47] Vägledningen nås via denna webbsida https://www.digg.se/digital-identitet/e-legitimering/offentlig-aktor
[48] Redan nu efter att ha tecknat det kostnadsfria avtalet för förlitande aktörer om anslutning till Sweden Connect

Bedömning: DIGG:s tekniska ramverk behöver ses över för att precisera möjligheten att ange medarbetares pseudonym

Identitetsfederationens tekniska profiler kan behöva kompletteras för att stödja identitetsintyg som avser medarbetare (exempelvis gällande medarbetarens anställningsnummer) efter den ”skrivbords-PoC” som är planerad i nästa steg.

För att auktorisation av medarbetare ska kunna göras i digitala tjänster som exempelvis har behov av uppgift om medarbetarens roll krävs ytterligare åtgärder som ligger utanför denna förstudierapport.

Önskemål om federationsstöd för annan teknisk standard än SAML 2.0, främst OpenID Connect, har framförts och hänsyn till detta behöver tas i vidareutveckling av infrastrukturen i takt med att standarder finns.

Bedömning: vägledning och kommunikation om de föreslagna möjligheterna är en kritisk framgångsfaktor

I takt med att nya avtalsmöjligheter tas fram måste information spridas så att aktörerna kan agera. Utöver information om nya avtalsmöjligheter, är det viktigt att DIGG lyfter fram information om vilka avtalsparter som erbjuder vad i klartext på webben, så att medarbetare och avtalsparter ges goda förutsättningar att navigera bland möjligheterna[49].

Bedömning: det är viktigt att eID-utfärdare, arbetsgivare och förlitande aktörer tar tillvara de nya möjligheterna

Aktörernas funktioner är till viss del, men inte helt och hållet, anpassade till DIGG:s digitala infrastruktur. Detta gäller främst de förlitande aktörer som har kopplat upp sig mot den svenska eIDAS-noden (”Foreign eID”) eller Valfrihetssystem 2017 E-legitimering (Freja eID+). I stort sett alla parter har någon funktion som stödjer den underliggande standarden (SAML 2.0).

Några eID-utfärdare har svarat att de inte omedelbart kan ansluta sig till identitetsfederationen eller är godkända av DIGG men att de vill skapa förmågorna över tid. Samma sak är aktuellt för de förlitande aktörerna, de kan behöva göra justeringar som kan kräva avrop eller budgetering. Synpunkter har kommit in om att parterna till viss del kan vilja göra på ett annat tekniskt sätt, exempelvis internt, även över tid och att det föreslagna avtalet bör vara öppet för detta.

[49] Se även värdeerbjudanden och produkter/tjänster i Bilaga 2

Slutsats: I snävare krets, exempelvis i förhållande till upphandlade lösningar, kan även andra inloggningsmetoder förekomma än de som är godkända av DIGG

Många förlitande aktörer är måna om att endast godkända e-legitimationer ingår. För andra förlitande aktörer kan det exempelvis räcka med ”flerfaktorsautentisering” som lägsta krav. Principen som råder är att det är den på eID förlitande aktören som avgör vilken lägsta tillitsnivå som krävs.

Inom en viss krets av organisationer kan det därför finnas andra överenskommelser, exempelvis gällande e-legitimationer och andra inloggningsmetoder som inte kan bli godkända av DIGG därför att de inte uppfyller kraven.

6 Avtal om ersättningsfri e-legitimering

I fallet med medarbetares användning av e-legitimationer som är anskaffade av arbetsgivare[50] inkluderas normalt sett ersättning för användning av e-legitimationen i de avgifter som eID-utfärdaren enligt avtal får från den organisation som anskaffat e-legitimationerna. Därmed[51] blir det möjligt med ett civilrättsligt benefikt e-legitimeringsavtal mellan eID-utfärdare och förlitande aktörer[52].

Avtalsparterna i huvudvarianten är

a) godkända svenska **eID-utfärdare** och
b) (på eID) **förlitande aktörer** i Sverige[53].

Funktionen består av elektronisk identifiering (”e-legitimering”), där eID-utfärdaren tillhandahåller en identitets- och intygsfunktion. På begäran av en förlitande aktör i avtalet e-legitimerar eID-utfärdaren användare med av DIGG godkända e-legitimationer. I anslutning till detta ställer eID-utfärdaren, eventuell med hjälp av underleverantör, ut ett identitetsintyg, som stämplas i eID-utfärdarens namn, till den förlitande aktören.

Översiktliga villkor:

- Rätt tillitsnivå[54] kopplat till utfärdade e-legitimationer ska anges och eID-utfärdaren tillhandahåller en identitetsfunktion och en eller flera intygsfunktioner kopplade till dessa
- Parterna ska ha för avsikt att ingå i DIGG:s metadataregister och följa DIGG:s tekniska ramverk[55]
- Fler tekniska metoder[56] än de som avtalet hänvisar till får användas (exempelvis för ökad tillgänglighet internt)
- eID-utfärdaren tillhandahåller identitets- och intygsfunktioner utan ersättning

[50] Även andra ansvariga organisationer än arbetsgivare och även andra målgrupper än medarbetare är tänkta att kunna omfattas av avtalet
[51] En rättslig promemoria med en upphandlingsrättslig bilaga tas fram parallellt med denna förstudierapport
[52] Ett civilrättsligt avtal mellan eID-utfärdare och förlitande aktörer, med DIGG som avtalsadministratör och avtalsombud
[53] Privat sektors förlitande aktörer kan först inkluderas om författningsstöd finns för detta
[54] Enligt anvisning från DIGG
[55] https://www.swedenconnect.se/tekniskt-ramverk.html
[56] Begreppet intygsfunktion får i dessa fall tolkas i överförd bemärkelse, det kan exempelvis inkludera OCSP-response

- DIGG kan eventuellt vara tvungen ta ut en avgift om finansiering av DIGG:s arbete inte kan ordnas på annat sätt. Denna avgift ska dock inte vara transaktionsbaserad[57].

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

En förberedande rättslig analys har därför inletts inom ramen för pågående förstudiearbete. En enkel avtalskonstruktion skulle kunna nå stor framgång på kort tid[58] om möjligheten kommuniceras ut på ett bra sätt. Därmed kan eID:n för medarbetare börja användas på betydligt bredare front än hittills och tidigare ej nådda nyttor realiseras[59].

Utöver detta krävs ytterligare en avtalsvariant för att täcka behoven.

Avtalsparterna i denna variant är

a) svenska **arbetsgivare** och
b) (på arbetsgivares intyg) **förlitande aktörer** i Sverige[60].

Funktionen består av elektronisk identifiering, det vill säga att arbetsgivaren tillhandahåller en intygsfunktion och som underleverantör har arbetsgivaren eID-utfärdarens funktion enligt ovan, kopplad till av DIGG godkända e-legitimationer. På begäran av en förlitande aktör svarar arbetsgivares intygsfunktion efter att, vid behov, ha förnyat eID-utfärdarens identitetskontroll. Motsvarande översiktliga villkor som ovan ska gälla.

[57] Det vill säga inte utgöra en kostnad per transaktion
[58] Jämfört med införandet av valfrihetssystem
[59] Beskrivning av nyttor ingår i regeringsuppdragets rapport till regeringen (januari 2021)
[60] Privat sektors förlitande aktörer kan först inkluderas när författningsstöd finns för att göra detta

7 Medarbetares möjligheter till e-underskrifter

Enligt E-legitimationsenkäten 2019 var medarbetares underskriftsmöjligheter ett viktigt behov. En medarbetare kan exempelvis behöva

1) göra underskrift i en extern digital tjänst
2) skriva under en PDF som ska skickas i väg eller
3) skriva under ett internt personalärende.

Det är alltid en användare, dvs. i detta fall en medarbetare, som står bakom 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 i förekommande fall) bör analysera är om underskrift verkligen behövs vid övergång från papper till digitalt alternativ. Ibland kan den digitala tjänstens utformning 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 lokal underskriftsfunktion.

7.1 Huvudspår: fristående underskriftstjänst kopplad till den digitala tjänst där användaren befinner sig

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. Den kan användas både för personalens interna underskrifter och externa målgruppers underskrifter i organisationens digitala tjänster. Kammarkollegiet erbjuder ramavtal för avrop av fristående underskriftstjänst inom Programvaror och tjänster 2019.

Ett viktigt krav vid upphandling är att ha klart för sig vilken säkerhetsnivå underskrifter som högst ska nå upp till: 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. Dessutom är det viktigt att analysera hur underskriftstjänsten ska införas kopplat till tjänster där den ska användas, hantering av sekretesskänslig information, samt hur validering och bevarande ska lösas.

Idag används fristående underskriftstjänster vanligen för att skapa avancerade e-underskrifter.

7.2 Validering av underskrifter som skapas hos förlitande aktör

Så fort underskriften har skapats med stöd av en fristående underskriftstjänst i anslutning till den digitala tjänsten kan underskriften enkelt valideras eftersom den förlitande aktören rår över underskriftslösningen. Det finns ett förslag baserat på ett Vinnovaprojekt om att det efter validering vore värdefullt att ställa ut ett valideringsintyg[61] i klartext. Arbetsgruppen anser att det är en god idé, se vidare under punkt 7.5 om långtidsvalidering.

7.3 I vissa fall finns behov av lokal underskrift

När den på underskriften förlitande aktören 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 underskriftsfunktion. Så kan vara fallet vid gränsöverskridande transaktioner eller för att det internt inte är så vanligt med e-underskrifter.

Om det inte passar med fristående underskriftstjänst finns det därför skäl för arbetsgivaren att överväga anskaffning av lokal underskriftsfunktion exempelvis i samband med anskaffning av eID till medarbetare. 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 eller kommun- och regiongemensam funktion hänvisar till eller erbjuder en för behovet förberedd fristående underskriftstjänst som kan användas mot självkostnadspris per underskrift, 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 aktören, som vid behov validerar underskriftscertifikatet. Om handlingen kommer in externt ifrån kan validering vara utmanande på den avancerade e-underskiftsnivån (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 aktören. Bolagsverket och Skatteverket är två exempel på organisationer som ibland får in underskrifter som inte kan valideras

[61] Läs utkast till tekniska specifikationer för valideringsintyg i punkt 15 -17 på https://docs.swedenconnect.se/technical-framework/

och därför i många fall avvisas. I denna fråga krävs samarbete på internationell nivå.

I takt med ökad digitalisering kommer valideringsutredningar som görs hos många förlitande aktörer att totalt sett bli mycket kostsamma. Det finns därför ett stort behov av ett förvaltningsgemensamt stöd för validering. Den offentliga utredningen ”reboot” (SOU 2017:114) föreslog att DIGG ska ha ett sådant uppdrag.

7.5 Långtidsvalidering med stöd av valideringsintyg

En annan fråga som det finns behov av att lösa är den komplexitet som uppstår vid försök att validera elektroniska underskriftscertfikat 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, men denna metod för långtidsvalidering kan innebära mycket kostnadskrävande rutiner.

Arbetsgruppen ser två alternativa lösningar på problemet:

1) att validera direkt efter mottagandet, och därefter förlita sig på att validering har gjorts eller
2) att validera direkt efter mottagandet, ställa ut ett valideringsintyg i klartext och stämpla det med ett certifikat som inte löper ut och därefter förlita sig på valideringsintyget.

Valideringsintyget förändrar inte den elektroniska handlingen eller dess underskrift utan utgör ett tillägg som också följer med handlingen i dess bevarande om inget gallras. Långtidsvalidering av valideringsintyget kommer att fungera väl.

På underskriftsområdet finns det därmed behov av ett utökat förvaltningsgemensamt stöd. Den offentliga utredningen om betrodda tjänster (I 2020:01) har i uppdrag att se hur den offentliga förvaltningens användning av bland annat underskriftstjänster kan öka.

8 Risker och konsekvenser

Denna rapport föreslår en att ny avtalsmöjlighet om elektronisk identifiering tas fram av DIGG. Den viktigaste konsekvensen av ett lyckat införande är att eID-utfärdarens eID blir än mer framgångsrikt, samtidigt som både arbetsgivare och medarbetare blir nöjda över att deras eID kan användas brett som arbetsredskap utan att transaktionskostnader uppstår. Det föreslagna avtalet träffar privata och offentliga eID-utfärdare på likvärdigt sätt. Flertalet eID-utfärdare tar redan idag betalt av den eID-anskaffande arbetsgivaren och erbjuder kostnadsfria transaktioner.

Vi ser följande risker kopplat till förslag i denna rapport:

1. Långsam anslutning av förlitande aktörer, exempelvis statliga myndigheter, till avtalet
2. Långsam anslutning av eID-utfärdare till avtalet, samt d:o arbetsgivare
3. Icke-fungerande marknad för eID leder till för höga kostnader för den eID-anskaffande parten
4. Ett fåtal profiler för medarbetarens pseudonym accepteras inte av tillräckligt många eller antalet profiler blir för många och brister därmed i bred användbarhet mellan aktörerna
5. Spretiga krav vid upphandling av fristående underskriftstjänst, exempelvis kring pseudonym, leder till onödigt kostsamma underskriftstjänster
6. Avtalet som föreslås i denna rapport ersätts av annan reglering.

Den viktigaste åtgärden kopplat till alla risker är god kommunikation. Läs mer om riskerna, orsaker, påverkan och åtgärder i Bilaga 3 – Risk- och konsekvensanalys.

9 Plan för fortsatt arbete

9.1 Aktiviteter hos DIGG

Övergripande förslag till plan för fortsatt arbete[62]:

December 2020 – december 2021

1. Leda en ”skrivbords-PoC” för några möjliga tillkommande sektorsoberoende attribut (pseudonym, organisation).
2. Informera om förstudierapporten och bidra till rapportering av regeringsuppdraget
3. Ta fram civilrättsliga avtal om elektronisk identifiering utan ersättning
4. Vid behov, komplettera profiler i DIGG:s tekniska ramverk
5. Bidra med underlag till DIGG:s löpande uppdrag om vägledning och stöd inom området så att förlitande aktörer får bättre stöd för att veta vad de bör anskaffa och vilka övergripande krav som bör ställas, samt vid behov till kompletteringar av regelverk.
6. Kommunicera om möjligheten ”eID för medarbetare”

9.2 Aktiviteter hos övriga aktörer

För ett lyckat införande krävs att följande aktörer också utvecklar sina förmågor:

- eID-utfärdare vidareutvecklar eID:n och intygsfunktioner baserat på behoven
- Arbetsgivare anskaffar eID till sina medarbetare och andra målgrupper
- Förlitande aktörer finjusterar sina anslutningar så att medarbetares eID:n finns som valbara inloggningsalternativ.

[62] Under förutsättning att tillräcklig finansiering inom byggblocket finns

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
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**
E-legitimering	Se **elektronisk identifiering**
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-förordningens definition)

Förlitande aktör (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 personers, organisationers och sakers identitetsbegrepp och identifieringsprocess. I denna förstudie: personers (individers) identitet
Identitetsintyg	Intyg som efter kontroll av användarens identitet stämplas och skickas till **förlitande aktör**
IdP	Intygsfunktion som ställer ut **identitetsintyg**
Medarbetare	Här: **användare** (exempelvis medarbetare, konsult, förtroendevald, elev, boende) vars **eID** har anskaffats på ett sådant sätt att ersättning för eID-utfärdarens kostnad för **elektronisk identifiering** ingår
Metadataregister	Här: det tekniskt läsbara aktörsregistret till stöd för e**lektronisk identifiering**
Organisatorisk tillit	Här: att en organisation, vanligen baserat på författning eller avtal, litar på att en annan organisation har autentiserat användaren på en tillräckligt hög tillitsnivå i förhållande till krav i författning eller avtal
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**

Bilaga 2 - Uppdragets utförande

Förstudiearbetet har bedrivits inom regeringsuppdraget Att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (I2019/03306/DF), där medarbetares ”digitala identitet” har visat sig vara viktigt för att nå framgång.

Som underlag för denna förstudierapport har arbetsmöten hållits på distans under perioden 2020-05-11 och 2020-11-30. Bemanningen har bestått av:

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

I tillägg till denna bemanning finns det fortsatt ett behov av juridiska resurser för att arbeta vidare med det föreslagna avtalet och resurser för att arbeta med en skrivbords-PoC (proof of concept) för medarbetares pseudonymer.

Bilaga 3 - Värdeerbjudanden

Business Model Canvas (BMC) för Byggblock Identitet

Business Model: Identitet

Datum: 2020-11-19
Version: 0.75

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

- Utveckling, förvaltning, drift och support av identitetsfederation (Sweden Connect)
- Juridisk kompetens för avtalshantering och attributförsörjning
- Informationssäkerhet för tillitsramverk, certifikatsutfärdande och attributförsörjning
- Andra byggblock (Tillitsramverk, Auktorisation, Mina ombud m.fl.)

Värdeerbjudande

- Enkel tillgång till elektronisk identifiering av privatpersoner
- Enkel tillgång till elektronisk identifiering av medarbetare
- Stöd till välfungerande funktioner för elektroniska underskrift
- Stöd till välfungerande funktioner för elektronisk stämpel för organisationer
- Stöd till välfungerande funktioner för elektronisk identifiering av smarta saker
- Enkelt att få reda på svenska eID:n som godkänts av DIGG och vilka som finns i vilka avtal
- Digital infrastruktur för användning av eID inom Sverige och utomlands
- Möjlighet för svenskar att identifieras sig utomlands
- Möjlighet för svenska aktörer att identifiera privatpersoner och medarbetare med utländskt eID

Kundrelation

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

Kanaler

Webb - digg.se, swedenconnect.se
DIGG Kundtjänst
Sociala medier
Konferenser (t.ex. DIGG-dagar & Offentliga rummet)
Forum (t.ex. användarforum för digital infrastruktur och Sweden Connect)

Kunder & Kundsegment

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

Utfärdare av eID:
- Offentliga aktörer
- Privata aktörer

Arbetsgivare (tillhandahållare av eID för medarbetare):
- 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

- Enklare för svenskar att använda utländska digitala tjänster
- Ökad möjlighet till anonymisering och pseudonymisering
- Den digitala infrastrukturen för e-underskrifter och e-stämplar utvecklas
- Ökad spårbarhet, informationssäkerhet och integritet
- eID fungerar även utanför Sverige
- Användning av ny och befintlig infrastruktur ökar genom vägledningar och checklistor m.m.

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

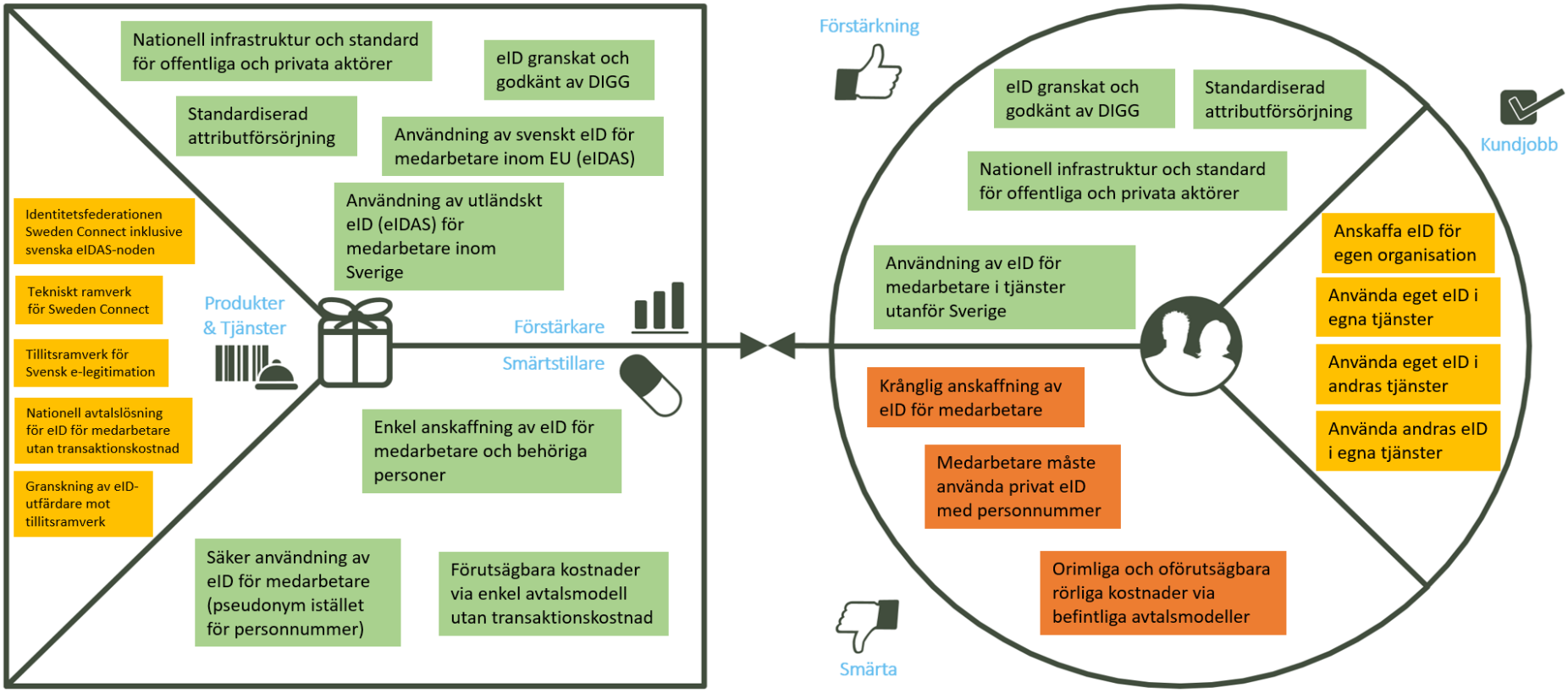
Värdeerbjudande — Kundsegment

Datum: 2020-11-19

Version: 0.75

Enkel tillgång till elektronisk identifiering av medarbetare

Arbetsgivare / Förlitande parter



Bilaga 4 – Risk- och konsekvensanalys

ID	Namn	Händelse	Orsak	Påverkan	Åtgärd
1	Långsam anslutning av förlitande aktörer	Svårt att kommunicera ”ännu ett avtal”	Frågan är väldigt outsourcad till leverantörer	Långsamt införande, missnöjda medarbetare m.fl.	Kommunikation både med förlitande aktörer och deras leverantörer om att avtalet innebär en viktig möjlighet
2	Långsam anslutning av eID-utfärdare (eller arbetsgivare med eID-utfärdare som underleverantör)	För få eID-utfärdare ansluter sig inom ett år efter avtalet finns	Om avtalets innehåll skulle bli hindrande	Långsamt införande, sjunkande tillit från förlitande aktörer och medarbetare	God kommunikation under framtagning av avtal och därefter
3	Icke-fungerande marknad för eID	eID-anskaffande parter upplever att eID-alternativen inte täcker behoven eller är för dyra	För få aktörer, icke fungerande marknad	Missnöjda parter	Kammarkollegiets ramavtalsupphandling Uppmuntra att fler anskaffningsalternativ finns och värna att det även fortsatt finns offentliga alternativ

4	Svårt att standardisera medarbetares pseudonym	Ett fåtal profiler för medarbetarens pseudonym accepteras inte av tillräckligt många eller antalet profiler blir för många och brister därmed i bred användbarhet mellan aktörerna	Alla vill ha det på sitt sätt	Långsamt införande, missnöjda parter	Gör ”skrivbords-PoC” i samverkan med alla som är intresserade
5	Spretiga krav vid upphandling av fristående underskriftstjänst, exempelvis kring pseudonym	Om DIGG inte bidrar tillräckligt till ensade eller kända krav	Olika kunder vill ha igenom sina krav därför att DIGG inte har anpassat specifikationer eller kunder inte förstått att de finns	Dyrare fristående underskriftstjänster	Vidareutveckla specifikationer och kommunicera
6	Lag i stället för avtal	Om ny lag skulle ersätta avtal	Om den offentliga utredningen skulle lägga ett lagförslag som går igenom	På sikt ersätta det här föreslagna avtalet	Börja avtalsmässigt enkelt för att minimera resursåtgång. Arbetsgruppen bedömer att det ändå alltid behövs något liknande avtal.