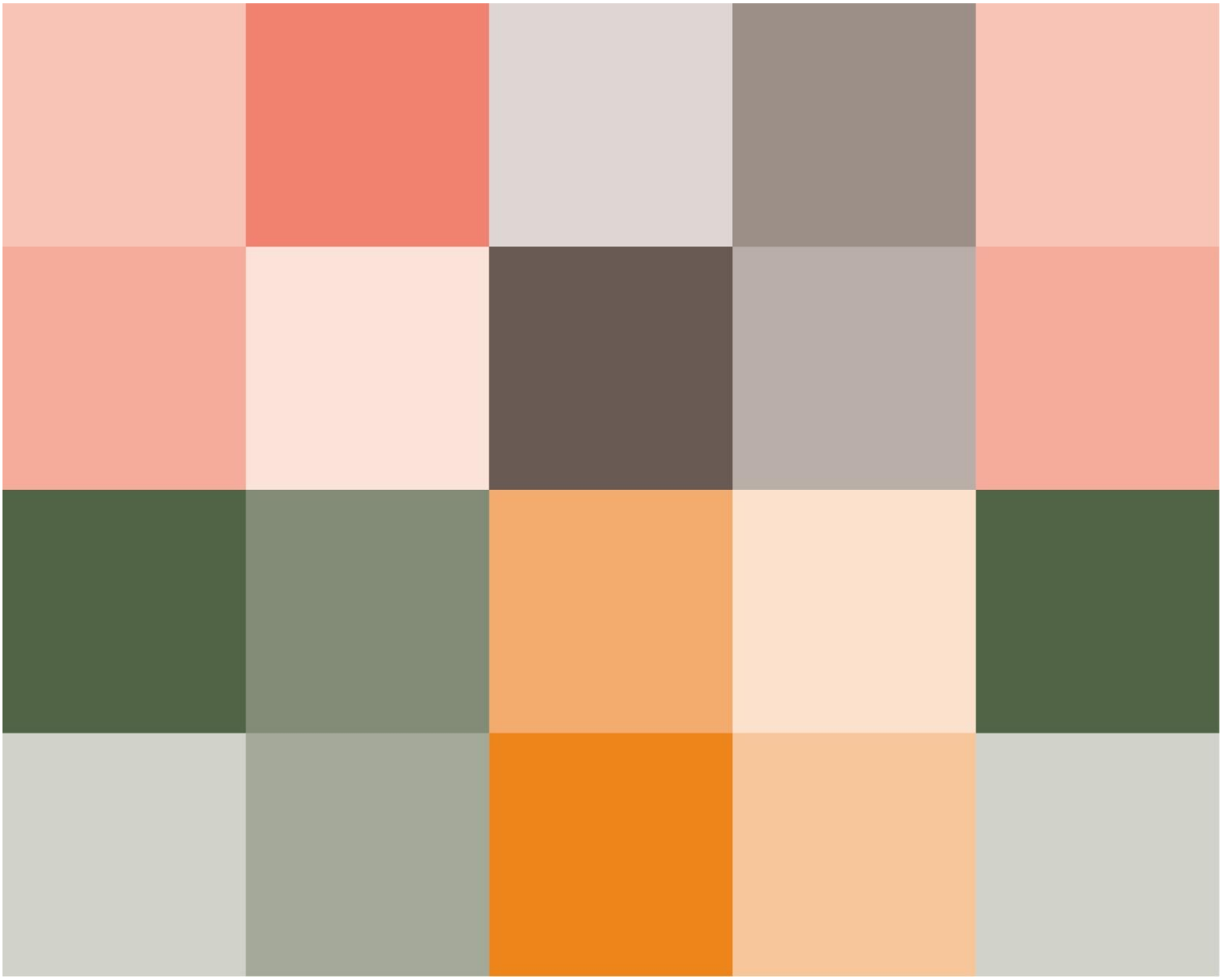


Utveckling av det svenska e-legitimationssystemet

2021-11-23 version 1.0

DNR: 2021-2493

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Innehållsförteckning

1 Inledning

Digitala tjänster används numera i stor utsträckning i det svenska samhället. Det finns idag ett stort antal offentliga och privata tjänster som erbjuder åtkomst med hjälp av e-legitimation, och nya tjänster lanseras kontinuerligt.

De tjänster som tillhandahålls av offentlig sektor sträcker sig från de som majoriteten av Sveriges befolkning använder, som att lämna in deklarationer och kommunicera med vården, till tjänster som riktar sig till en smalare målgrupp, som att göra en bygganmälan angående eldstad till kommunens byggnadsnämnd eller att ansöka om skolskjuts. Under 2020 användes e-legitimation över 400 miljoner gånger i offentliga e-tjänster. Skatteverket, Försäkringskassan och 1177.se var de tre största aktörerna.

Syfte med detta dokument är att ge en nulägesbild av det svenska e-legitimationssystemet och lämna översiktliga förslag på utveckling som krävs för att Sverige skall lyckas framåt. Förslag till åtgärder finns i avsnitt 8. Dessa är uppräknade efter problemområde och inte inbördes prioriterade.

2 Elektronisk identifiering i Sverige

Redan 2002 kunde bankerna identifiera 2,7 miljoner svenskar elektroniskt på ett tillförlitligt sätt i sina internetbanktjänster som använde ett antal olika identifieringslösningar, exempelvis bankdosor. Därför föll det sig naturligt att banker svarade på statens upphandling av elektronisk identifiering i offentliga digitala tjänster. För detta, och för att underlätta den tekniska integrationen och kunna identifiera medborgarna på ett enhetligt sätt, lanserades den gemensamma bankinfrastrukturen BankID 2003.

BankID tillhandahålls av det av banker samägda bolaget Finansiell ID-teknik BID AB (”BID”) och utgivning till användare sköts av elva[1] svenska banker.

År 2003 använde 27 000 personer BankID för att lämna in sin deklaration elektroniskt till Skatteverket. Sedan dess har användningen ökat exponentiellt, särskilt sedan 2011 då Mobilt BankID lanserades.

År 2019 användes BankID av 84 % av den svenska befolkningen över 16 år[2].

I november 2020 hade 98% mellan 18 och 67 år ett eller flera BankID:n[3]. BankID användes ca 400 miljoner gånger i offentlig sektors e-tjänster 2020, vilket motsvarar 7,9 % av BankID:s 5,1 miljarder transaktioner det året.

Våren 2021 har BankID åtta miljoner användare.

De offentliga myndigheternas tidiga införande av digitala tjänster och elektronisk identifiering ledde, vid sidan av internetbankerna, till ökad acceptans hos allmänheten.

Telia levererade identifiering med sin e-legitimation i statens upphandling redan från start. I skrivande stund ges Telias e-legitimation endast ut via arbetsgivare, till medarbetare. Ytterligare e-legitimationer har tillkommit, från såväl den privata

[1]Banker som ger ut BankID https://www.bankid.com/kontakt/utfaerdare

[2] Svenskarna och Internetundersökningen:https://svenskarnaochinternet.se/english/

[3] BankID:s årsstatistik för 2020: https://www.bankid.com/assets/bankid/stats/2020/statistik-2020-12.pdf

som den offentliga sektorn, däribland Freja eID Plus, AB Svenska Pass, EFOS och SITHS.

2.1 Myndigheten för digital förvaltning

DIGG har i uppgift att samordna och stödja digitaliseringsarbetet inom den offentliga förvaltningen. DIGG ansvarar för den gemensamma digitala infrastrukturen inom den offentliga förvaltningen, däribland den för elektronisk identifiering. Myndigheten följer och analyserar utvecklingen på detta område och bistår regeringen med rådgivning för digital policyutveckling samt främjar användningen av sådana tjänster.

DIGG:s roll är samordnande, vilket innebär att alla offentliga myndigheter ansvarar för sina egna e-tjänster, inklusive upphandling av elektronisk identifiering och e-underskrift till dessa tjänster. För att hjälpa den offentliga sektorn att anskaffa effektiva och säkra tjänster för identifiering och underskrift tillhandahåller DIGG avtal och annan gemensam infrastruktur för detta. Den svenska infrastrukturen för identifiering och underskrift beskrivs i avsnitt 2.

2.2 Utveckling av en gemensam infrastruktur

Flera olika e-legitimationer på marknaden innebär utmaningar för myndigheterna. Brist på standardisering riskerar att leda till inlåsning av leverantörer och höga genomförandekostnader på grund av behovet av att anpassa sig till flera grundläggande tekniska gränssnitt.

För att åtgärda detta har en standardiserad infrastruktur för tillhandahållande av eID-tjänster och e-underskrifter utvecklats för att samordna och förenkla för de offentliga myndigheterna, och för att främja ytterligare utveckling av digitala tjänster. Utöver valfrihetssystem och tillitsramverk ingår därför en nationell identitetsfederation, Sweden Connect, i infrastrukturen.

E-legitimationsutfärdare är med sina intygsfunktioner är leverantörer i Sweden Connect. När användaren legitimerar sig skickar e-legitimationsutfärdaren ett identitetsintyg i ett standardiserat format till förlitande aktörer[4] (e-tjänsten). Sweden Connect inkluderar även den svenska eIDAS-noden kopplad till utländska

[4] Endast offentliga myndigheter får våren 2021 ingå som förlitande aktörer. Målgruppen är på väg att breddas.

e-legitimationer, och framöver även till svenska e-legitimationer som används utomlands.

Sweden Connect stöder för närvarande den tekniska standarden SAML 2.0[5]. De centrala delarna av Sweden Connect är de tekniska specifikationerna och metadata som beskriver aktörerna och deras förmågor, i kombination med säkra rutiner för anslutning och incidenthantering. DIGG ansvarar för ledning och drift av Sweden Connect.

[5]Arbete pågår för att komplettera med den tekniska metoden OpenID Connect i federation.

3 Det svenska eID-systemet

DIGG tillhandahåller det svenska systemet för elektronisk identifiering. Det består av en infrastruktur uppbyggd av följande hörnstenar:

En rättslig ram

Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG[6] — eIDAS-förordningen

- Lag (2016: 561) om kompletterande bestämmelser till eIDAS-förordningen[7]
- Folkbokföringslagen (1991: 481)[8]
- Lag (2013: 311) om valfrihet med avseende på tjänster för elektronisk identifiering
- Förordning (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering
- Förordning (2018: 1486) med instruktion för Myndigheten för digital förvaltning[9]

En avtalsstruktur

Nationell trafik

- Valfrihetssystem/auktorisationssystem
- Kommande avtal om förbetald elektronisk identifiering (eID för medarbetare)

[6] HTTPS://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[7] HTTPS://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2016561-med-kompletterande-bestammelser_sfs-2016-56173.01.ENG

[8] HTTPS://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/folkbokforingslag-1991481_sfs-1991-481

[9] HTTPS:////www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20181486-med-instruktion-for_sfs-2018-1486

Internationell trafik

- Avtal för förlitande aktörer om anslutning till Sweden Connect och den svenska eIDAS-noden
- Avtal för anmälda e-legitimationsutfärdare om elektronisk identifiering utomlands

Avtalsbilagor

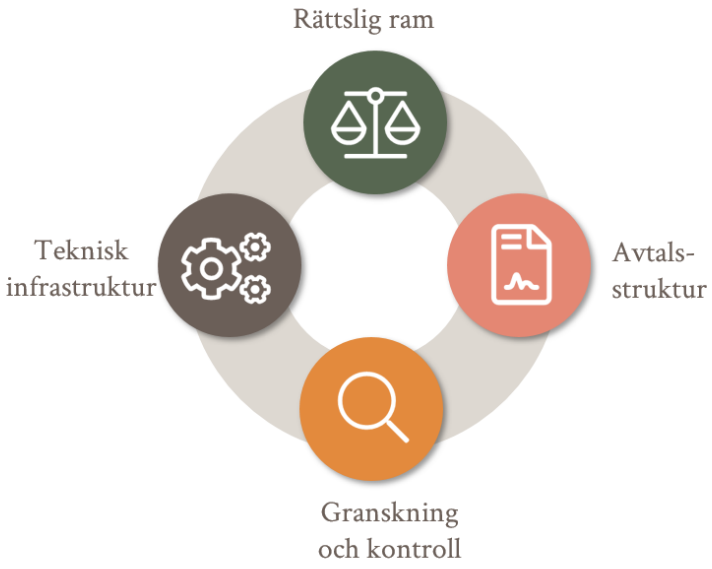
- Tillitsramverket för Svensk e-legitimation
- Tekniskt ramverk för Sweden Connect
- Behandling av personuppgifter
- Avgifter (kommande bilaga)
- Regler för den praktiska hanteringen av infrastrukturen (kommande bilaga)

Granskning och kontroll

- Granskning av de e-legitimationsutfärdare och identitetsintygsutfärdare som ansöker till DIGG
- Efter godkänd granskning skrivs licensavtal om
    - incidentrapportering,
    - årliga revisionsrapporter,
    - återkommande granskning och
    - rätten att få använda kvalitetsmärket Svensk e-legitimation

En teknisk infrastruktur

- Sweden Connect – DIGG:s identitetsfederation
- eIDAS-noden



Figur 1: Hörnstenarna i det svenska e-ID-systemet

Tillsammans skapar hörnstenarna ett öppet ekosystem för e-legitimationsutfärdarna. Alla eID-utfärdare som genomgått granskning enligt tillitsramverket har rätt att ingå avtal med DIGG om elektronisk identifiering i, för närvarande, offentlig förvaltnings e-tjänster. Nya eID-utfärdare som kommer in på marknaden kan ansluta sig till successivt. Om de är godkända för kvalitetsmärket och används i minst en offentlig e-tjänst kan de också ansöka om att omfattas av den svenska anmälan till eIDAS för elektronisk identifiering utomlands.

3.1 Rättslig ram

eIDAS-förordningen, tillsammans med lagen (2016: 561) om kompletterande bestämmelser till eIDAS-förordningen, fastställer den rättsliga grunden för användningen av e-legitimation och e-underskrifter för både privat och offentlig användning. Genom ändringar i brottsbalken (1962: 700) år 2013 fick[10] digitala identitetshandlingar och elektroniska underskrifter samma straffrättsliga skydd som traditionella identitetshandlingar och undertecknade handlingar. Detta

[10] HTTPS://www.government.se/government-policy/judicial-system/the-swedish-criminal-code/

innebär att manipulationer eller missbruk av dessa omfattas av bestämmelserna i brottsbalken.

I förordning med instruktion (2018:1486) har den svenska regeringen gett DIGG ansvaret för att:

1. Ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift
2. Tillhandahålla och administrera valfrihetssystem
3. Främja den offentliga sektorns användning av elektronisk identifiering och -underskrift
4. Ansvara för den svenska eIDAS-noden
5. Anmäla svenska e-legitimationer enligt eIDAS

DIGG ansvarar för eIDAS-noden för gränsöverskridande elektronisk identifiering i enlighet med eIDAS-förordningen. Myndigheten ges också befogenhet att utfärda nationella bestämmelser om krav på e-legitimationsutfärdare och att anmäla system till EU-kommissionen för gränsöverskridande autentisering.

Lagen (2013: 311) om valfrihetssystemet för elektronisk identifiering utgör grunden för upphandling av e-legitimering till den offentliga sektorn och föreskriver att tjänsteleverantörer ska behandla godkända e-legitimationsutfärdare lika, på ett icke-diskriminerande sätt. Slutanvändaren ges frihet att välja den lämpligaste e-legitimationen för ändamålet. En offentlig myndighet ska ansvara för förvaltningen av valfrihetssystemen och samordna mellan e-legitimationsutfärdarna och de förlitande aktörerna. DIGG har fått det ansvaret.

Enligt folkbokföringslagen registreras personer som är stadigvarande bosatta i Sverige med personnummer i folkbokföringsregistret. Personer som har återkommande ärenden med svenska myndigheter registreras med samordningsnummer i samma register. Folkbokföringsregistret används som grund för registrering och utfärdande av medel för elektronisk identifiering. Mer information om det svenska folkbokföringsregistret finns på Skatteverkets webbplats.

3.2 Avtalsstruktur

En e-legitimationsutfärdare får ingå avtal med DIGG om tillhandahållande av e-legitimationstjänster inom ramen för det svenska eID-systemet. Både privata och

offentliga organ som utfärdar e-legitimation är välkomna att ansöka som leverantörer. De kontraktsenliga kraven publiceras på DIGG: s webbplats[11].

Innan en e-legitimationsutfärdare erbjuds att ingå ett avtal med DIGG, måste eID-utfärdaren i vissa fall tecknat licensavtalet för kvalitetsmärket. Detta licensavtal och dess bilagor kräver att utfärdaren följer tillitsramverket och rapporterar incidenter till DIGG, etc. Det ger också rätt att använda kvalitetsmärket i förhållande till produkter och marknadskommunikation. Kvalitetsmärket beskrivs närmare i avsnitt 3.2.

Licensavtalet är nödvändigt för att en utfärdare ska omfattas av den anmälda e-legitimationssystemet i enlighet med eIDAS-förordningen. DIGG har rätt att säga upp avtal om eID-utfärdaren inte uppfyller alla krav.

3.3 Granskning och kontroll

Som en del av ansvaret för att förvalta infrastrukturen för elektronisk identifiering och genom avtal med e-legitimationsutfärdare granskar och godkänner DIGG utfärdare enligt Tillitsramverket för Svensk e-legitimation och övriga avtalskrav som nämns i 2.2. Granskningsprocessen och löpande kontroll beskrivs närmare i avsnitt 3.3.

3.4 Teknisk infrastruktur

Den tekniska infrastrukturen består av den nationella identitetsfederationen Sweden Connect, som kopplar e-legitimationsutfärdare till förlitande aktörer med e-tjänster. Sweden Connect inkluderar även den svenska eIDAS-noden, som i sin tur består av en central eIDAS Connector kopplad till utländska e-legitimationer och Sveriges eIDAS Proxy Service kopplad till svenska e-legitimationer. En mer detaljerad beskrivning av Sweden Connect finns i kapitel 5.

[11] HTTPS://www.digg.se

4 Det svenska regelverket

I Tillitsramverket för Svensk e-legitimation fastställs en gemensam uppsättning krav för utfärdare av svenska e-legitimationer. Kraven bygger på internationella standarder[12] samt erkända och etablerade principer.

Kraven är indelade i tre olika klasser, s.k. tillitsnivåer, som motsvarar utfärdarens olika tekniska och operativa kontroller och förtroende för att identiteten hos en person som tilldelas en elektronisk identifiering är den som gäller för den påstådda identiteten.

Kraven är uppbyggda enligt en allmänt accepterad modell för elektronisk identifiering, där hanteringen av e-legitimation är indelad i tre olika faser:

1. ansökan,
2. utgivning och
3. autentisering.

I var och en av dessa faser krävs vissa säkerhetsåtgärder och säkerhetskontroller för att upprätthålla den angivna säkerhetsnivån. Dessutom finns krav som riktar sig till utfärdarnas ledning och organisation.

4.1 Tillitsnivåer

Tillitsnivåerna grundar sig på en konsekvensanalysbaserad modell för riskbedömning, som definierar sex olika riskområden. Modellens konsekvenser är uppdelade i *begränsade, måttliga, betydande* och *höga.*

Det är den förlitande aktören som väljer den lägsta tillitsnivå som krävs för att få tillgång till deras tjänster. Detta görs i förhållande till de potentiella konsekvenserna i verksamheten av en felaktig identifiering av en användare och med hänsyn till eventuella författningskrav.

[12] Däribland ISO 27001 och ISO 29115 (delar)

Riskområde	Tillitsnivå 1	Tillitsnivå 2	Tillitsnivå 3	Tillitsnivå 4
Olägenhet, oro eller ryktesskada	Begränsad	Måttlig	Betydande	Allvarlig
Finansiell skada eller skadeståndsansvar	Begränsad	Måttlig	Betydande	Allvarlig
Röjande av känsliga uppgifter till obehöriga	*Ska inte användas*	Måttlig	Betydande	Allvarlig
Brottsyttringar	*Ska inte användas*	Begränsad	Betydande	Allvarlig
Skada på verksamhet eller allmänintresse	*Ska inte användas*	Begränsad	Måttlig	Allvarlig
Personsäkerhet	*Ska inte användas*	*Ska inte användas*	Måttlig	Betydande

Tabellen ovan kan fungera som vägledning. Där anges ett antal riskområden (raderna) med en rekommenderad tillitsnivå (kolumnerna) att använda beroende på hur risknivån bedöms (redovisas med begreppen begränsad, måttlig, betydande, allvarlig och ska inte användas) inom det området i den verksamhet som avses. Om konsekvenserna är allvarliga bör således krav på tillitsnivå 4 ställas.

Om en felaktig identifiering kan leda till negativa konsekvenser på flera områden är det den allvarligaste konsekvensen som avgör vilken säkerhetsnivå som krävs. Förekomsten av flera risker inom olika områden anses i allmänhet inte vara kumulativ.

Motsvarande modell definieras av Myndigheten för samhällsskydd och beredskap (MSB) i publikationen Modell för klassificering av information[13], men denna

[13] HTTPS: //rib.msb.se/filer/pdf/25602.pdf

modell har endast tre nivåer och inkluderar inte påverkansnivån för begränsad. Tillitsramverket för Svensk e-legitimation inkluderar begränsad för att vara helt i linje med den internationella definitionen av säkerhetsnivåer[14]. Av samma skäl finns det en tillitsnivå 1 med i bilden, som motsvarar en elektronisk identifiering där användarens verkliga identitet inte verifieras. Tillitsnivå 1 är för närvarande inte inkluderad i Tillitsramverket för Svensk e-legitimation.

För närvarande är det tillitsnivå 3 (av 2 – 4) som kravställs av många förlitande aktörer. Avsikten med tillitsnivå 3 är att det ska ge samma säkerhetsnivå som en traditionell fullvärdig id-handling, men samtidigt göra det möjligt att utfärda och tillhandahålla en sådan e-legitimation på distans på ett så effektivt sätt som möjligt.

För tjänster med lägre risk, kan tillitsnivå 2 användas. Den försäkran som tillhandahålls motsvarar i stort sett en engångskod som förmedlas via vanlig post. En s.k. tvåfaktors autentiseringsmetod krävs på nivå 2 i Tillitsramverket för Svensk e-legitimation, men beviskraven är mindre stränga.

Tillitsnivå 4 är avsedd att tillgodose de högsta säkerhetsbehoven. För denna nivå måste utfärdande, leverans och förnyelse ske personligen, och det finns särskilt stränga krav på utfärdarens riskhantering och interna kontroller. För nivå 4 är endast hårdvarubärare tillåtna.

De svenska tillitsnivåerna 2, 3 och 4 uppfyller var och en kraven i eIDAS tillitsnivåer låg (low), väsentlig (substantial) och hög (high).

4.1.1 Jämförelse mellan tillitsnivåer

Regelverken mellan eIDAS tillitsnivåer och de svenska tillitsnivåerna uppvisar stora likheter:

- Båda regelverken är formulerade på samma nivå och har samma omfattning.
- Båda regelverken definierar tre tillitsnivåer.
- Sverige har varit delaktig i utformningen av eIDAS genomförandeförordning 2015/1502, därför bär formuleringarna i de båda regelverken påtagliga likheter.

[14] SO/IEC 29116, avsnitt 6.

- Därtill innehåller 2015/1502 ytterligare regler som tar hänsyn till andra medlemsländers olika seder och bruk.

Det som skiljer dem åt är framförallt:

- På den lägsta nivån (2) gjorde vi i Sverige en skärpning i Tillitsramverket för Svensk e-legitimation, som innebär att denna svarar mot datainspektionens krav på "stark autentisering". Detta i syfte att göra nivån mer användbar, t.ex. inom skolväsendet.

- På den högsta nivån (4) krävs i Sverige personligt besök för att skaffa och förnya en e-legitimation, och detta behöver ske minst vart 5:e år. I genomförandeförordningen saknas bestämmelser om att e-legitimationens giltighet ska begränsas i tid, och utfärdande kan ske på distans (i princip på samma premisser som vår nivå 3, exempelvis genom internetbank). Man kan inom eIDAS nivå ”hög” också förnya sin e-legitimation på distans med en annan e-legitimation anmäld på nivån 'hög', vilket inte är tillåtet på svenska nivå 4.

4.2 Det svenska kvalitetsmärket

Det svenska kvalitetsmärket ”Svensk e-legitimation” visar en e-legitimation är godkänd i enlighet med Tillitsramverket för Svensk e-legitimation. Det utfärdas av DIGG till e-legitimationsutfärdare som har genomgått och passerat en granskningsprocess kopplad till tillitsramverket. Endast eID-utfärdare som uppfyller kraven i tillitsramverket, är godkända av DIGG och tecknar tillhörande licensavtal med DIGG, får använda kvalitetsmärket i sina e-legitimationer och för marknadskommunikation.

Det är upp till varje offentlig myndighet att kräva att en e-legitimation ska bära kvalitetsmärket. Det är också frivilligt för e-legitimationsutfärdare att ansöka om kvalitetsmärket. Kvalitetsmärket har med tiden blivit mycket respekterat, vilket innebär att alla

ledande e-legitimationsutfärdare har genomgått granskningen och är angelägna om att behålla kvalitetsmärket.

Kvalitetsmärket är i praktiken en förutsättning för e-legitimationsutfärdare ska kunna tas med i svensk anmälan enligt eIDAS-förordningen.

4.3 Granskningsprocessen

DIGG granskar utfärdare av e-legitimationer. Myndigheten ser till att endast utfärdare med godkänd granskning, och ingått ett avtal med myndigheten och passerat lämpliga tekniska tester, anmäls och därmed får användas i gränsöverskridande sammanhang.

I denna egenskap har myndigheten följande mandat:

- Att genomföra initiala granskningar för att bedöma efterlevnaden av tillitsramverket och bedömning av överensstämmelse enligt tekniskt ramverk för Sweden Connect.
- Kontinuerligt övervaka utfärdares överensstämmelse med ramverken.
- Besluta om deltagarnas inträde i avtal om kvalitetsmärket, e-legitimering och identitetsfederationen.
- Vara kontaktpunkt för incidenter kopplade till e-legitimering
- Vidta åtgärder i händelse av bristande överensstämmelse med förvaltningsramen och den tekniska ramen.

4.3.1 Tillämpning och revision

En utfärdare[15] kan ansöka om det svenska kvalitetsmärket genom att skicka ett ansökningsformulär till DIGG, som finns på DIGG:s webbplats[16]. Ansökningsformulärets struktur liknar en certifieringspraxis (CPS)[17] och kräver att utfärdare tillhandahåller utförliga beskrivningar av sin praxis och de tjänster som tillhandahålls av dem. Den organisation som ansöker om kvalitetsmärket måste också acceptera de villkor som anges i licensavtalet.

[15] Eller leverantör som vill få sin intygsfunktion godkänd (kvalitetsmärke inte aktuellt)
[16] HTTPS://www.digg.se/
[17] Enligt definitionen i RFC 3647, https://tools.ietf.org/html/rfc3647

Figur 3: Ansökningsprocessen

Granskningsprocessen leds av en samordnare från DIGG, som bildar en granskningsgrupp när ansökan har mottagits. Granskningsgruppen genomför en inledande granskning av ansökans efterlevnad av tillitsramverket. Efter den inledande granskningen inleder granskningsgruppen sedan en fördjupad granskning av eID-utfärdaren på grundval av det ursprungliga resultatet. Den fördjupade granskningen omfattar ett besök på plats och stickprov för att samla in objektiva bevis på efterlevnad inom viktiga kontrollområden.

Granskningsgruppen bedömer om utfärdaren uppfyller kraven i tillitsramverket eller inte. Vid avvikelser bedömer granskningsgruppen om utfärdaren kommer att kunna rätta till avvikelserna inom en rimlig tidsram. I så fall får utfärdaren en tidsfrist för rättelse.

När granskningen är slutförd presenterar granskningsgruppen resultaten för en referensgrupp som består av medlemmar från andra offentliga myndigheter. Gruppen ges möjlighet att lämna synpunkter och begära förtydliganden av resultatet av granskningen. Referensgruppens roll är stödjande och syftar till att främja öppenhet i granskningsprocessen.

Granskningsgruppen skriver sedan ett slutligt yttrande. I händelse av ett sannolikt avslag ges utfärdaren möjlighet att dra tillbaka sin ansökan. I så fall avslutas granskningen och inga ytterligare åtgärder krävs av utfärdaren eller från DIGG.

Det slutliga yttrandet läggs sedan fram för generaldirektören för DIGG, som har befogenhet att besluta om

- Godkännande
- Godkännande med reservation
- Avslag

Vid godkännande inbjuds utfärdaren att underteckna licensavtalet, vilket ger utfärdaren rätten att använda kvalitetsmärket i förhållande till sina produkter och i sin marknadskommunikation.

Generaldirektören får besluta om godkännande med reservation, vilket innebär att utfärdarens ansökan innehåller brister som kräver ytterligare prövning, men som inte medför någon ökad risk för de förlitande parterna och därför inte utgör ett hinder för godkännande. Ett godkännande med en reservation måste alltid innehålla en maximal tidsfrist, t.ex. 12 månader. När tiden har förflutit görs ytterligare en översyn för att kontrollera de kvarstående frågorna i reservationen.

4.3.2 Kontinuerlig övervakning

Efter godkännande av en utfärdare och tecknande av licensavtalet ska utfärdaren lämna in sin årliga internrevisionsrapport till DIGG inom en angiven tidsram efter det att internrevisionen avslutats, i enlighet med licensavtalet. Internrevisionsrapporten granskas av DIGG. Om det finns skäl att ifrågasätta resultaten av revisionen eller om kraven inte efterlevs får DIGG inleda en inspektion. En inspektion kan också inledas baserat på en ändringsbegäran från utfärdaren, eller i händelse av en incident. Incidentrapportering är en obligatorisk skyldighet enligt licensavtalet och i eIDAS-fallet även enligt lag.

Figur 4: Kontinuerlig övervakningsprocess

Inspektionsprocessen följer grovt den tidigare ingående granskningsprocessen, med stickprov och insamling av objektiva bevis på överensstämmelse inom ramen för inspektionen. Vid avvikelser bedömer granskningsgruppen om den utgör en omedelbart ökad risk. Om så är fallet kan granskningssamordnaren kräva att utfärdaren omedelbart avbryter tjänsten. Granskningsgruppen bedömer också om utfärdaren kommer att kunna rätta till avvikelserna inom rimlig tid. I så fall får utfärdare en tidsfrist för rättelse.

Efter en presentation för referensgruppen i enlighet med det granskningsförfarande som beskrivs i 3.2.1 överlämnas det slutliga yttrandet till generaldirektören för DIGG, som har befogenhet att besluta om

- Fortsatt godkännande
- Fortsatt godkännande med reservation
- Uppsägning av avtal

4.4 Förvaltning av tillitsramverket

DIGG förvaltar Tillitsramverket för Svensk e-legitimation och beslutar om eventuella ändringar eller tillägg. Ändringar eller tillägg ska meddelas berörda intressenter och får verkan senast 180 dagar efter offentliggörandet, såvida inte särskilda omständigheter föreligger, såsom allvarliga säkerhetshot eller lagändringar, eller om ändringen eller ändringen endast avser frågor av uppenbar mindre betydelse, såsom förtydliganden av en bestämmelse.

Innan beslut fattas om en ändring eller tillägg är myndigheten också skyldig att samråda med intressenterna. DIGG beslutar om formerna för sådana samråd, men kan besluta att verkställa sitt beslut innan DIGG har fullgjort sin skyldighet att samråda om särskilda omständigheter, t.ex. om det föreligger ett överhängande hot.

5 Skaffa en svensk e-legitimation

DIGG tillhandahåller information till privatpersoner om möjligheten att skaffa e-legitimation och vad som är viktigt att tänka på. Informationen finns på DIGG:s webbplats elegitimation.se. När det i stället är en medarbetare som skaffar e-legitimation är det arbetsgivarens anvisningar, i kombination med e-legitimationsutfärdarens process, som blir aktuella att följa.

En kvalitetsmärkt svensk e-legitimation får endast utfärdas på begäran av den sökande, men ansökningsprocessen kan på annat sätt variera beroende på de förfaranden som tillämpas av utfärdaren av e-legitimationen. I grund och botten ska ansökan om en kvalitetsmärkt e-legitimation kopplas till ett personnummer eller ett samordningsnummer som bygger på styrkt identitet. Detta innebär att den första registreringen i folkbokföringen och tilldelningen av ett personnummer (eller ett samordningsnummer) måste ha skett innan e-legitimationen kan utfärdas. Detta är också en förutsättning för att den sökande ska kunna styrka sin identitet med hjälp av en fullgod id-handling.

5.1 Sju steg för att verifiera en identitet

De svenska offentliga och privata sektorerna har enats om ett gemensamt sjustegsförfarande[18], som ursprungligen utvecklats av Svenska Bankföreningen, för att verifiera en fysisk persons identitet i de fall där kontrollen av deras identitet är nödvändig. Dessa sju steg tillämpas för utfärdande av identitetshandlingar, men också för alla andra betydande ekonomiska eller juridiska transaktioner. Det kan till exempel gälla ansökan om bolån. Organisationer som tillämpar de sju stegen stödjer rutinerna på en handbok med detaljerade instruktioner om identitetskontroll. Det finns även tillgång till en onlineutbildning, en utbildningsplan och läromedel.

[18] HTTPS://www.desjustegen.se/information/handboken/

5.2 Tillåtna id-handlingar

Tillåtna id-handlingar är de som allmänt erkända nationellt. De består av ett dokument med foto, personnummer (eller samordningsnummer), fullständigt namn, underskrift av personen och kan gälla upp till 10 år.

Aktuella id-dokument är:

- Svenskt nationellt ID-kort,
- Svenskt pass,
- Svenskt körkort,
- Skatteverkets id-kort, och
- Id-kort som utfärdats av arbetsgivare eller banker och som har certifierats enligt SIS: s säkerhetsstandarder[19] med SIS-märkning om överensstämmelse.

Utländska id-handlingar räknas inte som tillräckliga id-handlingar eftersom de inte innehåller svenskt personnummer eller samordningsnummer

(eller samordningsnummer), fullständigt namn, underskrift av personen och kan gälla upp till 10 år.

5.3 Om sökanden inte har en tillräcklig id-handling

Som en allmän regel måste den som ansöker om e-legitimation först skaffa en tillräcklig id-handling innan han eller hon kan ansöka om e-legitimation. Undantaget från denna regel, om det är tillräcklig id-handling, innehåller också en e-legitimation, en situation som för närvarande endast gäller Skatteverkets id-kort.

För att ansöka om en tillräcklig id-handling utan att ha en sådan handling måste ett godkänt intyg intyga sökandens identitet. En intygsutfärdare måste vara:

- make, maka, registrerad partner eller sambo
- barn eller barnbarn över 18 år
- förälder eller vårdnadshavare som är registrerad med föräldrarättigheter

[19] http://www.sis.se/produkter/foretagsorganisation/finans-bank-valuta-forsakring/ss6143142015
https://www.sis.se/produkter/foretagsorganisation/finans-bank-valuta-forsakring/ss6143312011

- syskon över 18 år
- mor- och farföräldrar
- offentligt anställd som har ett yrkesmässigt förhållande till sökanden, en formellt utsedd förvaltare eller en formellt utsedd familjehemsförälder
- företrädare för en nuvarande arbetsgivare, där anställningen har pågått i minst ett år.

Intygsutfärdaren ska i samtliga fall

- vara över 18 år gammal,
- närvara personligen tillsammans med den sökande,
- känna sökanden väl och bevisa relationen,
- visa lämplig ID-handling och
- Skriv under ett intyg som bekräftar den sökandes korrekta identitetsuppgifter.

Sambandet kommer att kontrolleras av e-legitimationsutfärdaren genom att använda befolkningsregistret eller skattehandlingarna för att bekräfta att den sökande har en relation till den sökande.

6 Sweden Connect är en nationell identitetsfederation

Sweden Connect är den nationella identitetsfederationen, som bygger på de ramverk som utvecklats av DIGG. Sweden Connects metadataregister innehåller information om parterna som ingår i federationen. Genom metadata får parterna information om andra parters tjänster, inklusive den information som krävs för säker leverans av identitetsintyg. Varje parts metadata förvaltas av parten själv och ska uppfylla det tekniska ramverket för Sweden Connect m.m. Kvalitetsmärkta e-legitimationsutfärdare som ingår e-legitimeringsavtal med DIGG och uppfyller kraven i det tekniska ramverket får delta som Identity Providers (IdPs) i federationen. Dessutom får förlitande aktörer[20] och tillhandahållare av attribut[21] registrera metadata om IdP:er, som kategoriseras efter om de har tillitsgodkänts av DIGG eller inte.

I Sweden Connect deltar eIDAS-noden för Sverige. Den består av den centrala eIDAS Connectorn som intygsfunktion (IdP) för utländska e-legitimationer. eIDAS-noden består även av Sveriges eIDAS Proxy Service som agerar förlitande aktör (SP) i Sweden Connect mot anmälda svenska e-legitimationer, för vidarebefordran av identitetsintyg till utländska förlitande aktörer.

Utdrag från identitetsfederationens mest centrala del, metadataregistret, stämplas elektroniskt av DIGG (federationsoperatören) så att alla parter kan lita på innehållet. Metadatafilen innehåller information om alla deltagare i federationen, inklusive information om från de certifikat som krävs för säker kommunikation och informationsutbyte mellan tjänster. Metadata innehåller också annan viktig information för hantering av identitetsintyg, t.ex. tekniska adresser, information om tillitsnivåer, tjänstekategorier och information tänkt att visas i användargränssnitt. Eftersom infrastrukturen är baserad på ett centralt metadataregister är det nödvändigt att registret uppdateras kontinuerligt och att

[20] Baserat på anslutningsavtalet för förlitande aktörer till Sweden Connect
[21] När e-legitimeringsavtalen kopplade till eID för medarbetare finns framme

federationens deltagare alltid använder den senaste versionen av uppgifterna. Samtidigt är det viktigt att parterna använder sin lokala kopia, eftersom de behöver kunna klara sig utan tillgång till det centrala metadataregistret i några dagar.

Eftersom metadatafilen är stämplad elektroniskt av DIGG är det tillräckligt för deltagarna för att kunna verifiera en motpart genom den öppna nyckel som anges i certifikatet i metadata. Certifikatet används därför endast som behållare för den allmänna nyckeln.

6.1 Tekniskt ramverk

Tekniskt ramverk[22] för Sweden Connect är utvecklat för att stödja en nationell identitetsfederation baserad på den internationella standarden SAML 2.0 (i framtiden även OpenID Connect). Inom den nationella federationen tar organisationer med e-tjänster rollen som förlitande aktörer (SAML 2.0 SP), och e-legitimationsutfärdare m.fl. som utfärdar identitetsintyg tar rollen som leverantörer av identitetsintyg (IdP). De förlitande aktörerna får därmed identitetsintyg i ett standardiserat format från sina identitetsleverantörer i federationen.[23]

6.2 Inträde in och utträde ur identitetsfederationen

För att kunna delta i den nationella federationen behöver parterna skriva under ett avtal med DIGG där bland annat Tekniskt ramverk för Sweden Connect är avtalsbilaga. För identitetsintygsleverantörer gör DIGG även en överensstämmelsebedömning för att säkerställa att identitetsleverantören följer specifikationerna i det svenska eID tekniska ramverket. Huvudsyftena med dessa bedömningar är att säkerställa interoperabilitet och upptäcka eventuella kompatibilitetsproblem. Både intygsleverantörer och förlitande aktörer med e-tjänster kan testa sin funktion, sitt metadata och få support av DIGG.

Innan metadata registreras i Sweden Connects produktionsmiljö granskar DIGG om metadatat uppfyller kraven i tekniskt ramverk och det avgörs om

[22] HTTPS://www.docs.swedenconnect.se/technical-framework/latest/00_-_Swedish_eID_Framework_-_Introduction.html

[23] HTTPS://docs.swedenconnect.se/technical-framework/

intygsfunktionen är tillitsgranskad, eller inte. Före registrering behöver deltagaren även testa metadata i Sweden Connects QA-miljö.

Enligt avtal kan DIGG stänga av deltagare från Sweden Connect om en allvarlig händelse inträffar. Avtalet kan också sägas upp och då deltagaren stängs då av permanent.

Avtals- och metadatahanteringen är idag manuell. Det innebär att den dels är ineffektiv, dels kan innehålla kvalitetsbrister och att vi riskerar sämre förtroende från externa parter. Därför föreslår vi utveckling av självservice för såväl avtalshanteringen som metadatahanteringen senast 2022.

6.3 eIDAS-noden

Sveriges eIDAS Proxy Service deltar som medlem i Sweden Connect. Svenska eIDAS Proxy Service fungerar som en förlitande part, och konverterar identitetsintyg från anmälda svenska e-legitimationsutfärdares intygsfunktioner (IdP:er). De svenska eID-utfärdarna följer Tekniskt ramverk för Sweden Conenct och den svenska eIDAS-noden omvandlar identitetsintygen enligt eIDAS interoperabilitetsspecifikationer och riktar dem till den eIDAS Connector i utlandet som begärde identitetsintyget från Sverige.

7 Historisk beskrivning

I Sverige är inte invånarna enligt lag skyldiga att bära med sig id-handlingar. Detta har medfört att de offentliga myndigheterna historiskt sett inte, utöver de svenska passen till svenska medborgare, har varit ansvariga för att utfärda identitetshandlingar till personer som är bosatta i landet. Samtidigt hade bankerna ett starkt intresse av att deras kunder hade id-handlingar och utfärdade därför id-kort till sina kunder.

Det svenska körkortet har i många fall accepterats som id-handling och till följd av det europeiska rörlighetsdirektivet 2005 införde Sverige de nationella id-korten som utfärdas av Polismyndigheten.

År 2009 började Skatteverket utfärda identitetshandlingar för att fylla luckan för invånare som varken är svenska medborgare (och därför inte kan få det nationella ID-kortet) eller en kund hos en svensk bank, en inte helt ovanlig situation för en person som flyttar till Sverige.

Genom exempelvis bankdosor kunde bankerna redan 2002 identifiera 2,7 miljoner svenskar elektroniskt på ett tillförlitligt sätt.

7.1 Utvecklingen av det svenska systemet för e-legitimering

Sedan början av 2000-talet har offentliga myndigheter upphandlat elektronisk identifiering från privata leverantörer, delvis baserat på att bankerna var framgångsrika med att identifiera sina kunder elektroniskt. Avsikten med att gå upphandlingsvägen var att täcka in de e-legitimationer som användare kunde skaffa och samtidigt driva på innovativ utveckling, som privat sektor ansågs mest lämpad för.

För att svara på statens upphandling av elektronisk identifiering i offentliga digitala tjänster, och för att underlätta den tekniska integrationen och kunna identifiera medborgarna på ett enhetligt sätt, lanserades den gemensamma bankinfrastrukturen BankID år 2003. I statens ramavtal levererade några banker BankID-transaktioner och Telia och Nordea levererade transaktioner kopplade till sina egna lösningar.

På grund av ändringar i lagstiftningen om offentlig upphandling 2008 var det inte längre möjligt att upphandla flera leverantörer för samma typ av tjänster (BankID-transaktioner). Vid denna tidpunkt hade myndigheterna också konstaterat det

kritiska beroendet av BankID för utvecklingen av den digitala förvaltningen, på grund av dess dominerande marknadsställning. De tekniska lösningar som då tillhandahölls var dessutom kostsamma att ansluta till och underhålla.

Det svenska eID-systemet har från 2009 och framåt formats av flera olika offentliga utredningar. E-delegationens första delbetänkande (SOU 2009:86) föreslog införande av valfrihetssystem för elektronisk identifiering, där användarens val av e-legitimation skulle styra vilken leverantör som skulle få betalt. Detta skulle främja mångfald genom att göra det möjligt för nya leverantörer att tillhandahålla tjänster som motsvarar BankID på samma villkor.

I den efterföljande offentliga utredningen (SOU 2010:104) lades grunden till en ny myndighet för samordning av den offentliga sektorns användning av e-legitimation, som fick i uppgift att tillhandahålla valfrihetssystem för elektronisk identifiering. E-legitimationsnämnden inrättades den 1 januari 2011 och började arbeta med att inrätta ett valfrihetssystem. Denna modell gjorde det möjligt att använda tjänster från olika leverantörer utan att varje offentlig myndighet behövde underteckna nya avtal med varje leverantör eller genomföra nya tekniska integrationer för varje leverantör.

En annan del av valfrihetssystemet innebar enhetliga säkerhetskrav, kallat tillitsramverk, som varje leverantör av eID-tjänster behövde uppfylla för att kunna ingå avtal och tillhandahålla elektronisk identifiering. Efter granskning, godkännande och licensavtalstecknande har e-legitimationsutfärdare rätt att använda kvalitetsmärket Svensk e-legitimation i linje med de genomförda offentliga utredningarna. E-legitimationsnämnden byggde dessutom med en leverantörs hjälp upp metadataregister.

Lagen (2013: 311)[24] om valfrihetssystem i fråga om tjänster för elektronisk identifiering trädde i kraft den 1 juli 2013. År 2014 annonserade E-legitimationsnämnden det första valfrihetssystemet, som erbjöd den infrastruktur som de offentliga utredningarna kommit fram till behövdes för att både myndigheter och e-legitimationsutfärdare skulle kunna tillträda som förlitande

[24] HTTPS: //www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2013311-om-valfrihetssystem-i-fraga-om_sfs-2013-311

aktörer och leverantörer. Några statliga myndigheter tillträdde, men inga leverantörer anslöt sig.

Dessutom var minst tre myndigheter; Försäkringskassan, Arbetsförmedlingen och CSN inte nöjda med säkerhetskraven och de tekniska kraven. Det ledde till att MSB med stöd av FRA och FOI gjorde en säkerhetsgranskning som blev klar våren 2014. Deras rapport innehöll 22 punkter, varav 20 åtgärdades av E-legitimationsnämnden. En av de kvarvarande två handlade om att den tekniska metoden SAML 2.0 inte ger ett fullgott stöd till så kallade native appar[25]. Den sista punkten rörde användbarhetsbrister i den planerade centrala listan över valbara e-legitimationer (anvisningstjänsten). Den centrala anvisningstjänsten lades ned.

Ett kritiskt datum inföll 1 juli 2016, då de förlängda avropsavtalen på det gamla ramavtalet löpte ut. Det blev brådskande att få acceptans för avtalsvillkoren hos BankID och Telia, som vid den tidpunkten var de väletablerade e-legitimationerna på den svenska marknaden. Ett nytt valfrihetssystem togs fram, ”2016 Övergångstjänst”, som både BankID och Telia tillträdde med ett antal offentliga myndigheter som förlitande parter sent under våren 2016. Detta valfrihetssystem hade en begränsad löptid och innehåll dessutom inte villkor som staten långsiktigt var nöjd med, främst andra tekniska metoder än SAML 2.0. E-legitimationsnämnden beslutade i samband med detta om att lägga ned metadataregistret och ta ned annonseringen av det första valfrihetssystemet, eftersom ingen leverantör tillträtt trots att det hade gått några år.

Strax därefter uppstod trots allt en ny aktör på e-legitimationsmarknaden, Freja, och de kunde erbjuda tjänster som passade med statens långsiktigt önskade krav. Därför togs ytterligare ett valfrihetssystem fram, ”2017 E-legitimering”.

Parallellt med detta visade det sig att införandet av ”Foreign eID” (eIDAS-förordningen) i svenska offentliga digitala tjänster skulle underlättas om det fanns en förvaltningsgemensam eIDAS-nod, som i gränssnittet mot de svenska förlitande aktörerna uppträdde i teknisk federation som en intygsfunktion (SAML 2.0-IdP). På samma sätt kunde även svenska myndigheters anslutning till Freja underlättas.

[25] Vilket framöver kan lösas genom att införa OpenID Connect som alternativ metod till SAML 2.0 inom ramen för DIGG:s tekniska ramverk

Därför skapades en ny federation, Sweden Connect, med ett metadataregister, denna gång med stöd av SUNET som driftleverantör. Valet att välja drift hos en statlig myndighet, och utveckla med hjälp av egna expertkonsulter, byggde på bistra erfarenheter från den tidigare upphandlingen av en väletablerad privat leverantör som i praktiken hade svårt att nå säkerhetskraven m.m. i sitt åtagande.

Freja eID Group AB med Freja eID Plus gick med i valfrihetssystem 2017 E-legitimering i augusti 2018, efter att tidigare under året blivit godkända för kvalitetsmärket Svensk e-legitimation. Samma månad inrättades myndigheten för digital förvaltning (DIGG) och E-legitimationsnämndens ansvarsområden överfördes därefter till den nya myndigheten.

Men hur gick det med BankID och Telia? De accepterade inte villkoren i ”2017 E-legitimering” och ”2016 Övergångstjänst” var på väg att löpa ut. Därför togs valfrihetssystem ”2018 E-legitimering” fram, med ungefär samma villkor som i ”2016 Övergångstjänst”. Finansiell ID-teknik BID AB tillträdde ”2018 E-legitimering” avseende BankID, till skillnad från i ”2016 Övergångstjänst” där bankerna var leverantörer och förlitande myndighet fick avgöra vilken bank som skulle få betalt. Varken ”2018 E-legitimering” eller ”2017 E-legitimering” har något slutdatum inbyggt.

Valfrihetssystemen är föreslagna att ersättas av auktorisationssystem under 2022, vilket innebär ett obligatorium för statliga myndigheter att ansluta till.

7.2 eIDAS

EU:s eIDAS-förordning om elektronisk identifiering beslutades 2014. Medlemsstaterna fick i och med det möjlighet att förbereda sig för att anmäla sina e-legitimationer och ta emot identitetsintyg från utländska e-legitimationer, enligt eIDAS-reglerna.

Sverige var mycket aktiva i arbetet med att ta fram utkast till eIDAS tillitsramverk för e-legitimering. Innan beslut gjordes dock en del kompromisser som Sverige och andra länder var tvungna att acceptera, vilket ledde till att skyddet på tillitsnivå ”hög” enligt eIDAS ligger något lägre än tillitsnivå ”4” i Sverige.

Sverige var även aktiva i interoperabilitetsarbetet som föregick beslut om eIDAS interoperabilitetsregler för e-legitimering. Även här blev det inte exakt den

lösning Sverige önskade sig, där en av bristerna är att det saknas ett EU-gemensamt metadataregister. En annan brist har att göra med hur SAML 2.0 implementeras. EU-kommissionen försökte förenkla för länderna genom att ta fram en programvara för eIDAS-noderna, men programvaran har haft sina problem. Dessutom var det viktigt att i möjligaste mån förenkla för alla anslutande svenska förlitande aktörer, däribland myndigheter och kommuner. Sverige (E-legitimationsnämnden) beslutade därför att utveckla egen programvara för den svenska eIDAS-noden, vilket har varit ett lyckosamt beslut så här långt. Den klarar både eIDAS-interoperabilitetskrav åt det internationella hållet och det svenska tekniska ramverket för Sweden Connect mot svenska e-tjänster.

Processen för anmälan av e-legitimationer består av:

1. E-legitimationslandet föranmäler sina e-legitimationer, regelverk och processer.
2. Andra medlemsstater genomför s.k. peer review av föranmälda e-legitimationer. Efter tre frågeomgångar sammanfattas resultatet i en rapport från peer review-länderna. Cooperation Network gör därefter ett ställningstagande.
3. E-legitimationslandet anmäler sina e-legitimationer etc, efter eventuell förbättring för att skapa förtroende och inte gå emot ställningstagandet.
4. EU-kommissionen publicerar anmälda e-legitimationer i EU:s offentliga förteckning.
5. Därefter har de andra länderna tolv månader på sig att erkänna de anmälda e-legitimationerna.

De första bindande datumen för elektronisk identifiering trädde i kraft i september 2018. Senast då skulle varje land a) ha en fungerande eIDAS-nod i produktion och b) alla offentliga e-tjänster med krav på e-legitimation (tillitsnivå ”väsentlig” eller ”hög”) skulle vara anslutna till eIDAS-noden för att erkänna de utländska e-legitimationerna som anmäldes i september 2017, vilket var första möjliga månad för anmälan.

Det första landet som anmälde sina e-legitimationer var Tyskland, som anmälde redan i september 2017. Därmed fanns ingen tvekan om att alla andra länder behövde uppfylla sina skyldigheter. Sedan Tyskland anmälde 2017 har ytterligare elva länder anmält e-legitimationer, varav Storbritannien dessvärre

tog bort sin anmälan med anledning av Brexit. Under våren 2021 har Malta, Frankrike och Sverige föranmält e-legitimationer.

Åter till 2017. Dåvarande E-legitimationsnämnden höll ett stort antal informationsmöten för myndigheter, kommuner och regioner om kraven på offentliga organs erkännande, och om hur anslutning till eIDAS-noden skulle göras. SKR skrev en vägledning för kommuner och regioner. Gotlands kommun och ett antal andra offentliga myndigheter skötte sig utmärkt och var uppkopplade mot eIDAS-noden i tid, i september 2018.
Tyvärr kan vi dock under våren 2021 konstatera[26] att ett stort antal offentliga organ ännu inte är anslutna till eIDAS-noden. Den 1 juni träder svenska lag- och förordningsregler i kraft som förtydligar krav på att ansluta sig till DIGG:s eIDAS-nod, med undantag för Säkerhetspolisen och myndigheter under Försvarsdepartementet.

Dessutom förordnar regeringen att privata aktörer ska få möjlighet att ansluta sig till DIGG:s eIDAS-nod för uppkoppling mot utländska e-legitimationer. DIGG får ta ut avgifter från de som frivilligt ansluter sig.

[26] Finns beskrivet i regeringens proposition (2020/21:81) om kompletterande bestämmelser till eIDAS-förordningen

8 Utmaningar och förslag till åtgärd

Det svenska e-legitimationssystemet fungerar i stort relativt väl och Sverige är ett av länderna i världen med störst användning av e-legitimationer. Sverige har dock en del återstående utmaningar, inte minst har pandemin visat behovet av att alla har möjlighet att identifiera sig digitalt. Det finns ett antal föreslagna och påbörjade initiativ, dessa lyfter vi inte upp nedan.

Utmaningarna består dels av brist i tillgången till e-legitimationer för alla, dels av att digitala tjänster inte tillåter alla e-legitimationer som når upp till begärd tillitsnivå. Det pågår dessutom en snabb internationell utveckling inom området och frågan om gränsöverskridande e-legitimering ligger högt på den politiska agendan inom EU i och med den pågående revideringen av eIDAS-förordningen.

8.1 Utanförskap – nationellt

Inom Sverige består utanförskapet av att alla inte kan skaffa eller nyttja en e-legitimation. Utanförskapet gäller olika grupper; äldre, personer med funktionsnedsättning, de utan personnummer osv. Vi har fortfarande för få e-legitimationer på marknaden, sett till det totala anpassningsbehovet för olika grupper.

Vi föreslår följande åtgärder för att minska utanförskapet.

8.1.1 Åtgärd 1: En statligt utfärdad e-legitimation till alla medborgare och folkbokförda ett brådskande behov

DIGG anser att man bör genomföra Id-kortsutredningen (SOU 2019:14) förslag om en statlig e-legitimation utfärdad av Polisen eller en annan statlig myndighet. Ett alternativ till detta, om genomförandet drar ut på tiden, är regeringen överväger att ge Försäkringskassan i uppdrag att utfärda EFOS till folkbokförda på Skatteverkets id-kort.

Sverige är ett av få länder inom EU som inte har en statlig e-legitimation. Även de privata svenska e-legitimationsutfärdarna ställer sig positiva till att staten skulle stå för en e-legitimation på den högsta tillitsnivån.

En statlig e-legitimation skulle ge flera positiva effekter:

- Det saknas idag i Sverige en e-legitimation på den högsta tillitsnivån riktad till allmänheten som även finns med i statens e-legitimeringsavtal eller kan användas utomlands i enlighet med eIDAS-förordningen. I flera av de pågående internationella initiativen inom EU förutsätts att användaren har en e-legitimation som är anmäld på den högsta tillitsnivå. Svenska medborgare och företag riskerar därför att ställas utanför de nya möjligheterna. Sverige riskerar att inte leva upp till den föreslagna ändringen av eIDAS-förordningen där Sverige inom tolv månader efter ikraftträdande ska erbjuda svenskar digitala plånböcker (wallets) under en e-legitimation på den högsta tillitsnivån. DIGG bedömer att behovet hittills inte har tillgodosetts av marknadens aktörer och ser inte heller att det kommer att ske i närtid. EFOS på kort är föranmäld enligt eIDAS-förordningen på den högsta tillitsnivån och har klarat de andra eIDAS-ländernas granskning väl.

- En statlig e-legitimation möjliggör id-växling från den säkra statliga e-legitimationen till andra e-legitimationer. Just denna grundidentifiering som staten därmed skulle utföra är idag det största hindret för nya e-legitimationsutfärdare att ta sig in på marknaden, då den kräver möjlighet att på plats kontrollera identiteten på den sökande. Även befintliga e-legitimationsutfärdare skulle över tid ha nytta av detta.

- Identifiering och legitimationskontroll av den sökande inför utfärdande av en e-legitimation på den högsta tillitsnivån är svårt, vilket motiverar att uppgiften utförs av Polisen, alternativt Skatteverkets id-kortverksamhet, som har den kompetens som krävs.

- En statlig e-legitimation enligt Id-kortsutredningens förslag blir genom utlandsbeskickningar tillgänglig för även utlandsbosatta svenskar med personnummer (inte bara folkbokförda i Sverige).

- Samhällets robusthet förbättras om den statliga e-legitimationens tekniska utformning är helt skild från BankID, Freja och andra e-legitimationer.

8.1.2 Åtgärd 2: Alla digitala tjänster ska acceptera alla e-legitimationer med tillräcklig tillitsnivå

DIGG anser att man bör lagstifta om att alla offentliga myndigheter ska ansluta till auktorisationssystem för elektronisk identifiering och därmed godta alla av DIGG godkända e-legitimationer som finns med under förutsättning att e-legitimationen i det aktuella fallet når erforderlig tillitsnivå.

Att utöka kretsen som träffas av obligatoriet till även kommuner och regioner skulle öka efterfrågan på nya e-legitimationer. Den uppfattas idag av e-legitimationsmarknaden som för liten då digitala tjänster bara godtar de etablerade e-legitimationerna som det stora flertalet använder. Detta gör det svårt för nya e-legitimationsutfärdare att få lönsamhet i att utveckla nya e-legitimationslösningar och få dem granskade och godkända av DIGG. Här är auktorisationssystem med obligatorisk anslutning av statliga myndigheter som förlitande parter ett steg i rätt riktning, men ytterligare åtgärder krävs som ökar incitamenten för kommunala och regionala digitala tjänster att välkomna alla godkända e-legitimationer som DIGG har avtal med.

Detta skulle även ligga i linje med de krav som ställs på Sverige genom eIDAS-förordningen.

8.1.3 Åtgärd 3: Utöka DIGG:s uppdrag till förlitande aktörer i privat sektor

DIGG anser att myndigheten ska få i uppdrag att ge stöd till offentliga aktörer, inte endast offentlig förvaltning, så att privata utförare av välfärd också ingår i uppdraget. I ett kommande steg bör möjligheten för alla intresserade privata förlitande svenska aktörer att ansluta till DIGG:s e-legitimeringsavtal, särskilt till DIGG:s ersättningslösa avtal, utredas.

DIGG har för närvarande skyldighet att ansluta privata förlitande parter till eIDAS-noden och kommer därför att ha en naturlig avtalskontakt med dessa aktörer. På sikt kan rätten att ta ut ytterligare avgifter utredas, men en utökning av DIGG:s instruktion skulle kunna vara ett första steg som möjliggör detta, särskilt till DIGG:s ersättningslösa avtal kopplat till e-tjänstelegitimationer.

Ett exempel på behov är vikten av att verka för att en offentlig e-tjänstelegitimation ska bli möjlig att använda hos apotek, friskolor och privata utförare av vård och omsorg.

8.1.4 Åtgärd 4: Lagstifta om tillgång till digitala tjänster

DIGG anser att man bör lagstifta om att offentliga e-tjänsteägare inte i onödan får begränsa tillgången till e-tjänster.

E-tjänster som inte hanterar sekretessbelagd information eller känsliga personuppgifter skulle normalt sett kunna öppnas upp för e-legitimationer på lägre tillitsnivå, exempelvis tillitsnivå 2 enligt Tillitsramverket för Svensk e-legitimation. Idag krävs i vissa fall för hög tillitsnivå i e-tjänster, vilket stänger möjligheten för grupper att använda en e-legitimation på lägre tillitsnivå för enklare tjänster, t.ex. för att köpa bussbiljetter. Detta skapar ett onödigt utanförskap.

I EU-förordningen om en gemensam digital ingång till Europa (SDG-förordningen) ställs krav på att EU-medborgare ska kunna få samma tillgång till e-tjänster som de svenska medborgarna har. Det innebär att myndigheter, kommuner och regioner behöver öppna upp för andra identitetsbegrepp. E-tjänster ska därmed tillåta andra identitetsbegrepp än personnummer, i den mån det är relevant. Det svenska e-legitimationssystemet breddas till fler personidentitetsbegrepp och idag kan man få en e-legitimation med ett styrkt svenskt samordningsnummer enligt det svenska tillitsramverket under förutsättning av det finns e-legitimationsutfärdare som medger det, med tillräckligt säkra rutiner.

Därutöver är det viktigt att digitala tjänster anpassas till det i SOU 2021:57 Om folkbokföring, samordningsnummer och identitetsnummer föreslagna identitetsnumret i den takt förslaget realiseras.

Slutligen bör enligt betänkandet Användning av e-legitimation i tjänsten i den offentliga förvaltningen (SOU 2021:62) en unik pseudonym som arbetsgivaren tillhandahåller användas vid inloggning i tjänsten bland annat för att värna om medarbetares personliga integritet.

8.1.5 Åtgärd 5: Utred begränsningar för anskaffning och användning av e-legitimationer

DIGG anser att regeringen bör tillsätta en utredning som föreslår sätt att hantera de restriktioner ett förvaltarskap medför med avseende på e-legitimationer.

Det saknas möjlighet att hindra personer som måste företrädas av en förvaltare från att via en e-legitimation utnyttja digitala tjänster personen ej är behörig att

använda. Frågan har fallit mellan stolarna i offentliga utredningar och därmed saknas idag förslag till åtgärder. Utredningen skulle även kunna omfatta förslag till åtgärder som förhindrar personer som är misstänkta eller dömda för bedrägerier att fortsätta använda e-legitimationer i brottsligt syfte. Ju fler som får tillgång till e-legitimation, desto viktigare är denna fråga.

8.1.6 Åtgärd 6: Alla offentligfinansierade tjänster ska acceptera alla godkända e-tjänstelegitimationer

DIGG anser att regeringen ska genomföra åtgärderna som föreslås i betänkandet Användning av e-legitimation i tjänsten i den offentliga förvaltningen (SOU 2021:62) om att statliga myndigheter ska erkänna e-legitimationer som används av offentliga aktörer. Se även över möjligheten att utöka kretsen som omfattas av kravet på erkännande till alla offentliga aktörer.

DIGG anser dessutom att Försäkringskassan bör få sin uppgift att tillhandahålla den statliga e-legitimationen EFOS författningsreglerad. En utökad målgrupp från statliga myndigheters personal till – på frivillig grund - offentliga myndigheters personal, samt folkbokförda och medborgare bör då övervägas.

E-legitimationssystemet ska omfatta medarbetares möjligheter att identifiera sig och skriva under elektroniskt utan att använda en e-legitimation man anskaffat för privat bruk, helst utan att personnummer måste ingå i transaktionen.

DIGG har tagit fram ett ersättningslöst e-legitimeringsavtal mellan utfärdare av e-tjänstelegitimation och förlitande parter. DIGG har i samverkan även tagit fram en teknisk profil som stödjer användning av anställningsnummer hos en viss organisation som pseudonym för personnummer (i linje med bedömningen i SOU 2021:62 om användning av e-tjänstelegitimationer). DIGG är på väg att ta fram avtal som stödjer att arbetsgivare skickar identitetsintyg (”partsintyg”) till förlitande parter.

Försäkringskassan/EFOS förväntas bli den första utfärdaren av e-tjänstelegitimation som ansluter sig till det nya ersättningslösa avtalet eftersom detta är en av förutsättningarna för dem att bli anmälda av DIGG för användning av EFOS utomlands enligt eIDAS-förordningen. SITHS och Freja har också möjlighet att bli tidiga in i det nya avtalet. När en medarbetare med EFOS, SITHS eller Freja ska använda sin e-legitimation externt är det mycket viktigt att e-legitimation finns med i den förlitande partens lista över valbara e-legitimationer.

Erfarenheter från införande av nya godkända e-legitimationer för privatpersoner visar att det finns en betydande tröghet i att utöka listor över valbara e-legitimationer. Därför är det viktigt med central styrning för att åstadkomma resultat.

8.1.7 Åtgärd 7: Grundidentifiering på servicekontor

DIGG anser att regeringen ska ge Statens servicecenter i uppdrag att genomföra så kallad grundidentifiering på de statliga servicekontoren. Detta är en mycket efterfrågad funktion av såväl offentliga som privata aktörer, inklusive de privata e-legitimationsutfärdarna.

Grundidentifiering består av identifiering av den individ som ansöker om att få en e-legitimation utfärdad. I begreppet läggs vanligen in att individen behöver inställa sig personligen vilket behövs i två fall. För det första behövs det alltid när en e-legitimation på den högsta tillitsnivån ska utfärdas eller förnyas. För det andra behövs det när användaren inte har en tillräckligt säker eller tillåten e-legitimation att visa upp över internet inför utfärdande av en annan e-legitimation.

Servicekontorens grundidentifiering bör på för e-legitimationsutfärdarna frivillig grund stödja alla e-legitimationsutfärdare som är godkända av DIGG oavsett tillitsnivå och omfatta åtminstone e-tjänstelegitimationer.

8.2 Utanförskap internationellt

eIDAS-förordningen öppnar möjligheten att identifiera sig i svenska digitala tjänster med en utländsk e-legitimation. DIGG ansvarar för den svenska eIDAS-noden som förmedlar e-legitimeringen över landsgränsen och ansluter nya länder löpande. Många offentliga digitala tjänster har öppnat för utländsk e-legitimering (”Foreign eID”) i sina tjänster men i praktiken kommer användaren till ett så kallat väntrum utan möjlighet att använda de digitala tjänsterna.

För att leva upp till målen för EU:s inre marknad är det viktigt att i svenska e-tjänster även överväga e-legitimationslandets personidentitetsbegrepp vid gränsöverskridande elektronisk identifiering. Reglerna följer av EU:s eIDAS-förordning.

8.2.1 Åtgärd 8: Bredda digitala tjänster till utländska personidentitetsbegrepp

DIGG anser att den i avsnitt 8.1.4 föreslagna lagstiftningen ska även inkludera utländska personidentitetsbegrepp (enligt eIDAS-förordningen) i de digitala tjänster riktade mot privatpersoner som saknar krav i författning om att det måste vara ett svenskt identitetsbegrepp (personnummer) vid identifiering av användare.

Digitala tjänster där svenskt personnummer inte är helt nödvändigt som personidentitetsbegrepp bör byggas ut för att som ett alternativ även kunna hantera utländska identitetsbegrepp i enlighet med eIDAS-förordningen. Kraven på att e-legitimationslandets personidentitetsbegrepp både unikt ska peka på endast en individ och ska vara beständigt över tid kommer att öka i den kommande versionen av eIDAS-förordning (”eIDAS 2.0”). Trycket från EU på att Sverige ska öka möjligheterna för transaktioner inom den inre marknaden förväntas också öka, däribland i genomförandet av SDG-förordningen.

8.2.2 Åtgärd 9: Stöd koppling mellan utländska och svenska personidentitetsbegrepp

DIGG anser att staten behöver skapa ett statligt organiserat stöd för användare som vill koppla ihop sitt utländska personidentitetsbegrepp med sitt svenska personidentitetsbegrepp.

De personer som loggar in med en utländsk e-legitimation och som även innehar ett svenskt identitetsbegrepp ska ges möjlighet att knyta sin utländska e-legitimation till sitt svenska identitetsbegrepp (personnummer, styrkta samordningsnummer eller kommande identitetsnummer) för att kunna nyttja tjänster som kräver svenska personidentitetsbegrepp.

För privatpersoner krävs därför en för användaren frivillig, nationell kopplingsfunktion, som med viss tillitsnivå baserat på utarbetade rutiner, kopplar ihop det utländska personidentitetsbegreppet med det svenska. Det måste utredas hur denna koppling skall sparas, i ett register eller på annat sätt under användarens kontroll. Svenska digitala tjänster eller den svenska eIDAS-noden ska kunna ta del av kopplingen, vid behov baserat på användarens samtycke. Här finns internationell inspiration från bland annat Danmark. Vi föreslår att regeringen utser en ansvarig myndighet, med författningsstöd för verksamheten.

Den föreslagna digitala plånboken innebär ytterligare en möjlighet att lagra flera personidentitetsbegrepp, under förutsättning att de som bör utfärda attesterade

attribut (personidentitetsbegrepp) också gör detta. Utfärdandet måste ske på ett säkert sätt som skapar tillit till kopplingen. Därutöver måste förlitande parter börja använda sig av användares digitala plånböcker för att lösningen ska vara framgångsrik.

För medarbetare med utländsk e-legitimation kommer den andra avtalsvarianten som DIGG tar fram i enlighet med förstudierapporten eID för medarbetare att stödja att den svenska arbetsgivaren håller reda på kopplingen mellan det utländska personidentitetsbegreppet och anställningsnumret, och skickar med det svenska anställningsnumret i sitt intyg till förlitande parter i Sverige. I övriga fall bör den utländska medarbetaren ingå i målgruppen som den svenska arbetsgivaren anskaffar en svensk e-legitimation till, med anställningsnummer i identitetsintyget från e-legitimationsutfärdaren.

8.2.3 Åtgärd 10: Öka de digitala möjligheterna för dem utan styrkt svenskt personidentitetsbegrepp

DIGG anser att Migrationsverket ska få i uppdrag att tillhandahålla en svensk digital identitet för dem som inte kan få en svensk e-legitimation. Ge Migrationsverket nödvändigt författningsstöd för att koppla identiteten till biometriska uppgifter i syfte att undvika att en och samma person får flera identiteter i Sverige.

En person som inte kan identifiera sig tillräckligt vid ansökan om svenskt personidentitetsbegrepp eller svensk e-legitimation bör ändå ges ökade möjligheter i det digitala samhället jämfört med idag.

Baserat på kontroll mot biometriska uppgifter bör Migrationsverket därför utfärda en digital identitet som individen kan använda i de tjänster där det viktigaste är att veta att det är samma individ som återkommer flera gånger. Dessa digitala identiteter bör inte kallas e-legitimation, men bör som inloggningsmetod ges möjlighet att delta i DIGG:s digitala infrastruktur. Nivån når inte upp till tillitsnivåerna i Tillitsramverket för Svensk e-legitimation, men skulle kunna användas i DIGG:s identitetsfederation Sweden Connect eller i en liknande federation.

8.3 Elektroniska underskrifter

Det finns risk att Sverige halkar efter i hanteringen av elektroniska underskrifter, särskilt över landsgränsen. Användningen av elektroniska underskrifter behöver därför underlättas.

8.3.1 Åtgärd 11: Inför gemensam valideringstjänst och utökad tillitsförteckning

DIGG anser att regeringen ska genomföra förslagen i delbetänkandet Vem kan man lita på? (SOU 2021:9) gällande valideringstjänst och ge PTS uppdrag att hålla den utökade nationella tillitsförteckningen. Överväg möjligheten att ge DIGG i uppdrag att hålla en temporär nationell tillitsförteckning för e-underskrifter och e-stämplar i avvaktan på detta.

Det är svårt för statliga myndigheter och andra förlitande parter att avgöra om man kan lita på en elektronisk underskrift (eller -stämpel) som inkommer till myndigheten. I delbetänkandet Vem kan man lita på (SOU 2021:9) föreslås DIGG få i uppdrag att tillhandahålla en förvaltningsgemensam valideringstjänst och PTS få i uppdrag att ge ut föreskrifter med de krav som saknas i eIDAS-förordningen för att uppnå avancerade elektroniska underskrifter och -stämplar. Genomför de förslag som krävs för att i praktiken göra det möjligt för DIGG att tillhandahålla en valideringstjänst. DIGG har påbörjat arbetet med valideringstjänsten för att ge instruktionsenligt stöd till myndigheterna kopplat till e-underskrifter, men det saknas uppdrag för att hålla en nationell tillitsförteckning på nivån under den kvalificerade. En tillitsförteckning under den kvalificerade nivån är enligt DIGG:s uppfattning viktig eftersom underskrifter som inte är kvalificerade dominerar den svenska marknaden och även dessa måste kunna valideras av aktörer inom den offentliga förvaltningen. För det fall DIGG tillhandahåller en sådan förteckning kan det vara en temporär lösning till dess att förslaget avseende tillitsförteckning i SOU 2021:9 genomförs.

8.3.2 Åtgärd 12: Utöka DIGG:s stöd vid anskaffning av underskriftstjänster

DIGG anser att regeringen ska genomföra förslagen i Vem kan man lita på? (SOU 2021:9) om att utöka DIGG:s stöd inom e-underskriftsområdet.

Det är svårt för offentliga myndigheter att avgöra vilka av marknadens tjänster som är lämpliga att anskaffa. Det räcker inte med att de uppfyller eIDAS-förordningens relativt otydliga minimikrav, anskaffningen måste även uppfylla kraven på att hushålla med offentliga medel. Den av DIGG rekommenderade fristående underskriftstjänsten är endast en komponent, som behöver kompletteras med mer myndighetsnära funktioner för att stödja hela underskriftsflödet. De ramavtal som underskriftstjänster upphandlas från är för svåra att nyttja för offentliga aktörer med genomsnittliga kunskaper kring

anskaffning av underskriftslösningar. Komplettera därför valideringstjänsten och tillitsförteckningen med sätt att underlätta för offentliga aktörer att välja lösningar som både uppfyller lagstiftningens krav, hushållar med offentliga medel, stödjer verksamheten och är bra för samhället. Denna åtgärd går i linje med förslag i SOU 2021:9 om att utöka DIGG:s stöd inom e-underskriftsområdet.

Om DIGG planerar att införa stöd inom området i form av funktioner ska konsekvenser för marknaden beskrivas och övervägas inför beslut.

8.3.3 Åtgärd 13: DIGG ska tillhandahålla en fristående underskriftstjänst för små behov

DIGG anser att regeringen ska ge DIGG i uppdrag att utreda förutsättningarna för att tillhandahålla en fristående underskriftstjänst för aktörer med små behov.

DIGG bör tillhandahålla en fristående underskriftstjänst inklusive stödtjänst för aktörer med små behov. Denna kan driftas hos en myndighet ex Försäkringskassan. DIGG kan tillhandahålla öppen programvara, tillgänglig för alla.

Privatpersoner och mindre organisationer saknar i allmänhet de resurser och kompetenser som krävs för att arbeta med elektroniska underskrifter. Deras låga volymer gör dem inte heller intressanta för de kommersiella leverantörerna.

Över tid kan DIGG vid behov ges möjlighet att avgiftsfinansiera tjänsten för att undvika att den nyttjas av aktörer som annars skulle ha nyttjat kommersiella leverantörers tjänster.

8.3.4 Åtgärd 14: Genomför Id-kortsutredningens förslag om kvalificerad underskriftsmöjlighet

DIGG anser att regeringen bör tillsätta en utredning för att utreda förutsättningarna för DIGG att vidareutveckla den föreslagna fristående underskriftstjänsten i DIGG:s regi att inkludera även kvalificerade underskrifter och ge svenska användare med eIDAS digitala plånböcker möjlighet att skriva under med tjänsten. Ett alternativt förslag är att ge Försäkringskassan i uppdrag att tillhandahålla EFOS på eIDAS-nivå ”hög” till privatpersoner och småföretag, och inkludera möjligheten till kvalificerad e-underskrift.

Kopplat till Id-kortsutredningen förslag om statligt utfärdad e-legitimation föreslogs även möjlighet för användaren att skriva under med kvalificerade

underskrifter, vilket vanligen krävs vid underskrifter där den förlitande parten finns i utlandet.

Syftet med förslaget vore att erbjuda både privatpersoner och organisationer möjlighet att hantera krav från utländska motparter på att handlingar ska vara undertecknade med kvalificerad elektronisk underskrift. Framförallt är det en viktig möjlighet för företrädare för svenska företag som idag utestängs från att lämna anbud i utländska upphandlingar därför att anbudstiden är för kort för att de ska hinna anskaffa de kommersiella alternativ som finns.

Förslaget går i linje med den eIDAS-revidering som är föreslagen (3 juni 2021), där varje medlemsstat blir skyldig att erbjuda medborgare möjligheten till kvalificerad underskrift kopplat till sin digitala plånbok som medlemsstaten blir skyldig att erbjuda.

Det vore möjligt för DIGG att vidareutveckla den i åtgärd 13 planerade fristående underskriftstjänsten på det sättet. DIGG skulle då behöva gå igenom en överensstämmelsebedömning (”certifiering”) som utförs av ett ackrediterat organ i Sverige eller i annat land inom EU/EES.

Ett annat alternativ vore att låta EFOS bli den statliga e-legitimationen på id-kort till medborgare och folkbokförda och därmed även ge i uppdrag till Försäkringskassan att stå för den kvalificerade underskriftstjänsten som användaren behöver ha kopplad till såväl e-legitimationen som till den framtida digitala plånboken.

8.4 Användarens kontroll över sin data

I andra länder är samtalen om användarens integritet och kontroll över hur identitetsuppgifter används betydligt mer framträdande än i Sverige. Det är troligt att det kommer påverka utvecklingen även i Sverige, samtidigt som lösningar som är nödvändiga för att ge användaren ökad kontroll kan innebära nya möjligheter att hantera svårlösta problem.

8.4.1 Åtgärd 15: Överväg en statlig digital plånbok byggd på gemensamma standarder

DIGG anser att regeringen bör tillse ett statligt alternativ avseende förslaget i eIDAS 2.0 om digitala plånböcker. I den nyligen föreslagna eIDAS-revideringen framgår att varje medlemsstat ska tillhandahålla en digital plånbok (wallet) till medborgarna. Säkerställ att det finns ett statligt alternativ som komplement till

Sveriges modell med flera olika, privata och offentliga, utfärdare. En statligt utfärdad wallet skulle ge ett robustare, mindre sårbart system. Det skulle också minska utanförskapet då en användare inte behöver uppfylla privata utfärdares krav för tillhandahållande. Det är en statlig angelägenhet att tillse att medborgare kan identifiera sig, jmf med utgivandet av pass.

8.5 Kompetens

Vi har i Sverige en kompetensbrist inom området digital identitet och e-underskrift. Det visar sig tydligt i svårigheten att rekrytera kompetent personal till området och är ett av största hindren för en god utveckling av det svenska eID-systemet och optimalt nyttjande av det. Det är ett komplicerat område som tar tid att lära sig vilket gör att det tar tid att bygga kompetens. Detta gäller såväl de specifika eID-frågorna som generella informationssäkerhetsfrågor. Det gäller på alla nivåer; såväl på expert och utvecklarnivå som hos beslutsfattare, verksamhetsutvecklare och användare.

8.5.1 Åtgärd 16: Öka intresset och kunskapen för området med hjälp av konferenser och webbinarier

DIGG anser att regeringen bör bidra till ett ökat fokus på främjandeaktiviteter genom att tillskjuta medel till identitetsområdet. Främjandeaktiviteterna bör ta särskild höjd för frågan om användarens kontroll över sin data.

DIGG och andra myndigheter med främjandeuppdrag bör öka ansträngningarna att sprida kunskap genom att arrangera och delta i konferenser, utbildningar och ordna webbinarier. I tillägg till det behöver skriftliga kommunikationen vidareutvecklas på digg.se, elegitimation.se, swedenconnect.se samt på andra parters webbsidor om området.

Det pågår ett paradigmskifte i synen på användarens integritet och utvecklingen internationellt går mot att ge användaren kontroll över sin data och bestämmanderätt över hur identitetsuppgifter används och sprids. Parallellt med utvecklande av tekniska lösningar krävs stora åtgärder inom främjande och kunskapsspridning, både till offentlig sektor, men även till resten av samhället, för att hantera de förändrade förutsättningar dessa förslag ger det befintliga e-legitimationssystemet i Sverige.

8.5.2 Åtgärd 17: Öka intresset för området med hjälp av samarbete med lärosäten

DIGG anser att regeringen bör utlysa en professur och skapa utbildningar och forskningsprogram med inriktning mot digital identitetshantering.

Intresset för ämnet hos studenter bör ökas genom aktivt samarbete kring examensarbeten och forskningsuppdrag. Kompetensområdet spänner över flera av dagens forskningsområden vilket minskar akademiernas intresse för frågan och gör det mindre tydligt för nya studenter och doktorander.

8.6 Övrigt

8.6.1 Åtgärd 18: Reglera i författning att DIGG ska tillhandahålla kvalitetsmärket Svensk e-legitimation samt ska granska och godkänna ansökningar från e-legitimationsutfärdare

DIGG tillhandahåller idag kvalitetsmärket Svensk e-legitimation. Märket har kommit att bli mycket respekterat (se avsnitt 4.2) och ett flertal utfärdare på den svenska e-legitimationsmarknaden är granskade och godkända av DIGG. Märket skapades av E-legitimationsnämnden men det framgick inte av nämndens instruktion att den skulle tillhandahålla märket. DIGG tog över märket och hanteringen av det när myndigheten skapades men DIGG uppgiften framgår inte heller av DIGG:s instruktion. Utredningen om effektiv styrning av nationella digitala tjänster föreslog i sitt slutbetänkande bl.a. att märket och processen (ansökan etc.) kring det skulle regleras i lag och att det i förordning skulle framgå att digitaliseringsmyndigheten (DIGG) skulle granska och godkänna utfärdare (SOU 2017:114 s. 32-33 och s. 53).

DIGG:s uppfattning är att kvalitetsmärket fyller en viktig funktion på den svenska e-legitimationsmarknaden och att märket efterfrågas av bl.a. aktörer inom den offentliga förvaltningen. Vi anser emellertid att märket potentiellt kan ha en så stor inverkan på marknaden att det vore önskvärt att det i författning framgår att DIGG ska tillhandahålla märket och att utfärdare kan ansöka om att granskas. De utfärdare som lever upp till kraven ska godkännas. Det skulle innebära att nuvarande ordning och hantering får ett tydligt författningsstöd. Utredningen om effektiv styrning av nationella digitala tjänster föreslog i ovan nämnda betänkande en ny lag om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling. Att författningsreglera att DIGG ska tillhandahålla kvalitetsmärket behöver emellertid inte nödvändigtvis förutsätta att just det lagförslaget genomförs. Alternativa lösningar kan dock behöva utredas,

t.ex. av DIGG. Utredningar avseende författningsstöd för kvalitetsmärket bör beakta ett flertal aspekter, bl.a. sekretessfrågor.