Från: [redacted]
Ärende: Remiss av SOU 2021:62 Användning av e-legitimation i tjänsten i den offentliga förvaltningen – Svar senast 25/5 2022
Datum: den 21 februari 2022 11:01:35
Bilagor: Remissmissiv.pdf

SOU 2021:62: https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/06/sou-202162/

Utredningen om betrodda tjänsters slutbetänkande ”Användning av e-legitimation i tjänsten i den offentliga förvaltningen” (SOU 2021:62)

Remissinstanser

1. AB Svenska Pass
2. Angeno Business Solutions AB
3. Arbetsförmedlingen
4. Arbetsgivarverket
5. Arboga kommun
6. AREFF Systems AB
7. Arvika kommun
8. Bolagsverket
9. Boverket
10. Centrala studiestödsnämnden
11. Chalmers tekniska högskola AB
12. Comfact AB
13. Cygate AB
14. Domstolsverket
15. Dorotea kommun
16. E-hälsomyndigheten
17. Ekobrottsmyndigheten
18. Ekonomistyrningsverket
19. Finansiell ID-teknik

20. Freja eID Group AB
21. Föreningen XBRL Sweden
22. Företagarna
23. Försvarets materielverk
24. Försvarets radioanstalt
25. Försvarsmakten
26. Försäkringskassan
27. Förvaltningsrätten i Linköping
28. Gnosjö kommun
29. Gällivare kommun
30. Hogia Connect AB
31. Huddinge kommun
32. Hudiksvalls kommun
33. Hylte kommun
34. Härjedalens kommun
35. Ideella Föreningen Teknikföretagen i Sverige
36. IDEMIA Sweden AB
37. IIS – Internetstiftelsen i Sverige
38. Inera AB
39. Integritetsskyddsmyndigheten
40. Kammarkollegiet
41. Kammarrätten i Stockholm
42. Knivsta kommun
43. Kommerskollegium
44. Kronofogdemyndigheten
45. Kumla kommun

46. Landsorganisationen i Sverige
47. Lantmäteriet
48. Ljusdals kommun
49. Ludvika kommun
50. Lunds kommun
51. Länsstyrelsen i Uppsala län
52. Länsstyrelsen i Blekinge län
53. Länsstyrelsen i Skåne län
54. Länsstyrelsen i Stockholms län
55. Länsstyrelsen i Västerbottens län
56. Länsstyrelsen i Västernorrlands län
57. Länsstyrelsen i Örebro län
58. Markaryds kommun
59. Mullsjö kommun
60. Myndigheten för digital förvaltning
61. Myndigheten för samhällsskydd och beredskap
62. Naturvårdsverket
63. Nybro kommun
64. Patent- och registreringsverket
65. Pensionsmyndigheten
66. Polismyndigheten
67. Post- och telestyrelsen
68. Regelrådet
69. Region Dalarna
70. Region Gotland
71. Region Norrbotten

72. Region Sörmland
73. Riksarkivet
74. Ronneby kommun
75. Sala kommun
76. Scrive AB
77. Seriline Aktiebolag
78. Skatteverket
79. Socialstyrelsen
80. Solna kommun
81. Statens servicecenter
82. Statens skolverk
83. Statistiska centralbyrån
84. Statskontoret
85. Stockholms universitet
86. Strängnäs kommun
87. Sundsvalls kommun
88. Svensk e-identitet AB
89. Svenska institutet för standarder (SIS)
90. Svenskt Näringsliv
91. Sveriges advokatsamfund
92. Sveriges akademikers centralorganisation
93. Sveriges Kommuner och Regioner
94. Säkerhets- och försvarsföretagen
95. Säkerhetspolisen
96. TechSverige
97. Tjänstemännens centralorganisation

98. Totalförsvarets forskningsinstitut
99. Transportstyrelsen
100. Trollhättans kommun
101. Universitets- och högskolerådet
102. Upphandlingsmyndigheten
103. Valdemarsviks kommun
104. Varbergs kommun
105. Vetenskapsrådet
106. Vimmerby kommun
107. Västra Götalandsregionen
108. Växjö kommun
109. Åklagarmyndigheten
110. Åmåls kommun
111. Älvkarleby kommun
112. Ängelholms kommun
113. Örnsköldsviks kommun
114. Östersunds kommun

Remissvaren ska ha kommit in till Infrastrukturdepartementet **senast den 25 maj 2022**. Svaren bör lämnas per e-post till i.remissvar@regeringskansliet.se och med kopia till i.esd.remisser@regeringskansliet.se. Ange diarienummer I2021/01954 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i betänkandet.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Betänkandet kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Remissinstanserna kan utan kostnad beställa tryckta exemplar av betänkandet via ett beställningsformulär hos Elanders Sverige AB.

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria Svara på remiss (SB PM 2021:1). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Jessica Steinmetz
T.f. enhetschef

Kopia till

Elanders Sverige AB, e-postadress: betankande@elanders.com

Regeringskansliet

Remiss

2022-02-21
I2021/01954

Infrastrukturdepartementet
Enheten för samhällets digitalisering

Utredningen om betrodda tjänsters slutbetänkande ”Användning av e-legitimation i tjänsten i den offentliga förvaltningen” (SOU 2021:62)

Remissinstanser

1. AB Svenska Pass
2. Angeno Business Solutions AB
3. Arbetsförmedlingen
4. Arbetsgivarverket
5. Arboga kommun
6. AREFF Systems AB
7. Arvika kommun
8. Bolagsverket
9. Boverket
10. Centrala studiestödsnämnden
11. Chalmers tekniska högskola AB
12. Comfact AB
13. Cygate AB

Telefonväxel: 08-405 10 00
Fax: 08-24 46 31
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Malmtorgsgatan 3
E-post: i.registrator@regeringskansliet.se

14. Domstolsverket
15. Dorotea kommun
16. E-hälsomyndigheten
17. Ekobrottsmyndigheten
18. Ekonomistyrningsverket
19. Finansiell ID-teknik
20. Freja eID Group AB
21. Föreningen XBRL Sweden
22. Företagarna
23. Försvarets materielverk
24. Försvarets radioanstalt
25. Försvarsmakten
26. Försäkringskassan
27. Förvaltningsrätten i Linköping
28. Gnosjö kommun
29. Gällivare kommun
30. Hogia Connect AB
31. Huddinge kommun
32. Hudiksvalls kommun
33. Hylte kommun
34. Härjedalens kommun

35. Ideella Föreningen Teknikföretagen i Sverige
36. IDEMIA Sweden AB
37. IIS – Internetstiftelsen i Sverige
38. Inera AB
39. Integritetsskyddsmyndigheten
40. Kammarkollegiet
41. Kammarrätten i Stockholm
42. Knivsta kommun
43. Kommerskollegium
44. Kronofogdemyndigheten
45. Kumla kommun
46. Landsorganisationen i Sverige
47. Lantmäteriet
48. Ljusdals kommun
49. Ludvika kommun
50. Lunds kommun
51. Länsstyrelsen i Uppsala län
52. Länsstyrelsen i Blekinge län
53. Länsstyrelsen i Skåne län
54. Länsstyrelsen i Stockholms län
55. Länsstyrelsen i Västerbottens län

56. Länsstyrelsen i Västernorrlands län
57. Länsstyrelsen i Örebro län
58. Markaryds kommun
59. Mullsjö kommun
60. Myndigheten för digital förvaltning
61. Myndigheten för samhällsskydd och beredskap
62. Naturvårdsverket
63. Nybro kommun
64. Patent- och registreringsverket
65. Pensionsmyndigheten
66. Polismyndigheten
67. Post- och telestyrelsen
68. Regelrådet
69. Region Dalarna
70. Region Gotland
71. Region Norrbotten
72. Region Sörmland
73. Riksarkivet
74. Ronneby kommun
75. Sala kommun
76. Scrive AB

77. Seriline Aktiebolag
78. Skatteverket
79. Socialstyrelsen
80. Solna kommun
81. Statens servicecenter
82. Statens skolverk
83. Statistiska centralbyrån
84. Statskontoret
85. Stockholms universitet
86. Strängnäs kommun
87. Sundsvalls kommun
88. Svensk e-identitet AB
89. Svenska institutet för standarder (SIS)
90. Svenskt Näringsliv
91. Sveriges advokatsamfund
92. Sveriges akademikers centralorganisation
93. Sveriges Kommuner och Regioner
94. Säkerhets- och försvarsföretagen
95. Säkerhetspolisen
96. TechSverige
97. Tjänstemännens centralorganisation

98. Totalförsvarets forskningsinstitut
99. Transportstyrelsen
100. Trollhättans kommun
101. Universitets- och högskolerådet
102. Upphandlingsmyndigheten
103. Valdemarsviks kommun
104. Varbergs kommun
105. Vetenskapsrådet
106. Vimmerby kommun
107. Västra Götalandsregionen
108. Växjö kommun
109. Åklagarmyndigheten
110. Åmåls kommun
111. Älvkarleby kommun
112. Ängelholms kommun
113. Örnsköldsviks kommun
114. Östersunds kommun

Remissvaren ska ha kommit in till Infrastrukturdepartementet **senast den 25 maj 2022**. Svaren bör lämnas per e-post till i.remissvar@regeringskansliet.se och med kopia till i.esd.remisser@regeringskansliet.se. Ange diarienummer I2021/01954 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt

lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i betänkandet.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Betänkandet kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Remissinstanserna kan utan kostnad beställa tryckta exemplar av betänkandet via ett beställningsformulär hos Elanders Sverige AB.

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria Svara på remiss (SB PM 2021:1). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Jessica Steinmetz
T.f. enhetschef

Kopia till

Elanders Sverige AB, e-postadress: betankande@elanders.com

Användning av e-legitimation i tjänsten i den offentliga förvaltningen

SLUTBETÄNKANDE AV
UTREDNINGEN OM
BETRODDA TJÄNSTER

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:62

Användning av e-legitimation i tjänsten i den offentliga förvaltningen

Slutbetänkande av
Utredningen om betrodda tjänster

Stockholm 2021

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:62

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2021

ISBN 978-91-525-0172-6 (tryck)
ISBN 978-91-525-0173-3 (pdf)
ISSN 0375-250X

Till statsrådet Anders Ygeman

Regeringen beslutade den 12 mars 2020 att tillkalla en särskild utredare med uppdrag att utreda och lämna förslag för ökad och standardiserad användning av betrodda tjänster i syfte att höja säkerheten och stärka tilliten när de används i den offentliga förvaltningen.

Som särskild utredare förordnades från och med den 23 mars 2020 målkanslichefen Henrik Ardhede.

Den 17 december 2020 beslutades om tilläggsdirektiv till utredningen.

Som sekreterare i utredningen anställdes från och med den 23 mars uppdragsledaren Eva Sartorius och från och med den 30 mars 2020 juristen Philip Levin. Eva Sartorius avslutade sitt arbete i utredningen den 31 augusti 2020 och från och med samma dag förordnades seniora handläggaren Björn Scharin som utredningssekreterare.

Som experter att biträda utredningen förordnades den 27 april 2020 näringspolitiska experten och förbundsjuristen My Bergdahl (IT & Telekomföretagen), seniora digitala strategen Anna Fors (Försäkringskassan), ramavtalsförvaltaren Pedra Herdegen (Kammarkollegiet), tjänsteområdesansvarig Lotta Hämäläinen (Myndigheten för digital förvaltning), sektionschefen Lotta Nordström (Sveriges Kommuner och Regioner), seniora handläggaren Björn Scharin (Post- och telestyrelsen), it-arkitekten David Skullered (E-hälsomyndigheten), chefen Dag Ströman (Sveriges Certifieringsorgan för IT-säkerhet vid Försvarets materielverk), seniora handläggaren Gustav Söderlind (Myndigheten för samhällsskydd och beredskap), departementssekreteraren Sophie Ankarcrona Thelin (Infrastrukturdepartementet) och utredaren Benjamin Yousefi (Riksarkivet).

Björn Scharin entledigades från sitt uppdrag som expert den 31 augusti 2020 och den 1 september 2020 förordnades uppdragsledaren Eva Sartorius (Myndigheten för digital förvaltning) att vara expert i utredningen.

Utredningen, som har tagit sig namnet Utredningen om betrodda tjänster, redogör för uppdraget med användande av vi-form även om det inte funnits fullständig samsyn i alla delar.

Utredningen överlämnade delbetänkandet *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9) den 15 februari 2021.

Utredningen överlämnar härmed slutbetänkandet *Användning av e-legitimation i tjänsten i den offentliga förvaltningen* (SOU 2021:62). Uppdraget är med detta slutfört.

Göteborg i juni 2021

Henrik Ardhede

/Philip Levin
Björn Scharin

Innehåll

Bilagor

Vissa förkortningar

EU-rättsakter

EU:s förordning om en gemensam digital ingång	Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012
Dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG
eIDAS-förordningen	Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

Övriga förkortningar

a.a.	anfört arbete
AD	Arbetsdomstolens domar
API	Application Program Interface
DIGG	Myndigheten för digital förvaltning
Dir.	Kommittédirektiv
Ds	Departementsserien
EU	Europeiska unionen
f./ff.	följande sida/sidor
FIDUS	Federationsförbund för IDentitetshantering, Utbildning och Skola
ENISA	Europeiska unionens cybersäkerhetsbyrå
eSam	eSamverkansprogrammet
HSA	Hälso- och sjukvårdens adressregister
IdP	Identitetsintygsutfärdare inom SAML
IEC	International Electrotechnical Commission
IMY	Integritetsskyddsmyndigheten
ISO	International Organization for Standardization
LIS	Ledningssystem för informationssäkerhet
MIG	Migrationsöverdomstolen
MSB	Myndigheten för samhällsskydd och beredskap

NOBID	Nordic-Baltic co-operation on digital identities
PKI	Public Key Infrastructure
prop.	Regeringens proposition
Sambi	Samverkan för behörighet och identitet inom hälsa, vård och omsorg
SAML	Security Assertion Markup Language
SIS	Svenska institutet för standarder
SITHS	Säker IT-användning i Hälso- och Sjukvården
SKR	Sveriges Kommuner och Regioner
SOU	Sveriges Offentliga Utredningar
SP	Tjänsteleverantör inom SAML
SSI	Self Sovereign Identity
Sunet	Swedish University Computer Network
SWAMID	Swedish Academic Identity Federation
XML	Extensible Markup Language

Sammanfattning

Inledning

Den del av utredningens uppdrag som redovisas i detta betänkande omfattar kartläggning och analys av den offentliga förvaltningens behov av åtgärder avseende användning av e-legitimation i tjänsten samt förslag på sådana åtgärder.

Användningen av e-legitimation i tjänsten innefattar användning av privata e-legitimationer eller e-tjänstelegitimationer för att fullgöra en arbetsuppgift. Med e-tjänstelegitimation avses i detta betänkande en e-legitimation för den som tjänstgör vid eller innehar uppdrag för en organisation och som anskaffats av den organisationen.

E-legitimationer som används i tjänsten inom förvaltningen har enligt vår kartläggning tre huvudsakliga användningsområden: autentisering i interna system, stöd för skapande av elektroniska underskrifter samt organisationsöverskridande användning. En stark drivkraft bakom den ökade användningen av e-legitimationer inom den offentliga förvaltningen är behovet av starkare former av autentisering.

Kartläggning av den offentliga förvaltningens behov

Vår kartläggning visar att det i dagsläget inom den offentliga förvaltningen finns ett antal utmaningar med koppling till användning av e-legitimation i tjänsten.

Ett problemområde är svårigheterna med organisationsöverskridande användning av e-tjänstelegitimationer. Det finns i dag olika e-tjänstelegitimationer inom den offentliga förvaltningen och användning av dem över organisationsgränserna är i huvudsak begränsad till vissa sektorer där sådan åtkomst möjliggörs genom s.k. identitetsfederationer. Det är därför vanligt förekommande att privata e-legitimationer används i tjänsten för autentisering i externa e-tjänster.

Sådan användning kan medföra en hel del administration då det oftast innefattar att exempelvis varje enskild kommun måste ha en behörighetsadministratör för varje extern e-tjänst som deras anställda eller uppdragstagare använder sig av.

Det sistnämna kopplar till att det saknas ett system för att även medarbetarens behörighet framgår vid autentisering i andra aktörers e-tjänster. Vår kartläggning har emellertid inte visat att det i första hand är yrkesroller eller titlar som avgör om en person ska uppfattas som behörig av förlitande part. Den gemensamma nämnare aktörerna har gett uttryck för att de efterfrågar är att veta vilken organisation en person företräder. Det kan emellertid inte uteslutas att ytterligare attribut i vissa fall är nödvändiga och att behoven inom detta område kan komma att öka.

Ett hinder för användning av e-legitimation i tjänsten finns för anställda eller uppdragstagare som inte finns med i det svenska folkbokföringsregistret. Detta då avsaknaden av personnummer medför att de inte kan få en svensk e-legitimation. Detta drabbar både nyanlända personer och personer från andra länder som arbetar här under en begränsad period och därför inte folkbokförs i Sverige. Problematiken uppstår även för s.k. gränsgångare som bor i ett annat land men som arbetar i Sverige. Dessa hinder kan uppstå inom olika delar av förvaltningen men problemen förefaller vara vanligast förekommande inom utbildnings- samt hälso- och sjukvårdssektorerna.

En stor andel av välfärden inom offentlig sektor tillhandahålls i dagsläget genom privata utförare. Det finns därför ett tydligt behov av att ge dessa utförare samma förutsättningar som aktörer inom det offentliga vad gäller tillgång till olika e-tjänster som krävs för att de ska kunna fullgöra sina uppdrag.

Ett robust och tillförlitligt e-legitimationssystem förutsätter att det går att lita på grundidentifieringen av respektive användare. Det har under kartläggningen tydligt framkommit att en förutsättning för att e-tjänstelegitimationer ska kunna användas över organisationsgränserna är att organisationerna inom förvaltningen känner tillit till den grundidentifiering som sker. Det har också framkommit att grundidentifieringen är invecklad och kostsam för utfärdarna. Vidare visar kartläggningen att det finns ett stort behov av att kunna utfärda nya elektroniska identitetshandlingar genom s.k. id-växling.

Kartläggningen visar även att det finns ett behov av ökat stöd inom området och att detta behov framför allt finns hos mindre aktörer.

Användning av privata e-legitimationer i tjänsten

Användning av privata e-legitimationer i tjänsten är enligt vår bedömning tillåten. Det kräver emellertid att det finns en överenskommelse mellan arbetsgivare och arbetstagare om sådan användning. Vid användning av privata e-legitimationer aktualiseras en rad olika aspekter som ska beaktas i form av bl.a. personuppgiftsbehandling, efterlevnad av användarvillkor samt informationssäkerhet. Vår sammantagna bedömning är att användning av privata e-legitimationer i tjänsten endast bör förekomma när det inte är möjligt att använda e-tjänstelegitimationer för att fullgöra en arbetsuppgift.

Statliga myndigheter under regeringen ska tillhandahålla e-tjänstelegitimationer till anställda och uppdragstagare

Med utgångspunkt från vår bedömning vad gäller användning av privata e-legitimationer i tjänsten föreslår vi att e-tjänstelegitimationer ska tillhandahållas den som tjänstgör vid eller innehar uppdrag för en statlig myndighet under regeringen och, som för att kunna fullgöra sina arbetsuppgifter, behöver styrka sin identitet eller tjänsteställning. Användning av privata e-legitimationer föreslås endast få ske för id-växling, som kontinuitetslösning eller för det fall en särskild arbetsuppgift, som kräver användning av e-legitimation hos tredje part, inte kan genomföras med en e-tjänstelegitimation.

Ett ramverk för organisationsöverskridande användning av e-tjänstelegitimationer

För att skapa bättre förutsättningar för organisationsöverskridande användning av e-tjänstelegitimationer föreslår vi att det ska införas en ny lag som skapar ett ramverk för sådan användning. I syfte att möjliggöra sådan användning ska Myndigheten för digital förvaltning (DIGG) tillhandahålla ett system för erkännande av e-tjänstelegitimationer.

Statliga myndigheter ska åläggas ett krav på att erkänna e-tjänstelegitimationer som används av anställda och uppdragstagare hos offentliga aktörer för åtkomst till e-tjänster som statliga myndigheter tillhandahåller. Begreppet offentliga aktörer omfattar i den före-

slagna lagen statliga myndigheter, kommuner, regioner, offentligt styrda organ och privata aktörer som yrkesmässigt bedriver verksamhet inom vissa utpekade områden som till någon del är offentligt finansierad.

Kravet på erkännande gäller endast e-tjänstelegitimationer som uppfyller fastställda krav. Enbart e-tjänstelegitimationer som efter ansökan har godkänts av DIGG omfattas av kravet på erkännande. DIGG föreslås kunna ta ut en avgift för denna granskning. Kravet på erkännande gäller vidare bara om e-tjänstelegitimationen har samma tillitsnivå eller högre än den nivå som krävs för åtkomst till den aktuella e-tjänsten.

Även e-tjänstelegitimationer som inte är godkända får efter genomförd självskattning och anmälan ingå i systemet, men det är då frivilligt för statliga myndigheter att erkänna sådana e-legitimationer i sina e-tjänster.

Regeringen ska ges möjlighet att meddela undantag från kravet på erkännande. Vi föreslår att tre undantag ska införas. Statliga myndigheter ska inte behöva erkänna e-tjänstelegitimationer om erkännandet medför allvarliga säkerhetsrisker. Kravet på erkännande av e-tjänstelegitimationer ska vidare inte gälla för e-tjänster som endast riktar sig till enskilda. En statlig myndighet ska inte heller behöva erkänna en e-tjänstelegitimation om den aktuella e-tjänsten redan är ansluten till ett sektorspecifikt system för erkännande av e-tjänstelegitimationer.

Utfärdare av e-tjänstelegitimationer ska rapportera säkerhetsincidenter till DIGG och myndigheten ska kunna besluta att en e-legitimation tillfälligt eller tills vidare inte ska ingå i systemet. Vid allvarliga säkerhetsincidenter ska DIGG kunna besluta att en e-tjänstelegitimation tas bort från systemet.

En samverkande infrastruktur mellan offentlig och privat sektor

Det är viktigt både för digitaliseringen av offentlig sektor och samhällets digitalisering i stort att det för elektronisk identifiering finns en samverkande infrastruktur mellan offentlig och privat sektor. Då detta är en fråga som ligger utanför utredningens uppdrag lämnar vi emellertid inga förslag i denna del. Vi anser dock att systemet för

erkännande av e-tjänstelegitimationer bör utvecklas till att även omfatta privat sektor och att denna fråga bör utredas vidare.

Översyn av det svenska tillitsramverket

Vi föreslår att regeringen ska ge DIGG i uppdrag att se över det svenska tillitsramverk som myndigheten tillhandahåller. Dels med anledning av att ramverket bör harmoniseras med tillitsnivåerna i eIDAS-förordningen. Dels att indirekta krav på personnummer uppställer hinder för vissa personer som arbetar inom den offentliga förvaltningen att få e-tjänstelegitimationer trots att de har tillförlitliga identitetshandlingar som medför att en säker grundidentifiering kan göras.

En framtida lösning för attributshantering

Utredningen bedömer att en framtida lösning för attributshantering bör bygga på att attributen med behörighetsinformation i huvudsak tillhandahålls av arbets- eller uppdragsgivaren i stället för att uppgifterna samlas i stora nationella register eller finns i respektive e-tjänst.

Ökat stöd avseende användning av e-tjänstelegitimationer

Vi bedömer att det bör ges mer stöd till den offentliga förvaltningen vad avser användning av e-tjänstelegitimationer. Utifrån DIGG:s befintliga uppgift att främja användningen av elektronisk identifiering och då tekniska frågor rörande e-tjänstelegitimationer inte sällan är sammankopplade med användning av elektroniska underskrifter bedömer vi att DIGG med de ökade anslag vi föreslår i vårt delbetänkande vad gäller ökat stöd inom området betrodda tjänster bör kunna möta upp det behov av stöd som finns vad gäller de tekniska aspekterna. De juridiska frågorna bör därtill kunna hanteras inom ramen för det ökade rättsliga stöd DIGG ska erbjuda den offentliga förvaltningen.

Bättre förutsättningar för id-växling

Vi bedömer att en statlig e-legitimation som kan användas för id-växling i enlighet med förslaget som lämnades av 2017 års ID-kortsutredning bör införas för att skapa förutsättningar för enklare och billigare utfärdande av e-tjänstelegitimationer samt en mer diversifierad marknad.

1 Författningsförslag

1.1 Förslag till lag om erkännande av medel för elektronisk identifiering

Härigenom föreskrivs följande.

Inledande bestämmelser

1 § Denna lag innehåller bestämmelser om erkännande av medel för elektronisk identifiering.

2 § Lagen påverkar inte sådant erkännande av medel för elektronisk identifiering som följer av Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen), i den ursprungliga lydelsen.

Ordförklaringar

3 § Med offentlig aktör avses

1. en statlig eller kommunal myndighet,
2. en beslutande församling i en kommun eller region,
3. ett sådant offentligt styrt organ som avses i andra stycket,
4. en sammanslutning som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och som består av

a) en eller flera myndigheter eller församlingar som anges i 1 och 2, eller

b) ett eller flera organ enligt andra stycket,

5. en privat aktör som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som

a) aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),

b) utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125),

c) bedrivs enligt socialtjänstlagen (2001:453), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga eller lagen (1993:387) om stöd och service till vissa funktionshindrade, eller

d) utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken, och

6. en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller för utbildning på forskarnivå.

Med offentligt styrt organ avses en sådan juridisk person som tillgodoser behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och

1. som till största delen är finansierad av staten, en kommun, en region eller en sådan offentlig aktör som avses i första stycket 1–4,

2. vars verksamhet står under kontroll av staten, en kommun, en region eller en sådan offentlig aktör som avses i första stycket 1–4, eller

3. i vars styrelse eller motsvarande ledningsorgan mer än halva antalet ledamöter är utsedda av staten, en kommun, en region eller en sådan offentlig aktör som avses i första stycket 1–4.

4 § I övrigt har ord och uttryck i denna lag samma betydelse som i eIDAS-förordningen, i den ursprungliga lydelsen.

Erkännande av medel för elektronisk identifiering

5 § När medel för elektronisk identifiering krävs för att få tillgång till en nättjänst som tillhandahålls av en statlig myndighet, ska medel som av en offentlig aktör tillhandahålls för aktörens anställda eller uppdragstagare erkännas för autentisering för tjänsten om

1. medlet för elektronisk identifiering är godkänt för användning i det system som avses i 6 §, och

2. tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den statliga myndigheten kräver för åtkomst till nättjänsten.

Regeringen får meddela undantag från kravet på erkännande enligt första stycket.

System för erkännande av medel för elektronisk identifiering

6 § Den myndighet som regeringen bestämmer ska tillhandahålla ett system för erkännande av medel för elektronisk identifiering (systemet).

Regeringen eller den myndighet regeringen bestämmer får meddela närmare föreskrifter om systemet och användningen av det.

7 § Den myndighet som avses i 6 § första stycket får behandla personuppgifter i systemet om det är nödvändigt för erkännande av medel för elektronisk identifiering i anslutna nättjänster.

Denna lag träder i kraft den 1 januari 2024.

1.2 Förslag till förordning om erkännande av medel för elektronisk identifiering

Härigenom föreskrivs följande.

Inledande bestämmelser

1 § Denna förordning innehåller bestämmelser som kompletterar lagen om erkännande av medel för elektronisk identifiering.

Ordförklaringar

2 § Ord och uttryck i denna förordning har samma innebörd som i lagen om erkännande av medel för elektronisk identifiering.

Undantag från kravet på erkännande av medel för elektronisk identifiering

3 § En statlig myndighet behöver inte erkänna medel för elektronisk identifiering enligt 5 § lagen om erkännande av medel för elektronisk identifiering om

1. tillgång till den aktuella nättjänsten ges genom ett sektorspecifikt system för erkännande av elektronisk identifiering,
2. användning av medlet är förenat med allvarliga säkerhetsrisker, eller
3. nättjänsten enbart riktar sig till enskilda.

System för erkännande av medel för elektronisk identifiering

4 § Statliga myndigheter som tillhandahåller nättjänster som omfattas av kravet på erkännande av medel för elektronisk identifiering i 5 § lagen om erkännande av medel för elektronisk identifiering ska ansluta sådana nättjänster till systemet för erkännande av medel för elektronisk identifiering (systemet) som avses i 6 § samma lag.

Vid användning av medel för elektronisk identifiering som avses i 5 § lagen om erkännande av medel för elektronisk identifiering får personnummer endast överföras i systemet om

1. krav på användning av personnummer föreskrivs i lag eller annan författning, eller
2. användning av annan identitetsbeteckning inte är möjlig.

5 § Myndigheten för digital förvaltning ska tillhandahålla systemet.

Myndigheten för digital förvaltning får efter samråd med Myndigheten för samhällsskydd och beredskap meddela föreskrifter om krav på medel för elektronisk identifiering som ingår i systemet och krav som avser förlitande parter.

6 § Myndigheten för digital förvaltning får efter ansökan godkänna ett medel för elektronisk identifiering för användning i systemet. Myndigheten ska vid en sådan ansökan granska medlet utifrån de krav som har meddelats med stöd av 5 § andra stycket.

Myndigheten för digital förvaltning ska offentliggöra att ett medel för elektronisk identifiering har godkänts för användning i systemet.

Myndigheten för digital förvaltning får efter samråd med Myndigheten för samhällsskydd och beredskap meddela föreskrifter om ansöknings- och granskningsförfarandet i första stycket.

7 § Medel för elektronisk identifiering som inte är godkänt enligt 6 § första stycket får ingå i systemet om utfärdaren bedömer att medlet lever upp till de krav som meddelats med stöd av 5 § andra stycket.

Utfärdaren ska anmäla till Myndigheten för digital förvaltning att medlet ska ingå i systemet.

Utfärdaren ska till förlitande parter i systemet eller Myndigheten för digital förvaltning på begäran lämna ut uppgifter som ligger till grund för bedömningen att medlet för elektronisk identifiering lever upp till de krav som meddelats med stöd av 5 § andra stycket.

Myndigheten för digital förvaltning ska efter anmälan offentliggöra att ett medel för elektronisk identifiering som inte är godkänt ingår i systemet.

Myndigheten för digital förvaltning får efter samråd med Myndigheten för samhällsskydd och beredskap meddela föreskrifter om förfarandet för anmälan och anslutning av medel som inte är godkända till systemet.

Hantering av säkerhetsincidenter

8 § Utfärdare av medel för elektronisk identifiering som ingår i systemet ska utan dröjsmål rapportera säkerhetsincidenter till Myndigheten för digital förvaltning samt till förlitande parter som påverkas av incidenten.

9 § Myndigheten för digital förvaltning får besluta att det godkända medel för elektronisk identifiering som en säkerhetsincident avser tills vidare eller under en begränsad period inte längre är godkänt för användning i systemet.

Om en säkerhetsincident avser ett medel för elektronisk identifiering som inte är godkänt får Myndigheten för digital förvaltning besluta att medlet tills vidare eller under en begränsad period inte längre ingår i systemet.

Om Myndigheten för digital förvaltning bedömer att en säkerhetsincident är allvarlig får den besluta att medlet för elektronisk identifiering inte längre ska ingå i systemet.

Myndigheten för digital förvaltning får bestämma att beslut enligt denna paragraf ska gälla omedelbart.

10 § Myndigheten för digital förvaltning får efter samråd med Myndigheten för samhällsskydd och beredskap meddela föreskrifter om hantering av säkerhetsincidenter samt rapportering av sådana incidenter.

11 § En statlig myndighet som med stöd av 3 § väljer att inte erkänna ett medel för elektronisk identifiering ska utan dröjsmål rapportera det till Myndigheten för digital förvaltning samt ange skälen till varför myndigheten inte erkänner medlet.

Överklagande

12 § I 40 § förvaltningslagen (2017:900) finns bestämmelser om överklagande till allmän förvaltningsdomstol. Andra beslut än beslut enligt 6 och 9 §§ får dock inte överklagas.

Denna förordning träder i kraft den 1 januari 2024.

1.3 Förslag till förordning om ändring i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte

Härigenom föreskrivs i fråga om förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte

dels att rubriken till förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte ska ha följande lydelse,

dels att det ska införas en ny paragraf, 5 §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Förordning om statliga myndigheters elektroniska informationsutbyte	**Förordning om statliga myndigheters *medel för elektronisk identifiering och* elektroniska informationsutbyte**
	5 §[1]
	En myndighet ska tillhandahålla medel för elektronisk identifiering för den som tjänstgör vid eller innehar uppdrag för myndigheten och som för att kunna fullgöra sina arbetsuppgifter behöver styrka sin identitet eller tjänsteställning elektroniskt.
	Användning av en anställds eller uppdragstagares privatägda medel för elektronisk identifiering i tjänsten får endast ske
	1. för identifiering i samband med utfärdande medel för elektronisk identifiering som tillhandahålls av myndigheten,

[1] Tidigare 5 § upphävd genom 2018:360.

2. som kontinuitetslösning om medel för elektronisk identifiering som tillhandhålls av myndigheten inte är tillgänglig, eller

3. när arbetsuppgiften inte kan fullgöras med medel för elektronisk identifiering som tillhandahålls av myndigheten.

Med medel för elektronisk identifiering avses detsamma som i artikel 3.2 i 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, i den ursprungliga lydelsen.

Denna förordning träder i kraft den 1 januari 2024.

1.4 Förslag till förordning om ändring i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning

Härigenom föreskrivs att 18 § i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	18 §
Myndigheten får ta ut avgifter av de myndigheter som har anslutit sig till valfrihetssystem för säker elektronisk identifiering enligt 3 § 3 och för utbildningsverksamhet.	Myndigheten får ta ut avgifter *1.* av de myndigheter som har anslutit sig till valfrihetssystem för säker elektronisk identifiering enligt 3 § 3, *2. för sådan granskning av medel för elektronisk identifiering som avses i 6 § förordningen om erkännande av medel för elektronisk identifiering,* och *3.* för utbildningsverksamhet.

Denna förordning träder i kraft den 1 januari 2024.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 12 mars 2020 kommittédirektiv om att ge en särskild utredare i uppdrag att utreda förutsättningarna för ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen i syfte att höja säkerheten och stärka tilliten när betrodda tjänster används. Av utredningsdirektiven framgår att utredaren ska

- kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster,
- lämna förslag på sådana åtgärder, särskilt när det gäller att
  - tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen,
  - kunna validera och bevara elektroniska underskrifter, och
  - kunna använda e-legitimation i tjänsten, och
- lämna nödvändiga författningsförslag.

Regeringen beslutade den 17 december 2020 om tilläggsdirektiv. Av tilläggsdirektiven följer att den del av uppdraget som avser åtgärder för ökad och standardiserad användning av betrodda tjänster enligt punktuppställningen ovan, med undantag för strecksatsen om att kunna använda e-legitimation i tjänsten, ska redovisas senast den 15 februari 2021.

Resterande delar av uppdraget som framgår av utredningens ursprungliga direktiv ska enligt tilläggsdirektiven slutredovisas den 30 juni 2021.

Utredningens direktiv finns bifogade till betänkandet i bilaga 1 och 2.

2.2 Utredningens arbete

Utredningsarbetet påbörjades i slutet av mars 2020. Under utredningstiden har vi haft åtta sammanträden med expertgruppen. Till följd av den rådande pandemin har alla utredningens möten genomförts digitalt.

Utredningen överlämnade delbetänkandet *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9) den 15 februari 2021.

Den del av utredningens uppdrag som redovisas i detta betänkande omfattar kartläggning och analys av den offentliga förvaltningens behov av åtgärder avseende användning av e-legitimation i tjänsten samt förslag på sådana åtgärder.

En del av kartläggningsarbetet har bestått av att ta del av befintligt skriftligt underlag. En central källa i detta arbete har varit den s.k. e-legitimationsenkäten som Myndigheten för digital förvaltning (DIGG), Sveriges Kommuner och Regioner (SKR) samt Regeringskansliet genomförde 2019. DIGG och SKR har släppt varsin rapport baserat på resultatet av enkäten.[1] Uppgifter om relevanta behov och utmaningar har också inhämtats från andra skriftliga källor.[2]

För att komplettera det skriftliga underlaget har vi vidare haft ett 50-tal möten och samtal med aktörer i offentlig förvaltning samt med e-legitimationsutfärdare. Vad gäller frågan om användning av privat e-legitimation i tjänsten har vi även haft kontakter med arbetsgivarorganisationer och fackliga centralorganisationer.

I syfte att inhämta synpunkter från en bredare grupp av myndigheter och leverantörer har vi också under utredningstiden genomfört sammanlagt fem digitala möten med öppen anmälan. Vid det första mötet för representanter för offentlig förvaltning i maj 2020 medverkade ca 220 deltagare. Vid detta möte diskuterades bl.a. använd-

[1] DIGG, *E-legitimering inom den offentliga förvaltningen – Enkätundersökning 2019* (dnr 2019-389) och SKR, *Rapport enkät e-legitimationer – 2019 Kommuner och Regioner*, mars 2020.
[2] Bl.a. *reboot – omstart för den digitala förvaltningen (*SOU 2017:114), DIGG, *eID för medarbetare – Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte* (dnr 2019-582), 14 december 2020 och Inera, *IAM Strategi Med kommunernas behov i fokus*, 5 maj 2020.

ning av e-legitimation i tjänsten. Övriga möten har emellertid varit fokuserade på användning av betrodda tjänster.

Vi har enligt våra direktiv haft att beakta relevant arbete som bedrivs inom Regeringskansliet och utredningsväsendet samt särskilt beakta det arbete som bedrivs hos DIGG. Vi har under utredningstiden haft flera möten och kontakter med DIGG. Vi har även haft kontakt med flera statliga utredningar, däribland Cybersäkerhetsutredningen (Fö 2019:01), It-driftsutredningen (I 2019:03) och utredningen om e-recept inom EES (S 2020:10).

Vi har vidare enligt våra direktiv haft att undersöka och översiktligt redovisa hur de frågor som uppdraget omfattar hanteras i andra länder som är jämförbara med Sverige. I detta syfte har vi utöver en granskning av tillgängligt material på internet haft kontakter med myndighetsrepresentanter i vissa utvalda länder. Vi har vidare tagit del av den undersökning som genomfördes under 2020 av Nordic-Baltic co-operation on digital identities (NOBID).[3]

Vi har också presenterat vårt uppdrag för olika nätverk och arbetsgrupper.

2.3 Utredningens prioriteringar

I relation till den begränsade tid vi haft till förfogande har vi valt att prioritera frågor som enligt vår bedömning kan åstadkomma störst nytta för den offentliga förvaltningen som helhet.

2.4 Betänkandets disposition

I kapitel 3 definieras några för betänkandet centrala begrepp och termer.

I kapitel 4 redogörs för gällande rätt inom området.

Kapitel 5 innehåller en kronologisk översikt över användning av e-legitimation i tjänsten i Sverige.

I kapitel 6 redogörs för e-legitimationsområdet i Sverige.

I kapitel 7 presenterar vi resultatet av vår kartläggning av den offentliga förvaltningens behov avseende användning av e-legitimation i tjänsten.

Kapitel 8 innehåller en översiktlig internationell utblick.

[3] Hinsberg, Hille m.fl., *Study on Nordic-Baltic Trust Services*, 2020.

I kapitel 9 redogör vi för utredningens bedömningar och förslag.

I kapitel 10 redogör vi för konsekvenserna av våra förslag.

I kapitel 11 behandlas ikraftträdande och i kapitel 12 finns författningskommentarerna.

3 Definitioner av vissa centrala begrepp och termer

3.1 Identitet

Det finns inte någon legaldefinition av begreppet identitet. Vad gäller identitetsbegreppet som sådant kan det i vissa sammanhang ha en subjektiv dimension, exempelvis en persons självbild.[1] Det kan här även noteras att begreppet identitet också används i förhållande till objekt med koppling till t.ex. sakernas internet och robotiserade processer.[2] I detta betänkande avses emellertid med identitet endast viss information rörande en person som är att anse som objektiva fakta.

När det gäller vilken typ av information som kan hänföras till objektiva fakta om en person så avses identiteten vid prövning av en ansökan om beviljande av svenskt medborgarskap bestå av sökandens namn, födelsetid och, som huvudregel, medborgarskap.[3] Utöver dessa uppgifter framförde 2017 års ID-kortsutredning att även uppgift om bostadsadress kan hänföras till identitetsbegreppet.[4] Digitaliseringsrättsutredningen lyfte att det inom ramen för deras kartläggning framförts att andra unika identitetsmarkörer såsom biometriska uppgifter kan bli aktuella att använda i framtiden utöver personnummer.[5] Vi kan dock inte se att detta behov i dagsläget föreligger för e-legitimationer som används i tjänsten. Det som för utredningen är av relevans vad gäller en persons identitet är dennes namn och personidentifieringsuppgifter (se avsnitt 3.5). Utöver detta kan vissa attribut med koppling till en person vara av betydelse (se mer om attribut i avsnitt 3.15).

---

[1] *Id-kort för folkbokförda i Sverige* (SOU 2007:100), s. 25.
[2] Se t.ex. Inera, *IAM Strategi Med kommunernas behov i fokus*, 5 maj 2020, s. 8.
[3] Prop. 1997/98:178 s. 8 och MIG 2010:17.
[4] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 90.
[5] *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 76 f.

3.2 Personuppgift och personuppgiftsansvarig

Med personuppgifter avses enligt artikel 4.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), härefter kallad dataskyddsförordningen, varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsansvarig är enligt artikel 4.7 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

3.3 Pseudonymisering

Av artikel 4.5 i dataskyddsförordningen följer att pseudonymisering är behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person. Skillnaden mellan pseudonymisering och anonymisering är att det senare innebär att avidentifiering skett på ett sådant sätt att uppgifterna inte längre kan användas för att identifiera en specifik registrerad.[6]

[6] Skäl 26 i dataskyddsförordningens ingress.

3.4 Identitetshandling

En identitetshandling används för att en person ska kunna identifiera sig, eller styrka sin identitet. En identitetshandling är alltså ett dokument som innehåller vissa identitetsuppgifter, med vilket en person kan bevisa sin identitet.[7] Begreppet identitetshandling får enligt vår bedömning anses vara teknikneutralt och kan avse både en fysisk identitetshandling eller en e-legitimation.

3.5 Personidentifieringsuppgift m.m.

I artikel 3.3 i förordning (EU) 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, härefter kallad eIDAS-förordningen, definieras personidentifieringsuppgifter som en uppsättning uppgifter som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person. Det rör sig således bl.a. om identitetsbeteckningar för att identifiera en fysisk person och det kan exempelvis vara ett personnummer, samordningsnummer eller annan unik identifierare i form av exempelvis en tjänsteidentitet. Det kan här noteras att det inom EU pågår arbete med det som kallas för ”Self Sovereign Identity” (SSI). SSI bygger på tanken att individen själv skapar och har kontroll över sina attribut som används för att identifiera denne och delar med sig av de attribut som behövs för att använda en viss tjänst.[8]

De vanligaste personidentifieringsuppgifterna i Sverige för enskilda individer är personnummer och samordningsnummer. Personnummer är enligt 18 § folkbokföringslagen (1991:481) avsett att utgöra en identitetsbeteckning för varje folkbokförd person. Även om personen skulle avregistreras från folkbokföringen, exempelvis vid utflyttning, behåller personen sitt personnummer. Personnumret och den historiska informationen som är kopplad till detta finns kvar i folkbokföringsdatabasen. Personnummer består i dag av födelsetiden, som anges med sex siffror (ååmmdd), ett tresiffrigt födelsenummer

[7] *Id-kort för folkbokförda i Sverige* (SOU 2007:100), s. 25 och *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 90.
[8] Se mer om SSI i *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9), s. 75 f.

och en kontrollsiffra. Födelsenumret är udda för män och jämnt för kvinnor. Mellan födelsetiden och födelsenumret sätts ett bindestreck som byts ut mot ett plustecken när en person fyller 100 år.

Även personer som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall och som inte ska folkbokföras, tilldelas enligt 5 och 18 b §§ folkbokföringslagen ett personnummer om han eller hon har rätt att vistas i landet och uppfyller de allmänna kraven för folkbokföring.

Med anledning av att födelsenumren för vissa födelsetider tagit slut har det i 18 § tredje stycket folkbokföringslagen införts en möjlighet för Skatteverket att vid sådana förhållanden i stället ange födelsedagen med en närliggande dag i månaden.

För att tilltron till personnumret som identifikationsbegrepp skulle upprätthållas ansågs tilldelningen av personnummer behöva grundas på en identitetskontroll som uppfyllde höga anspråk på säkerhet. Det var därför även med hänsyn till att identiteten ofta var osäker för personer som fick personnummer utan att vara folkbokförda som det beslutades att personnummer skulle reserveras för de som folkbokfördes i landet. Risken för personförväxling och behovet av en säker kommunikation mellan myndigheter ansågs dock kräva en enhetlig personbeteckning även beträffande personer som inte är folkbokförda. För dessa personer skulle i stället fastställas en annan unik beteckning än personnummer och därför infördes samordningsnummer.[9]

Av 18 a § folkbokföringslagen följer att ett samordningsnummer tilldelas en person som inte är eller har varit folkbokförd efter begäran från en myndighet eller ett annat organ som regeringen bestämmer.

Skatteverket får enligt 5 § folkbokföringsförordningen (1991:749) tilldela samordningsnummer på begäran av en statlig myndighet eller en enskild utbildningsanordnare som har tillstånd att utfärda vissa examina enligt lagen (1993:792) om tillstånd att utfärda examina, och som i sin verksamhet behöver ett samordningsnummer för en person för att undvika personförväxling eller för att utbyta information om personen med andra myndigheter eller organisationer. Skatteverket får också på eget initiativ tilldela samordningsnummer för registrering i beskattningsdatabasen. Samordningsnummer får sedan den 18 juni 2021 enligt 18 a § folkbokföringslagen även efter

[9] Prop. 1997/98:9 s. 78 ff.

ansökan av enskild tilldelas personer som har en sådan anknytning till Sverige att denne kan antas behöva en identitetsbeteckning. Personen måste då inställa sig personligen hos Skatteverket och styrka sin identitet. I likhet med vad som gäller för personnummer är det viktigt att en persons identitet är klarlagd när han eller hon får ett samordningsnummer. Den enskildes identitet ska därför som huvudregel vara fastställd även för att denne ska kunna tilldelas ett samordningsnummer. Det organ som begär att en person ska tilldelas samordningsnummer har enligt 5 a och 5 b §§ folkbokföringsförordningen till uppgift att bedöma om hans eller hennes identitet kan anses fastställd. Även om det råder osäkerhet om en persons identitet, får samordningsnummer tilldelas för vissa angivna ändamål. Så är enligt 5 a § folkbokföringsförordningen exempelvis fallet när det gäller personer som ska registreras i beskattningsdatabasen och inom rättsväsendet. Ungefär hälften av alla personer som tilldelats samordningsnummer tillhör dessa grupper där någon identitet inte har fastställts.

Samordningsnumret är konstruerat som ett personnummer men med sifferkombinationer som inte kan förekomma i ett personnummer på så sätt att siffrorna för dag adderas med 60. Motsvarigheten till personnumrets födelsenummer benämns i samordningsnumret individnummer. Kontrollsiffran beräknas med samma metod som beträffande personnumret.

På motsvarande sätt som personnummer är samordningsnummer unika såtillvida att två identiska samordningsnummer inte förekommer. Om en person med ett samordningsnummer senare blir folkbokförd ersätts samordningsnumret med ett personnummer. Individens koppling till samordningsnumret finns emellertid kvar i registret.

I september 2019 tillsatte regeringen en utredning för att bl.a. föreslå åtgärder som åstadkommer ett säkrare system för samordningsnummer och ökar numrens användbarhet i samhället.[10] Uppdraget ska redovisas senast den 1 juli 2021.

I direktiven lyfter regeringen fram att det för majoriteten av tilldelade samordningsnummer råder en osäkerhet om den enskildes identitet och uppgifterna är därmed inte alltid pålitliga. Samtidigt kan vissa tilldelade samordningsnummer grunda sig på en fullgod identitetskontroll. Skillnaden i den kontroll som görs av de aktörer som begär ett samordningsnummer varierar och samhällets kunskap om

[10] Dir. 2019:54.

vilken identifiering som ligger till grund för ett samordningsnummer är bristfällig. Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden beskrev bl.a. att flera myndigheter uppmärksammat att falska uppgifter lämnas i syfte att få samordningsnummer som i sin tur kan leda till utbetalningar från välfärdssystemen. Även om ett samordningsnummer inte ger några rättigheter eller förmåner i sig, kan det finnas ett behov av numren t.ex. för handläggning av förmåner som ska betalas ut.[11] Utredningen om effektiv styrning av nationella digitala tjänster bedömde vidare att identitetskontrollen vid tilldelning av samordningsnummer inte är av den kvalitet som önskas för att samhällsfunktionerna ska kunna lita på att samordningsnummersystemet fungerar som det ska och att detta också påverkar folkbokföringens förmåga att upprätthålla god registerkvalitet.[12]

Personnummer och samordningsnummer utgör inte känsliga personuppgifter i dataskyddsförordningens mening, men behandlingen av dessa uppgifter omfattas genom nationell lagstiftning av särskilda villkor (se mer om detta i avsnitt 9.2.1).

3.6 Identifiering och autentisering

Av artikel 3.1 i eIDAS-förordningen framgår att elektronisk identifiering är 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.

I artikel 3.5 i eIDAS-förordningen definieras autentisering som 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. Svenska datatermgruppen definierar det som kontroll av uppgiven identitet, t.ex. vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelande mellan användare.[13] Internetstiftelsen å sin sida definierar autentisering som att helt enkelt kunna visa upp och styrka sin identitet för en annan part.[14]

[11] *Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra* (SOU 2017:37), s. 248 och s. 293.
[12] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 334.
[13] www.termado.com/DatatermSearch/?ss=autentisering (hämtad 2021-06-14).
[14] https://internetstiftelsen.se/guide/digitala-identiteter/ordlista/ (hämtad 2021-06-14).

Det förekommer flera olika metoder av autentisering. I samband med autentisering brukar det talas om en-, två- eller flerfaktorsautentisering. Användning av lösenord eller PIN-kod brukar ses som enfaktorsautentisering som baseras på något en person vet eller kan. Med dessa metoder går det egentligen bara att veta att lösenordet och PIN-koden används, men inte av vem, särskilt inte eftersom många personer använder samma lösenord till flera tjänster och att flera tjänster drabbats av intrång som har medfört åtkomst till lösenord. Tvåfaktorsautentisering kan vara en kombination av lösenord, dvs. något som personen kan med något som personen har, exempelvis ett smartkort eller en applikation i en mobiltelefon, alternativt i kombination med någon form av inloggning med biometrisk avläsning, t.ex. med fingeravtryck. Även andra autentiseringslösningar kan användas som koddosor, USB-stickor, engångslösenord via sms m.m.

En mer generell definition av tvåfaktors- eller flerfaktorsautentisering är autentisering där det krävs två respektive flera olika tekniska lösningar för att en användare ska kunna styrka sin identitet.[15]

Ett annat begrepp som förekommer med koppling till autentisering är stark autentisering. Det förekommer även reglering som ställer krav på stark autentisering eller flerfaktorsautentisering (se mer om detta i avsnitt 4.3). Med stark autentisering avses ofta kontroll av uppgiven identitet på två olika sätt.[16] Kommissionens nyligen lämnade förslag till ändringar i eIDAS-förordningen innehåller även en definition av stark autentisering.[17]

I 1 kap. 4 § lagen (2010:751) om betaltjänster definieras ”stark kundautentisering” som en autentisering som grundas på användning av två eller flera komponenter, kategoriserade som kunskap (något som bara användaren vet), innehav (något som bara användaren har) och unik egenskap (något som användaren är), som är fristående från varandra så att det förhållandet att någon har kommit över en av komponenterna inte äventyrar de andra komponenternas tillförlit-

[15] A.a.

[16] Se t.ex. definitionen av stark autentisering i 2 kap. Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

[17] I skrivande stund finns ingen officiell översättning av förslaget (COM(2021) 281 final) men i den engelska språkversionen definieras begreppet på följande sätt: ‘strong user authentication’ means an authentication based on the use of two or more elements categorised as user knowledge, possession and inherence that are independent, in such a way that the breach of one does not compromise the reliability of the others, and is designed in such a way to protect the confidentiality of the authentication data.

lighet, och som är utformad för att skydda autentiseringsuppgifterna mot obehörig åtkomst.

3.7 Förlitande part

I artikel 3.6 i eIDAS-förordningen definieras förlitande part som en fysisk eller juridisk person som förlitar sig på en elektronisk identifiering eller betrodda tjänster. Inom ramen för detta betänkande avser det framför allt aktörer som tillhandahåller e-tjänster.

3.8 E-legitimation

Begreppen e-legitimation och elektronisk identitetshandling förekommer inte eIDAS-förordningen. Där används i stället medel för elektronisk identifiering som i artikel 3.2 definieras som en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster.

Med begreppet e-legitimation avses en identitetshandling som kan användas för att identifiera innehavaren på elektronisk väg. Med hjälp av en e-legitimation kan innehavaren identifiera sig och myndigheter eller andra aktörer som har e-tjänster få en bekräftelse på vem personen är. En e-legitimation innehåller, liksom en fysisk identitetshandling, uppgifter som entydigt kan kopplas till en viss person.[18] Alla former av medel för elektronisk identifiering kan således inte anses utgöra en e-legitimation utan det krävs att det rör sig om en handling som har en både tydlig och säker koppling till innehavarens identitet. Detta sker vanligtvis, men inte uteslutande, genom en certifikatbaserad lösning.

En e-legitimation kan finnas som en applikation i en mobiltelefon eller surfplatta eller som en fil på en dator. Den kan också finnas på en fysisk bärare, såsom ett smartkort. Kortet innehåller då ett chip där informationen lagras.[19]

Utredningen om effektiv styrning av nationella digitala tjänster använde begreppet elektronisk identitetshandling i stället för e-legitimation. Anledningen var att en identitetshandling syftar till att visa en individs identitet och används för att kontrollera att individen är

[18] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 129.
[19] A.a.

den som han eller hon utger sig för att vara medan begreppet legitimation säger något om personens behörighet. Utredningen menade att begreppet e-legitimation är missvisande eftersom det antyder att det rör sig om uppgifter som utvisar både identitet och behörighet.[20] 2017 års ID-kortsutredning använde emellertid begreppet e-legitimation med motiveringen att det är ett inarbetat begrepp som bl.a. används i det tillitsramverk som DIGG ansvarar för och som gäller för det kvalitetsmärke som för närvarande benämns Svensk e-legitimation (se mer om tillitsramverket och kvalitetsmärket i avsnitt 6.3). Utredningen noterade vidare att det även är det begrepp som huvudsakligen används av de nuvarande svenska utfärdarna av e-legitimationer. Vi delar den bedömning som gjordes av 2017 års ID-kortsutredning och använder oss därför av begreppet e-legitimation.

Vad gäller författningstext är dock medel för elektronisk identifiering eller elektronisk identifiering de uttryck som används både i eIDAS-förordningen och nationella författningar. I författningsförslagen kommer därför dessa begrepp att användas i stället för e-legitimation eller e-tjänstelegitimation.

3.9 E-legitimation i tjänsten m.m.

Vad avser fysiska identitetshandlingar som används i tjänsten förekommer i allmänt språkbruk ofta begreppet tjänstelegitimation i kortform (”tjänsteleg”). I författning förekommer dock endast begreppet tjänstekort för de fysiska identitetshandlingar som utfärdas för medarbetare i offentlig sektor. Av 1 § förordningen (1958:272) om tjänstekort följer att tjänstekort får utfärdas för den som tjänstgör vid eller innehar uppdrag för statligt eller kommunalt organ och som för sina tjänsteåligganden regelmässigt behöver kunna styrka sin identitet eller tjänsteställning. Ett tjänstekort ska enligt 4 § samma förordning som huvudregel innehålla uppgifter om innehavarens namn och tjänst eller uppdrag och vara försett med ett välliknande fotografi av innehavaren och med hans eller hennes namnteckning. Uppgiften om namn ska vidare åtminstone omfatta efternamn och första bokstaven i tilltalsnamn. Ett tjänstekort får även innehålla uppgift om personnummer eller annat identifikationsnummer för innehavaren. På kortet ska det anges vilken myndighet som har utfärdat det, var

[20] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 171 f.

kontroll av kortet kan göras samt kortets nummer och giltighetstid. Av 13 § andra stycket i förordningen framgår att Polismyndigheten, efter samråd med Försvarsmakten, får meddela ytterligare föreskrifter om tjänstekort. Enligt 5 § Polismyndighetens föreskrifter och allmänna råd om tjänstekort (PMFS 2020:4) får tjänstekort förses med elektroniska egenskaper för att kortet ska fungera vid elektronisk identifiering och behörighetskontroll. Tjänstekort är vidare enligt 4 § Skatteverkets föreskrifter om identitetskort (SKVFS 2009:14) en godtagbar identitetshandling om det utfärdats av en svensk statlig myndighet eller om det är SIS-märkt.[21] Ett SIS-märkt tjänstekort innebär att det tillverkats av en licensierad tillverkare och utfärdats av en godkänd utfärdare enligt vissa standarder.[22]

Med e-legitimation i tjänsten avses i detta betänkande en e-legitimation som används för att fullgöra en arbetsuppgift. Det kan både röra sig om en privat e-legitimation eller en e-legitimation som anskaffats av arbetsgivaren.

Begreppet e-tjänstelegitimation användes bl.a. av E-delegationen och definierades då som en e-legitimation som knyts både till en organisation (med namn och organisationsnummer) och till en fysisk person (med namn och unik beteckning).[23] Även om begreppet kan föra tankarna till en legitimation som behövs för att använda en e-tjänst är det emellertid ett begrepp som tidigare använts och som enligt vår mening tydligt markerar att det rör sig om en e-legitimation med koppling till antingen en anställning eller ett uppdrag. Med e-tjänstelegitimation avses i detta betänkande således en e-legitimation för den som tjänstgör vid eller innehar uppdrag för en organisation och som anskaffats av organisationen. En e-tjänstelegitimation kan, men behöver inte nödvändigtvis, också innehålla uppgifter om användarens anställning och/eller behörighet, dvs. ytterligare uppgifter utöver identiteten. I DIGG:s förstudierapport används uttrycket ”eID för medarbetare” (se mer om förstudien i avsnitt 5.8.1). Medarbetare omfattar enligt DIGG:s definition utöver anställda även uppdragstagare, förtroendevalda, elever och andra som är knutna till en part som vill anskaffa e-legitimationer för sina målgruppers räkning.[24]

[21] SIS står för Svenska institutet för standarder.
[22] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 123 ff.
[23] *Strategi för myndigheternas arbete med e-förvaltning* (2009:86), s. 125 ff.
[24] DIGG, *eID för medarbetare – Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte* (dnr 2019-582), 14 december 2020, s. 3.

För en sammanfattning av hur begreppen ovan används inom ramen för detta betänkande se tabellen nedan.

Tabell 3.1 Vissa begrepp rörande e-legitimation i tjänsten

Begrepp	Definition
Tjänstekort	Fysisk identitetshandling för den som tjänstgör vid eller innehar uppdrag för statligt eller kommunalt organ och som kan förses med elektroniska egenskaper för att kortet ska fungera vid elektronisk identifiering och behörighetskontroll.
E-legitimation i tjänsten	En e-legitimation som används för att fullgöra en arbetsuppgift. Det kan både röra sig om en privat e-legitimation eller en e-legitimation som anskaffats av arbetsgivaren. Kan både finnas i en applikation eller på en fysisk bärare.
E-tjänstelegitimation	En e-legitimation för den som tjänstgör vid eller innehar uppdrag för en organisation och som anskaffats av organisationen. E-tjänstelegitimation kan utöver identitetsuppgifter även innehålla uppgifter om användarens anställning och/eller behörighet. Kan både finnas i en applikation eller på en fysisk bärare.

3.10 Grundidentifiering

En kontroll av en persons identitet syftar till att utreda om personen är den han eller hon utger sig för att vara, här vanligen i samband med ansökan om en e-legitimation. Identitetskontrollen kan bestå av två delar. Det kan vara fråga om att göra en kontroll av att vissa uppgivna personuppgifter verkligen utgör en identitet och att uppgifterna inte är falska. En sådan kontroll görs som regel genom slagning i officiella register. Det kan också handla om att kontrollera om en viss fysisk person stämmer överens med en viss (registrerad) identitet, dvs. vissa personuppgifter. Den sistnämnda kontrollen kan göras genom en jämförelse mellan en person och en identitetshandling.[25] En felaktig id-handling kan vara oriktig på i huvudsak två olika sätt. Dels kan det vara fråga om att innehavaren (eller annan) tillverkat en falsk handling eller ändrat en id-handlings ursprungliga, riktiga, personuppgifter och ersatt dessa med falska uppgifter. Dels kan det vara fråga om att innehavaren (eller annan) uppgett oriktiga uppgifter vid utfärdandet av id-handlingen, som då i och för sig är riktigt utfärdad men innehåller felaktiga uppgifter.[26] Det senare kan

[25] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 90.
[26] *Id-kort för folkbokförda i Sverige* (SOU 2007:100), s. 25 f.

således ske i samband med det som kallas för grundidentifiering, dvs. den identitetskontroll som sker i samband med utfärdandet av en id-handling.

Utredningen om effektiv styrning av nationella digitala tjänster analyserade några av de befintliga grundidentifieringsprocesserna.[27] Av genomgången framgick att processerna skilde sig åt och att olika krav ställs inför utfärdande av olika identitetshandlingar. Detta gällde såväl för de fysiska identitetshandlingar som staten respektive privata aktörer utfärdade som för e-legitimationer.[28]

I nästan alla processer gällde att individen ska styrka sin identitet. Då handlade det om att sammanföra registrerade uppgifter om en viss individ med en viss fysisk person. Med registrerade uppgifter avsågs framför allt sådana uppgifter som framgår av folkbokföringsregistret. Sättet som individen kunde styrka sin identitet på skilde sig åt. Hade individen redan en viss sorts identitetshandling var den ofta tillräcklig för att styrka identiteten. Om individen saknade en identitetshandling av visst bestämt slag krävdes att andra personer med vissa närmare angivna kopplingar till individen intygade dennes identitet.[29]

Det som skilde de olika identitetshandlingarna åt var primärt ansöknings- och utlämnandeprocessen. Där ställdes i många fall krav på att individen ska inställa sig personligen hos den utfärdande aktören vid såväl ansökan som utlämnande. I vissa fall fanns det dock inga sådana krav, exempelvis var det möjligt att hämta ut ett körkort via ett postombud.[30] Ytterligare en skillnad var hur uppgifter om individen dokumenteras, dvs. i vissa fall ansvarade utfärdaren för att fotografera eller ta fingeravtryck av individen, i andra fall kunde individen ta med sig eller skicka in ett fotografi som hade tagits av annan men som ofta skulle uppfylla vissa kriterier.

Utredningen bedömde att det inte är alla processer som leder fram till identitetshandlingar som grundar sig på utförd grundidentifiering. För att en process ska innehålla grundidentifiering bedömde

[27] 6 § passlagen (1978:302), 3 § andra stycket förordningen (2005:661) om nationellt identitetskort, 2 § lagen (2015:899) om identitetskort för folkbokförda i Sverige, 3 kap. 15 § körkortsförordningen (1998:980) samt processen vid utfärdande av BankID.
[28] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 173 ff.
[29] Skatteverkets föreskrifter om identitetskort, SKVFS 2009:14 och Rikspolisstyrelsens föreskrifter och allmänna råd om polismyndigheternas hantering av pass och nationellt identitetskort, RPSFS 2009:14, FAP 530-1.
[30] 8 kap. 3 § körkortsförordningen (1998:980) samt Transportstyrelsens föreskrifter om utlämnande av körkort, TSFS 2014:17.

utredningen att vissa styrande principer skulle vara uppfyllda. Dessa principer var att:

- ansökan om en identitetshandling måste göras vid ett personligt besök hos den utfärdande aktören,
- individen ska styrka sin identitet på ett tillförlitligt sätt,
- den utfärdande aktören ansvarar för att dokumentera fysiska kännetecken genom att åtminstone ta ett fotografi av individen, och
- identitetshandlingen ska lämnas ut vid ett personligt besök hos utfärdaren.[31]

3.11 Identitetsintygsutfärdare och identitetsintyg

Identitetsintygsutfärdare är den som utfärdar identitetsintyg. Ett identitetsintyg är ett av en identitetsintygsutfärdare utställt intyg i elektronisk form med uppgifter om en användares identitet och eventuella attribut.[32] Identitetsintyget kan endast användas vid ett tillfälle. Utfärdande av identitetsintyg sker ibland av e-legitimationsutfärdaren, men det förekommer också att identitetsintyget utfärdas av en separat identitetsintygsutfärdare.

3.12 Identitetsfederation m.m.

En identitetsfederation kan antingen syfta till att undvika att en förlitande part måste sluta bilaterala avtal med varje e-legitimationsutfärdare alternativt komplettera de elektroniska identitetshandlingarna med tjänster för ett säkert utbyte av rollbaserade behörighetsstyrande attribut åt federationens e-tjänster. Ytterligare ett syfte med en identitetsfederation är att utbyta teknisk och administrativ information om förlitande parter och identitetsintygsutfärdare på ett säkert och effektivt sätt. En identitetsfederationen innebär alltså att en aktör utses som ansvarig för federationen (federationsoperatör), och att varje aktör som vill ansluta sig till federationen måste följa ett uppställt regelverk – såväl tekniskt som tillitsbaserat – samt åtar sig att genomgå prövning och granskning med avseende på säker-

[31] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 175 ff.
[32] *E-legitimationsnämnden och Svensk e-legitimation* (SOU 2010:104), s. 173.

het och uppfyllelse av uppställda regelverk.[33] Vad som innefattas i detta åtagande och ansvar kan dock variera mellan olika federationer med hänsyn till federationens syfte, vilka aktörer som kan ansluta sig till federationen samt respektive sektors behov och regelverk. Som gemensam nämnare finns emellertid alltid att det i en federativ lösning finns en tredje part som skapar en grund för tillit och effektiviserar administrationen mellan parterna. Identitetsfederationer behandlas ytterligare i avsnitt 6.6.

En interfederation är en överenskommelse mellan två eller flera federationsoperatörer som ingår i ett förbund för att sammansluta federationerna. Interfederation äger rum när en användare från en federation får åtkomst till en tjänst som är registrerad i en annan federation[34].

I detta sammanhang bör även den engelska termen ”identity broker/ID-broker” nämnas. Någon allmänt vedertagen svensk översättning av termen finns inte. Denna funktion är dock lik den som en identitetsfederation uppfyller fast i formen av en kommersiell tjänst där en part via ett och samma tekniska gränssnitt kopplar samman förlitande parter med flera olika e-legitimationsutfärdare och därigenom möjliggör för användare att nyttja sin e-legitimation i de anslutna tjänsterna.

3.13 Id-växling

Med id-växling avses i betänkandet när en e-legitimation som utfärdas efter en grundidentifiering kan utgöra underlag vid utfärdande av andra e-legitimationer.[35] Id-växling kan emellertid också förekomma i andra sammanhang.

3.14 Behörighet och befogenhet

De juridiska begreppen behörighet och befogenhet och den s.k. fullmaktsläran har sin grund i lagen (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område (avtalslagen), men har

[33] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 270.
[34] Enligt Skolverkets ordlista från konferensen tekniksnack om digitala nationella prov, https://www.skolverket.se/download/18.6b138470170af6ce9141f6/1583847378476/Ordlista%20Skolverkets%20tekniksnack.pdf.
[35] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 321.

även relevans utanför det civilrättsliga området. Skillnaden mellan dessa begrepp brukar förenklat beskrivas som att behörighet betecknar vad en fullmäktig kan göra och befogenhet vad en fullmäktig får göra.[36]

Av 10 § andra stycket avtalslagen följer att där någon såsom anställd i annans tjänst eller eljest i följd av avtal med annan intager en ställning, varmed enligt lag eller sedvänja följer viss behörighet att handla å dennes vägnar, anses han hava fullmakt att företaga rättshandlingar, som falla inom gränserna för denna behörighet. Detta kallas för en ställningsfullmakt. Även en anställd eller uppdragstagare inom den offentliga förvaltningen som inte har behörighet att företa sådana rättshandlingar som avses i avtalslagen har inom ramen för dennes anställning eller uppdrag behörighet att utföra olika åtgärder eller ta del av viss information. Med behörighet avses således vad medarbetaren eller uppdragstagaren kan göra och befogenheten är vad denne person får göra. En sådan behörighet kan också vara kopplad till en kvalifikation man har, exempelvis att en person är licensierad sjuksköterska. En offentliganställd som överskrider sin behörighet eller befogenhet kan drabbas av olika påföljder.[37]

3.15 Attribut

Med attribut avses i relation till e-legitimationer uppgifter om exempelvis behörighet, uppdrag, roll eller andra egenskaper, som i traditionell miljö lämnas genom att visa upp en legitimation eller ge in registreringsbevis, fullmakter eller liknande handlingar. Det kan vara fråga om sådana attribut som t.ex. behörighet att agera för en juridisk persons räkning i egenskap av ställföreträdare eller fullmäktig, en särskild roll såsom lärare, läkare eller sjuksköterska eller någon annan uppgift av betydelse om en individ, t.ex. uppgift om anställning inom visst företag eller visst uppdrag för en angiven huvudman. Attribut kan vara ett eller flera och kan innehålla vilken information

[36] Grönfors, Kurt, Dotevall, Rolf, *Avtalslagen En kommentar*, JUNO Version: 5A, Kommentar till 2 kap. 10 § första stycket avtalslagen.
[37] Se t.ex. *När makten gör fel – Den offentliga tjänstemannens ställning och ansvar* (SOU 1996:173).

som helst.[38] Kommissionens nyligen lämnade förslag till ändringar i eIDAS-förordningen innehåller även en definition av attribut.[39]

3.16 Organisationstillit

Mottagande av handlingar eller åtkomst till system eller uppgifter som sker mellan myndigheter behöver inte innebära att någon autentisering av enskild medarbetare sker eller någon kontroll av dennes rätta behörighet eller befogenhet. Det brukar benämnas som organisationstillit. Det var E-delegationen som etablerade denna princip i syfte att effektivisera arbetet med informationsutbyte mellan offentliga aktörer. Principen bygger på att det vid informationsutbyte inom ramen för myndigheternas samverkans- och serviceskyldighet räcker att kontrollera att den andra parten är den myndighet som den uppger sig vara, eftersom en myndighet vanligtvis kan lita på att en handläggare som agerar för en annan myndighets räkning är behörig att företräda myndigheten.[40]

[38] *E-legitimationsnämnden och Svensk e-legitimation* (SOU 2010:104), s. 26 och 37 f.
[39] I skrivande stund finns ingen officiell översättning av förslaget (COM(2021) 281 final) men i den engelska språkversionen definieras begreppet på följande sätt: 'attribute' is a feature, characteristic or quality of a natural or legal person or of an entity, in electronic form.
[40] eSam, *En effektiv informationsförsörjning*, juni 2017, s. 63.

4 Gällande rätt

4.1 Inledning

Användningen av e-legitimationer är i dag omfattande i Sverige och de används bl.a. inom och i kontakter med den offentliga förvaltningen. Utredningen om effektiv styrning av nationella digitala tjänster bedömde att området för elektronisk identifiering är underreglerat.[1] Med undantag för eIDAS-förordningen och dess kompletterande bestämmelser finns det inga författningar som direkt reglerar e-legitimationer. Vi har inte heller identifierat några svenska lagar eller förordningar som uttryckligen föreskriver att e-legitimationer måste användas. Däremot finns det bestämmelser i myndighetsföreskrifter avseende användning av e-legitimationer.[2] De krav som finns gällande autentisering (se avsnitt 4.3) är emellertid en tydlig drivkraft bakom den ökade användningen av e-legitimationer.

Utöver bestämmelser som på olika sätt har koppling till användning av e-legitimationer finns det författningar och nyligen lämnade författningsförslag som rör anskaffning av tjänster för elektronisk identifiering. Vi redogör för dessa bestämmelser i avsnitt 6.5.4.

4.2 eIDAS-förordningen

4.2.1 Bestämmelser om elektronisk identifiering

Inom EU finns bestämmelser om elektronisk identifiering i eIDAS-förordningen. Förordningen innehåller även bestämmelser om betrodda tjänster, dessa kommer emellertid inte att beröras ytterligare

[1] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114) s. 170.
[2] Se exempelvis 3 § Lantmäteriets föreskrifter om digital ansökan i inskrivningsärenden (LMFS 2017:4) och 4 § Patent- och registreringsverkets föreskrifter om elektronisk varumärkesansökan (PRVFS 2011:3 V:9).

i detta betänkande.[3] I detta avsnitt följer en redogörelse över de bestämmelser i förordningen som vi anser är av relevans för området e-legitimation i tjänsten. Det är inte en fullständig redogörelse för förordningens bestämmelser om elektronisk identifiering.

Förordningens syfte vad gäller elektronisk identifiering är att säkerställa en väl fungerande inre marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering. Medel för elektronisk identifiering definieras i artikel 3.2 som en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster. E-legitimationer är ett medel för elektronisk identifiering och vi använder oss för enkelhetens skull i det fortsatta av begreppet e-legitimationer i möjligaste mån. Det kan dock inte uteslutas att medel för elektronisk identifiering omfattar även andra lösningar för autentisering än e-legitimationer.

I förordningen används vidare termen system för elektronisk identifiering, som i artikel 3.4 definieras som ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person. I det fortsatta kallar vi dessa system för e-legitimationssystem för att inte göra texten onödigt svårläst.

Förordningen reglerar vad som gäller när e-legitimationer används över landsgränserna inom EU genom att dels ställa krav på e-legitimationerna, dels ställa krav på medlemsstaterna att erkänna e-legitimationer från andra medlemsstater. Förordningen gäller enligt artikel 2.1 e-legitimationssystem som har anmälts av en medlemsstat och enligt skäl 12 i förordningens ingress syftar förordningen till att undanröja hinder för gränsöverskridande användning av e-legitimationer som används i medlemsstaterna för autentisering för åtminstone offentliga tjänster. Däremot är syftet med förordningen enligt samma skältext inte att ingripa i fråga om e-legitimationssystem och tillhörande infrastrukturer som inrättats i medlemsstaterna. Förordningen ska således inte tolkas som att den ställer krav på e-legitimationer som endast används nationellt, kraven på legitimationerna aktualiseras först när de ska användas över landsgränserna.

[3] Betrodda tjänster behandlas i delbetänkandet *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9).

4.2.2 Anmälan av e-legitimationssystem för gränsöverskridande användning

För att e-legitimationer ska kunna användas i andra medlemsstater krävs att medlemsstaten där e-legitimationen har sitt ursprung har anmält det aktuella e-legitimationssystemet. Ett system får anmälas om det uppfyller ett antal krav som föreskrivs i artikel 7 i förordningen.[4] Det är endast medlemsstater som kan anmäla system, men det behöver inte vara medlemsstaten som utfärdar e-legitimationerna i systemet. E-legitimationerna kan vara utfärdade av den anmälande medlemsstaten, på uppdrag av den anmälande medlemsstaten eller oberoende av den anmälande medlemsstaten men erkännas av medlemsstaten.

En anmälan delas in i tre steg. Det första steget är s.k. föranmälan. Under detta steg förser den anmälande medlemsstaten andra medlemsstater med information om det system som anmäls. Nästa steg är ett ”peer review”-steg. Under detta steg granskas kvaliteten och säkerheten i det anmälda systemet utifrån kraven i eIDAS-förordningen och aktuell genomförandeförordning. Det sista steget är formell anmälan och publicering i EU:s officiella tidning. I skrivande stund har 14 medlemsstater anmält ett eller flera e-legitimationssystem.[5] Ytterligare medlemsstater har föranmält e-legitimationssystem, däribland Sverige som gjorde en föranmälan i december 2020.

Med anmälan av e-legitimationssystem följer ansvar för medlemsstaten. Om säkerhetsincidenter inträffar, exempelvis intrång, som påverkar tillförlitligheten i systemets gränsöverskridande autentisering ska den anmälande medlemsstaten enligt artikel 10.1 utan dröjsmål tillfälligt upphäva eller återkalla den gränsöverskridande autentiseringen eller de berörda utsatta delarna i systemet samt informera andra medlemsstater och kommissionen. Medlemsstaten åläggs enligt artikel 11.1 även skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla vissa skyldigheter. Skyldigheterna relaterar bl.a. till att medlemsstaten ska se till att den aktuella fysiska eller juridiska personen tillskrivs de personidentifieringsuppgifter som unikt representerar personen.

[4] Se mer i *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 280 f.
[5] https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS (hämtad 2021-06-13).

Enligt artikel 7 e ska den part som utfärdar e-legitimationer inom ett anmält system se till att legitimationerna tilldelas rätt person i enlighet med de tekniska specifikationer, standarder och förfaranden som gäller för den relevanta tillitsnivån. Om utfärdaren avsiktligt eller på grund av oaktsamhet genom underlåtenhet inte uppfyller denna skyldighet är utfärdaren enligt artikel 11.2 ansvarig för skada som åsamkats en fysisk eller juridisk person vid en gränsöverskridande transaktion.

4.2.3 Förordningens tre tillitsnivåer

Förordningen fastställer tre tillitsnivåer för de e-legitimationer som utfärdats inom ett e-legitimationssystem: låg, väsentlig och hög. Tillitsnivåerna bör enligt skäl 16 i förordningens ingress återge graden av tillit till en e-legitimation vid fastställande av en persons identitet och skapa visshet om att den person som gör anspråk på en viss identitet faktiskt är den person som har tilldelats denna identitet. Tillitsnivån låg ska ge en begränsad grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet och nivån väsentlig ska ge en väsentlig grad av tillförlitlighet. Tillitsnivån hög ska ge en högre grad av tillförlitlighet än tillitsnivån väsentlig avseende en persons påstådda eller styrkta identitet.

Vår bedömning är att tillitsnivåerna genom förordningen är fullharmoniserade vid gränsöverskridande användning av e-legitimationer. Detta mot bakgrund av förordningens syfte att undanröja hinder för gränsöverskridande användning av e-legitimationer som används i medlemsstaterna för autentisering för åtminstone offentliga tjänster. Förordningen ger inte uttryck för att medlemsstaterna har möjlighet att ställa andra krav på tillit för tillgång till sina nättjänster vid gränsöverskridande autentisering. Som framgår av avsnitt 4.2.1 syftar förordningen inte till att ingripa i fråga om e-legitimationssystem och tillhörande infrastrukturer som inrättats i medlemsstaterna. Det är när e-legitimationer som ingår i systemen ska användas över gränserna som förordningens bestämmelser aktualiseras. Det bör därmed vara möjligt för medlemsstaterna att t.ex. tillämpa nationella tillits-

nivåer, något förordningen för övrigt tar höjd för.[6] Dessa bör emellertid i så fall endast kunna tillämpas vid nationell användning av e-legitimationer.

Enligt skäl 16 i förordningens ingress beror tillitsnivån på den grad av tillit en e-legitimation ger i fråga om en persons påstådda eller styrkta identitet med beaktande av olika processer (t.ex. styrkande och kontroll av identitet, och autentisering), förvaltningsverksamhet (t.ex. den enhet som utfärdar e-legitimationer och förfaranden för att utfärda sådana medel) och de tekniska kontroller som tillämpas. I kommissionens genomförandeförordning (EU) 2015/1502 fastställs tekniska minimispecifikationer och förfaranden för respektive tillitsnivå. Dessa ska användas för att specificera tillitsnivån för e-legitimationer som utfärdats inom ett anmält e-legitimationssystem. Specifikationerna och förfarandena bygger på den internationella standarden ISO/IEC 29115.[7] Utöver de delar som nämns ovan avser de bl.a. också krav på effektiva ledningssystem för informationssäkerhet.

4.2.4 Den offentliga förvaltningen ska erkänna utländska e-legitimationer

För att uppnå förordningens syfte innehåller den bestämmelser om s.k. ömsesidigt erkännande av e-legitimationssystem. Det kan kortfattat beskrivas som att medlemsstaterna ska erkänna varandras anmälda system. I artikel 6 i förordningen föreskrivs att när det enligt nationell rätt eller enligt nationella administrativa förfaranden krävs elektronisk identifiering där e-legitimationer och autentisering används för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ i en medlemsstat, ska de e-legitimationer som utfärdats i en annan medlemsstat erkännas i den första medlemsstaten för gränsöverskridande autentisering för tjänsten. Nättjänst definieras inte i förordningen men tjänster som vi i Sverige kallar e-tjänster omfattas. För att ömsesidigt erkännande ska bli aktuellt krävs dock

[6] Artikel 12 i förordningen rör samarbete och interoperabilitet och där föreskrivs vad interoperabilitetsramverket ska bestå av. Enligt artikel 12.4 b ska ramverket bl.a. bestå av sammankoppling av nationella tillitsnivåer för anmälda system för elektronisk identifiering med tillitsnivåerna enligt i förordningen.

[7] ISO står för International Organization for Standardization och IEC International Electrotechnical Commission. Båda är standardiseringsorgan. Se mer om dessa organ i *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9), s. 111.

att tre förutsättningar är uppfyllda. E-legitimationen ska vara utfärdad inom ramen för ett anmält e-legitimationssystem. Tillitsnivån för e-legitimationen ska motsvara en tillitsnivå som är lika hög eller högre än den tillitsnivå som det berörda offentliga organet kräver för åtkomst till nättjänsten, förutsatt att tillitsnivån för e-legitimationen motsvarar tillitsnivån väsentlig eller hög. Den sista förutsättningen är att det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten.

Förordningens krav på ömsesidigt erkännande gäller inte för e-legitimationer på tillitsnivå låg eller för nättjänster som använder tillitsnivå låg för åtkomst. För anmälda e-legitimationer som motsvarar tillitsnivån låg gäller i stället att dessa får erkännas av det offentliga organ som tillhandahåller nättjänsten, men det är inget krav.

Erkännandet av e-legitimationssystem ska ske senast tolv månader efter det att kommissionen offentliggör förteckningen över anmälda system. Det kan i sammanhanget noteras att trots kravet på erkännande av anmälda medel för elektronisk identifiering innebär det inte att den som loggat in på detta sätt i praktiken alltid har möjlighet att använda tjänsterna.[8] Det är vanligt att den som använder en utländsk e-legitimation för att logga in i en svensk e-tjänst i dagsläget hamnar i ett s.k. digitalt väntrum där det inte går att utföra det förfarande tjänsten avser. Det kan dock för vissa e-tjänster komma att förändras i och med att EU-förordningen (EU) 2018/1724 om en gemensam digital ingång[9] börjar tillämpas, härefter kallad EU:s förordning om en gemensam digital ingång.[10]

4.2.5 Översyn av eIDAS-förordningen

Kommissionen presenterade den 3 juni 2021 ett förslag till ändringar i eIDAS-förordningen.[11] De föreslagna ändringarna av förordningen består dels av att nuvarande bestämmelser ändras eller tas bort, dels av helt nya bestämmelser. Ändringarna avser både elektronisk iden-

[8] Skatteverket, *Fördjupad utredning rörande koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar*, 21 januari 2019, s. 31.
[9] Europaparlamentets och rådets förordning (EU) 2018/1724 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012.
[10] Förordningen innehåller bl.a. krav som avser gränsöverskridande tillgång till onlineförfaranden (artikel 13).
[11] COM(2021) 281 final.

tifiering och betrodda tjänster. I detta avsnitt redogör vi kortfattat för valda delar av förslaget.

Vad gäller elektronisk identifiering föreslår kommissionen att det ska införas en europeisk digital identitetsplånbok (”European Digital Identity Wallet”). Det är enligt definitionen en produkt och en tjänst som låter användaren spara identitetsuppgifter och attribut rörande t.ex. kvalifikationer samt attribut som är kopplade till användarens identitet. Enligt förslaget ska medlemsstaterna utfärda plånböckerna till fysiska och juridiska personer. De kan också utfärdas på uppdrag av medlemsstaterna eller självständigt, men erkännas av medlemsstaterna (jfr artikel 7 a i eIDAS-förordningen avseende e-legitimationssystem). Plånböckerna ska accepteras av medlemsstaterna för åtkomst till nättjänster som tillhandahållas av myndigheter. Privata förlitande parter inom vissa utpekade sektorer ska också acceptera dem för åtkomst till sina e-tjänster, under förutsättning att tjänsten omfattas av krav på att använda stark autentisering. Enligt skäl 9 i förordningsförslagets ingress kan plånböckerna användas för institutionella behov hos bl.a. offentliga förvaltningar och internationella organisationer. Det går emellertid inte i nuläget att bedöma om plånböckerna kan möta de behov vi har identifierat avseende användning av e-legitimation i tjänsten (se mer om behoven i kapitel 7).

Vidare föreslår kommissionen ändringar kopplade till anmälan av system för elektronisk identifiering. Sådana system kan certifieras av offentliga eller privata organ som har utpekats av medlemsstaterna. De behöver då inte gå igenom peer review-processen, som förordningen i dagsläget förutsätter.

När det gäller betrodda tjänster föreslår kommissionen en utökning av de tjänster som ska anses utgöra betrodda tjänster.

4.3 Krav avseende autentisering

4.3.1 EU:s allmänna dataskyddsförordning

Dataskyddsförordningen och dess bestämmelser om behandling av personuppgifter driver enligt vår uppfattning på användningen av e-legitimationer. Förordningen föreskriver under vilka förutsättningar personuppgifter får behandlas samt principer som ska gälla vid sådan behandling. I artikel 5.1 f föreskrivs principen om integritet och konfidentialitet som innebär att personuppgifterna ska behandlas på

ett sätt som säkerställer lämplig säkerhet för uppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder. Vidare ska enligt artikel 32 personuppgiftsansvariga och personuppgiftsbiträden vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå i samband med behandling av personuppgifter.

Säkerhetsnivån ska vara lämplig i förhållande till risken för personuppgiftsincidenter. Enligt ett onlineverktyg för att bedöma säkerhet för behandling av personuppgifter som EU:s cybersäkerhetsbyrå (ENISA) tillhandahåller är tvåfaktorsautentisering att föredra för tillgång till system som behandlar personuppgifter, om risken bedöms vara hög.[12]

Behandling av särskilda kategorier av personuppgifter, s.k. känsliga personuppgifter, är som huvudregel enligt artikel 9.1 i förordningen förbjuden men får ske under vissa förutsättningar. Integritetsskyddsmyndigheten (IMY) har uttalat att all digital kommunikation av integritetskänsliga personuppgifter, t.ex. uppgifter om skulder, hälsa och lagöverträdelser, generellt kräver krypterad överföring samt att mottagare autentiseras med stark autentisering.[13] Detta har också bekräftats i ett flertal tillsynsbeslut där IMY har konstaterat att känsliga personuppgifter måste skyddas av stark autentisering.[14] IMY har vidare uttalat att exempelvis e-legitimationer kan användas för att uppnå stark autentisering.[15]

4.3.2 Bestämmelser om säkerhetsskydd

Säkerhetsskyddslagens (2018:585) tillämpningsområde omfattar enligt 1 kap. 1 § första stycket den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet).

Säkerhetspolisen har med stöd av delegation i säkerhetsskyddsförordningen (2018:658) utfärdat föreskrifter om säkerhetsskydd (PMFS 2019:2). I 4 kap. regleras informationssäkerhet i informations-

[12] www.enisa.europa.eu/risk-level-tool/help (hämtad 2021-06-13).
[13] www.imy.se/lagar--regler/inkassolagen/digitala-inkassokrav/ (hämtad 2021-06-13).
[14] Se exempelvis Datainspektionens beslut den 27 februari 2016 (dnr 1805-2015).
[15] Datainspektionens beslut den 18 november 2015 (dnr 2445-201)4.

system. Av 4 kap. 12 § följer att alla utställda identiteter i ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara unika över tid. Åtkomsten ska vara spårbar till individ, system eller resurs. Vad gäller autentisering ska verksamhetsutövaren enligt 4 kap. 14 § se till att autentisering vid åtkomst till informationssystem som har betydelse för säkerhetskänslig verksamhet baseras på flera faktorer (flerfaktorsautentisering). Vidare ska verksamhetsutövaren enligt 4 kap. 15 § fastställa tekniska eller administrativa regler för utformning, byte och hantering av lösenord, om sådana används för att ge tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet. Reglerna ska bl.a. innehålla bestämmelser om återanvändning av lösenord samt lösenordens längd och komplexitet.

Verksamhetsutövaren ska även enligt 4 kap. 16 § ge kod eller lösenord som ger tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet ett säkerhetsskydd som motsvarar det säkerhetsskydd som informationssystemet ska ha enligt skyddsdimensioneringen. Vid användning av central funktion för identifiering eller behörighetskontroll, ska verksamhetsutövaren därtill enligt 4 kap. 17 § se till att denna funktion ges ett säkerhetsskydd som motsvarar det högsta säkerhetsskydd som de anslutna informationssystemen ska ha enligt skyddsdimensioneringen.

4.3.3 Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter

Av Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7) framgår av 4 kap. 5 § att flerfaktorsautentisering ska användas vid

1. egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk,
2. systemadministrativ åtkomst till informationssystem, och
3. åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd.

Av 4 kap. 6 § följer att myndigheten ska ha interna regler för hantering av autentiseringsuppgifter med krav på

1. längd och komplexitet,
2. när byte ska ske,
3. hur distribution ska ske, och
4. hur autentiseringsuppgifterna ska skyddas.

För de myndigheter som har ett särskilt ansvar för krisberedskapen enligt 10 § förordning (2015:1052) om krisberedskap och bevakningsansvariga följer av 5 kap. 1 § att dessa myndigheters åtgärder vid höjd beredskap ska, utöver vad som framgår av bl.a. 4 kap. i föreskrifterna använda flerfaktorsautentisering och realtidsövervakning för informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag.

4.3.4 Krav rörande autentisering inom hälso- och sjukvården

Av 3 kap. 15 § Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) följer att om vårdgivaren använder öppna nät vid behandling av personuppgifter, ska denne bl.a. ansvara för att elektronisk åtkomst eller direktåtkomst till uppgifterna föregås av stark autentisering.

I Handbok vid tillämpningen av HSLF-FS 2016:40 konstaterar Socialstyrelsen att användning av en e-legitimation är en etablerad metod för stark autentisering.[16]

4.3.5 Krav rörande autentisering i den finansiella sektorn

Sedan den 14 september 2019 finns regler om stark kundautentisering inom EU. Reglerna innebär i korthet att det krävs att man autentiserar sig med säkra metoder när man loggar in på sitt betalkonto online, initierar en elektronisk betalningstransaktion, eller genomför någon betalkontoåtgärd på distans som kan innebära en

[16] Socialstyrelsen, *Journalföring och behandling av personuppgifter i hälso- och sjukvården Handbok vid tillämpningen av Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården*, mars 2017, s. 26.

risk för s.k. svikligt förfarande, dvs. bedrägeri eller andra former av missbruk.

Reglerna om stark kundautentisering följer av 5 b kap. 4 § lagen (2010:751) om betaltjänster och kommissionens tekniska standarder för sträng kundautentisering och säker kommunikation (RTS(EU)2018/389). Dessa tekniska standarder är en del av genomförandet av det andra betaltjänstdirektivet.[17]

[17] Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG.

5 E-legitimation i tjänsten inom den offentliga förvaltningen – en kronologisk översikt

5.1 Inledning

Det har sedan 90-talet funnits flera utredningar, rapporter, projekt och initiativ som på olika sätt berört frågor med koppling till e-legitimation i tjänsten. Inom ramen för detta kapitel kommer den kronologiska översikten dock att ta avstamp i E-delegationens arbete som påbörjades 2009. Specifika e-tjänstelegitimationer som tagits fram inom den offentliga förvaltningen berörs inte nedan. Dessa redogörs i stället för i kapitel 6.

5.2 E-delegationen

E-delegationen var en expertgrupp inom e-förvaltning som bedrev sitt arbete mellan 2009–2015 och som bl.a. hade i uppdrag att utforma en strategi för myndigheternas arbete med e-förvaltning vilket innefattade hur den offentliga sektorns försörjning av e-legitimationer bör genomföras i framtiden.[1]

I E-delegationens första betänkande från 2009 berördes frågan om e-tjänstelegitimationer. Delegationen konstaterade då att det hade gjorts flera försök att få e-tjänstelegitimationer att fungera på ett samordnat sätt inom myndigheter och företag men att det hade visat sig svårt att enas kring begrepp så länge det är oklart vilka frågor som ska lösas med e-tjänstelegitimationer. Tre behov hade enligt delegationen varit föremål för särskilda diskussioner. Ett första behov var att e-tjänstelegitimationen krävs för att utmönstra personnum-

[1] Dir. 2009:19.

mer ur de e-legitimationer som används i tjänsten så att anställda m.fl. ska kunna skriva under handlingar elektroniskt utan att deras personnummer därigenom exponeras. Ett andra behov var att e-tjänstelegitimationen i sig, genom kompletterande information i själva legitimationen, ger stöd för förenklade, automatiserade rutiner så att förlitande part kan kontrollera att innehavaren är juridiskt behörig att agera för det i legitimationen angivna organets räkning. Ett tredje behov var att företag och myndigheter för sina anställda och uppdragstagare ska kunna ansöka om elektroniska legitimationshandlingar, förse berörda personer med sådana legitimationer, sätta upp ramar för hur de får användas och ges rätt att spärra legitimationen, t.ex. när anställningen eller uppdraget upphört.[2] Delegationen hade följande slutsatser vad gäller e-tjänstelegitimationer:

- Genom e-tjänstelegitimationer kan personnummer utmönstras ur e-legitimationer som används i tjänsten.
- Förutsättningar ges också för företag och myndigheter att ansöka om elektroniska legitimationshandlingar för sina anställda och uppdragstagare, förse dem med sådana legitimationer, sätta upp ramar för hur de får användas och vid behov spärra dem.
- E-tjänstelegitimationer ska utformas så att de kan användas inom hela den offentliga sektorn och näringslivet. De ska också anpassas för en federationslösning, som på sikt ska kunna ge stöd även för juridisk behörighetskontroll.[3]

5.3 Utredningen om bildande av en e-legitimationsnämnd

Utredningen om bildande av en e-legitimationsnämnd utarbetade ett förslag till en ny nationell modell för att använda e-legitimationer som också omfattade e-tjänstelegitimationer.[4] Utredningen framförde att medan användaren själv får anskaffa privat e-legitimation är det arbets- eller uppdragsgivaren som ansöker om och tilldelar den

[2] *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86), s. 125.
[3] A.a.
[4] *E-legitimationsnämnden och Svensk e-legitimation* (SOU 2010:104), s. 24.

anställde en e-tjänstelegitimation.[5] E-tjänstelegitimationer förutsätts även finansieras av arbetsgivarna.[6]

Till e-legitimationer skulle det vidare enligt utredningens förslag gå att knyta attributsintyg med t.ex. uppgift om anställning hos en viss arbetsgivare eller visst uppdrag för en angiven huvudman.[7] Utredningen fann att en ansluten utfärdare kan ansvara för både de e-legitimationer och de identitetsintyg som denne tillhandahåller. I praktiken kunde det enligt utredningen inte heller uteslutas att en myndighet eller ett offentligt ägt bolag blir utfärdare av e-tjänstelegitimationer och identitetsintyg, men att denna fråga behövde utredas vidare.[8] För anställda inom en region borde regionen enligt utredningen själv vara identitetsutfärdare, förutsatt att de uppfyller kraven för Svensk E-legitimation, då det är regionen som av den anställde uppfattas som utfärdare. Motsvarande synsätt borde enligt utredningen tillämpas även för annan offentlig verksamhet.

Utredningen bedömde vidare att en användare kan bruka en privat e-legitimation även i egenskap av företrädare för annan och den som har tilldelats en e-tjänstelegitimation får, om arbets- eller uppdragsgivaren godtar det, bruka e-tjänstelegitimationen också för egen räkning.[9]

Utredningen presenterade också ett förslag till regelverk för infrastrukturen kring e-legitimationer. Av detta regelverk framkommer bl.a. att en användare av en e-tjänstelegitimation får använda den endast i enlighet med instruktioner från arbets- eller uppdragsgivaren. Vidare bestämmer en arbets- eller uppdragsgivare som anskaffar e-tjänstelegitimationer inom ramen för sin arbetsledningsrätt hur e-tjänstelegitimationen får brukas av användaren. En arbets- eller uppdragstagare ska också göra en spärranmälan snarast efter att denne upptäckt att det finns anledning att spärra en e-tjänstelegitimation som denne tilldelat en arbets- eller uppdragstagare. Anledning att spärra kan föreligga bl.a. om arbets- eller uppdragsförhållandet upphört eller om en personlig kod kan ha blivit tillgänglig för någon annan.[10]

[5] A.a. s. 26.
[6] A.a. s. 107.
[7] A.a. s. 26.
[8] A.a. s. 29 f.
[9] A.a. s. 192.
[10] A.a. s. 207.

5.4 E-legitimationsnämnden

E-legitimationsnämnden inrättades 2011 och den lades ned i samband med att verksamheten flyttades över till DIGG. Nämnden hade bl.a. i uppgift att stödja och samordna den offentliga förvaltningens behov av säkra metoder för identifiering och elektroniskt undertecknande.

Vad gäller e-legitimation i tjänsten ansåg E-legitimationsnämnden att nämndens avtal och kravställning inte hindrade att en privat e-legitimation används i tjänsten. Anskaffning av en e-legitimation i tjänsten var i stället en fråga om arbetsgivarens upphandling av e-legitimationer och användningsområdet för dessa legitimationer var enligt nämnden en arbetsrättslig fråga mellan arbetsgivaren och arbetstagaren. Information om roller och behörighet som den förlitande parten kan behöva ska hämtas in genom attributtjänster. I den lösning nämnden föreslog skulle det enligt deras bedömning varit enkelt att koppla in sådana tjänster på ett standardiserat sätt. Nämnden noterade dock att det fanns ytterligare frågor att lösa vad gäller användning av e-legitimation i tjänsten, exempelvis vilken roll en person ikläder sig vid ett visst tillfälle och att dessa frågor behövde utredas vidare.[11]

5.5 Utredningen om effektiv styrning av nationella digitala tjänster

Utredningen om effektiv styrning av nationella digitala tjänster gjorde bedömningen att arbetstagare inte ska använda sina privata e-legitimationer i tjänsten och att det är arbetsgivares ansvar att säkerställa att arbetstagare kan identifiera sig elektroniskt när de utför sina arbetsuppgifter. Utredningen konstaterade att det finns olika sätt för arbetsgivare att lösa elektronisk identifiering för arbetstagare inom sin organisation och i relation till andra, men att tekniken bör följa de strukturer som finns i fråga om ansvar för att arbetstagare har de medel som behövs för att utföra arbetet.[12]

[11] E-legitimationsnämnden, *Fortsatt försörjning av tjänster för e-legitimering och e-underskrift* (Dnr: 131 645711-15/9513), 25 oktober 2016.
[12] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 271 f.

Utredningen ansåg att arbetsgivare som ställer krav på elektronisk identifiering för att en individ ska kunna utföra sina arbetsuppgifter, också ska förse individen med det medel som krävs för att göra detta och att en elektronisk identitetshandling som arbetstagare använder i tjänsten alltså är att betrakta som ett verktyg för tjänsten. Utredningen bedömde vidare att om en arbetsgivare kräver att en anställd använder privat utrustning i arbetet måste detta framgå av anställningsavtalet. Annars gäller principen att arbetsgivaren tillhandahåller den utrustning arbetet kräver. Vad gäller it-utrustning måste även arbetsgivarens personuppgiftsansvar vägas in. Om personuppgifter behandlas i tjänsten på en privat anordning har arbetsgivaren personuppgiftsansvaret och är därför skyldig att kontrollera utrustningen i fråga. Detta kan innebära att arbetsgivaren får del av den anställdes privata information. Det torde enligt utredningen därför vara mindre lämpligt att arbetsgivare kräver att anställda ska använda elektronisk identitetshandling på en privat mobiltelefon. Vid användning av privat elektronisk identitetshandling på kort uppstår inte samma komplikation.[13]

Utredningen flaggade också för risken att om upphandling sker, att den leverantör staten väljer för en eventuell statlig e-legitimation får en dominerande ställning även på marknaden för e-tjänstelegitimationer. Om den elektroniska identitetshandlingen levereras av en myndighet innebär det i stället att staten konkurrerar med leverantörer på denna marknad.[14]

Vad gäller identitetskontroll framhöll utredningen att arbetsgivare i många fall måste kontrollera identiteten hos sina anställda, åtminstone i samband med att de anställs. I de fall arbetsgivaren kontrollerar identiteten på en arbetstagare görs det genom att individen visar upp en fysisk identitetshandling. Ibland måste arbetsgivaren också göra säkerhetskontroller på individen. De fysiska identitetshandlingar som staten utfärdar har alltså en betydelse i den identitetskontroll som arbetsgivare gör av sina arbetstagare. Även om anställningsförfaranden oftast innefattar personliga besök hos arbetsgivaren bedömde utredningen att en statlig e-legitimation på sikt kunde användas på motsvarande sätt.[15]

[13] A.a. s. 272 f.
[14] A.a.
[15] A.a. s. 273 f.

Utredningen bedömde också att det var viktigt med samordning av elektronisk identifiering i tjänsten och att de lösningar som tas fram ska fungera såväl inom den egna organisationen som i relation till andra aktörer. Utredningen lyfte vidare fram samarbetsavtalet mellan Försäkringskassan och Inera AB (se mer om detta i avsnitt 5.7) och föreslog att DIGG skulle bedöma om den lösning som togs fram i det projektet kunde utvecklas till att bli en förvaltningsgemensam digital funktion.[16]

5.6 2017 års ID-kortsutredning

2017 års ID-kortsutredning berörde i sitt betänkande inte användning av e-legitimation i tjänsten. Utredningen behandlade dock frågan om grundidentifiering (se mer om grundidentifiering i avsnitt 3.10). Utredningen bedömde att med en säker grundidentifiering som görs av en myndighet vid ett personligt besök minskar risken för att fel person får tillgång till en e-legitimation. Utredningen framhöll emellertid att det är både kostsamt och svårt att utföra grundidentifiering. Utredningen föreslog att Polismyndigheten skulle ha ansvaret för grundidentifiering och utfärdande av statliga fysiska identitetshandlingar dvs. pass och statligt identitetskort.[17] Utredningen föreslog även att Polismyndigheten skulle utföra grundidentifiering samt utfärdande av den statliga e-legitimationen som enligt utredningens förslag, efter ansökan, skulle finnas på det statliga identitetskortet. Utredningen konstaterade att en e-legitimation som utfärdas av en statlig myndighet efter en grundidentifiering av en myndighet vid ett personligt besök kan utgöra underlag för idväxling.[18] En sådan e-legitimation skulle således även kunna användas vid utfärdande av e-tjänstelegitimationer.

[16] A.a. s. 274.
[17] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 204.
[18] A.a. s. 319 ff.

5.7 Inera AB:s och Försäkringskassans samarbetsavtal om en gemensam lösning för tjänstelegitimationer

Inera AB och Försäkringskassan påbörjade i februari 2016 ett samverkansprojekt kring en gemensam lösning för e-tjänstelegitimationer inom offentlig sektor. Avsikten med samverkansprojektet var att ersätta både SITHS och MCA (se mer om SITHS och MCA i avsnitt 6.4.2) samt att identifieringslösningen skulle kunna användas tillsammans med annan infrastruktur och lokala identitetsintygsutfärdare så länge den lokala lösningen följde referensarkitekturen.[19]

I januari 2019 sades emellertid samarbetsavtalet upp med motiveringen att statliga myndigheter hade andra behov och kravbilder än Ineras kunder och att detta ledde till väldigt olika kostnader och att det därmed var mer logiskt att i stället ha två olika driftställen för tjänsten.[20]

5.8 Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte

År 2018 gav regeringen Bolagsverket, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, Skatteverket och DIGG i uppdrag att tillsammans analysera och lämna förslag som syftar till att skapa ökad säkerhet och effektivitet i samband med elektroniska informationsutbyten inom och med den offentliga sektorn.[21] Uppdraget resulterade i rapporten *Säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn*. I rapporten föreslogs fyra kategorier av förvaltningsgemensamma byggblock i ett ekosystem med förvaltningsgemensam digital infrastruktur för informationsutbyte: digitala tjänster, informationsutbyte, informationshantering samt tillit och säkerhet.[22] Regeringen lämnade i december 2019 ett nytt uppdrag till tidigare nämnda myndigheter samt MSB och Riksarkivet att tillsammans etablera en förvaltningsgemensam digital

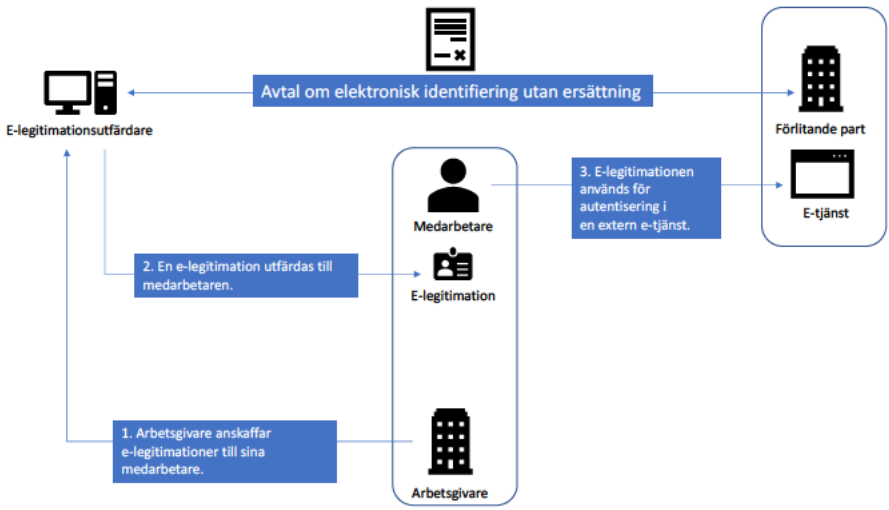
[19] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 269 f.
[20] https://forsakringskassan.se/wps/poc?urile=wcm:path:/contentse_responsive/press/pressmeddelanden/inera-och-forsakringskassan (hämtad 2021-06-14).
[21] Uppdrag om ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn (Fi2018/02150/DF, FI2018/03037/DF och I2019/01061/DF).
[22] DIGG m.fl., *Säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn* (dnr 2019-100), s. 17 ff.

infrastruktur för informationsutbyte. Den 17 december 2020 beslutade regeringen om förlängd tid för uppdraget. Uppdraget ska slutrapporteras i december 2021.[23] En delredovisning skedde dock i slutet av januari 2021. I delredovisningen lämnades förslag på en lämplig struktur för arbetet med den förvaltningsgemensamma infrastrukturen för informationsutbyte, förslag på författning som reglerar myndigheternas uppgifter och ansvar, en långsiktig plan för arbetet samt redovisning av arbetet med enskilda byggblock.[24]

5.8.1 Förstudierapport inom byggblocket Identitet

Inom byggblocket identitet lämnades i november 2020 en förstudierapport med ett förslag om civilrättsliga avtal som knyter ihop e-legitimationsutfärdare med förlitande parter.[25]

Figur 5.1 Avtal om elektronisk identifiering utan ersättning



Källa: DIGG.

[23] Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (I2019/03306/DF, I2019/01036/DF [delvis], I2019/01361/DF [delvis] och I2019/02220/DF).
[24] DIGG m.fl. *Delredovisning – Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte* (AD 2019:582), 29 januari 2021.
[25] DIGG, *eID för medarbetare – Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte* (dnr 2019-582), 14 december 2020, s. 24.

Avtalen syftar till att knyta ihop e-legitimationsutfärdare med förlitande parter. Det ska även finnas en variant av avtal mellan arbetsgivare och förlitande parter för de transaktioner som går via arbetsgivaren. Avtalen ska enligt förslaget vara ersättningslösa.

Flödet i förslaget framgår av figuren ovan. Som grund för förslaget ska e-legitimationsutfärdaren teckna avtal med förlitande parter. I ett första steg anskaffar arbetsgivaren e-legitimationer till sina medarbetare från e-legitimationsutfärdare (1) som i sin tur utfärdar e-legitimationer till medarbetarna (2). När medarbetaren ska logga in i en extern tjänst med sin e-legitimation ska denne som huvudalternativ välja sin e-legitimation eller sin arbetsgivare i tjänstens lista över inloggningsalternativ (3). Om medarbetaren väljer sin arbetsgivare, görs valet av e-legitimation i stället i arbetsgivarens lista över valbara e-legitimationer om det behövs.

Den förlitande parten tar hjälp av sitt eller sina avtal om e-legitimering, beslutar om lägsta godtagbara tillitsnivå i sammanhanget och tar även stöd av DIGG:s metadataregister i Sweden Connect för att veta vilka e-legitimationer som ska visas upp som valbara för användaren. Den förlitande parten kan vara den helt externa organisation som användaren vill få tillträde hos, eller arbetsgivarens centrala inloggningsfunktion.

E-legitimationsutfärdaren svarar på begäran från förlitande part med ett i det externa huvudfallet krypterat identitetsintyg baserat på avtalsregler. Den förlitande parten dekrypterar identitetsintyget och avgör om ytterligare uppgifter om användaren ska hämtas in. Identitetsintyg som skickas mellan utfärdare och förlitande parter i Sverige passerar inte DIGG, utan går direkt mellan intygsutfärdaren och den förlitande parten. Både e-legitimationsutfärdaren och den förlitande parten kan ha underleverantörer.

När den på e-legitimationen förlitande parten är arbetsgivaren, kan arbetsgivaren, själv eller med stöd av underleverantör, i sin tur ställa ut intyg med stöd av sin egen intygsfunktion. 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 parter som arbetsgivaren har avtal med. Arbetsgivaren får baserat på avtal registrera sin identitetsintygsutfärdare i DIGG:s metadata och kan delegera till en underleverantör att bistå med teknisk kontaktperson

etc. I denna variant blir e-legitimationsutfärdaren underleverantör till arbetsgivaren.[26]

5.9 Samverkan mellan staten och Sveriges Kommuner och Regioner

5.9.1 Överenskommelse om digitalisering i skolväsendet

I november 2020 ingicks en överenskommelse mellan staten och SKR om digitaliseringens möjligheter för att främja kunskapsutveckling och likvärdighet i skolväsendet. Överenskommelsen innebär bl.a. att SKR ska arbeta för att stödja anskaffning av e-legitimationer och andra inloggningsmetoder.[27] Detta innefattar att se över vilken typ av federationslösningar som finns och vad som skulle fungera bäst för skolorna. Det inkluderar lämpliga ramavtal och teknik som erbjuds samt att säker och effektiv åtkomst till digitala resurser säkerställs.[28]

5.9.2 Avsiktsförklaring om utveckling av välfärdens digitala infrastruktur

Välfärdskommissionens uppdrag går ut på att identifiera och analysera konkreta åtgärder för att stärka kommunsektorns förmåga att tillhandahålla välfärdstjänster av god kvalitet i framtiden. Kommissionen samlar företrädare för stat, kommuner, regioner och centrala arbetstagarorganisationer. I december 2020 presenterade Välfärdskommissionen en avsiktsförklaring mellan regeringen och SKR om utveckling av välfärdens digitala infrastruktur.[29]

I avsiktsförklaringen konstateras att digitaliseringen av offentlig verksamhet ofta sker i stuprör och att kommuner, regioner, statliga myndigheter och privata utförare av offentligt finansierad välfärd under många år byggt och infört egna it-system och lösningar som inte alltid är kompatibla med varandra. Något som försvårar sam-

[26] A.a. s. 15 ff.
[27] www.regeringen.se/4abeae/contentassets/9a5edaa4192f42a6ada595d75eb98dcf/digitaliseringens-mojligheter-for-att-framja-kunskapsutveckling-och-likvardighet-i-skolvasendet (hämtad 2021-06-14).
[28] www.inera.se/nyheter/nyheter/sa-ska-skr-och-inera-stotta-digitaliseringen-i-sveriges-skolor/ (hämtad 2021-06-14).
[29] www.regeringen.se/pressmeddelanden/2020/12/valfardskommissionen-overens-om-okad-digitalisering-och-minskat-it-krangel/ (hämtad 2021-06-14).

arbetet mellan olika offentliga aktörer, men också kontakten med invånare och företag.[30]

Denna bristande samordning är enligt avsiktsförklaringen ett hinder för att uppnå digitaliseringens fulla potential och för att råda bot på detta behöver den förvaltningsgemensamma digitala infrastrukturen byggas ut. Vidare anförs att en gemensam digital infrastruktur kan underlätta för offentlig sektor att utveckla och anpassa sin egen digitala struktur. En sådan infrastruktur kan enligt avsiktsförklaringen exempelvis omfatta tekniska standarder, gemensamma informationsmängder och tjänster för informationsutbyte och identifiering. Det anges även att en ökad samordning av tekniska krav och standarder inom offentlig sektor kan gynna innovation och marknadsutveckling bland it-leverantörer till gagn för välfärden.[31]

Arbetet ska omfatta två delar, en kartläggnings- och analysfas samt en överenskommelsefas. Målsättningen är att arbetet ska vara klart till september 2021.[32]

[30] Regeringskansliet och Sveriges Kommuner och Regioner, *En avsiktsförklaring mellan staten och Sveriges Kommuner och Regioner om utveckling av välfärdens digitala infrastruktur*, 2020, s. 3.
[31] A.a.
[32] A.a. s. 4.

6 E-legitimationsområdet i Sverige

6.1 Inledning

En synpunkt som ofta förs fram rörande e-legitimationsområdet i Sverige är att det inte hänger samman. Vi delar denna bedömning. Det finns många olika lösningar och samarbeten inom området och även om det finns kopplingar och gemensamma nämnare skapar de olika delarna i dagsläget inte en sammanhållen och optimalt utformad helhet. Detta är troligen en starkt bidragande anledning till att många uppfattar området som svårtillgängligt och komplext. I detta kapitel beskrivs de olika delarna och avslutningsvis försöker vi i avsnitt 6.7 ge en sammanfattande bild av e-legitimationsområdet.

6.2 Teknik

För att förstå området är det viktigt att först förstå på en grundläggande nivå hur tekniken fungerar och vilka olika moment som förekommer i samband med användning av en e-legitimation. Vad gäller tekniken finns det olika sätt att identifiera en användare. Exempelvis genom användning av certifikat (Public Key Infrastructure [PKI]), via användning av engångslösenord eller med symmetrisk kryptering som en koddosa för autentisering till en identitetsintygsutfärdare.[1] Utfärdaren använder sedan autentiseringen för att ställa ut ett identitetsintyg som innehåller en användares elektroniska identitet och attribut där ett attribut skulle kunna vara ett personnummer. Identitetsintyget kan vidare innehålla uppgifter om tillitsnivå avseende det enskilda identitetsintyget.

[1] Se en beskrivning av hur PKI fungerar i *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9), s. 69 ff.

När en användare använder en e-legitimation i en e-tjänst i sin egen eller annans organisation sker det i ett flöde. I det flödet förekommer flera olika roller som kan tillhandahållas av den egna organisationen eller av externa parter. Rollerna är anvisningstjänst, identitetsintygsutfärdare, legitimeringstjänst, e-legitimationsutfärdare och behörighetskontrolltjänst.

Anvisningstjänst används i samband med inloggning till e-tjänster när e-tjänsterna tillåter användning av flera olika e-legitimationer från flera olika e-legitimationsutfärdare. Tjänsten låter en användare välja vilken e-legitimation den vill använda i e-tjänsten.

I legitimeringstjänsten legitimerar sig användaren genom att använda sin e-legitimation, t.ex. ange koden för att använda nyckeln på ett smartkort eller en mobil e-legitimation. Tjänsten kontrollerar e-legitimationen och skickar vidare resultatet till identitetsintygsutfärdaren.

Utfärdare av identitetsintyg tar emot och kontrollerar legitimeringen som skett av legitimeringstjänsten mot utfärdaren av e-legitimationer. Därefter utfärdas identitetsintyget som stämplas av identitetsintygsutfärdaren så att förlitande part kan kontrollera intygets äkthet.[2]

E-tjänsten kan vid behov kontrollera behörighetsinformation som finns i tjänstens register eller i förekommande fall hämta det från en behörighetskontrolltjänst.

6.3 Tillitsramverket och kvalitetsmärket Svensk e-legitimation

Av 3 § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning framgår att DIGG ska främja användningen av elektronisk identifiering. Som ett led i det arbetet förvaltar och utvecklar myndigheten tillitsramverket för kvalitetsmärket Svensk e-legitimation.[3] Ramverket syftar till att etablera gemensamma krav för utfärdare av kvalitetsmärkta svenska e-legitimationer.[4] Det togs ursprungligen fram av E-legitimationsnämnden, vars arbetsuppgifter

[2] I Valfrihetssystem 2017 E-legitimering finns ett krav att stämplingen av identitetsintyget ska göras i e-legitimationsutfärdarens namn, t.ex. Freja, så att helhetsansvaret tas av en part och den huvudansvariga parten benämns ”e-legitimationsutfärdare”. Underleverantörer är tillåtna, men inte i eget namn.
[3] DIGG, *Tillitsramverk för kvalitetsmärket Svensk e-legitimation* (dnr 2019-278), 19 september 2019.
[4] A.a. s. 2.

övertogs av DIGG när den myndigheten bildades. Tillitsramverket är kopplat till kvalitetsmärket Svensk e-legitimation och riktar sig till utfärdare av e-legitimationer som tilldelas kvalitetsmärket (se avsnitt 6.3.3).

Ramverket bygger på den internationella standarden ISO/IEC 29115, ISO/IEC 27000-serien och andra internationella ramverk, men vissa nationella anpassningar har gjorts.[5] I ramverket fastställs krav som riktar sig mot utfärdare av e-legitimationer. Kraven avser bl.a. kontroller av den person som tilldelas en e-legitimation för att säkerställa att personen är den han eller hon utger sig för att vara. Kraven är indelade i olika nivåer: 2, 3 och 4. Kraven ökar för respektive nivå.

Tillitsnivå 1 definieras i ISO/IEC 29115 men har ingen motsvarighet i tillitsramverket eller i eIDAS-förordningens tillitsnivåer. Denna nivå kräver ingen legitimering, utan det räcker med att exempelvis ange namn och e-postadress.[6] Nivåerna heter tillitsnivåer men kallas ofta också för LoA (”Level of Assurance”). Samtliga tre tillitsnivåer innebär minst tvåfaktorsautentisering och stark autentisering, men graden av säker grundidentifiering och övrig skyddsnivå vid autentisering skiljer sig åt (se mer om detta nedan).

Det är i normalfallet upp till förlitande part att avgöra vilken lägsta tillitsnivå som ska krävas för tillgång till en e-tjänst. Till stöd för denna bedömning finns vägledning från DIGG[7], SKR[8] och MSB[9]. Grunden är informationsklassning i kombination med bedömning av vilken skada en felaktig identifiering skulle kunna leda till. Vissa författningar och tillsynsbeslut ger också vägledning vad avser sådana bedömningar (se avsnitt 4.3 om krav på autentisering).

[5] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 181.
[6] www.digg.se/digital-identitet/e-legitimering/tillitsnivaer (hämtad 2021-06-14).
[7] DIGG, *Vägledning till uppfyllande av tillitsramverkets krav för kvalitetsmärket Svensk e-legitimation* (dnr 2019-278), 19 september 2019.
[8] SKR, *Vägledning för anslutning till eIDAS*, 17 januari 2020.
[9] MSB, *Vägledning – säkerhetsåtgärder i informationssystem för statliga myndigheter (förhandsutgåva), 1 september 2020*.

6.3.1 Övergripande krav som avser utfärdares verksamhet

Övergripande krav på den verksamhet som utfärdare av e-legitimationer bedriver är bl.a. att de ska teckna och vidmakthålla för verksamheten erforderliga försäkringar samt ha förmåga att bära risken för skadeståndsskyldighet. Utfärdare ska för de delar av verksamheten som berörs i tillitsramverket ha ett ledningssystem för informationssäkerhet (LIS) som i tillämpliga delar baseras på ISO/IEC 27001 eller motsvarande likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet. Kravet på ett fungerande LIS ökar för högre tillitsnivåer. Ramverket innehåller också bl.a. krav på bakgrundskontroll innan personer antar vissa roller som är av särskild betydelse för säkerheten. Ett exempel på skillnader i krav för de olika nivåerna är att för nivå 3 och 4 ska utfärdare genom hela kedjan i utfärdandeprocessen säkerställa att separation av arbetsuppgifter tillämpas på ett sådant sätt att ingen på egen hand har möjlighet att tillskansa sig en e-legitimation i en annan persons namn. Ett krav som inte gäller för nivå 2. Ramverket innehåller även krav som avser teknisk säkerhet, exempelvis att elektroniska kommunikationsvägar som nyttjas i verksamheten för överföring av känsliga uppgifter ska skyddas mot insyn, manipulation och återuppspelning.

6.3.2 Krav kopplade till ansökan och utfärdande

Ramverket innehåller ett antal krav som avser ansökan om att få en e-legitimation utfärdad och själva utfärdandet. Utfärdare ska föra register över anslutna användare och de tilldelade e-legitimationerna. De ska också tillhandahålla en spärrtjänst där användaren kan spärra sin e-legitimation.

Utfärdare ska kontrollera att uppgifter knutna till en ansökan om utfärdande av e-legitimation är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register. Tillitsnivå 2 och 3 tillåter identifiering av sökanden på distans med en annan e-legitimation med kvalitetsmärket Svensk e-legitimation på minst tillitsnivå 3, om avtalsvillkoren för den e-legitimationen tillåter det.

DIGG har sammanfattat tillitsnivå 2–4 på följande sätt.[10]

Tillitsnivå 2

- Användarens identitet verifieras genom att bevisa innehav av en tillhörighet som bara användaren kan antas förfoga över. Exempel kan vara kod som skickats i kodkuvert till sökandes folkbokföringsadress.
- Användaren identifieras genom exempelvis engångslösenord från dosa eller mobiltelefon.
- Det finns en viss tillit till identiteten, och krav på tvåfaktorsautentisering.

Tillitsnivå 3

- Användarens identitet verifieras på likvärdigt sätt som vid utgivning av en fullgod svensk legitimationshandling. E-legitimationen kan utfärdas på distans om utfärdaren redan har identifierat mottagaren, t.ex. i samband med öppnandet av ett bankkonto eller vid en anställning.
- Användaren identifieras genom exempelvis en skyddad app i en smarttelefon.
- Det finns en hög tillit till identiteten, och krav på tvåfaktorsautentisering.

Tillitsnivå 4

- Användarens identitet verifieras vid personligt besök genom en fullgod svensk legitimationshandling, både första gången och vid förnyelse vart femte år.
- Användaren identifieras genom en e-legitimation som skyddas i ett särskilt chip, som kan finnas på t.ex. ett plastkort, en mobiltelefon eller en USB-enhet.

[10] www.digg.se/digital-identitet/e-legitimering/tillitsnivaer (hämtad 2021-06-14).

- Det finns en mycket hög tillit till identiteten, och krav på tvåfaktorsautentisering.

6.3.3 Kvalitetsmärket Svensk e-legitimation

Utfärdare som vill använda sig av kvalitetsmärket Svensk e-legitimation måste uppfylla kraven i tillitsramverket. Syftet med märket är att offentliga och privata aktörer med e-tjänster som kräver e-legitimation ska kunna lita på e-legitimationer som har märket och att användare ska kunna känna sig trygga med att det är en säker identitetshandling. En utfärdare som vill använda märket ansöker om det hos DIGG som gör en granskning utifrån tillitsramverket och beslutar om utfärdaren lever upp till kraven. Beslutet avser vilken nivå den aktuella e-legitimationslösningen lever upp till. Dessa publiceras på DIGG:s webbplats. I skrivande stund är godkända e-tjänstelegitimationer EFOS för tillitsnivå 3 och 4 samt Freja eID Plus, Mobilt EFOS, SITHS och Mobilt SITHS för tillitsnivå 3. Godkända e-legitimationer för privatpersoner är AB Svenska Pass för tillitsnivå 3 och 4 samt BankID på fil, BankID på kort, Mobilt BankID och Freja eID Plus för tillitsnivå 3.

Tillitsramverket och kvalitetsmärket Svensk e-legitimation regleras inte i författning och det finns inga bestämmelser om att ramverket eller kvalitetsmärket ska finnas. Utredningen om effektiv styrning av nationella digitala tjänster föreslog att det i lag skulle regleras att ramverket skulle vara en del av infrastrukturen för elektronisk identifiering och att kvalitetsmärket skulle regleras i samma lag.[11] Förslaget har inte genomförts.

6.4 E-legitimationer på den svenska marknaden

6.4.1 Inledning

Nedan redogörs för de utfärdare av e-tjänstelegitimationer och privata e-legitimationer som utredningen identifierat i dagsläget finns på marknaden. E-legitimationer som endast eller huvudsakligen förekommer i näringslivet, exempelvis ID06 inom byggbranschen, finns dock inte med i sammanställningen. Inte heller e-tjänstelegi-

[11] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 31 ff.

timationer som utfärdas av en offentlig aktör enbart för anställda inom den egna organisationen.

6.4.2 E-tjänstelegitimationer

eduID

eduID är en e-legitimation som förvaltas och utvecklas av Swedish University Computer Network (Sunet) och som används av organisationer inom utbildning och forskning. eduID är en federerad identitet, dvs. en användaridentitet som kan användas inom flera olika organisationer. Den används av både studenter och anställda.[12]

EFOS

Generaldirektörerna för Arbetsförmedlingen, Försäkringskassan och Skatteverket skrev 2007 under ett avtal om samverkan mellan myndigheter där ett av målen var att ge medborgaren större tillgänglighet. I samband med detta tecknade även Försäkringskassan och Skatteverket ett avtal för etablering av servicekontor. Detta ledde i sin tur till att Försäkringskassan tog ansvaret som gemensam certifikatutfärdare för att möjliggöra att medarbetare på servicekontoren kunde få åtkomst till flera myndigheters system. Denna lösning kallades MCA vilket står för Myndighets CA och där CA är en akronym för den engelska termen för certifikatutfärdare (”certificate authority”).[13] Inera och Försäkringskassan påbörjade 2016 ett samverkansprojekt kring en gemensam lösning för e-tjänstelegitimation inom offentlig sektor som benämndes EFOS (”E-identitet För Offentlig Sektor”). Då var det sju myndigheter som använde tjänsten. Avsikten med samverkansprojektet var att ersätta både SITHS och MCA, men samarbetsavtalet sades upp 2019 (se mer om detta i avsnitt 5.7).

Försäkringskassan fortsatte därefter arbetet med EFOS på egen hand. I skrivande stund är det ca 42 000 medarbetare inom den offentliga förvaltningen som har EFOS och utöver Försäkrings-

[12] https://eduid.se/faq.html (hämtad 2021-06-14).
[13] www.efos.se/ (hämtad 2021-06-14).

kassan används lösningen av 19 andra statliga myndigheter. I certifikaten framgår det vilken myndighet användaren tillhör.

Under år 2021 räknar Försäkringskassan med att EFOS kommer ha ca 51 000 användare. Försäkringskassan har till utredningen uppgett att de emellanåt även får förfrågningar från kommuner och att det inte finns några hinder mot att kommunerna använder EFOS, men att det förutsätter att kommunerna bedömer att anskaffningen är förenlig med upphandlingslagstiftningen.

EFOS e-legitimation är godkänd enligt kvalitetsmärket Svensk e-legitimation på tillitsnivå 3 och 4. EFOS finns också i en mobil variant, Mobilt EFOS, som är godkänd på tillitsnivå 3. EFOS är även föranmäld för att kunna användas gränsöverskridande i enlighet med eIDAS-förordningens bestämmelser.[14]

Expisoft AB

Expisoft AB (Expisoft) har gett ut e-tjänstelegitimationer sedan 2007. Expisofts lösning är en e-tjänstelegitimation som inte innehåller personnummer för innehavaren av legitimationen, däremot innehåller den tjänsteidentitetsnummer. Lösningen finns både i fil- och kortbaserat format och ingår i bolagets säkerhetsprogramvara ExpiClient. Expisoft har två utgivare, en för fil- och en för kortbaserade legitimationer. Utfärdande av identitets- och funktionsintyg sker oftast via andra aktörer som då även tecknar avtal med slutkunden.

Freja Organisations eID

Freja Organisations eID ägs, förvaltas och utvecklas av Freja eID Group AB (härefter Freja). Organisations eID är en lösning som alla organisationer kan anskaffa. Organisations eID bygger på de identiteter som utfärdas av Freja eID (se mer om Freja eID i avsnitt 6.4.3). Vid utfärdande av Freja Organisations eID får användaren först ett Freja eID och därefter ett Freja Organisations eID. Dessa e-legitimationer är dock skilda och har bl.a. olika API:er.[15] Freja står för

[14] www.digg.se/om-oss/nyheter/2021/efos-ingar-nu-i-sveriges-foranmalan-till-eidas (hämtad 2021-06-14).

[15] API står för ”Application Program Interface” och är enligt Svenska datatermgruppens definition ett gränssnitt som gör det möjligt att i program och insticksmoduler utnyttja funk-

grundidentifieringen av användarna. Anskaffande organisation kan välja om användarna ska vara identifierade med verifierad ID-handling (”Extended”) eller om de ska ha en av DIGG granskad e-legitimation på tillitsnivå 3 (”Plus”).

Det är inte personnumret som ligger till grund för identifieringen av användaren utan ett ID-begrepp/attribut kopplat till organisationen. Attribut kopplade till användarens roll i organisationen är också möjlig.

Freja eID Plus är godkänd enligt kvalitetsmärket Svensk e-legitimation på tillitsnivå 3.

Nexus SmartID

Technology Nexus Secured Business Solutions AB (Nexus) tillhandahåller en central programvara för administration, utgivning och livscykelhantering av e-legitimationer. Nexus tillhandahåller en utfärdarportal där det går att utveckla och skapa certifikat. Vidare finns en självserviceportal där användaren bl.a. kan ID-växla mellan olika bärare. Utfärdandet av e-tjänstelegitimationer kan ske av Nexus kunder eller av Nexus själva. Vid det tidigare scenariot står kunden som certifikatutgivare. Kunden får funktioner/gränssnitt att använda för att identifiera användare samt beställa och utfärda e-legitimationer på olika bärare. Kunden får även ett regelverk från Nexus för hur arbetet ska utföras. Kunden blir då en registreringsfunktion som identifierar användaren och registrerar de uppgifter som ska finnas i certifikaten mot Nexus tjänst. Vid det senare scenariot är det Nexus som är certifikatutgivare och är tjänsteleverantör i stället för teknikleverantör.

SITHS

SITHS är en akronym för ”Säker IT-användning i Hälso- och Sjukvården” och är en identifieringstjänst som bl.a. består av en e-legitimation. SITHS togs fram 2005 och initialt var det Telia som byggde lösningen. SITHS förvaltas och utvecklas numera av Inera AB (härefter Inera). Inera ägs av regioner, kommuner och SKR Företag.

tioner för vissa tjänster som finns tillgängliga i ett annat program eller i en funktionssamling. www.termado.com/DatatermSearch/?ss=api (hämtad 2021-06-13).

Bolagets uppdrag är att skapa förutsättningar för att digitalisera välfärden, genom att förse ägarna med gemensam digital infrastruktur och arkitektur.[16]

De organisationer som kan anskaffa SITHS e-legitimation är regioner, kommuner, statliga myndigheter och privata vårdgivare. För att kunna använda SITHS krävs i regel att organisationen även är ansluten till katalogtjänsten HSA som är en elektronisk katalog innehållande uppgifter om organisationer och personer inom vård och omsorg i Sverige.[17] Genom HSA får arbetstagaren en pseudonym att använda i stället för personnummer, ett s.k. HSA-id. Vissa verksamheter som använder SITHS, t.ex. apotek, är emellertid inte anslutna till HSA.

Regioner, kommuner och statliga myndigheter kan välja att ta fullt ansvar för tjänsten och själva ge ut de e-legitimationer organisationen behöver. Om de offentliga aktörerna inte vill ta detta ansvar eller bara har behov av att ge ut SITHS e-legitimationer till ett fåtal medarbetare kan de i stället ansluta via ett ombud som i sin tur ger ut e-legitimationen. Privata vårdgivare kan endast ansluta via ombud. Det finns både regioner och kommuner samt privata företag som agerar ombud. För användare som arbetar i flera regioner går det att lägga in flera olika certifikat. SITHS-korten innehåller tre certifikat som alla använder samma nyckelpar: ett certifikat med personnummer från Telia, ett med personnummer från Inera och ett med HSA-id från Inera. Telias e-legitimation som finns på korten används ibland för att komma in i vissa statliga myndigheters e-tjänster.

SITHS e-legitimation används i nuläget av ca 550 000 medarbetare inom vård- och omsorgssektorn. SITHS e-legitimation finns i två varianter. Dels i form av en Windowsklient som används tillsammans med de fysiska SITHS-korten, dels sedan våren 2021 genom Mobilt SITHS som kan installeras på en surfplatta eller mobiltelefon.

SITHS och Mobilt SITHS är godkända enligt kvalitetsmärket Svensk e-legitimation på tillitsnivå 3.

[16] www.inera.se/om-inera/ineras-uppdrag/ (hämtad 2021-06-14).
[17] HSA står för Hälso- och sjukvårdens adressregister.

Telia Company AB

Telia Company AB (Telia) erbjuder e-tjänstelegitimationer. Telia erbjuder också andra typer av certifikat där kunden själv definierar innehållet i certifikaten, men dessa är då enligt Telia inte att betrakta som e-legitimationer. Vidare kan det noteras att SITHS-korten, utöver Ineras e-legitimation, för närvarande även innehåller en e-legitimation från Telia.

Telia har även en ID-broker tjänst (se mer om sådana tjänster i avsnitt 3.12) som många e-legitimationsutfärdare i Norden och Baltikum är anslutna till.

6.4.3 Privata e-legitimationer

AB Svenska Pass

Skatteverkets identitetskort för folkbokförda i Sverige innehåller en e-legitimation som från och med september 2017 utfärdas av AB Svenska Pass (Svenska Pass). Bolaget har avtal med Skatteverket om att förse det fysiska id-kortet med en e-legitimation.[18] Det innebär att det är Svenska Pass och inte Skatteverket som har det juridiska ansvaret gentemot både innehavaren av e-legitimationen och de förlitande aktörer som ingått avtal med Svenska Pass. Fram till hösten 2017 var det Telias e-legitimation som fanns på Skatteverkets identitetskort. Det går inte längre att skaffa Telias e-legitimation för privatpersoner, men de som redan är utgivna fungerar så länge de är giltiga.

Det behövs en kortläsare och ett särskilt program som installeras på datorn för att kunna använda e-legitimationen.

För att skaffa e-legitimationen måste den sökande vara folkbokförd i Sverige, ha fyllt 13 år och kunna legitimera sig. Om den sökande är under 18 år måste denne ha tillstånd av sin vårdnadshavare.

Svenska Pass e-legitimation är godkänd enligt kvalitetsmärket Svensk e-legitimation på tillitsnivå 4.

[18] E-legitimationen är kopplad till innehavaren vilket är anledningen till att AB Svenska Pass redovisas under detta avsnitt. Påpekas bör dock att bolaget är ramavtalsleverantör i Kammarkollegiets ramavtal för e-tjänstelegitimationer (se avsnitt 6.5.3).

BankID

BankID har en dominerande ställning på den svenska marknaden för e-legitimationer. BankID ägs, förvaltas och vidareutvecklas av Finansiell ID-Teknik BID AB (härefter Finansiell ID-Teknik). Innan företaget bildades hade de stora bankerna i Sverige inlett ett arbete i ett bankkonsortium. Syftet med det arbetet var att ta fram en generell infrastruktur för elektroniska identitetshandlingar, som skulle uppfylla krav från myndigheter och banker samt kunna accepteras av allmänhet och företag. Finansiell ID-Teknik bildades 2002 och ägs av Danske Bank, Handelsbanken, Ikano Bank, Länsförsäkringar Bank, SEB, Skandiabanken och Swedbank.

Företagets kunder är de flesta av de stora svenska bankerna, som i sin tur säljer och förmedlar BankID. I dagsläget är det tio banker som utfärdar BankID.[19] Det finns tre olika varianter av BankID: Mobilt BankID, BankID på fil och BankID på kort.

Mobilt BankID innebär att användaren har sin e-legitimation i en mobiltelefon eller surfplatta. För att kunna hämta och använda Mobilt BankID krävs att användaren har installerat BankID-appen.

BankID på fil är en e-legitimation i en dator. För att kunna hämta och använda BankID på fil krävs att användaren har installerat BankID-programmet.

BankID på kort är en e-legitimation som är lagrad på ett smartkort. Förutom kortet och BankID-programmet krävs även att man har en kortläsare för att använda denna lösning.

Vilka lösningar som de olika bankerna erbjuder sina kunder skiljer sig åt.

Danske Bank, Nordea och Swedbank utfärdar alla tre BankID-lösningar. Handelsbanken och SEB utfärdar BankID på kort och Mobilt BankID. Länsförsäkringar, Skandia och Sparbanken syd utfärdar BankID på fil och Mobilt BankID. Ica Banken och Ålandsbanken utfärdar endast Mobilt BankID.

Antalet innehavare av BankID är, enligt statistik från Finansiell ID-Teknik, ca 8 miljoner och antalet användningstillfällen var under år 2020 ca 5,1 miljarder.[20]

[19] Det kan dock noteras att i valfrihetssystemet är Finansiell ID-Teknik leverantör och inte de enskilda bankerna.
[20] www.bankid.com/assets/bankid/stats/2020/statistik-2020-12.pdf (hämtad 2021-06-14).

För att kunna skaffa ett BankID måste en person ha ett svenskt personnummer och vara kund i någon av de banker som ger ut BankID. Respektive bank bestämmer själva vilken åldersgräns som krävs för att inneha ett BankID som de utfärdar. Om den sökande är under 18 år måste denne dock alltid ha tillstånd av vårdnadshavare.

BankID på fil, BankID på kort och Mobilt BankID är godkända enligt kvalitetsmärket Svensk e-legitimation på tillitsnivå 3.

Freja eID Plus

Freja eID Plus är en mobil e-legitimation som ägs, förvaltas och utvecklas av Freja. Vid utgången av första kvartalet 2021 hade Freja ca 142 000 registrerade användare och under den senaste 12 månaders perioden utfördes ca 1,1 miljoner transaktioner.[21]

För att skaffa Freja eID Plus krävs det att den som vill anskaffa e-legitimationen är folkbokförd i Sverige och kan legitimera sig. För att få Freja eID Plus måste denne även vara minst 8 år och då ha vårdnadshavarens godkännande. Barn som fyllt tretton år behöver inte vårdnadshavarens tillstånd.

Freja eID Plus är godkänd enligt kvalitetsmärket Svensk e-legitimation på tillitsnivå 3.

6.5 Anskaffning av e-legitimationer och tjänster för elektronisk identifiering

6.5.1 Inledning

Anskaffning av e-legitimationstjänster kan delas in i två huvudsakliga delområden. Dels anskaffning av en e-legitimation som görs av en privatperson eller en organisation som tillhandhåller e-tjänstelegitimationer till sina anställda. Detta kan även innefatta att anskaffa vissa tjänster som t.ex. möjliggör att en organisation på egen hand utfärdar e-legitimationer. Dels anskaffning av tjänster för att e-legitimationer ska kunna användas vid inloggning i exempelvis en myndighets e-tjänst.

[21] https://frejaeid-finansiell-info.s3.eu-north-1.amazonaws.com/Freja_eID_Group_Delarsrapport_1januari-31mars_2021.pdf (hämtad 2021-06-14).

6.5.2 Affärsmodeller för e-legitimationsutfärdare

Det finns i dagsläget två huvudsakliga affärsmodeller för e-legitimationsutfärdare i form av att ersättning antingen utgår från den som anskaffar e-legitimationen eller från förlitande part. Om ersättning utgår från förlitande part är det vanligast att ersättningen utgår per användningstillfälle. Vi väljer därmed att kalla den senare för den transaktionsbaserade modellen och den tidigare för anskaffningsmodellen.

Som framgått innebär den transaktionsbaserade modellen vanligen att en kostnad uppstår (ofta benämnd tickkostnad) varje gång e-legitimationen används. Exempelvis är tickkostnaden inom valfrihetssystemen 17 öre per transaktion (se mer om valfrihetssystem i avsnitt 6.5.4). Den grundläggande principen bakom denna modell är att den som får nyttan av användningen, dvs. gynnas av den säkra autentisering som användningen av en e-legitimation innebär, också ska betala för den.

Den anskaffningsbaserade modellen grundar sig på att den som anskaffar e-legitimationen också betalar för den. Denna modell är den som vanligen används av utfärdare av e-tjänstelegitimationer och utifrån de exempel vi sett är det vanligast med en fast avgift per tidsintervall eller en avgift per användare med begränsning i tid.

Det som tydligast skiljer modellerna åt är vem som betalar. Vad som prissätts och vad som utgör basen för betalningen kan emellertid variera och kombineras på olika sätt. Det går således även att inom ramen för den anskaffningsbaserade modellen låta kostnaden helt eller delvis styras av antalet transaktioner. Vad gäller den transaktionsbaserade modellen är BankID ett exempel på en e-legitimation som huvudsakligen använder sig av denna modell. Av våra kontakter med Finansiell ID-Teknik har dock framgått att det råder fri konkurrens mellan de banker som utfärdar BankID och att andra ersättningsformer kan förhandlas fram.

6.5.3 Anskaffning av e-legitimationer

Som framgår av avsnitt 6.4.3 anskaffas privata e-legitimationer av användaren direkt från utfärdaren eller ett ombud för denne.

En aktör inom den offentliga förvaltningen som vill anskaffa e-tjänstelegitimationer till sina anställda och uppdragstagare kan, beroende på de förutsättningar som råder, anskaffa tjänsterna direkt från en utfärdare, via en egen upphandling eller genom avrop från ramavtal. Vissa aktörer kan även välja att anskaffa vissa tjänster från externa aktörer och därefter själva utfärda e-legitimationen.

Kammarkollegiets ramavtal Identifiering och behörighet

Det statliga ramavtalet för området Kort för identifiering och behörighetkontroll löpte ut den 31 januari 2021 och är sedan den 23 mars 2021 ersatt av avtalet Identifiering och behörighet. Bakgrunden till att avtalet bytt namn är att det nya avtalet utöver kort också täcker fler olika typer av bärare i form av ringar, armband, USB-stickor och appar.[22] Avtalet omfattar även e-legitimationer och möjlighet att köpa produkter som tjänst utan eget ägande.[23] För att tydliggöra innebär dock anskaffning genom ramavtalet inte detsamma som ett externt förlitandeavtal likt det som ingås genom valfrihetssystemen (se avsnitt 6.5.4). Ramavtalet innefattar sju leverantörer varav AB Svenska Pass (se avsnitt 6.4.3) och Nexus (se avsnitt 6.4.2) är två av dem.[24] De ramavtalsleverantörer som inte själva tillhandahåller e-legitimationer har angett e-legitimationsutfärdare som underleverantörer.[25]

Avrop gällande e-legitimationer sker via förnyad konkurrensutsättning och vid avropet kan krav bl.a. ställas på tillitsnivåer enligt DIGG:s tillitsramverk eller kvalitetsmärkningen Svensk e-legitimation.[26] Avrop från ramavtalet kan göras av statliga myndigheter, kommuner och regioner. Avtalsperioden löper t.o.m. den 22 mars 2024

[22] www.avropa.se/contentassets/4f3fcc7b5f564baabfd1b3e3e34bae4a/idb_aberopade-foretag.pdf (hämtad 2021-06-14).
[23] www.avropa.se/ramavtal/ramavtalsomraden/it-och-telekom/identifiering-och-behorighet/identifiering-och-behorighet/?value=188146 (hämtad 2021-06-14).
[24] Övriga leverantörer är Angeno Business Solutions AB, AREFF Systems AB, Cygate AB, IDEMIA Sweden AB och Seriline Aktiebolag.
[25] www.avropa.se/contentassets/4f3fcc7b5f564baabfd1b3e3e34bae4a/idb_aberopade-foretag.pdf (hämtad 2021-06-12).
[26] Kammarkollegiet, *Kravkatalog Identifiering och behörighet (Version 1.1)*, 8 april 2021, s. 4.

med en förlängningsoption som maximalt kan utökas t.o.m. den 22 mars 2028.

6.5.4 Anskaffning av tjänster för elektronisk identifiering

Det förekommer som framgår av avsnitt 6.4 flera olika e-legitimationer på den svenska marknaden och det finns därför anledning för aktörer inom den offentliga förvaltningen att kunna erbjuda sina användare möjligheten att logga in i deras e-tjänster med olika e-legitimationer. Att det finns olika alternativ att tillgå medför även att tjänster blir mindre sårbara för det fall en viss e-legitimation skulle drabbas av tillgänglighetsproblem.

En myndighet som vill erbjuda möjligheten att logga in med e-legitimation kan anskaffa tjänster för elektronisk identifiering på olika sätt, exempelvis egen upphandling eller avrop från ramavtal. I Kammarkollegiets ramavtalsområden inom Programvaror och Tjänster finns t.ex. krav på att tjänster inom elektronisk identifiering ska kunna levereras.[27]

Avtal kan ingås direkt med e-legitimationsutfärdare eller ingås med en aktör som fungerar som mellanhand och erbjuder en tjänst som gör det möjligt för användarna att logga in med e-legitimationer från olika utfärdare (se mer om detta i avsnitt 3.12).

Ett annat alternativ för aktörer inom förvaltningen är att använda sig av valfrihetssystem för e-legitimationer. Förfarandet regleras i lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering. Enligt 2 § avses med valfrihetssystem ett förfarande där den enskilde har rätt att välja den leverantör som ska utföra tjänsten och som en upphandlande myndighet har godkänt och tecknat avtal med. Det finns två valfrihetssystem för e-legitimationer: Valfrihetssystem 2017 respektive 2018. Dessa administreras av DIGG som också tillhandahåller anslutningsavtal mellan leverantör av elektronisk identifiering direkt kopplad till vald e-legitimation och förlitande part. En myndighet som vill erbjuda sina användare att använda olika e-legitimationer är förlitande part och kan ansluta sig till valfrihetssystemen genom att ingå respektive avtal. I dagsläget är

[27] Kammarkollegiet, *Vägledning för avrop av tjänster för elektronisk identifiering och elektronisk underskrift från ramavtalsområden inom Programvaror och Tjänster 2019 (Version 2.0)*, 8 april 2020, s. 4.

52 aktörer ansluta till ett eller båda valfrihetssystemen i egenskap av förlitande parter.[28]

I en nyligen lämnad promemoria föreslås att valfrihetssystemen ska ersättas av ett auktorisationssystem.[29] I promemorian föreslås också att statliga myndigheter som har behov av tjänster för elektronisk identifiering ska använda de tjänster som tillhandahålls genom auktorisationssystemet. Konsekvensen av det är enligt promemorian att statliga myndigheter inte kan välja andra anskaffningsformer, exempelvis egen upphandling av tjänsterna eller avrop på ramavtal.[30]

6.6 Federationer för identifiering och behörigheter

6.6.1 Inledning

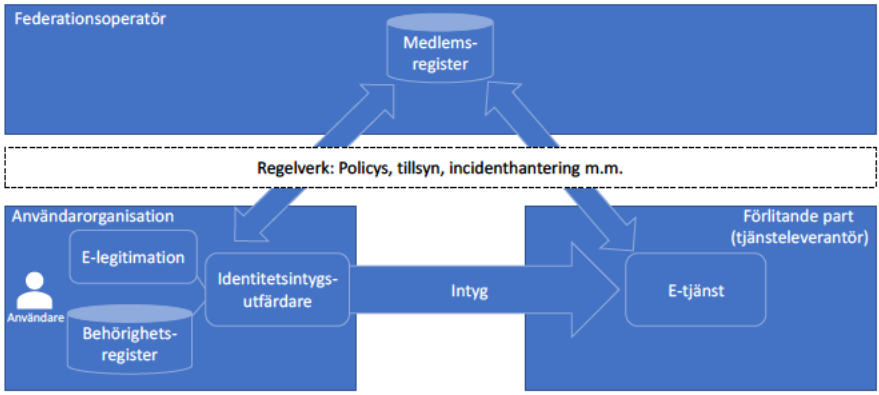
Vad som avses med en identitetsfederation framgår av avsnitt 3.12. Syftet med federationerna är att de förlitande parter som tillhandahåller e-tjänster ska kunna lita på identiteten och i förekommande fall behörigheten hos användaren av en tjänst.

Det finns en generell federation samt flera sektorsvisa och privata federationer i Sverige. Den generella federationen är Sweden Connect medan sektorspecifika är t.ex. Sambi, SWAMID och Skolfederation.[31] Stockholms stad och Karlstads kommun är exempel på organisationer som har egna federationer och det förefaller bli vanligare med egna organisations- eller koncerngemensamma federationer.

En identitetsfederation består av flera delar. Utöver att någon ska ansvara för själva federationen behövs det identitetsintygsutfärdare med tillgång till legitimeringsfunktion som sköter databaser med användaruppgifter och låter användare identifiera sig. Det behövs även förlitande parter som tillhandahåller e-tjänster (se figur 6.1). Det krävs därtill en anvisningstjänst för att hantera flera olika identitetsleverantörer och hjälpa användaren att hitta sin e-legitimation via leverantören eller sin organisation.

[28] www.digg.se/digital-identitet/e-legitimering/offentlig-aktor/nationell-e-legitimering#anslutna_organisationer (hämtad 2021-06-16).
[29] Promemoria, *Auktorisationssystem för elektronisk identifiering och för digital post*.
[30] A.a. s. 42.
[31] Federationen heter Skolfederation. Namnet anges därför inte i bestämd form.

Figur 6.1 Generaliserad översikt av en federationslösning



Källa: Apotekens Service AB, *Förstudierapport Identitets- och behörighetsfederation för eHälsa,* 15 juni 2012.

Reglerna i en federation omfattar vanligen kraven på identifiering men även tekniska- och organisatoriska säkerhetsåtgärder som deltagare behöver vidta. Normalt finns olika tillitsnivåer som ställer olika långtgående krav på en identitetsintygsutfärdare. Identitetsfederationer baseras vanligtvis på internationella standarder och används sedan länge i universitetsvärlden och inom det svenska skolväsendet men även för privata e-legitimationer. Det finns även i en federation överenskommelser eller avtal mellan identitetsleverantörer och förlitande parter om vad som ska skickas med i identitetsintyget och i förekommande fall andra attribut.

I metadataregistret för federationen finns uppgifter om de olika identitetsintygsutgivare som finns inom federationen och uppgifter om bl.a. de servercertifikat och stämplar de använder för att skydda överföringen och stämpla identitetsintygen. Det medför att en förlitande part kan känna igen tillhandahållaren av identitetsintyget och vice versa.

6.6.2 Sweden Connect

Sweden Connect är statens nationella identitetsfederation för elektronisk identifiering och inkluderar även Sveriges landsnod för gränsöverskridande åtkomst med stöd av eIDAS-förordningen (se mer om detta i avsnitt 4.2). DIGG ansvarar för och driver identitetsfederationen. Sweden Connect består av:

- Ett tekniskt ramverk.
- Metadata och kontaktinformation om alla anslutna aktörer.
- Avtal som knyter ihop förlitande parter med e-legitimationsutfärdare och den svenska eIDAS-noden.

En offentlig aktör som tillhandahåller en e-tjänst kan använda Sweden Connect både för uppkoppling mot svenska och utländska e-legitimationer. Det sker genom att denne tecknar avtal om Sweden Connect med DIGG och eventuellt även valfrihetssystem 2017 E-legitimering.

Det tekniska ramverket för Sweden Connect omfattar specifikationer för hur metadata ska användas och hur identitetsintyg ska begäras och levereras. Det tekniska ramverket utgår bl.a. från DIGG:s tillitsramverk.

6.6.3 Sambi

Sambi (Samverkan för behörighet och identitet inom hälsa, vård och omsorg) är tänkt att fungera som en nationell mötesplats för säker e-hälsa och länka samman e-tjänster och användarorganisationer.[32] Identitetsfederationen Sambi drivs av Internetstiftelsen och är öppen för alla aktörer inom vård-, hälso- och omsorgssektorn. Internetstiftelsen ansvarar för tillitsregler, tillitsgranskning, anslutningsavtal, tekniska krav, metadataregiser och hantering av s.k. Sambiombud.

Sambi används för inloggning över organisationsgränser av personal inom vård, omsorg och apotek. Sambi består av gemensamma regler och avtal och bygger på att deltagande organisationers säkerhetsarbete har granskats.

Sambi hänvisar till de e-legitimationer som har godkänts av DIGG. Det är obligatoriskt att ange e-legitimationens tillitsnivå från den identifiering av användaren som närmast föregått användarorganisationen (vårdgivarens) utställande av identitetsintyg.[33] Inom Sambi ställs krav på användarorganisationer gällande deras säkerhetsarbete som ska vara anpassat efter risker och säkerhetsbehov. Sambi erbjuder olika sätt för mindre aktörer att ansluta sig till federationen, t.ex. genom Sambiombud som paketerar teknik och administration i

[32] www.sambi.se (hämtad 2021-06-16).
[33] www.sambi.se/wp-content/uploads/2018/12/Sambi-Bilaga-2-Tekniska-krav-v1.52.pdf (hämtad 2021-06-14).

en tjänst som underlättar för användare att leva upp till kraven i tillitsramverket.[34]

6.6.4 SWAMID

Swedish Academic Identity Federation (SWAMID) är en identitetsfederation där de flesta lärosätena, forskningsnära och utbildningsnära myndigheter samt statliga muséer i Sverige ingår.[35] SWAMID drivs av Sunet[36]. I SWAMID finns kvalitetssäkrad inloggning av anställda, studenter och andra associerade i medlemsorganisationerna i Sverige. Det är också möjligt för en tjänsteägare att tillgängliggöra tjänsten även utanför Sverige genom interfederationen eduGAIN, t.ex. i resten av Norden, Europa, Nordamerika och Asien.

Syftet med identitetsfederationen är att sänka kostnaden för att hantera digitala identiteter inom och mellan organisationer. SWAMID:s policy och teknologi används för att etablera säkra och kontrollerbara associationer och transaktioner mellan identiteter och system. Medlemskap krävs för identitetsutfärdare och sådana organisationer som har användare som ska logga in i tjänster. För att bli godkänd ska organisationen visa att den uppfyller god praxis när det gäller identitetshantering.

SWAMID använder tre olika tillitsnivåer med definierade krav avseende profilen och granskningen av de olika nivåerna:[37]

– SWAMID Identity Assurance Level 1 – för personer och kallas för obekräftad användare. Användaren själv uppger informationen och ansvarar för denna.

– SWAMID Identity Assurance Level 2 – medlemsorganisationen vet vem det är och kallas för bekräftad användare. Lärosätet vet vem personen är och lärosätet ansvarar för kontot. SWAMID granskar tillitsdeklarationen.

[34] www.sambi.se/sambiombud/ (hämtad 2021-06-14).
[35] https://wiki.sunet.se/display/SWAMID (hämtad 2021-06-14).
[36] www.sunet.se/services/identifiering/swamid (hämtad 2021-06-14).
[37] https://wiki.sunet.se/display/SWAMID/SWAMID+Policy#SWAMIDPolicy-Tillitsprofiler (hämtad 2021-06-14).

– SWAMID Identity Assurance Level 3 – högre krav på att lärosätet vet vem personen är, kallas även verifierad användare. All inloggning sker som flerfaktorsautentisering. SWAMID granskar tillitsdeklarationen med hjälp av ett granskningsprotokoll.

6.6.5 Skolfederation

Syftet med Skolfederation är att underlätta svensk utbildningssektors användning av digitala tjänster och läromedel. Det görs genom att tillhandahålla en infrastruktur för inloggning som underlättar åtkomst till tjänster för elever och lärare ute på skolor runtom i landet. Tjänsten är en identitetsfederation, där förlitande parter litar på skolhuvudmäns användaridentifiering. Med Skolfederation får elever och lärare en standardiserad inloggningslösning och kan nå alla tjänsterna i skolmiljön, både de som finns i skolan och de som skolan abonnerar på via internet. Inom ramen för Skolfederation erbjuds också en lösning för att skapa, ändra och ta bort skolans användare hos federationens tjänsteleverantörer på ett standardiserat vis, s.k. federerad provisionering. Internetsstiftelsen är federationsoperatör för Skolfederation och Svenska institutet för standarder har inom ramen för TK 450/AG 4 tagit fram de attribut som skickas i identitetsintygen.

Skolfederation är öppen för:

- Skolhuvudman för någon av de skolformer som räknas upp i skollagen (2010:800) och som genom det allmänna eller det privata anordnar utbildning, eller
- utbildningsanordnare som bedriver utbildningar vid vilka studiestöd kan lämnas enligt studiestödsförordningen (2000:655) och dess tillhörande bilaga.
- En svensk myndighet som arbetar med skolan.
- En leverantör av e-tjänster som har rekommenderats av en skolhuvudman att bli medlem i Skolfederation.

För närvarande tillämpas tillitsnivåerna ”Bas” och ”2FA” inom Skolfederation. Målsättningen är att alla medlemmar på sikt ska kunna hantera en tillitsnivå motsvarande 2FA.

– Bas – godkänd medlem i Skolfederation: Bas medför inga andra krav än de som följer med medlemskapet i Skolfederation.
– 2FA – tvåfaktorsautentisering: Den skyddsklass för e-legitimationer och utställande av identitetsintyg vars grad av skydd motsvarar IMY:s krav på stark autentisering, då it-systemet är tillgängligt via internet och innehåller integritetskänsliga uppgifter. Ingen granskning av kravets efterlevnad görs av Skolfederation, utan detta åvilar skolhuvudmannen.

Valet av tillitsnivå styrs av e-tjänstens krav och baseras på de risker och skada som en felaktig identifiering kan medföra avseende användarens säkerhet, obehag eller oro samt tjänsteleverantörens renommé och rykte. Även ekonomisk skada och legala krav beaktas.

6.6.6 Interfederationen FIDUS

En interfederation är en överenskommelse mellan två eller flera federationsoperatörer som ingår i ett förbund för att sammansluta federationerna. Interfederation äger rum när en användare från en federation får åtkomst till en tjänst som är registrerad i en annan federation.[38]

Skolverket har tagit fram interfederationen FIDUS, som i nuläget ansluter Skolfederation och SWAMID, främst för användning i samband med digitala nationella prov. Fler federationer kan anslutas i framtiden. FIDUS står för Federationsförbund för IDentitetshantering, Utbildning och Skola.[39]

[38] Enligt Skolverkets ordlista från konferensen tekniksnack om digitala nationella prov, www.skolverket.se/download/18.6b138470170af6ce9141f6/1583847378476/Ordlista%20Skolverkets%20tekniksnack.pdf (hämtad 2021-06-14). Men även ”Federation för identiteter hos utbildning och skola” förekommer, www.skolfederation.se/nyhetsbrev/2018_04/ (hämtad 2021-06-14).
[39] www.skolverket.se/download/18.7f8c152b177d982455e1d17/1617176591317/VT2020-Fragestund-for-tekniker.pdf (hämtad 2021-06-14).

6.6.7 Tekniska lösningar för federerade identiteter och behörigheter

Det finns flera olika standarder som kan användas i identitetsfederationer. Användningen baseras dock på någon form av identitetsintyg från identitetsintygsutfärdare[40]. Standarderna har likartade byggstenar men är formaterade på olika sätt och använder olika tekniska lösningar.

SAML

Security Assertion Markup Language (SAML) är en öppen standard för federerad autentisering.[41] SAML version 2.0 används bl.a. av Sweden Connect, Skolfederation, Sambi och SWAMID. Det sker genom att skicka identitetsintyg från identitetsintygsutfärdare (förkortas IdP inom SAML) till förlitande parter (förkortas SP inom SAML). Det möjliggör säker kommunikation mellan användare och e-tjänster. SAML använder XML för kommunikationen mellan IdP och SP.[42] Det sker genom s.k. SAML assertions (identitetsintyg), en sorts XML-dokument som skickas till förlitande part. SAML är en standard som inte reglerar implementationen av aktuella identitetsfederationer på detaljnivå. För att kunna federera med SAML på ett effektivt sätt behöver ett antal vägval göras och dokumenteras. Den tekniska dokumentationen utgörs av dessa vägval och närmare reglering av hur standarden används, exempelvis i det tekniska ramverket för Sweden Connect.[43]

Identitetsfederering via SAML är baserat på att identitetsintygsgivare och förlitande parter litar på varandra och därmed kan verifiera de underskrifter och stämplar som används i SAML-kommunikationen. Rent tekniskt baseras denna tillit på att respektive parter litar på varandras URL:er och tillhörande servercertifikat. Tillitsprocessen automatiseras via användning av SAML metadata. Specifikationen av metadata är framtagen av OASIS för att underlätta administration av större federationer. Federationen definieras då av

[40] Även kallade IdP eller identity provider i SAML och OpenID provider i OPenIDconnect.
[41] Standardiserad av OASIS (The Organization for the Advancement of Structured Information Standards).
[42] Förkortningen XML står för Extensible Markup Language. XML är en teknisk standard för strukturmärkning av textbaserade elektroniska dokument.
[43] https://swedenconnect.se/tekniskt-ramverk.html (hämtad 2021-06-20).

ett register i XML-format som är stämplat med federationsoperatörens certifikat. Filen innehåller information om identitetsfederationens medlemmar inklusive deras servercertifikat. Eftersom metadatafilen är stämplad av federationsoperatören räcker det med att jämföra ett servercertifikat med dess motsvarighet i metadatat. En infrastruktur baserad på ett centralt federationsregister förutsätter att registret uppdateras kontinuerligt samt att federationsmedlemmarna alltid använder den senaste versionen av filen. För att kunna använda metadata krävs en central aggregator som kontinuerligt hämtar lokal metadata från federationsdeltagarna och uppdaterar och stämplar federationsregistret.

I identitetsfederationer har e-tjänster och motsvarande förlitande parter rollen som SP medan legitimeringstjänster som utfärdar identitetsintyg intar rollen som IdP och därmed är den som autentiserar användaren, oavsett mot vilken e-tjänst som användaren legitimerar sig. För de fall där e-tjänsten behöver mer information om användaren t ex. uppgift om behörighet, kan en fråga ställas till en attributtjänst (Attribute Authority [AA]), inom federationen, om sådan relevant attributtjänst finns, eller annars med stöd av OAuth 2.0 utanför federationen. Genom en attributsförfrågan kan e-tjänsten erhålla nödvändig kompletterande information för att kunna auktorisera användaren och ge tillgång till e-tjänsten eller motsvarande.

OAuth 2.0

OAuth 2.0 är ett standardiserat protokoll för auktorisation. Protokollet utvecklas och förvaltas av en arbetsgrupp inom IETF.[44] Syftet med protokollet är att underlätta användningen av behörighetsinformation för tredje part, dvs. användare i mobilappar, system m.m. OAuth 2.0 är ett ramverk som kontrollerar auktorisation till skyddade resurser. Protokollet kan använda resurser från en server för användarens räkning utan att användaren behöver autentisera sig. Protokollet gör det genom att tillåta att identitetsintygsutfärdare skickar vidare attributsintyg till tredje part när användaren godtar det. Det används bl.a. i mobilappar som t.ex. Facebook när appen frågar om tillstånd att använda mobiltelefonens kontakter för att ansluta till de

[44] Av Internet Engineering Taskforce, IETF, ramverket i RFC 6749.

av kontakterna som har Facebook. Det finns fyra roller enligt OAuth 2.0:

– Resursägare
– Klient
– Resursserver
– Auktorisationsserver

Resursägaren är användaren som tillåter att en applikation får tillgång till dennes uppgifter. Klienten är applikationen som vill använda användarens uppgifter, t.ex. en e-tjänst. Innan den gör det måste den auktoriseras av användaren och auktorisationen ska valideras via ett API. Resursservern lagrar användarens konto och auktorisationsservern verifierar användarens identitet.

OpenID Connect

OpenID Connect är ett identitetslager på OAuth 2.0-protokollet.[45] OpenID Connect började som proprietära lösningar från bl.a. Google som sedan har blivit industristandard.[46] Det är den standard som används när inloggning via exempelvis Google, Microsoft eller Facebook används för att identifiera sig mot en annan aktörs tjänst, t.ex. forum eller e-handelswebbplats. OpenID Connect bygger på OAuth 2.0 för att tillhandahålla identifieringstjänster. OpenID Connect har ett antal tillägg till OAuth 2.0-protokollet genom ett ID-token, vilket är ett säkerhetstoken i formen av ett JSON Web Token (JWT), som gör att klienten kan verifiera användarens identitet. ID-token hämtar även användarens grundläggande profil där ett API returnerar information om användaren. Det pågår arbete med att skapa en OpenID Connect-profil för Sweden Connect, utöver de SAML-profiler som används, och för att DIGG ska kunna ge federativt stöd för OpenID Connect i framtiden.

[45] https://openid.net (hämtad 2021-06-14).
[46] OpenID Connect kontrolleras av Open ID Foundation.

6.6.8 Attributshantering

Det är svårt men viktigt, inte minst ur ett informationssäkerhetsperspektiv, att underhålla behörighetsregister. Det ställs även i dataskyddsförordningen[47] rättsliga krav på att myndigheter har behörighetsstyrning och, för de aktörer som omfattas, krav genom MSB:s föreskrifter om informationssäkerhet för statliga myndigheter[48] samt MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter[49].

Det finns flera möjliga lösningar på att tillhandahålla attribut. Det kan vara nationella register eller tjänster, det kan också ske lokalt hos e-tjänsten eller hos arbets- eller uppdragsgivaren. Det är i dag vanligt att den som tillhandahåller en e-tjänst som personer från andra organisationer använder har ett behörighetsregister. Antingen direkt i tjänsten eller genom att en eller ett par personer från de organisationer som använder e-tjänsten administrerar konton för de egna användarna. Det finns också exempel på nationella centrala register med attribut som t.ex. HSA-katalogen inom hälso- och sjukvården. Det gör att om en person slutar eller av andra skäl inte längre ska ha rätt att hantera ett förfarande för sin organisation behöver organisationen inte bara ändra i sina egna register utan även i alla externa e-tjänster där personen har behörighet.

Ett annat sätt att hantera det är att användarorganisationen själva tillhandahåller den behörighetsinformation som behövs. Det möjliggör dessutom att det för en organisation bara är ett register som behöver uppdateras och underhållas även om detta kan innefatta att kontroller behöver ske mot andra centrala register, exempelvis mot registret över legitimerad hälso- och sjukvårdspersonal (HOSP) för att hämta eller validera uppgifter om en anställd.

På motsvarande sätt som identitetsintyg som tillhandahålls av en identitetsintygsutfärdare kan en offentlig aktör vara, själv eller via en extern part, attributtjänst och tillhandahålla attributsintyg med aktuell behörighetsinformation om sina anställda. För de fall där e-tjänsten behöver mer information om användaren som loggar in, exempelvis uppgift om behörighet kan en fråga ställas till en attributtjänst som genom en s.k. attributbegäran (”attribute query”) kan erhålla nöd-

[47] Exempelvis för att förhindra en personuppgiftsincident såsom t.ex. obehörigt röjande eller obehörig åtkomst.
[48] MSBFS 2020:6.
[49] MSBFS 2020:7.

vändig kompletterande information. Härvid kan teoretiskt sett alla typer av e-legitimationer, även de som inte innehåller några specifika personuppgifter, såsom koddosor för generering av engångslösenord, användas för inloggning mot en myndighet som kräver såväl personnummer som ytterligare information om behörighet. Där de identifieringsuppgifter som behövs överförs i identitetsintyget och de attribut som krävs kan överföras i ett attributsintyg. Det finns för närvarande få attributstjänster på det svenska e-legitimationsområdet. Inom ramen för de olika federationerna finns det profiler eller format för identitetsintyg. Vissa federationer, Skolfederation och Sambi har dessutom tagit fram attributsprofiler.[50] Sambi:s attributsprofil förvaltas av Inera. Vad gäller Skolfederation har attributsprofilen tagits fram av SIS.[51]

Det finns exempel på länder som har försökt arbeta med stora centrala behörighetsregister för att lösa problemen med att ge behörigheter till användare. Centrala register skulle inte lösa problemet med att underhålla aktuell behörighetsinformation på en plats. Det skulle vidare samla uppgifter som kan vara mycket känsliga ur ett säkerhets- och dataskyddsperspektiv. Det finns även länder och organisationer som arbetar med att lagra behörighetsinformationen i egna certifikat på t.ex. smarta kort, men detta leder till en problematisk underhållssituation eftersom roller och behörigheter ofta ändras, vilket då kräver att nya certifikat utfärdas.

Bolagsverket tillsammans med andra myndigheter arbetar, inom ramen för uppdraget om förvaltningsgemensam digital infrastruktur för informationsutbyte, med en nationell infrastruktur för standardiserad digital fullmaktshantering.[52] Infrastrukturen är tänkt att göra det möjligt att kunna agera med hjälp av fullmakter eller skapa fullmakter även i egna digitala tjänster och API:er finns för det syftet. Möjligheten att kunna hålla fullmaktsregister åt de som inte har egen kapacitet undersöks också. Anslutna organisationer ges åtkomst till ett administrativt gränssnitt för att konfigurera sina fullmaktsmallar. De får även behörigheter för fullmakter som gäller hos dem. Följande API:er erbjuds:

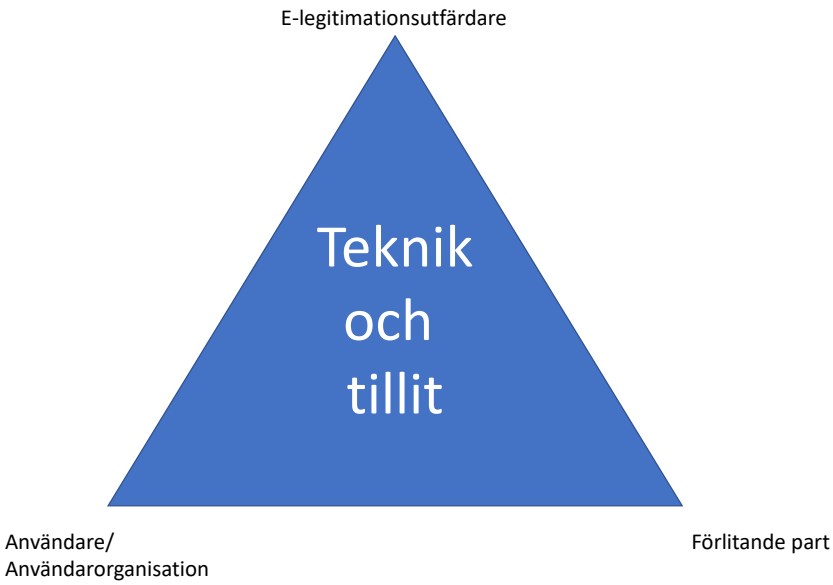
[50] www.sambi.se/wp-content/uploads/2019/05/Sambi_Attributspecifikation_1.5.pdf (hämtad 2021-06-14).
[51] www.skolfederation.se/wp-content/uploads/2018/10/Skolfederation_Attributprofil_4_1.pdf (hämtad 2021-06-14).
[52] *Gode män och förvaltare – en översyn.* (SOU 2021:36), s. 434 f.

- API för firmateckningstjänsten – Används för att se vilka och i vilken kombination firmatecknare kan signera en fullmakt.
- API:er för digital fullmaktsförmedlare (DFM) – Används för att skapa fullmakt, hämta fullmaktsmall, ta bort, använda och visa fullmakt.

6.7 En sammanfattande bild

I de tidigare avsnitten beskrivs de olika delarna av e-legitimationsområdet i Sverige. Förenklat uttryckt är de mest grundläggande förhållandena inom e-legitimationsområdet de som existerar mellan e-legitimationsutfärdare, användaren av e-legitimationer (eller användarorganisationer om det rör sig om e-tjänstelegitimationer) samt förlitande parter med e-tjänster som kräver autentisering med e-legitimationer.

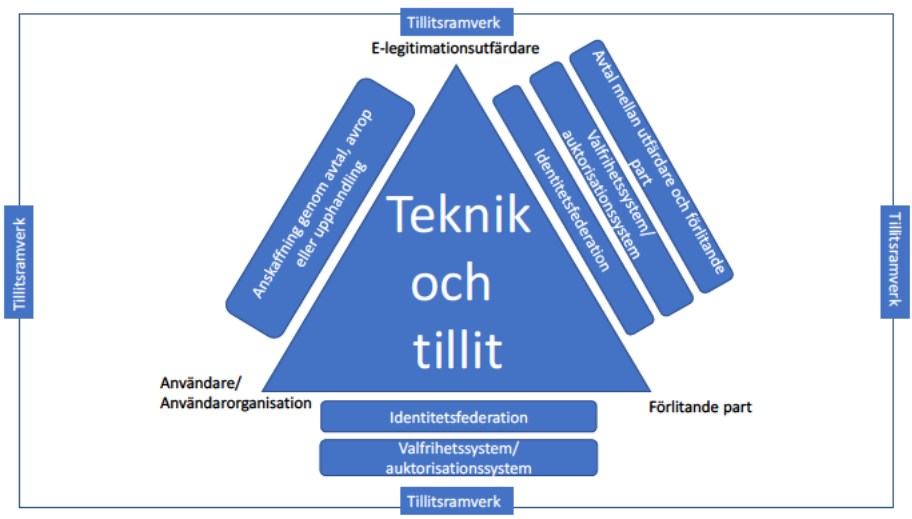
Figur 6.2 Grundläggande förhållanden inom e-legitimationsområdet



Det är inte alltid tre separata aktörer som innehar dessa roller och vad gäller e-tjänstelegitimationer kan arbetsgivaren i vissa fall även vara e-legitimationsutfärdaren. E-legitimationsutfärdaren är inte heller alltid identitetsintygsutfärdaren. Till detta finns även andra tekniska

komponenter som inte framgår av figuren, exempelvis attributregister. Sett till området som helhet är det emellertid viktigt att utgå från dessa tre roller för att förstå hur de olika delarna hänger samman. En grundläggande förutsättning för att systemet ska fungera är därtill att det både finns en teknisk infrastruktur samt att det finns tillit mellan de aktörer som har respektive roll.

Figur 6.3 Grundläggande förhållanden samt stödstrukturer



För att åstadkomma tillit och den tekniska infrastruktur som behövs krävs ytterligare aktörer och stödstrukturer. Systemet är inte beroende av ett tillitsramverk för att fungera. Ramverket skapar emellertid en stabil grund som främjar tillit och underlättar interaktioner genom att skapa en gemensam referensram samt en granskning som alla aktörer kan förlita sig på. Exempelvis kan användaren utgå från tillitsramverket för att försäkra sig om att en e-legitimation uppfyller vissa krav på säkerhet. En arbetsgivare som anskaffar e-legitimationer till sina anställda kan därtill vid upphandling kravställa utifrån en viss tillitsnivå utan att i upphandlingsunderlaget behöva gå ner på teknisk detaljnivå. Detsamma gäller vid avrop från ramavtal som inom den offentliga förvaltningen är en mycket viktig stödstruktur för att underlätta anskaffning av e-tjänstelegitimationer. Även i det förfarandet skapar tillitsramverket tydlighet för alla inblandande parter.

I relationen mellan e-legitimationsutfärdare och förlitande part skapar ramverket förutsättningar för att utifrån allmänt vedertagna nivåer bestämma den tillitsnivå som krävs för åtkomst till dennes e-tjänster. På samma sätt kan ramverket användas för att uppställa krav i identitetsfederationer alternativt i valfrihetssystemen eller det föreslagna auktorisationssystemet. Funktioner som i sin tur underlättar sammankopplingen mellan utfärdare och förlitande part. De skapar därtill förutsättningar för användare och användarorganisationer att få åtkomst till den förlitande partens e-tjänster.

7 Den offentliga förvaltningens behov avseende e-legitimation i tjänsten

7.1 Kartläggning av behov

Den del av utredningens uppdrag som redovisas i detta betänkande omfattar kartläggning och analys av den offentliga förvaltningens behov av åtgärder avseende användning av e-legitimation i tjänsten samt förslag på sådana åtgärder. En beskrivning av hur kartläggningsarbetet har genomförts framgår av avsnitt 2.2. Det har inte varit möjligt för oss att ta del av eller inhämta uppgifter om behov avseende e-legitimation i tjänsten från alla aktörer i den offentliga förvaltningen. Bilden är med andra ord inte heltäckande. Utifrån det skriftliga underlag vi har haft tillgång till och de muntliga uppgifter vi inhämtat har vi emellertid identifierat ett antal behov och utmaningar på området där vi upplever att det finns en samsyn bland berörda aktörer.

7.2 Användningsområden för e-legitimationer i tjänsten

E-legitimationer som används i tjänsten inom förvaltningen har enligt vår kartläggning tre huvudsakliga användningsområden: Autentisering i interna system, identifiering som en del i processen att skapa elektroniska underskrifter samt organisationsöverskridande användning. Användningen av e-legitimationer kan i detta avsnitt avse både användning av privata e-legitimationer eller e-tjänstelegitimationer.

Frågor om e-legitimation i tjänsten besvarades av sammanlagt 114 myndigheter i E-legitimationsenkäten från 2019, varav 89 svarande var kommuner. Av de svarande uppgav 89 procent att de har behov av e-legitimation för autentisering i interna system, 87 procent att de har behov av organisationsöverskridande användning och 83 procent att de har behov av e-legitimationer i samband med skapandet av elektroniska underskrifter.[1]

7.2.1 Autentisering i interna system

Ett grundläggande behov hos myndigheter är identitets- och behörighetshantering vilket innefattar att säkerställa att endast behöriga personer ges åtkomst till myndigheternas it-miljöer och it-system samt att åtkomst till information och funktioner är anpassade efter vad personen har rätt att ta del av. Det samlingsnamn vi använder för dessa miljöer och system är interna system och det kan exempelvis vara handläggarsystem, ekonomisystem eller datorprogram för att skicka e-post. De autentiseringsmetoder som utifrån vår kartläggning förefaller mest utbredda är användning av användarnamn och lösenord samt smarta kort, varav vissa kort även är bärare för e-legitimationer. Lösningar med mobiltelefoner som bärare används också och användning av sådana lösningar förväntas öka. Bärarna av e-legitimationen kan i många fall användas till mer än autentisering i interna system, t.ex. genom att ge åtkomst till lokaler eller utskriftsfunktioner. Det förekommer vidare att olika typer av autentiseringsmetoder används inom samma myndighet beroende på vilket system det rör sig om.

7.2.2 Skapande av elektroniska underskrifter

Den offentliga förvaltningen ser ett ökat behov av att kunna skapa elektroniska underskrifter.[2] För många av de lösningar som används för att skapa elektroniska underskrifter inom förvaltningen används e-legitimationer för att identifiera personen som i steget därefter

[1] SKR, *Rapport enkät e-legitimationer – 2019 kommuner och regioner*, s. 18.
[2] *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen (*SOU 2021:9*)*, s. 121.

skriver under. Det kan exempelvis vara beslut som skrivs under elektroniskt eller e-post som skrivs under elektroniskt och krypteras.[3]

7.2.3 Organisationsöverskridande användning

Det elektroniska informationsutbytet mellan myndigheter är omfattande. Sådana utbyten kan genomföras från system till system. De kan också genomföras genom att anställda vid en myndighet loggar in i en e-tjänst som en annan myndighet tillhandahåller och lämnar eller hämtar uppgifter i den tjänsten. Kartläggningen visar att e-legitimationer är en lösning som används för autentisering för att ge tillgång till e-tjänster. Exempel på tjänster är Skatteverkets e-tjänst för att lämna kontrolluppgifter, Försäkringskassans tjänst LEFI Online och Riksgäldens tjänst Statens internbanks system (SIBS). Ytterligare ett exempel är identifiering för videomöten, där legitimering av deltagare sker internt i organisationer eller för deltagare från andra organisationer. Exempelvis har Försäkringskassan numera en lösning för videomöten med regionerna som innebär att när vissa personuppgifter diskuteras används e-legitimationer för att identifiera deltagarna och på så sätt leva upp till kraven i Socialstyrelsens föreskrifter.[4] Liknande autentiseringslösningar torde även kunna användas för att komma runt behovet av motringningar vid andra fall av muntliga utlämnanden av patientupplysningar.

När en person loggar in i en e-tjänst som är avsedd för företrädare för organisationer, t.ex. myndigheter eller företag, kan den som tillhandahåller e-tjänsten ha ett behov av att säkerställa vilken organisation personen företräder. Det kan alltså behöva säkerställas att en person som ska lämna uppgifter från t.ex. en kommun faktiskt företräder kommunen. Kartläggningen visar att ett vanligt sätt att lösa det i dag är att det till e-tjänsten är kopplat en administratörsfunktion. En eller flera personer vid t.ex. en kommun myndighet ges behörighet att i administratörsfunktionen registrera vilka personer vid kommunen som får logga in i den aktuella e-tjänsten som tillhandahålls av t.ex. en statlig myndighet, exempelvis genom att registrera personernas personnummer. Om personen autentiserar sig med e-legitimation kan personnumret användas för att säkerställa att

[3] SKR, *Rapport enkät e-legitimationer – 2019 kommuner och regioner*, s. 18.
[4] HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.

det är rätt person och att personen företräder kommunen samt är behörig att använda tjänsten på kommunens vägnar.

Det har under kartläggningsarbetet inte framkommit att e-legitimationer i dagsläget används över landsgränserna i tjänsten. Som framgår av avsnitt 4.2.2 har Sverige lämnat in en föranmälan avseende e-legitimationssystem enligt eIDAS-förordningen. I dagsläget finns emellertid inget svenskt e-legitimationssystem som kan användas över gränserna inom ramen. Det är visserligen möjligt för exempelvis myndigheter att erkänna e-legitimationer från andra medlemsstater, men någon förekomst av sådan användning har vi inte identifierat. Däremot visar kartläggningsarbetet att svenska myndigheter ser behov av att deras anställda i framtiden ska kunna använda e-legitimationer gentemot myndigheter i andra medlemsstater eller att svenska myndigheter ska kunna erkänna e-legitimationer från anställda vid myndigheter i andra medlemsstater.

7.3 Användning av privata e-legitimationer i tjänsten

Ovan beskrivs de tre huvudsakliga användningsområden vi har identifierat för användning av e-legitimation i tjänsten. Kartläggningen visar att det är vanligt förekommande att anställda inom den offentliga förvaltningen använder sina privata e-legitimationer inom alla tre användningsområden.

Vår bedömning är att ett antal faktorer ligger bakom denna utbredda användning. Användning av e-legitimationer är redan omfattande i samhället och många har en privat e-legitimation. Anställda är vana vid att använda e-legitimationer i egenskap av privatpersoner och använder dem frekvent för att genomföra diverse ärenden och transaktioner. Tidigare har även anskaffning av e-tjänstelegitimationer upplevts som problematisk (se avsnitt 7.6.1).

En annan faktor som driver på utvecklingen för både privata e-legitimationer och e-tjänstelegitimationer är behovet av att skydda information och att säkerställa att rätt person tar del av den. Vi bedömer att det inom förvaltningen råder en uppfattning om att e-legitimationer överlag har en stark koppling till de personer som använder dem och att det därför är lämpligt att använda e-legitimationer för att säkerställa en säkrare autentisering. Till det hör också olika krav eller rekommendationer avseende autentisering som för-

valtningen måste beakta. Det kan finnas krav eller rekommendationer att använda sig av exempelvis tvåfaktorsautentisering, stark autentisering eller liknande (se mer om detta i avsnitt 4.3). Användning av e-legitimationer kan vara ett sätt att leva upp till sådana krav. Inom e-hälsoområdet pågår även arbete på EU-nivå om en rekommendation om att krav på tillitsnivå hög enligt eIDAS-förordningen för åtkomst till uppgifter inom området.[5]

7.3.1 Användningen av privata e-legitimationer väcker frågor

Användningen av privata e-legitimationer inom förvaltningen beror enligt vår uppfattning på att de anses säkerställa den tillitsnivå som myndigheterna efterfrågar samtidigt som både vissa arbetsgivare och arbetstagare kan uppleva det som en smidig lösning. Vi kan dock konstatera att det råder delade meningar inom förvaltningen om anställda bör använda privata e-legitimationer i tjänsten. Vissa aktörer inom förvaltningen som har ingått i vår kartläggning har gett uttryck för att de anser att sådan användning är helt i sin ordning, med utgångspunkt att det viktiga är att identifiera rätt person. Liknelser har bl.a. gjorts med att anställda använder sina körkort inom ramen för sin anställning. Kartläggningen visar emellertid även att användningen av privata e-legitimationer också väcker frågor inom förvaltningen och att det bland flera aktörer finns en tveksamhet eller motvilja mot sådan användning.

Vissa aktörer har uppgett att det kan finnas ett motstånd mot att använda sin privata e-legitimation inom ramen för sin anställning. Motståndet kan bl.a. grunda sig i att anställda inte vill att deras personnummer exponeras eller att de i allmänhet inte är bekväma med att använda sin privata e-legitimation i tjänsten. Andra aktörer har däremot uppgett att de inte upplever något motstånd bland deras anställda i denna fråga.

Möjligheten att få tillgång till privata e-legitimationer i Sverige är ofta förknippat med ett krav på innehav av ett svenskt personnummer. Personer som arbetar inom förvaltningen och som saknar personnummer kan därför inte utföra arbetsuppgifter som kräver en privat svensk e-legitimation för att genomföra.

[5] eHAction, *D8.2.4 – Common eID Strategy for Health in the European Union*, s. 34 f.

Användning av privata e-legitimationer väcker också frågor om risker och riskhantering. Exempelvis vilka risker arbetsgivaren måste bära när dess anställda använder privata e-legitimationer inom ramen för anställningen. Om privata e-legitimationer används för att logga in i e-tjänster kan det i sin tur ställa krav på fullgod behörighetshantering, för att inte riskera att en person kan fortsätta att logga in i tjänsten efter det att denne har avslutat sin anställning.

De administratörsfunktioner som i många fall är förknippade med e-tjänster som företrädare ska använda syftar till att säkerställa att företrädaren är behörig att företräda sin myndighet. Det är primärt myndigheten som avgör det, inte förlitande part. För att denna ordning ska fungera tillfredsställande krävs att den myndighet som delar ut behörighet till sina anställda säkerställer full livscykelhantering avseende behörigheten. Om personen i fråga inte längre är behörig, t.ex. för att anställningen upphör, måste behörigheten tas bort. Det är emellertid inte självklart att åtkomsttilldelningen i praktiken följer förändringar som borde påverka tilldelningen.[6] Om autentisering i den aktuella e-tjänsten görs med privat e-legitimation finns annars risken att personen fortsatt kan autentisera sig i tjänsten och att det för förlitande part uppfattas som att personen fortfarande företräder myndigheten. Aktörer inom förvaltningen med många olika verksamhetsgrenar, såsom kommuner, kan behöva hantera många administratörsfunktioner gentemot många olika myndigheter.

Ytterligare en fråga som ett flertal aktörer inom förvaltningen har lyft är om de kan kräva att någon som är anställd vid en annan myndighet ska använda sin privata e-legitimation i tjänsten.

7.4 Användning av e-tjänstelegitimationer

Som framgår ovan tillhandahåller aktörer inom förvaltningen olika lösningar för autentisering av sina anställda i interna system. Dessa lösningar är vanligen framtagna för att möta behovet av autentisering internt och vår uppfattning är att många aktörer inom förvaltningen inte uppfattar dem som e-legitimationer. Detta kan bero på avsaknaden av en tydlig och vedertagen definition av vad som utgör en e-legitimation. Lösningarna kan emellertid bygga på samma teknik som e-legitimationer och finnas på samma typer av bärare. Smarta

[6] Inera, *IAM Strategi – Med kommunernas behov i fokus*, 20 maj 2020, s. 9.

kort som endast används för autentisering internt innehåller exempelvis i många fall ett certifikat som används för autentisering, dvs. samma teknik som är vanlig i e-legitimationer. Även om lösningarna är framtagna för att möta interna behov har många myndigheter uttryckt önskemål om att den lösning de använder internt också ska kunna användas över organisationsgränserna.

Kartläggningen visar att det finns ett flertal statliga myndigheter, kommuner och regioner som tillhandahåller e-tjänstelegitimationer till sina anställda. Inom hälso- och sjukvårdssektorn är användningen av SITHS omfattande. Regionerna tillhandahåller SITHS till en stor del av sina anställda men inom många kommuner tillhandahålls lösningen endast till en begränsad krets som behöver åtkomst till e-tjänster som kräver autentisering med SITHS. SITHS används bl.a. för inloggning i tjänster såsom Nationell patientöversikt och Intygstjänster.[7] Det finns också federationer, t.ex. Sambi och Skolfederation, inom vilka elektroniska identitetsintyg utställda av arbetsgivaren kan användas över organisationsgränserna. Vad gäller e-tjänstelegitimationer i allmänhet som inte omfattas av en federation visar kartläggningen att de i dagsläget nästan uteslutande används för autentisering i interna system och inte kan användas för autentisering i tjänster som andra myndigheter tillhandahåller.

En annan aspekt som kan leda till utmaningar vid användning av e-tjänstelegitimationer är att exempelvis en läkare kan arbeta för olika regioner samtidigt alternativt ha flera olika arbetsställen och uppdrag inom samma region eller att en person t.ex. kan ha två olika roller inom en kommun som både anställd och förtroendevald. Även avsaknad av personnummer utgör en utmaning (se avsnitt 7.6.4).

7.5 E-tjänstelegitimationer efterfrågas

Den sammantagna bild vi får av kartläggningen är att många aktörer i den offentliga förvaltningen ser behov av användning av e-tjänstelegitimationer. Behoven avser de tre användningsområden som framgår av avsnitt 7.2.

Efterfrågan grundar sig i ett flertal faktorer. Vissa e-tjänstelegitimationer uppfattas bl.a. som en helhetslösning som minskar behovet av alternativa autentiseringsmetoder. Vi kan dock konstatera att

[7] www.inera.se/tjanster/alla-tjanster-a-o/siths-identifieringstjanst/ (hämtad 2021-06-14).

vissa e-tjänstelegitimationer som används inom förvaltningen i dag möter behov inom främst en sektor. Socialstyrelsen menar t.ex. i rapporten *E-hälsa och välfärdsteknik i kommunerna 2020* att SITHS-korten är anpassade för hälso- och sjukvårdens personalgrupper men att det saknas generella alternativ som ger samma nivå på säkerheten också för socialtjänstens personal.[8]

Dessutom uppfattas e-legitimationer som en lösning som kan erbjuda hög säkerhet och en säkrare autentisering (jfr avsnitt 7.3).

Som framgår av avsnitt 7.3.1 finns det inom delar av förvaltningen en motvilja mot att använda privata e-legitimationer i tjänsten. E-tjänstelegitimationer ses som ett sätt att minska behovet av att använda privata e-legitimationer. Möjligheten att i e-tjänstelegitimationer använda andra personidentifieringsuppgifter än personnummer är ytterligare en faktor som driver på efterfrågan. Detsamma gäller möjligheten att kunna koppla legitimationen till organisationen och eventuellt ytterligare attribut. Vidare bedömer vi att en starkt drivande faktor vad gäller efterfrågan på e-tjänstelegitimationer är förhoppningen att de ska kunna användas över organisationsgränserna. Det är i anslutning till detta viktigt att påpeka att myndigheter inte nödvändigtvis vill anskaffa nya autentiseringslösningar till sina anställda. Som tidigare nämnts är förhoppningen i stället hos vissa att deras nuvarande lösningar ska kunna användas gentemot andra organisationer.

7.6 Utmaningar vid användning av e-tjänstelegitimationer i den offentliga förvaltningen

E-tjänstelegitimationer efterfrågas av förvaltningen men kartläggningen visar att området är förenat med ett flertal utmaningar. Bilden bekräftas i *Rapport enkät e-legitimationer*, där SKR konstaterar att området är det som tydligast träder fram som en utmaning för kommuner och regioner men även statliga myndigheter inom e-legitimationsområdet.[9] Vidare konstaterar Socialstyrelsen i rapporten *E-hälsa och välfärdsteknik i kommunerna 2020* att det är ett problem att det saknas en standard för e-legitimationer som garanterar användarens

[8] Socialstyrelsen, *E-hälsa och välfärdsteknik i kommunerna 2020*, s. 71.
[9] SKR, *Rapport enkät e-legitimationer – 2019 kommuner och regioner*, s. 25.

identitet och roll vid arbete i den egna organisationen, och i samarbete med andra organisationer.[10]

7.6.1 Anskaffning av e-tjänstelegitimationer

I svar på E-legitimationsenkäten från 2019 framkom att det fanns myndigheter som ansåg att det var problematiskt att anskaffa e-tjänstelegitimationer till sina anställda och att det saknades alternativ på marknaden som motsvarade deras behov. Vissa gav även uttryck för att det i praktiken inte fanns några alternativ till användning av privata e-legitimationer. Vår bedömning är emellertid att situationen på relativt kort tid har förändrats. Vi kan konstatera att det i dagsläget finns ett flertal e-tjänstelegitimationer på marknaden. Även själva anskaffningen har underlättats genom Kammarkollegiets ramavtal Identifiering och behörighet från vilket statliga myndigheter, kommuner och regioner kan göra avrop (se mer om ramavtalet i avsnitt 6.5.3).

7.6.2 Användning av e-tjänstelegitimationer över organisationsgränserna

Det finns i dag olika e-tjänstelegitimationer inom den offentliga förvaltningen och möjligheterna att använda dem över organisationsgränserna är begränsade till olika sektorer och sektorsspecifika federationer. En myndighet som tillhandahåller e-tjänstelegitimationer till sina anställda kan inte räkna med att de kan användas för autentisering gentemot andra myndigheter. E-tjänstelegitimationer som omfattas av en federation kan med stor sannolikhet inte heller användas gentemot organisationer som inte ingår i federationen. Det kan således uppstå en situation där en anställd t.ex. har en e-tjänstelegitimation som används för autentisering i interna system, ett SITHS-kort för att kunna ta del av vårddokumentation och därutöver kan behöva använda sin privata e-legitimation för att få åtkomst till e-tjänster hos statliga myndigheter.

Användning av privata e-legitimationer i statliga e-tjänster leder även till en hel del administration då detta oftast innefattar att exempelvis varje enskild kommun måste ha en behörighetsadministratör

[10] Socialstyrelsen, *E-hälsa och välfärdsteknik i kommunerna 2020*, s. 8.

för varje e-tjänst som anställda vid kommunen använder sig av. Det är således många olika behörighetsregister hos många olika myndigheter som måste hållas uppdaterade. Detta medför en administrativ börda men det utgör också en informationssäkerhetsrisk om dessa register inte hålls uppdaterade.

Att det i dagsläget inte är möjligt att använda e-tjänstelegitimationer obehindrat mellan olika organisationer inom den offentliga förvaltningen beror enligt vår bedömning bl.a. på bristande tillit mellan aktörerna inom förvaltningen och, fram tills nyligen, avsaknad av tillräckligt många granskade och godkända e-tjänstelegitimationer. Vad gäller tilliten är det svårt för myndigheter att bedöma om den lösning en annan myndighet använder är tillräckligt säker och om myndigheten har fullgoda processer, policys etc. på plats. Förlitande part kan t.ex. sakna insyn i hur den andra aktören har säkerställt att e-tjänstelegitimationen har utfärdats till rätt person. För att öka tilliten mellan aktörerna inom förvaltningen i detta avseende har gemensamma processer och ramverk efterfrågats under vårt kartläggningsarbete. Att göra det möjligt att använda lösningar över organisationsgränserna kan också kräva tekniska anpassningar hos förlitande part eller hos e-legitimationsutfärdaren.

Förlitande parter har behövt anpassa sig efter den verklighet som råder och har i avsaknad av gemensamma lösningar och federationer många gånger utvecklat e-tjänster som kräver att anställda vid andra myndigheter autentiserar sig med sina privata e-legitimationer. Det är dock en lösning ett flertal myndigheter har uppgett att de vill sluta använda sig av och i stället övergå till autentisering med e-tjänstelegitimationer.

Som framgår av avsnitt 6.6 finns det ett antal sektorsspecifika identitetsfederationer. För aktörer inom den offentliga förvaltningen som måste vara ansluten till flera federationer innebär detta merkostnader och merarbete då olika federationer uppställer olika krav.

7.6.3 Osäkerheter avseende behörigheter och attribut

En person som är anställd vid en myndighet som i tjänsten autentiserar sig i en e-tjänst hos en myndighet gör det i egenskap av företrädare för sin myndighet. Alla anställda vid en myndighet har emellertid inte behörighet att vidta åtgärder på myndighetens vägnar.

Myndigheter vi har talat med har gett uttryck för att behörigheten är viktig i sammanhang när anställda ska logga in i andra aktörers e-tjänster. Det verkar emellertid inte i första hand vara roller eller titlar som avgör om en person ska uppfattas som behörig av förlitande part. Den gemensamma nämnare dessa aktörer har gett uttryck för är att de efterfrågar, utöver identiteten för en viss person, uppgift om vilken organisation personen företräder. Att veta att det är en viss person som företräder en viss offentlig aktör verkar således som utgångspunkt räcka för att förlitande parter ska acceptera att personen är behörig att företräda myndigheten. Det kan emellertid inte uteslutas att ytterligare attribut i vissa fall är nödvändiga och att dessa kan skilja sig åt mellan olika e-tjänster. Vidare har flertalet myndigheter, kommuner och regioner vi talat med sett det som att en nationell katalog inte är en lösning som är önskvärd ur ett säkerhets- eller dataskyddsperspektiv. De ser heller inte att behörighetshantering i respektive e-tjänst är en bra lösning eftersom det är svårt att underhålla när personer slutar eller byter roller inom en organisation. Flertalet pekar även på att behörighetsinformationen borde komma från respektive arbetsgivare som då får betydligt färre register att hantera gällande behörigheter. Det finns dock undantag till det inom t.ex. hälso- och sjukvården som har ett centralt register, HSA-katalogen.[11] Vidare finns det önskemål om att vissa grundläggande attribut, som t.ex. uppgifter om firmatecknare tillhandahålls centralt.

7.6.4 Anställda och uppdragstagare utan personnummer

Eftersom det som regel krävs ett svenskt personnummer för att kunna få en privat e-legitimation riskerar personer som saknar personnummer att stängas ute från e-tjänster som förvaltningen tillhandahåller. Kartläggningen visar att det inte är ett problem enbart avseende privata e-legitimationer. Det är också förenat med svårigheter för anställda och uppdragstagare inom förvaltningen som saknar personnummer att få en e-tjänstelegitimation. Det rör sig både om nyanlända personer och personer från andra länder som arbetar inom offentlig sektor under en begränsad period och därför inte folkbokförs i Sverige. Problematiken uppstår även för s.k. gränsgångare som bor i ett annat land men som arbetar i Sverige. Dessa hinder kan

[11] Det kan här noteras att vissa regioner också har lokala kataloger med attribut.

uppstå inom de flesta delar av förvaltningen men problemen förefaller vanligast förekommande inom utbildnings- samt hälso- och sjukvårdssektorerna. Exempelvis krävs personnummer för att vårdpersonal ska kunna få SITHS-kort som uppfyller kraven enligt tillitsnivå 3. Dessa personer är därför förhindrade att använda vissa tjänster där kraven på autentisering är satta på denna nivå.

7.6.5 Åtkomst för privata utförare

En stor andel av välfärden inom offentlig sektor tillhandahålls i dagsläget genom privata utförare. Dessa utförare behöver ges samma förutsättningar som aktörer inom det offentliga vad gäller tillgång till olika e-tjänster som krävs för att de ska kunna fullgöra sina uppdrag.

7.6.6 Oklarheter avseende DIGG:s tillitsramverk i förhållande till tillitsnivåerna i eIDAS-förordningen

Det har under kartläggningsarbetet framkommit att det både inom förvaltningen och hos utfärdare finns en osäkerhet kring hur DIGG:s tillitsramverk förhåller sig till tillitsnivåerna i eIDAS-förordningen. Svenska myndigheter verkar i stor utsträckning tillämpa DIGG:s tillitsramverk när de fattar beslut om vilken tillitsnivå de ska kräva för åtkomst till en e-tjänst. Likaså verkar ramverket vara utgångspunkt när myndigheterna anskaffar e-tjänstelegitimationer. Vid gränsöverskridande användning av e-legitimationer ska emellertid tillitsnivåerna i eIDAS-förordningen tillämpas (se avsnitt 4.2.3).

7.6.7 Säker grundidentifiering och möjlighet till id-växling

Ett robust och tillförlitligt e-legitimationssystem förutsätter att det går att lita på grundidentifieringen av respektive användare. Det har under kartläggningen tydligt framkommit att för att e-tjänstelegitimationer ska kunna användas över organisationsgränserna måste organisationerna känna tillit till den grundidentifiering som sker. Det har vidare framkommit att det kan vara svårt för myndigheter att bedöma de metoder som används samt att grundidentifieringen är invecklad och kostsam för utfärdarna.

Därtill visar kartläggningen att behovet av att kunna skapa nya elektroniska identitetshandlingar, s.k. id-växling, är stort. En säker grundidentifiering som tillåter id-växling har av många myndigheter framförts som önskvärt eftersom de dels slipper göra en ny grundidentifiering när en ny handling ska skapas, dels kan lita på elektroniska identitetshandlingar eftersom den identifiering som ligger till grund för dem är säker.

7.6.8 Behov av stöd

54 procent av de som besvarade E-legitimationsenkäten uppgav att de har behov av mer information om e-legitimation i tjänsten.[12] Denna bild bekräftas av våra kontakter med DIGG, Kammarkollegiet och SKR. Behovet kommer framför allt från mindre aktörer och de frågor som ställs rör allt från kostnader till grundläggande tekniska och juridiska aspekter. Frågor om e-legitimation i tjänsten är också ofta sammankopplad med frågor om elektroniska underskrifter. Det framstår bland vissa aktörer finnas stor begreppsförvirring och en osäkerhet kring vad det är de egentligen behöver. De har därmed svårt att anskaffa rätt tjänster med anknytning till både elektronisk identifiering och elektroniska underskrifter.

[12] DIGG, *E-legitimering inom den offentliga förvaltningen – Enkätundersökning 2019* (dnr 2019-389), s. 24.

8 Internationell utblick

8.1 Danmark

I Danmark är det sedan ett antal år tillbaka obligatoriskt för invånare att använda digitala självbetjäningstjänster samt att ta emot digital post från myndigheter.[1] NemID är den dominerande e-legitimationslösningen i Danmark och den används av ca 4,7 miljoner personer.[2] E-legitimationerna utfärdas av företaget Nets DanID på uppdrag av danska staten.[3] För närvarande pågår arbete med att gå över från NemID till den nya lösningen MitID, som också kommer att utfärdas av Nets DanID.

Till NemID är ett register kopplat som innehåller s.k. kärnidentiteter som avser varje person. Varje person har ett unikt nummer och till det numret finns andra uppgifter kopplade, exempelvis personnummer och namn. Det är emellertid inte personnumret som är det unika nummer som används för att identifiera en enskild individ inom ramen för NemID.

NemID utfärdas till en person i egenskap av privatperson men den kan också användas inom ramen för en anställning. För anställda finns möjlighet att använda NemID medarbejdersignatur som är ett certifikat som kan användas till att identifiera sig som medarbetare från en verksamhet eller en organisation. Detta ska inte förväxlas med en elektronisk underskrift, men med NemID medarbejdersignatur går det att bl.a. skriva under elektroniskt, logga in i e-tjänster och, i vissa fall, även logga in i interna it-system.[4] Genom att använda NemID medarbejdersignatur kopplas identiteten till ett organisationsnummer, som medför att en person kan vidta handlingar på en

[1] https://en.digst.dk/policy-and-strategy/mandatory-digitisation/self-service/ (hämtad 2021-06-14).
[2] https://en.digst.dk/digitisation/eid/next-generation-nemid/ (hämtad 2021-06-14).
[3] A.a.
[4] www.nemid.nu/dk-da/om-nemid/erhverv/ (hämtad 2021-06-14).

organisations vägnar.[5] Det finns i dagsläget ca 1,5 miljoner NemID medarbejdersignatur utfärdade. De används främst av offentligt anställda men det finns också användare inom privat sektor.

För tillgång till e-tjänster som tillhandahålls av offentliga aktörer, såsom statliga myndigheter och kommuner, finns en gemensam inloggningslösning som heter NemLog-in.[6] Genom att använda lösningen behöver användaren endast logga in en gång för att ges tillgång till alla tjänster. Genom att använda NemLog-in går det att koppla ytterligare attribut till det unika nummer som är kopplat till respektive NemID. För den som använder NemID medarbejdersignatur går det alltså att koppla fler attribut än organisationen till identiteten. Läkare eller revisorer i kommuner kan exempelvis autentisera sig utifrån sin yrkesroll för att få tillgång till offentliga register eller andra tjänster som endast personer med rätt behörighet har tillgång till. Attribut om en enskild person kan hämtas från olika källor såsom centrala register (t.ex. danska patientsäkerhetsregistret vad gäller läkare). Dessutom kan arbetsgivare lägga till attribut för sina anställda.

Eftersom NemID ska ersättas av MitID pågår arbete med att fasa ut NemID medarbejdersignatur. Den kommer att ersättas med en lösning som benämns MitID Erhverv.[7]

8.2 Estland

I Estland har staten tagit ett helhetsansvar vad gäller digitala identiteter och lösningar för autentisering. Det är obligatoriskt för medborgare i Estland och medborgare från andra EU-länder som bor i Estland permanent att ha ett nationellt ID-kort som tillhandahålls av staten.[8] Kortet är försett med ett chip och kan användas som e-legitimation för autentisering gentemot en stor mängd e-tjänster, både offentliga och sådana som tillhandahålls av företag eller andra organisationer. Det finns också lösningar för andra bärare, såsom mobiltelefoner.

[5] Se följande exempel: https://medarbejdere.au.dk/en/administration/it/guides/security/employeesignature/ (hämtad 2021-06-13).
[6] https://en.digst.dk/digitisation/nemlog-in/ (hämtad 2021-06-14).
[7] https://migrering.nemlog-in.dk/nemlog-in-erhvervslosning/ (hämtad 2021-06-14).
[8] www.id.ee/en/rubriik/introduction/ (hämtad 2021-06-13).

Med e-legitimationen kan en person identifiera sig. Uppgifter som används i processen är namn och en personidentifieringsuppgift som har flera likheter med svenska personnummer. E-legitimationen används både när en person ska utföra handlingar i egenskap av privatperson och när handlingar utförs som representant för en organisation. Information om roller eller behörigheter för personer finns i olika register, exempelvis inom hälso- och sjukvårdsområdet[9] och utbildningsområdet.[10] Om en person ska logga in i en e-tjänst i egenskap av representant, t.ex. för ett företag eller för en myndighet, görs en förfrågan från e-tjänsten till aktuellt register. För flera av de register som finns går det, utöver automatiserad behandling, också att göra manuella sökningar.

8.3 Finland

I Finland finns ett antal olika e-legitimationer och i likhet med den svenska marknaden utfärdas dessa bl.a. av banker.[11] När det gäller lösningar för organisationer tillhandahåller Myndigheten för digitalisering och befolkningsdata s.k. organisationskort, som är ett smartkort avsett för anställda.[12] Kortet är knutet både till organisationen och den anställde och kan bl.a. användas för inloggning i organisationens egna datasystem, inloggning i den offentliga förvaltningens e-tjänster samt som ett led i skapandet av elektroniska underskrifter. Certifikatet innehåller bl.a. den anställdes namn, e-postadress, organisation samt enhet inom organisationen. Om en anställning upphör ska det aktuella kortet spärras. Organisationskort används av många aktörer inom den offentliga förvaltningen i Finland. Enligt uppgift används emellertid även andra lösningar av anställda i tjänsten, t.ex. mobila certifikat för anställda samt privata e-legitimationer.[13]

Inom områdena socialtjänst och hälsa finns gemensamma lösningar som också tillhandahålls av Myndigheten för digitalisering och befolkningsdata som bl.a. möjliggör autentisering. Exempelvis finns ett yrkeskort som är avsett för yrkesutbildade personer inom dessa områden, t.ex. läkare, farmaceuter, sjuksköterskor och socio-

[9] Health Board Registers (Terviseameti Registrid): https://mveeb.sm.ee/Tervishoiutootajad/ (hämtad 2021-06-13).
[10] Estonian Education Information System (EHIS): www.ehis.ee/ (hämtad 2021-06-13).
[11] Hinsberg, Hille m.fl., *Study on Nordic-Baltic Trust Services*, 2020, s. 33.
[12] https://dvv.fi/sv/organisationskort (hämtad 2021-06-14).
[13] E-post från Transport- och kommunikationsverket, 6 maj 2021.

nomer.[14] Det rör sig om yrken för vilka det finns register över de som har rätt att utöva yrket.[15] Med kortet kan personer inom de yrken som omfattas autentisera sig i datasystem samt skriva under patientjournaler och recept elektroniskt. Yrkeskortet är avgiftsfritt, men det kan tillkomma en avgift för registrering och kontroll av uppgifter kopplade till beställning av kortet. För personal inom social- och hälsoområdet som inte omfattas av de yrken som kan få yrkeskortet finns ett personal- och aktörskort som kan användas för autentisering i it-system och e-tjänster.[16]

Statens center för informations- och kommunikationsteknik (Valtori) tillhandahåller systemet Virtu som kan användas av anställda vid myndigheter för att logga in i myndighetens egna tjänster och i tjänster som tillhandahålls av andra myndigheter.[17] Systemet syftar till att skapa tillit mellan utfärdare av identiteter och förlitande parter. Ett stort antal myndigheter och e-tjänster är ansluta till systemet.[18]

I Finland finns även tjänsten Suomi.fi-fullmakter genom vilken privatpersoner, företag och samfund kan ge någon annan fullmakt att sköta ärenden på deras vägnar.[19]

Det pågår ett projekt för att utveckla den digitala identiteten i Finland.[20] Projektet ska pågå fram till mitten av 2023 och ett av målen är att ge alla som behöver möjlighet att identifiera sig elektroniskt i den offentliga förvaltningens tjänster. Detta ska även gälla vid utförandet av arbetsuppgifter.

8.4 Norge

I Norge finns ett antal utfärdare av e-legitimationer. De flesta utfärdas av privata företag men det finns också en lösning som tillhandahålls av den statliga myndigheten Digitaliseringsdirektoratet. Myndigheten tillhandahåller även en gemensam inloggningslösning

[14] https://dvv.fi/sv/yrkeskort-for-social-och-halsovarde (hämtad 2021-06-13).
[15] Exempelvis Registren över yrkesutbildade personer inom social-, hälso- och sjukvården: https://julkiterhikki.valvira.fi/ (hämtad 2021-06-13).
[16] https://dvv.fi/sv/personal-och-aktorskort-for-social-och-halsovarden (hämtad 2021-06-13).
[17] https://valtori.fi/sv/administrationstjanster-for-identiteter-och-atkomst (hämtad 2021-06-14).
[18] https://wiki.eduuni.fi/display/CSCVIRTU/Organisaatiot (hämtad 2021-06-14) samt https://wiki.eduuni.fi/display/CSCVIRTU/Palvelut (hämtad 2021-06-14).
[19] www.suomi.fi/fullmakter (hämtad 2021-06-13).
[20] https://vm.fi/sv/digital-identitet (hämtad 2021-06-14).

för offentliga e-tjänster som heter ID-porten.[21] Lösningen ger tillgång till över 1 000 statliga och kommunala e-tjänster.

Den del av e-legitimationsmarknaden som fokuserar på privatpersoner domineras av norska BankID (inte samma lösning som i Sverige), som tillhandahålls av ett antal norska banker.[22] Dessa e-legitimationer är privata men används enligt uppgift också när anställda ska använda e-tjänster.[23] På den norska marknaden finns emellertid också e-legitimationslösningar som är avsedda för användning i tjänsten.

Bestämmelser om användning av e-legitimation i tjänsten av anställda vid myndigheter finns i ”forskrift om elektronisk kommunikasjon med og i forvaltningen” (eForvaltningsforskriften).[24] Enligt 17 § i nämnd reglering ska myndigheter ge sina anställda anvisningar om vilka säkerhetstjänster och produkter de ska använda och hur de ska gå tillväga för att införskaffa utrustning och sådant som t.ex. certifikat och PIN-koder. Efter anvisning kan alltså anställda själva anskaffa t.ex. e-legitimationslösningar.[25] Enligt 19 § första stycket ska data för underskriftsframställning, certifikat och lösenord/PIN-koder som är ämnade för användning i tjänsten inte användas för andra ändamål. Vidare föreskrivs i 19 § andra stycket att personliga certifikat inte ska användas i tjänsten, med undantag för om de är utställda eller godkända för sådan användning. Slutligen krävs vid användning av elektroniska underskrifter enligt 18 § att myndigheten inhämtar samtycke från den anställda om utställande och utleverans av certifikatet.

På hälso- och sjukvårdsområdet finns Helsenettet som är en digital plattform för alla aktörer inom sektorn. Genom Helsenettet kan aktörer kommunicera samt utbyta personuppgifter och patientinformation.[26] Helsenettet drivs av Norsk helsenett, som är ett offentligt styrt organ som ägs av Helse- og omsorgsdepartementet. Inom Helsenettet finns en gemensam inloggningslösning som heter HelseID som också fungerar som en identitetsfederation.[27] Det går att använda olika e-legitimationslösningar för autentisering i HelseID.

[21] https://eid.difi.no/index.php/nb/id-porten (hämtad 2021-06-14).
[22] Hinsberg, Hille m.fl., *Study on Nordic-Baltic Trust Services*, 2020, s. 38.
[23] E-post från Digitaliseringsdirektoratet, 14 maj 2020.
[24] FOR-2004-06-25-988: https://lovdata.no/dokument/SF/forskrift/2004-06-25-988 (hämtad 2021-06-14).
[25] Se t.ex. Buypass för organisationer (bedrifter), som kan beställas av den anställde själv: www.buypass.no/produkter/elektroniskID (hämtad 2021-06-14).
[26] www.nhn.no/ (hämtad 2021-06-14).
[27] www.nhn.no/samhandlingsplattform/helseid (hämtad 2021-06-14).

9 Utredningens förslag

9.1 Utgångspunkter för utredningens förslag

Utredningen har, i den del som är aktuell för slutbetänkandet, i uppdrag att kartlägga och analysera den offentliga förvaltningens behov av åtgärder för att kunna använda e-legitimation i tjänsten samt att lämna förslag på sådana åtgärder.

E-legitimationsområdet som helhet är som tidigare konstaterats underreglerat. Detta har i sin tur lett till att det finns många olika lösningar och samarbeten inom e-tjänstelegitimationsområdet men att de olika delarna i dagsläget inte skapar en sammanhållen helhet. I efterföljande avsnitt presenteras de åtgärder vi, med beaktande av de prioriteringar den begränsade utredningstiden medfört, anser behövs för att tillgodose de identifierade behoven och som kan bidra till att skapa ett mer sammanhållet system.

Våra förslag utgår vidare utifrån hur det svenska e-legitimationsområdet är utformat. Identifierade behov hade kunnat tillgodoses genom den typen av mer centraliserad lösning som bl.a. återfinns i Danmark och Estland (se mer om dessa lösningar i kapitel 8). Detta hade emellertid krävt genomgripande förändringar som hade haft mycket stor påverkan på både offentlig och privat sektor. Om en sådan utveckling anses önskvärd behöver det enligt vår bedömning därför utredas i särskild ordning.

Som framgår av avsnitt 7.2.3 är organisationsöverskridande åtkomst ett av användningsområdena för e-legitimationer i tjänsten. Vad gäller sådan användning är det flera aktörer inom den offentliga förvaltningen som under kartläggningsarbetet betonat att de helst ser att informationsutbyten sker system till system i stället för att medarbetare loggar in i en annan aktörs e-tjänster. Vi ser även att utvecklingen rör sig i denna riktning och att det av olika anledningar är att föredra framför extern autentisering med e-tjänstelegitimationer.

Frågeställningar med koppling till sådana utbyten ligger dock utanför ramen för detta utredningsuppdrag. I avvaktan på en sådan övergång är extern autentisering med e-tjänstelegitimationer inom den offentliga förvaltningen dock en nödvändig lösning som det kommer finnas behov av i många år framöver.

Vi har i delbetänkandet berört frågan om digital delaktighet.[1] Det får, utifrån de olika författningar som berör tillgänglighet och diskriminering i arbetslivet, förutsättas att de e-legitimationer som används i tjänsten uppfyller sådana tillgänglighetskrav att en ökad användning av e-tjänstelegitimationer inte utesluter vissa grupper från att nyttja dem.

9.2 Användning av privata e-legitimationer i tjänsten

Utredningens bedömning: Användning av privata e-legitimationer i tjänsten är tillåten men det kräver att det finns en överenskommelse om detta.

Privata e-legitimationer i tjänsten bör endast användas när det inte är möjligt att använda e-tjänstelegitimationer för att fullgöra en arbetsuppgift eller när det av annan anledning är befogat.

Skälen för utredningens bedömning

Det har under en längre tid funnits frågor kring lämpligheten av användning av privata e-legitimationer i tjänsten. Utredningens kartläggningsarbete visar att både e-tjänstelegitimationer och privata e-legitimationer i dagsläget används av anställda eller uppdragstagare i den offentliga förvaltningen. Utredningen om effektiv styrning av nationella digitala tjänster bedömde att arbetsgivare som ställer krav på elektronisk identifiering för att en individ ska kunna utföra sina arbetsuppgifter också ska förse individen med det medel som krävs för att göra detta. Samt att en elektronisk identitetshandling som arbetstagare använder i tjänsten är att betrakta som ett verktyg för tjänsten. Om en arbetsgivare kräver att anställda ska använda privata e-legitimationer krävdes det enligt utredningens bedömning att det

[1] *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9), s. 138 ff.

framgår av anställningsavtalet. Flera remissinstanser, framför allt inom den kommunala sektorn, motsatte sig denna bedömning. I samband med vår kartläggning har vi också kommit i kontakt med aktörer som anser att användning av privata e-legitimationer bör vara tillåten. Det är även tydligt i våra kontakter med offentliga aktörer, arbetsgivarorganisationer och centrala fackliga organisationer att detta är en fråga som aktualiseras med jämna mellanrum. Vi ser det därför som påkallat att närmare gå igenom de olika aspekter som aktualiseras vid användning av en privat e-legitimation i tjänsten.

9.2.1 Behandling av personuppgifter

Den personuppgiftsbehandling som sker vid användning av privata e-legitimationer är vanligtvis en överföring av namn och personnummer till den förlitande parten. Om e-legitimationen använts för identifiering för att sedan underteckna en handling elektroniskt är dessa uppgifter även i regel möjliga att ta del av från den undertecknade handlingen och alla som har tillgång till den. Detta gäller emellertid inte om underskriftstjänsten är utformad på ett sådant sätt att dessa uppgifter inte inkluderas i underskriften.

Personnummer och samordningsnummer utgör inte känsliga personuppgifter i dataskyddsförordningens mening, men har ändå getts en särställning genom att medlemsstaterna med stöd av artikel 87 getts möjlighet att införa särskilda villkor för behandlingen. Villkoren ska i sådana fall säkerställa att identifikationsuppgifterna bara får användas med iakttagande av lämpliga skyddsåtgärder för de registrerades fri- och rättigheter.[2]

I Sverige har en sådan bestämmelse förts in i 3 kap. 10 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (härefter dataskyddslagen). Av paragrafen framgår att personnummer och samordningsnummer endast får behandlas utan samtycke när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Bestämmelsen motsvarar den som återfanns i 22 § i den numera upphävda personuppgiftslagen (1998:204). I 3 kap. 11 § dataskyddslagen anges att regeringen får meddela ytterligare föreskrifter om i vilka fall behandling av personnummer och sam-

[2] Prop. 2017/18:105, s. 101.

ordningsnummer är tillåten. Några sådana föreskrifter har i skrivande stund inte meddelats.

En bestämmelse om behandling av personnummer och samordningsnummer kan, oavsett om den tas in direkt i sektorsspecifik lag eller i förordning med stöd av bemyndigandet, tillåta behandling i andra fall än de som tillåts enligt den föreslagna bestämmelsen i dataskyddslagen. En avvikande bestämmelse måste dock leva upp till förordningens krav på lämpliga skyddsåtgärder för de registrerades fri- och rättigheter.[3]

Av förarbetena till 3 kap. 10 § dataskyddslagen framgår att bestämmelsen innebär att en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär ska göras. Omständigheter som bör tillmätas betydelse vid intresseavvägningen är exempelvis om det eftersträvade syftet med behandlingen kan uppnås på annat sätt, behandlingens omfattning och om den förutsätter samkörning av register. Bestämmelsen bör enligt förarbetena även tolkas och tillämpas på ett likartat sätt som 22 § personuppgiftslagen. Praxis kring tillämpningen av bestämmelsen i personuppgiftslagen bör således vara vägledande.[4] IMY har med beaktande av bestämmelsen uttalat att personnummer bör exponeras så lite som möjligt.[5]

Bestämmelsen i 3 kap. 10 § dataskyddslagen rör när behandling utan samtycke är tillåten. Det bör noteras att arbetsgivare i de flesta fall inte kan använda sig av samtycke som rättslig grund vid behandling av arbetstagares personuppgifter.[6]

Vid användning av en privat e-legitimation är det enligt vår bedömning inte självklart vem som har personuppgiftsansvaret för den behandling som sker. Det är de faktiska omständigheterna i det enskilda fallet som avgör vem som är personuppgiftsansvarig.

IMY har framfört att arbetsgivaren måste se till att all behandling av personuppgifter som utförs i tjänsten uppfyller dataskyddsförordningens krav, t.ex. i fråga om ändamål med behandlingen, gallring och säkerhet. Detta gäller enligt IMY oavsett om behandlingen sker på arbetsplatsen, i hemmet eller på en tjänsteresa. Arbetsgivaren

[3] A.a. s. 102.
[4] Prop. 2017/18:105, s. 199.
[5] www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/personnummer/ (hämtad 2021-06-14).
[6] www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/tillaten-behandling--vilka-krav-galler/rattslig-grund/ (hämtad 2021-06-12).

behöver därför enligt myndigheten lämna tydliga instruktioner som beskriver hur de anställda får behandla personuppgifter.[7]

Om e-legitimationen används för autentisering i interna system eller i samband med elektroniskt undertecknade av handlingar som sker inom den egna organisationen bör arbetsgivaren således anses vara personuppgiftsansvarig för denna behandling. Om den privata e-legitimationen däremot exempelvis används för att logga in i en tjänst hos en extern förlitande part och e-legitimationen är installerad på en privat mobiltelefon är förhållandet dock mer oklart. Arbetsgivaren har anvisat denna användning och den sker i tjänsten men den faktiska behandlingen sker helt och hållet mellan e-legitimationsutfärdaren och den förlitande parten. Även om arbetsgivaren rent formellt skulle bedömas ha personuppgiftsansvaret är det förenat med betydande svårigheter för arbetsgivaren att faktiskt utöva kontroll över den behandling som sker. Utredningen om effektiv styrning av nationella digitala tjänster bedömde att om personuppgifter behandlas i tjänsten på en privat anordning har arbetsgivaren personuppgiftsansvaret och är därför skyldig att kontrollera utrustningen i fråga. Något som enligt utredningen kan innebära att arbetsgivaren får del av den anställdes privata information.[8]

All behandling av personuppgifter måste enligt dataskyddsförordningen ha stöd i en rättslig grund. En arbetsgivare måste alltså säkerställa att det finns stöd för den behandling som sker. Även om sådant stöd finns måste även 3 kap. 10 § dataskyddslagen beaktas. En omständighet som enligt de ovan redovisade förarbetsuttalandena kan tillmätas betydelse vid intresseavvägningen är som ovan nämns om det eftersträvade syftet med behandlingen kan uppnås på annat sätt. Vad gäller användning av privata e-legitimationer i tjänsten får omständigheten att exponering av personnummer i många fall kan undvikas genom användning av e-tjänstelegitimationer där personnummer inte exponeras enligt vår bedömning anses starkt tala emot användningen vid en sådan intresseavvägning.

[7] www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/arbetsgivarens-personuppgiftsansvar/ (hämtad 2021-06-12).
[8] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 272.

9.2.2 Banksekretess vid användning av BankID

Vid användning av BankID överförs utöver namn och personnummer ytterligare en uppgift av relevans ur integritetshänseende. Detta då det indirekt går att dra slutsatsen att användaren är kund i en viss bank eftersom den utfärdande banken anges på certifikatet. Denna uppgift omfattas av den s.k. banksekretessen som framgår av 1 kap. 10 § lagen (2004:297) om bank- och finansieringsrörelse. Av paragrafens första stycke följer att enskildas förhållanden till kreditinstitut inte obehörigen får röjas. Banksekretessen är inte absolut eftersom endast obehörigt röjande av kundinformation är förbjuden. Av förarbetena till bestämmelsen framgår även att regeln om banksekretess är dispositiv så till vida att en kund i ett särskilt fall kan lämna sitt uttryckliga eller underförstådda samtycke till att banken lämnar ut uppgifter. Samtycke anses dock inte kunna lämnas på förhand genom att banken förelägger kunden allmänna villkor med ett sådant innehåll.[9]

I utfärdande bankers användarvillkor för BankID finns bl.a. följande exempel på skrivningar rörande detta.

> Skandinaviska Enskilda Bankens användarvillkor för BankID
>
> Kunden är medveten om och medger att:
>
> …
>
> - Kundens användning av BankID/Mobilt BankID hos någon annan än SEB medför att den parten kommer att få kännedom om vem som utfärdat Kundens BankID/Mobila BankID och att detta i sin tur innebär att Kundens sekretesskyddade uppgift om med vilken bank Kunden har ett avtalsförhållande avslöjas[10]
>
> Swedbanks användarvillkor för BankID
>
> När du använder ditt BankID registreras ditt namn, personnummer och kort- eller certifikatsnummer samt uppgift om vilken bank som utfärdat kortet eller det elektroniska certifikatet hos Banken eller hos annan där du använder ditt BankID. Detta medför att när du använder BankID

[9] Prop. 2002/03:139, s. 478 f.
[10] Skandinaviska Enskilda Banken, *Villkor Betalkonton och Betaltjänster, m.m. – Privat*, gällande fr.o.m. 19 april 2021, s. 15 f.

hos någon annan än Banken får denne kännedom om vilken bank som har utfärdat BankID:t, vilket annars är en uppgift som omfattas av sekretess.[11]

Av dessa två exempel på användarvillkor framgår att skrivningarna skiljer sig åt men att grundprincipen är att användaren, vid varje användningstillfälle som inte sker hos den utfärdande banken, underförstått lämnar sitt medgivande till att uppgiften om kundförhållandet med den utfärdande banken lämnas till tredje part. Således innebär varje användning av BankID i tjänsten, som inte sker hos den utfärdande banken, att en medarbetare lämnar sitt samtycke till att banksekretessen frångås.

9.2.3 Villkor för användning av privata e-legitimationer

Vid all användning av privata e-legitimationer förbinder sig användaren att följa vissa villkor. Som framgår av exemplen nedan varierar detaljnivån på användarvillkoren vad avser användarens skyldigheter.

Användarvillkor för Freja eID

Ett Freja eID är personligt och får inte användas av annan än Innehavaren. Freja eID är att betrakta som en värdehandling och ska därför förvaras och hanteras på ett betryggande sätt.

Innehavaren ansvarar för all användning av Tjänsten och för att sina inloggningsuppgifter skyddas mot obehörig åtkomst. Innehavaren ansvarar även för att skydda sin mobiltelefon, läsplatta eller motsvarande enhet mot otillåten användning och står för risken om någon obehörig använt Tjänsten.[12]

Nordeas användarvillkor för BankID

Ett BankID är personligt och får endast användas av dig. Du ska vidta nödvändiga åtgärder för att skydda dig mot att BankID används obehörigt. I miljöer där stöldrisken är stor ska särskild vaksamhet iakttas och BankID ska hållas under kontinuerlig uppsikt.

Du ansvarar för hur BankID används och står för risken om någon obehörig använt ditt BankID. Det innebär att du är ansvarig för skada eller förlust som åsamkas Banken, tredje man eller dig själv om du uppsåtligen eller genom oaktsamhet inte iakttar dessa villkor.

[11] Swedbank, *VILLKOR BankID-privat*, 1 april 2021, s. 2.
[12] https://frejaeid.com/allmanna-villkor/ (hämtad 2021-06-11).

BankID är att betrakta som en värdehandling och ska därför förvaras och hanteras på ett betryggande sätt. Du ska:

a) endast ladda ner BankID till enhet som du har kontroll över;

b) inte ladda ner BankID till enhet på oskyddad plats, t.ex. dator i offentlig miljö till vilken fler personer än du har tillgång;

…

d) inte överlåta möjligheten att disponera över BankID till annan (eller använda annans BankID);

e) inte använda BankID, eller möjliggöra annans användning av BankID, på ett sätt som bryter mot användarvillkoren, lag eller annan författning eller som ett led i brottslig handling av något slag, exempelvis bedrägeri, penningtvätt eller finansiering av terrorism;

…

Du ska även:

- säkert förvara Mobilt BankID, BankID på fil och BankID på kort.

…

- inte använda Mobilt BankID, BankID på fil eller BankID på kort på ett sätt som ger annan än dig möjlighet att använda ditt BankID för legitimerings- och underskriftsändamål,

- skydda din mobila enhet och dator mot obehörigt intrång t.ex. använda antivirusprogram, brandvägg samt använda de tillämpliga säkerhetsanordningar, exempelvis den mobila enhetens låskod, som den mobila enheten har,

…

- radera BankID på fil som nedladdats och lagrats på oskyddad plats (t.ex. dator till vilken andra personer har tillgång),

…[13]

[13] Nordea, *Allmänna villkor BankID* (9681V008).

Som framgår av de exemplifierade användarvillkoren är det användaren som står risken vid obehörig användning som skett uppsåtligen eller av grov oaktsamhet. Vid användning av privata e-legitimationer i tjänsten måste därför innehållet i dessa villkor beaktas av arbetsgivaren och en riskbedömning göras. Eftersom det är vanligt att sådana villkor regelbundet uppdateras är detta en kontroll som vidare behöver ske löpande. Sådana aspekter som särskilt bör beaktas är hur en mobiltelefon eller dator som tillhandahålls och ägs av arbetsgivaren förhåller sig till villkoren för det fall en anställd förväntas installera en e-legitimation på dessa. Detta gäller i synnerhet om det fordras att användning av e-legitimationen sker på delade enheter. Något som per definition inte borde vara uteslutet med hänsyn till nu gällande villkor men som kräver att användaren har kontroll över dels enheten, dels användningen av e-legitimationen på den aktuella enheten. Fråga har även väckts under kartläggningsarbetet om installation av programvara som låter arbetsgivaren utöva kontroll över en mobiltelefon skulle kunna anses stå i strid med användarvillkoren.

9.2.4 Arbetsrättsliga aspekter

För att använda en e-legitimation krävs i dagsläget tillgång till dator, mobiltelefon eller surfplatta. Enligt 2 kap. 7 § arbetsmiljölagen (1977:1160) ska arbetsgivare tillhandahålla personlig skyddsutrustning. Utöver det finns i svensk rätt ingen författningsreglerad skyldighet för arbetsgivare att tillhandahålla den utrustning som krävs för att en arbetstagare ska kunna utföra sitt arbete. Arbetsgivarens skyldighet att tillhandahålla arbetsutrustning såsom dator, mobiltelefon eller surfplatta brukar i stället regleras i kollektivavtal och det är vanligt förekommande att arbetsgivare enligt avtalen ska tillhandahålla denna typ av utrustning. Det kan sägas råda en princip om att arbetsgivaren tillhandahåller den utrustning arbetet kräver. Vid bedömning av om en person ska anses vara arbetstagare eller uppdragstagare vägs därtill in om arbetsgivaren tillhandahåller arbetsutrustning (jfr AD 2012 nr 24). Arbetsgivare och arbetstagare har dock möjlighet att avtala om att arbetstagarens privata utrustning ska användas.

Det finns inga bestämmelser som förbjuder användning av privata e-legitimationer i tjänsten. Arbetsgivare och arbetstagare har således möjlighet att komma överens om att en privat e-legitimation, och

för detta syfte, även en eventuell privat mobiltelefon, surfplatta eller dator, ska användas i tjänsten. Det finns inga formkrav för en sådan överenskommelse och den kan vara muntlig. Att privat utrustning nyttjas kan dock i teorin innebära en rätt till ersättning för arbetstagaren.

Det finns således inga hinder mot användning av en privat e-legitimation i tjänsten om överenskommelse om detta finns. Den stora arbetsrättsliga frågan rörande användning av e-legitimation i tjänsten är dock om arbetsgivaren har rätt att kräva att en arbetstagare ska använda sin privata e-legitimation i tjänsten om denne inte vill det.

Arbetsgivare har en omfattande rätt att leda arbetet (den s.k. arbetsledningsrätten). Arbetstagaren är skyldig att följa de beslut som arbetsgivaren fattar med stöd av arbetsledningsrätten så länge den utövas inom ramen för arbetstagarens arbetsskyldighet. Ett brott mot denna skyldighet kan utgöra arbetsvägran som kan leda till sanktioner såsom skadestånd, disciplinpåföljd eller till och med uppsägning eller avskedande.

Enkelt uttryckt kan man till arbetsledningsrättens område hänföra frågor om vem som ska utföra arbete, vilket arbete som ska utföras samt frågor om var, när och hur arbetet ska utföras. Gränserna för arbetsledningsrätten framgår i huvudsak av Arbetsdomstolens praxis. Arbetsdomstolen uttalade bl.a. följande i avgörandet AD 2015 nr 61.

> När det gäller arbetsledningsbeslut är den principiella utgångspunkten att arbetsgivaren kan fatta sådana beslut efter fritt val, i den mån inte annat följer av avtal eller lag. En ytterligare utgångspunkt är emellertid att arbetsledningsrätten ska utövas under iakttagande av lag och goda seder på arbetsmarknaden.

Vi bedömer att arbetsledningsrätten, och sanktioner vid arbetsvägran, inte kan användas för att förmå en arbetstagare att använda en privat e-legitimation i tjänsten. Bedömningen görs mot bakgrund av de integritetsaspekter som framgår av avsnitt 9.2.2 och 9.2.3 samt det faktum att den privata e-legitimationen är frikopplad från anställningen och utgör privat egendom.

Det har under kartläggningsarbetet också framförts att ett tvång att använda en privat e-legitimation skulle kunna stå i strid med artikel 8 i Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Enligt artikel 8 i Europakonventionen

har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Rättigheten är inte absolut och får under vissa förutsättningar inskränkas. Sådan inskränkning får endast ske med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till ett antal uppräknade ändamål. Rätten till skydd för privatlivet enligt artikel 8 är mångfacetterad och omfattar skydd mot en mängd åtgärder och företeelser. Även om artikeln givetvis måste beaktas anser vi det inte uppenbart att ett tvång att använda en privat e-legitimation i tjänsten hade kunnat utgöra en överträdelse av den aktuella artikeln.

Ytterligare en aspekt med arbetsrättslig koppling är att det vanligen krävs att arbetstagaren har ett svenskt personnummer för att få en privat e-legitimation och för att få BankID krävs även att denne är kund i en bank. Detta skapar ett digitalt utanförskap för vissa grupper i samhället eftersom de inte kan söka eller utföra arbetsuppgifter där det uppställs krav på användning av en privat e-legitimation. Detta skulle även kunna anses utgöra diskriminering av en arbetstagare.

9.2.5 Informationssäkerhetsaspekter

Vid användning av privata e-legitimationer i tjänsten måste en bedömning göras av arbetsgivaren om användningen är förenad med informationssäkerhetsrisker. En sådan bedömning måste bl.a. beakta relevanta författningskrav avseende informationssäkerhet. Enligt 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ansvarar varje myndighet för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Lagen kompletteras av MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6). Av 8 § i föreskrifterna framgår att en myndighet ska, innan den låter en extern aktör behandla information, utifrån informationsklassning och riskbedömning, hantera de risker en sådan behandling innebär. Myndigheten ska i avtal ställa krav på vilka säkerhetsåtgärder den externa aktören ska vidta och hur myndigheten följer upp dessa krav.

En myndighet måste således överväga de potentiella informationssäkerhetsrisker som användningen av privata e-legitimationer kan leda till. Det måste exempelvis säkerställas att den anställda inte kan fortsätta att använda sin privata e-legitimation på arbetsgivarens vägnar efter det att personen har slutat sin anställning vid myndigheten, eller kanske har bytt befattning som också innebär att personen inte längre har samma behörighet. Vidare kan det vara förenat med risker att myndigheten inte har full kontroll på och inte heller kan påverka vilka uppgifter som genom förfarandet lämnas ut om den anställde.

Ytterligare en omständighet som följer av att en privat e-legitimation används i tjänsten är att utfärdaren av den privata e-legitimationen vid varje användningstillfälle får reda på hos vilken förlitande part användaren har identifierat sig. Uppgifter som beroende på myndighet och befattning potentiellt skulle kunna anses vara känsliga ur ett informationssäkerhetsperspektiv.

Det får även generellt anses vara förenat med en större risk att någon obehörig får åtkomst till en privat e-legitimation eller den enhet som e-legitimationen finns på än vad som är fallet med en e-tjänstelegitimation som lagras på t.ex. ett smartkort eller en av arbetsgivaren tillhandahållen mobiltelefon där arbetsgivaren kan utöva en större kontroll över enheten.

Om man ser till risker på en mer övergripande nivå finns det även en fara i att förlita sig på enbart en tillhandahållare, bl.a. för förlitande parter och den offentliga förvaltningen i stort.[14] För det fall endast en e-legitimation i praktiken kan användas blir systemet sårbart om sådana e-legitimationer av någon anledning inte går att använda eller om förutsättningarna för användningen ensidigt ändras av e-legitimationsutfärdaren. Den aktuella e-legitimationen kan t.ex. utsättas för attacker som innebär att den inte går att använda under kortare eller i värsta fall längre perioder. Det skulle i förlängningen kunna resultera i stora problem för den offentliga förvaltningen i stort om det finns ett alltför starkt beroende av att kunna använda en viss e-legitimation. Om ett flertal aktörer finns på marknaden och förser den offentliga förvaltningen med e-legitimationer sprids riskerna vilket också bör resultera i att riskerna totalt sett för den

[14] För mer om denna typ av övergripande risker och hur de kan hanteras se *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9), s. 221 ff.

offentliga förvaltningen minskar på området eftersom en diversifiering av aktörer minskar landets sårbarhet för bl.a. cyberattacker.

Om en arbetsgivare låter anställda eller uppdragstagare använda sin privata e-legitimation i tjänsten bör med beaktande av omständigheterna ovan en riskanalys utföras.

9.2.6 Sammanfattande bedömning

Användning av privata e-legitimationer i tjänsten är inte förbjuden och det är möjligt för arbetstagare och arbetsgivare att komma överens om sådan användning. Vi bedömer emellertid inte att det finns något stöd för att en arbetsgivare kan tvinga en arbetstagare att använda sin privata e-legitimation i tjänsten. De dataskyddsaspekter som följer av att personnumret överförs till tredje part samt, för det fall det rör sig om BankID, det även kräver att medarbetaren medger avsteg från banksekretessen, får anses ge starkt stöd för att det hör till den privata sfären. Om en arbetsgivare uteslutande förlitar sig på användning av privata e-legitimationer skapas därmed en sårbarhet genom att arbetstagare inte kan arbetsledas att använda dem.

3 kap. 10 § dataskyddslagen får även starkt anses tala för att arbetsgivaren bör, när det är möjligt, använda sig av lösningar som inte innebär att arbetstagarens personnummer exponeras.

Andra aspekter som talar emot användning av privata e-legitimationer i tjänsten är informationssäkerhetsaspekterna. Om register inte uppdateras i direkt anslutning till att en person avslutar en anställning kan detta medföra fortsatt tillgång till uppgifter eftersom autentisering sker med ett medel som arbetsgivaren saknar kontroll över. Även de övriga i avsnitt 9.2.5 angivna informationssäkerhetsaspekterna talar emot användningen av privata e-legitimationer i tjänsten.

Vi har vid ett flertal tillfällen stött på att arbetsgivare gör liknelser vid krav om att arbetstagare ska inneha körkort när de förordar användning av privata e-legitimationer i tjänsten. Ett körkort är dock ett bevis om att man innehar en viss kvalifikation, dvs. att man får framföra olika typer av fordon. Det finns även i Sverige endast en myndighet som utfärdar körkort. När det gäller e-legitimationer finns det e-tjänstelegitimationer som en arbetsgivare kan anskaffa och det finns därmed, i motsats till körkortsliknelsen, andra alter-

nativ till användning av privata e-legitimationer. Inte heller när det gäller användningen av en annan privat fysisk id-handling i tjänsten är omständigheterna jämförbara. Detta då varken användningen av en sådan id-handling eller ett körkort kan ge upphov till överföring av sådana integritetskänsliga uppgifter eller medföra sådana informationssäkerhetsrisker som användningen av en privat e-legitimation.

Sammanfattningsvis anser vi att användning av privata e-legitimationer i tjänsten endast bör förekomma när det inte är möjligt att använda e-tjänstelegitimationer för att fullgöra en arbetsuppgift eller när det av annan anledning är befogat (jfr avsnitt 9.3).

9.3 Statliga myndigheter under regeringen ska tillhandahålla e-tjänstelegitimationer till sina anställda

Utredningens förslag: E-tjänstelegitimationer ska som huvudregel tillhandahållas den som tjänstgör vid eller innehar uppdrag för en statlig myndighet under regeringen och som för att kunna fullgöra sina arbetsuppgifter behöver styrka sin identitet eller tjänsteställning.

Användning av privata e-legitimationer får endast ske för idväxling, som kontinuitetslösning eller för det fall en särskild arbetsuppgift, som kräver användning av e-legitimation hos tredje part, inte kan genomföras med en e-tjänstelegitimation.

Nödvändiga bestämmelser ska införas i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte. Förordningens rubrik ska ändras till förordningen om statliga myndigheters medel för elektronisk identifiering och elektroniska informationsutbyte.

Skälen för utredningens förslag

I enlighet med den bedömning som görs i avsnitt 9.2 anser vi att användning av privata e-legitimationer i tjänsten som huvudregel inte bör förekomma inom den offentliga förvaltningen.

För tjänstekort som utfärdas av statliga eller kommunala myndigheter finns detaljerade bestämmelser i både förordningen (1958:272) om tjänstekort och Polismyndighetens föreskrifter och allmänna råd om tjänstekort (PMFS 2020:4). Med undantag för att det i 5 § PMFS 2020:4 framgår att tjänstekort får förses med elektroniska egenskaper för att kortet ska fungera vid elektronisk identifiering och behörighetskontroll saknas det i dagsläget reglering rörande användning, utformning och hantering av e-tjänstelegitimationer inom den offentliga förvaltningen.

Det finns stora skillnader mellan den statliga och den kommunala sektorn när det gäller regeringens möjligheter att styra inom detta område. För den statliga förvaltningen faller styrningen inom ramen för regeringens normgivningsområde genom den restkompetens som följer av 8 kap. 7 § regeringsformen (RF) då det rör de statliga myndigheternas organisation, arbetsuppgifter och inre verksamhetsformer.[15] Vad gäller kommuner och regioner ska principen om kommunal självstyrelse beaktas.

I 14 kap. 3 § RF anges att en inskränkning i den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett den. En lagstiftning som ställer upp krav för en kommunal verksamhet minskar generellt sett kommunernas möjligheter att själva göra prioriteringar i sin verksamhet. Bestämmelsen innebär att en regelmässig prövning av de kommunala självstyrelseintressena ska göras under lagstiftningsprocessen, med tillämpning av en proportionalitetsprincip. Vid införandet av denna bestämmelse i regeringsformen uttalade regeringen att proportionalitetsprövningen bör innefatta en skyldighet att undersöka om det ändamål som regleringen avser att tillgodose kan uppnås på ett för det kommunala självbestämmandet mindre ingripande sätt än det som föreslås. Om olika möjligheter finns för att nå samma mål bör riksdagen av hänsyn till principen om den kommunala självstyrelsen välja den reglering som lägger minst band på den kommunala självbestämmanderätten. Det bör framhållas att detta givetvis förutsätter att det i lagstiftningsprocessen har gjorts noggranna analyser av den påverkan olika förslag har på den kommunala självstyrelsen.[16] Det

[15] *Gröna boken – Riktlinjer för författningsskrivning* (Ds 2014:1), s. 11.
[16] Prop. 2009/10:80 s. 212 f.

finns vidare vissa nationella värden som generellt kan anses motivera en inskränkning av den kommunala självstyrelsen.[17]

Vår kartläggning har visat att många myndigheter, framför allt inom den statliga sektorn, redan tillhandahåller eller avser att tillhandahålla e-tjänstelegitimationer till sina anställda. Trots att användning av privata e-legitimationer i tjänsten från ett arbetsrättsligt perspektiv är tillåten, anser vi att det endast undantagsvis bör förekomma. Vi ser det därför som naturligt att föreslå att regeringen styr sina myndigheter i denna fråga. Inte minst med beaktande av de i avsnitt 9.2.6 angivna informationssäkerhetsaspekterna.

Vi ser det emellertid inte som en proportionerlig inskränkning i den kommunala självstyrelsen att staten ska besluta på vilket sätt kommuner och regioner som arbetsgivare ska agera i detta fall med hänsyn till det ändamål som regleringen avser att tillgodose. Den föreslagna regleringen ska därför bara omfatta statliga myndigheter under regeringen. Sådana bestämmelser kan emellertid få vägledande verkan även för myndigheter under riksdagen samt kommuner och regioner.

Vi föreslår inga undantag från vilka statliga myndigheter under regeringen som ska omfattas av förslaget. Vi ser dock att det vid en eventuell vidare beredning kan övervägas om det finns anledning att exempelvis undanta försvarsmyndigheterna.

Som framgår ovan bedöms regleringen kunna ske inom ramen för regeringens primärområde och därmed i förordning. Vad gäller bestämmelsernas placering finns den i tidigare avsnitt nämnda förordningen om tjänstekort. Även om viss koppling till e-tjänstelegitimationer finns kan det inte anses naturligt att föra in bestämmelser om e-tjänstelegitimationer i denna förordning. Att samla de aktuella bestämmelserna i en ny förordning kan med beaktande av det begränsade antal bestämmelser som föreslås inte heller anses befogat. Vi anser därför att de aktuella bestämmelserna bör föras in i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte. Detta med beaktande av att det finns en tydlig koppling mellan elektroniska informationsutbyten och användningen av e-tjänstelegitimationer. Att samla bestämmelserna skapar även ett mer sammanhållet regelverk över bestämmelser som omfattar statliga myndigheter inom dessa besläktade områden. Dessa tillägg bör dock speglas genom en ändring av förordningens rubrik till förordningen

[17] Statskontorets rapport (2011:17), *Kommunalt självstyre och proportionalitet*, s. 37 f.

om statliga myndigheters medel för elektronisk identifiering och elektroniska informationsutbyte.

Vi föreslår att det i förordningen föreskrivs att e-tjänstelegitimationer ska tillhandahållas den som tjänstgör vid eller innehar uppdrag för myndigheten och som för att kunna fullgöra sina arbetsuppgifter behöver styrka sin identitet eller tjänsteställning elektroniskt. Användning av privata e-legitimationer ska dock vara tillåten för det fall det behövs för id-växling, som kontinuitetslösning om e-tjänstelegitimationen är otillgänglig eller om en särskild arbetsuppgift, som kräver användning av e-legitimation hos extern förlitande part, inte kan genomföras med en e-tjänstelegitimation.

9.4 Ett ramverk för organisationsöverskridande användning av e-tjänstelegitimationer

9.4.1 En ny lag

Utredningens förslag: Den lagreglering som är nödvändig för att skapa ett ramverk för organisationsöverskridande användning av e-tjänstelegitimationer ska samlas i en ny lag benämnd lagen om erkännande av medel för elektronisk identifiering.

Lagen påverkar inte sådant erkännande av medel för elektronisk identifiering som följer av eIDAS-förordningen.

Skälen för utredningens förslag

Som framgår av avsnitt 7.6.2 är organisationsöverskridande åtkomst en av de stora utmaningarna vid användning av e-tjänstelegitimationer inom den offentliga förvaltningen. Organisationsöverskridande användning förekommer i dagsläget främst genom identitetsfederationer inom vissa sektorer. Det finns ett stort behov av en nationell infrastruktur för bredare åtkomst och det är även en grundläggande förutsättning för att användningen av e-tjänstelegitimationer ska nå dess fulla potential sett till den nytta de skapar för de myndigheter som tillhandahåller dem till sina anställda och uppdragstagare.

En stor del av den organisationsöverskridande åtkomst som äger rum sker emellertid genom att privata e-legitimationer används i tjänsten och huvuddelen av dessa e-tjänster tillhandahålls av statliga myndigheter. Antalet aktörer inom den offentliga förvaltningen som tillhandahåller e-tjänstelegitimationer ökar alltjämt och även utan beaktande av våra bedömningar och förslag i avsnitt 9.2 och 9.3 bedöms denna utveckling fortsätta. För att minska beroendet av användning av privata e-legitimationer i tjänsten är det således även av denna anledning av central betydelse att en nationell infrastruktur för organisationsöverskridande åtkomst tillskapas.

En given målsättning för den offentliga förvaltningen inom e-tjänstelegitimationsområdet är därtill att uppnå ett läge där det inte behövs flera olika e-legitimationer för att en anställd eller uppdragstagare ska kunna utföra sina arbetsuppgifter. Det underlättar både för den enskilde medarbetaren och är därtill det mest effektiva från ett förvaltningsövergripande perspektiv.

Användningen av privata e-legitimationer är därtill ofta förenad med ett administratörssystem där företrädare för respektive användarorganisation, exempelvis en kommun, delar ut behörigheter till anställda i kommunen. På så sätt kopplas personen, vanligen genom personnumret, ihop med den organisation denne företräder. Det har under kartläggningen framkommit att många aktörer inte ser denna lösning som tillfredsställande. Det har framförts både av aktörer som tillhandahåller e-tjänster med detta upplägg och av aktörer som har anställda och uppdragstagare som loggar in i e-tjänster samt behöver administrera behörigheterna. Argument som har framförts är bl.a. att det ställer krav på en välfungerande behörighetshantering hos respektive aktör. Om behörigheterna inte hanteras korrekt, t.ex. att en behörighet inte tas bort när en person slutar eller byter tjänst, uppstår även risk för obehörig åtkomst.

En enhetlig lösning för organisationsöverskridande användning underlättar även en övergång till starkare autentisering för e-tjänster där åtkomst i dagsläget sker med användarnamn och lösenord.

DIGG har i en förstudierapport lämnat ett förslag till en avtalsbaserad lösning för organisationsöverskridande åtkomst med e-tjänstelegitimationer (se mer om avtalet i avsnitt 5.8.1).[18] Det kommer att

[18] DIGG, *eID för medarbetare – Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte* (dnr 2019-582), 14 december 2020.

vara frivilligt att ansluta sig till detta avtalsbaserade system. DIGG har i förstudierapporten identifierat risker med förslaget i form av bl.a. långsam anslutning av förlitande parter, e-legitimationsutfärdare samt arbetsgivare till systemet.[19] Under vårt kartläggningsarbete har det även framkommit att flera offentliga aktörer ser långsam eller utebliven anslutning som en överhängande risk med DIGG:s förslag. Detta framförs ofta med hänvisning till att valfrihetssystemen för e-legitimation, som också byggt på frivillighet, haft en begränsad genomslagskraft och en låg anslutningsgrad. I en nyligen lämnad promemoria föreslås att en obligatorisk anslutning till detta system framöver ska gälla då statliga myndigheter som har behov av tjänster för elektronisk identifiering ska använda de tjänster som tillhandahålls genom systemet, som enligt förslaget ska benämnas auktorisationssystem (se avsnitt 6.5.4).[20]

Från och med 1 juni 2021 har det även i 1 a § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering införts ett krav om att offentliga organ som tillhandahåller en nättjänst som omfattas av kravet i artikel 6 i eIDAS-förordningen är skyldiga att ansluta tjänsten till den svenska noden för inkommande gränsöverskridande elektronisk identifiering. Således två exempel i närtid på ett skifte från frivillighet till obligatorisk anslutning inom e-legitimationsområdet.

Vi ser att det även vid skapande av förutsättningar för organisationsöverskridande åtkomst med e-tjänstelegitimationer inom den offentliga förvaltningen krävs tydlig styrning för att inom rimlig tid skapa en nationell infrastruktur för detta ändamål. Om den nuvarande ordningen kvarstår, eller om en lösning som helt bygger på frivillighet införs, är risken stor att det tar lång tid innan majoriteten av de berörda aktörerna är anslutna till ett sådant system. Myndigheterna kan även i brist på tydlig styrning fortsätta att skapa bilaterala eller andra multilaterala lösningar för organisationsöverskridande åtkomst. Avsaknad av tydlig styrning har enligt vår bedömning varit en starkt bidragande orsak till den fragmentering som i dagsläget existerar inom området.

[19] A.a. s. 25.
[20] Promemoria, *Auktorisationssystem för elektronisk identifiering och för digital post*, s. 41 ff.

Sammantaget anser vi att författningsreglering är nödvändig för att skapa det ramverk vi bedömer krävs för att en bredare organisationsöverskridande användning av e-tjänstelegitimationer ska bli en realitet.

Lagreglering av organisationsöverskridande erkännande av e-tjänstelegitimationer samt författningstekniska överväganden

Som framgår ovan tillhandahåller statliga myndigheter en stor del av de e-tjänster där organisationsöverskridande åtkomst inom den offentliga förvaltningen förekommer. Mot denna bakgrund ska det i lag ställas krav på att statliga myndigheter ska erkänna e-tjänstelegitimationer för tillgång till sina e-tjänster och att det ska vara obligatoriskt för dessa myndigheter att ansluta sina e-tjänster till det föreslagna systemet (se mer om systemet i avsnitt 9.4.3 och 9.4.5). Skäl för att ställa sådana krav på andra aktörer inom den offentliga förvaltningen har inte framkommit.

Vi ser därför att det finns behov av lagbestämmelser som, under vissa förutsättningar, ställer krav på statliga myndigheter att i sina e-tjänster tillåta användning av andra aktörers e-tjänstelegitimationer.

De aktuella lagbestämmelserna avser att lägga grunden för organisationsöverskridande användning av e-tjänstelegitimationer. Merparten av de bestämmelser som krävs bör dock regleras i förordning och myndighetsföreskrifter eftersom det framför allt rör sig om detaljbestämmelser av teknisk natur.

Eftersom det rör sig om ett mindre antal bestämmelser på lagnivå vore det lämpligt att infoga dessa i en redan gällande lag. I nationell lagstiftning finns endast en lag som direkt berör e-legitimationer och det är lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Sett till den lagens syfte och de bestämmelser den innehåller kan det emellertid enligt vår bedömning inte anses lämpligt att föra in de aktuella bestämmelserna som fordras i denna författning. Mot denna bakgrund bedöms det inte finnas någon befintlig lag där de aktuella bestämmelserna passar in. De nya lagbestämmelserna ska därför samlas i en särskild författning. Den nya lagen bör benämnas på ett sätt som avspeglar dess innehåll och tillämpningsområde, men som samtidigt är så pass allmänt hållen att den framöver kan kompletteras med bestämmelser som även rör den privata sektorn (jfr bedömningen i avsnitt 9.5). Vi

föreslår därför att lagen benämns lag om erkännande av medel för elektronisk identifiering.

Lagen påverkar inte sådant erkännande som följer av eIDAS-förordningen

I eIDAS-förordningen finns bestämmelser om att medlemsstaterna ska erkänna vissa medel för elektronisk identifiering som utfärdats i andra medlemsstater. [21] I artikel 6 i förordningen föreskrivs att när det enligt nationell rätt eller enligt nationella administrativa förfaranden krävs elektronisk identifiering där medel för elektronisk identifiering och autentisering används för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ i en medlemsstat, ska de medel som utfärdats i en annan medlemsstat erkännas i den första medlemsstaten för gränsöverskridande autentisering för tjänsten om i artikeln angivna krav är uppfyllda.

Tre förutsättningar ska vara uppfyllda för att kravet på erkännande ska aktualiseras. De två första är att e-legitimationen ska vara utfärdat inom ramen för ett anmält e-legitimationssystem och att tillitsnivån för e-legitimationen ska motsvara en tillitsnivå som är lika hög eller högre än den tillitsnivå som det berörda offentliga organet kräver för åtkomst till nättjänsten, förutsatt att tillitsnivån för e-legitimationen motsvarar tillitsnivån väsentlig eller hög. Den sista förutsättningen är att det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten (se mer om eIDAS-förordningen och krav på erkännande i avsnitt 4.2). Om förutsättningarna för erkännande är uppfyllda lämnas i eIDAS-förordningen inget utrymme för medlemsstaterna och dess myndigheter att inte erkänna e-legitimationen. Den lag vi föreslår påverkar inte kravet på erkännande enligt eIDAS-förordningen. För att tydliggöra detta ska det framgå av lagen.

[21] Som tidigare framgått används i förordningen medel för elektronisk identifiering, men e-legitimationer utgör ett sådant medel.

Lagen bör i framtiden kunna omfatta elektronisk identifiering av maskiner och mjukvaror

Det har under vårt kartläggningsarbete framkommit att det finns behov av att t.ex. mjukvaror som används av den offentliga förvaltningen ska kunna identifieras elektroniskt.[22] Det kan bl.a. röra sig om mjukvaror hos en aktör som automatiskt hämtar uppgifter från andra aktörer inom den offentliga förvaltningen eller robotar (”robotiserad processautomatisering” [RPA]). Det kan under sådan användning finnas behov av att elektroniskt kunna identifiera den aktuella mjukvaran. Det är ett rimligt antagande att användning av mjukvaror för bl.a. inhämtning och analys av uppgifter kommer öka inom den offentliga förvaltningen. Ökad användning av artificiell intelligens inom förvaltningen kan ytterligare öka behoven av denna typ av identifiering.

Då utrymme saknats för att fördjupa oss i dessa frågor och då det även får anses ligga utanför ramen för vårt uppdrag lämnar vi inga förslag vad gäller denna typ av identifiering. Den föreslagna lagen bör dock i framtiden även kunna omfatta sådan identifiering.

Pågående arbete bör kunna fortsätta även utan den föreslagna lagen

DIGG har i tidigare nämnd förstudierapport föreslagit ett system för organisationsöverskridande användning av e-tjänstelegitimationer.[23] Den föreslagna lagen innehåller bestämmelser om obligatorisk anslutning till ett system som möjliggör organisationsöverskridande åtkomst. Lagen är emellertid enligt vår bedömning ingen förutsättning för att ett sådant system utvecklas och tas i drift under frivilliga former. Framtagande och utveckling av ett sådant system bör emellertid givetvis beakta konsekvenserna av ett eventuellt genomförande av förslagen i detta betänkande.

[22] Se exempelvis INERA, *Fördjupad analys RPA – Fördjupad analys av identitet och åtkomststyrning för robotar* (version 1.0), 27 april 2020.
[23] DIGG, *eID för medarbetare – Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte* (dnr 2019-582), 14 december 2020.

9.4.2 Ord och uttryck i lagen

Utredningens förslag: Ord och uttryck i lagen ska ha samma betydelse som i eIDAS-förordningen.

Skälen för utredningens förslag

I eIDAS-förordningen definieras flera centrala termer inom e-legitimationsområdet. Flera av dessa termer avviker från de benämningar som används både i vardagligt språkbruk och inom ramen för detta betänkande.

I eIDAS-förordningen förekommer exempelvis inte termen e-legitimation. Däremot används termen medel för elektronisk identifiering, som i artikel 3.2 definieras som en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster. En definition som således omfattar både e-legitimationer och e-tjänstelegitimationer.

I detta betänkande har vi vidare använt termen e-tjänst för att beskriva elektroniska tjänster som är webbaserade. Det finns ingen vedertagen definition av vad som utgör en e-tjänst. E-delegationen definierade dock en e-tjänst som en tjänst som tillhandahålls via ett elektroniskt gränssnitt och som helt eller delvis utförs elektroniskt.[24] I eIDAS-förordningen används termen nättjänst. Någon närmare definition av termen nättjänst finns inte i förordningen men det får anses vedertaget att det som vi kallar för e-tjänster omfattas av termen nättjänster.

Som framgår av avsnitt 9.1 är bristande enhetlighet ett nuvarande problem på e-legitimationsområdet. Detta gäller även till viss mån de begrepp och termer som används. För att författningsbestämmelser inom e-legitimationsområdet ska vara enhetligt utformade bedömer vi att ord och uttryck i lagen bör ha samma betydelse som i eIDAS-förordningen och att det i lagen bör införas en särskild bestämmelse som anger detta.

För att bibehålla enhetlighet i detta betänkande används emellertid i följande avsnitt begreppen e-legitimation, e-tjänstelegitimation och e-tjänst i löptexten. I förslagsrutorna ska dock eIDAS-förord-

[24] *Uppgiftslämnarservice för företagen* (SOU 2015:33), s. 17.

ningens terminologi användas för att på sätt överensstämma med det som anges i författningsförslaget.

9.4.3 Statliga myndigheter ska erkänna e-tjänstelegitimationer i sina e-tjänster

Utredningens förslag: Kravet på erkännande i den nya lagen ska gälla för statliga myndigheters nättjänster där tillgång till tjänsten kräver användning av medel för elektronisk identifiering.

Skälen för utredningens förslag

Som framgår av avsnitt 9.4.1 tillhandahålls en stor del av e-tjänster, där organisationsöverskridande åtkomst inom den offentliga förvaltningen förekommer av statliga myndigheter. De krav som ställs för autentisering kan variera. Kravet i lagen om att statliga myndigheter ska erkänna vissa e-tjänstelegitimationer gäller enbart sådana e-tjänster där autentisering och annan användning av e-legitimationer inom ramen för tjänsten krävs. Kravet utesluter inte heller att även andra e-legitimationer kan användas i tjänsterna. Detta innebär att för det fall en e-tjänstelegitimation utöver autentisering krävs för att använda tjänsten gäller kravet på erkännande även för dessa moment, exempelvis som ett led i att skapa en elektronisk underskrift inom ramen för tjänsten. En tjänst där autentisering exempelvis enbart sker med användarnamn och lösenord omfattas emellertid inte av kravet på erkännande. De e-tjänstelegitimationer som måste erkännas ska dock uppfylla vissa krav (se avsnitt 9.4.4). Det finns vidare vissa undantag vad gäller krav om erkännande (se avsnitt 9.4.7).

Erkännande innebär att e-tjänstelegitimationen ska accepteras för tillgång till den aktuella e-tjänsten. Med hjälp av e-tjänstelegitimationen ska användaren kunna använda tjänsten, under förutsättning att eventuella behörighetskrav är uppfyllda. Vad användaren kan göra i en e-tjänst skiljer sig åt.

9.4.4 Lagen omfattar e-tjänstelegitimationer som tillhandahålls av offentliga aktörer

Utredningens förslag: De medel för elektronisk identifiering som av en offentlig aktör tillhandahålls för aktörens anställda eller uppdragstagare ska erkännas om kraven som ställs på dessa medel i övrigt är uppfyllda.

Skälen för utredningens förslag

Vad avser frågan om vilka aktörer vars anställda och uppdragstagare ska ha rätt att nyttja den organisationsöverskridande åtkomst som föreslås gör vi följande överväganden.

Genom lagen (2018:1937) om tillgänglighet till digital offentlig service uppställs krav om tillgänglighetsanpassning av webbplatser och mobila applikationer. I lagens förarbeten bedömde regeringen att tillämpningsområdet, i relation till det EU-direktiv lagen genomför i svensk rätt, skulle utvidgas till att även omfatta privata aktörer som yrkesmässigt bedriver verksamhet inom särskilt utpekade områden och som till någon del är offentligt finansierad.[25]

I ovan nämnd promemoria föreslås bl.a. att valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering ska ersättas av auktorisationssystem för sådana tjänster.[26] Vidare föreslås att även samma krets privata aktörer som omfattas av lagen om tillgänglighet till digital offentlig service ska kunna få använda de tjänster som tillhandahålls inom auktorisationssystemen.[27] Detta motiveras bl.a. med att den privata sektorns medverkan när det gäller digitala tjänster kan bidra till ökad användarnytta, tillväxt och innovation. I promemorian anförs vidare att stora delar av den kommunala verksamheten utförs i privat regi. De aktörer som verkar inom skolområdet, hälso- och sjukvårdsområdet samt socialtjänstområdet består till stor del av privata aktörer. Dessa behöver enligt promemorian ha samma förutsättningar att erbjuda digitala tjänster som de offentliga aktörer som verkar inom

[25] Prop. 2017/18:299 s. 33.
[26] Promemoria, *Auktorisationssystem för elektronisk identifiering och för digital post*, 21 december 2020, s. 1.
[27] A.a. s. 29.

samma område.[28] Ytterligare en aspekt som lyfts fram är att för att dessa aktörer ska kunna tillhandahålla digital service i form av digitala tjänster och digitala utskick krävs att de har tillgång till tjänster för elektronisk identifiering och för digital post. En fördel med att låta samma, tydligt definierade, krets som omfattas av kraven på tillgänglighet till digital offentlig service använda tjänster inom auktorisationssystem är enligt promemorian att de privata utförare som omfattas av kraven därmed får möjlighet att erbjuda denna service på samma villkor som de utförare som bedriver sin verksamhet i offentlig regi.[29] I delbetänkandet har vi föreslagit att samma krets aktörer som omfattas av kraven i lagen om tillgänglighet till digital offentlig service ska kunna använda den i betänkandet föreslagna nationella valideringstjänsten.[30] Vi anser att den ovan redovisade argumentationen även kan tillämpas vad gäller åtkomst till det nu aktuella systemet. Framför allt med beaktande av att det medför att alla utförare av offentligt finansierad verksamhet ges möjlighet att använda offentlig service med hjälp av digitala tjänster på lika villkor då det av kartläggningsarbetet framkommit att detta är ett tydligt behov (se avsnitt 7.6.5).

Mot denna bakgrund anser vi att samma krets aktörer som omfattas av kraven i lagen om tillgänglighet till digital offentlig service ska kunna använda systemet och att de på samma sätt som i den lagen tillsammans med myndigheterna som omfattas samlat ska benämnas offentliga aktörer.

Den krets av privata aktörer som ges tillgång till systemet blir då privata aktörer inom vissa områden som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad. Med offentlig finansiering avses ett direkt stöd eller betalning från det allmänna för att driva verksamheten. Det kan t.ex. vara fråga om bidrag till skolor med enskild huvudman som ges med stöd av skollagen, ersättning som ges med stöd av lagen (1993:1651) om läkarvårdsersättning eller verksamhet som upphandlas av det allmänna av privata utförare. Ett krav bör vara att finansieringen är kopplad till själva driften av verksamheten. Om viss ekonomisk ersättning från det allmänna inte avser själva driften av verksamheten bör alltså ersättningen inte med-

[28] A.a. s. 30.
[29] A.a. s. 31 f.
[30] *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9), s. 168 ff.

föra att verksamheten anses vara offentligt finansierad.[31] Att verksamheten är yrkesmässigt bedriven innebär att verksamheten bedrivs kontinuerligt och i förvärvssyfte.[32]

De aktörer som omfattas är de som bedriver verksamhet som

- aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),
- utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125), eller
- bedrivs enligt socialtjänstlagen (2001:453), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga, lagen (1993:387) om stöd och service till vissa funktionshindrade eller utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken.

Därtill omfattas enskilda utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller för utbildning på forskarnivå.

Att erbjuda möjlighet att använda systemet till samma krets aktörer som omfattas av kraven i lagen om tillgänglighet till digital offentlig service innebär att även offentligt styrda organ omfattas. Med offentligt styrt organ avses en sådan juridisk person som tillgodoser behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär och som uppfyller vissa krav avseende finansiering, kontroll eller styrelserepresentation.[33]

Utöver de aktörer som ovan angetts har det under kartläggningen även lyfts fram att det föreligger ett behov av att i ett system för organisationsöverskridande användning av e-tjänstelegitimationer också inkludera privata aktörer som yrkesmässigt bedriver verksamhet som utgör detaljhandel med läkemedel, verksamhet inom djurens hälso- och sjukvård samt hälso- och sjukvård som inte är offentligt finansierad. Även om dessa verksamheter har nära kopplingar till vissa verksamheter och e-tjänster som omfattas av den föreslagna

[31] Prop. 2016/17:31 s. 28.
[32] Prop. 2017/18:299 s. 87.
[33] Se mer om definitionen av offentligt styrt organ i prop. 2017/18:299 s. 30 f.

lagen är detta privata aktörer som inte utgör privata utförare av offentligt finansierad verksamhet eller har någon annan tydlig koppling till det offentliga. De bedöms därmed falla utanför ramen för utredningens uppdrag.

9.4.5 Ett system för erkännande av e-tjänstelegitimationer

Utredningens förslag: Det ska finnas ett system för erkännande av medel för elektronisk identifiering. Myndigheten för digital förvaltning ska tillhandahålla systemet.

Myndigheten för digital förvaltning får meddela föreskrifter om krav på medel för elektronisk identifiering som ingår i systemet och krav som avser förlitande parter.

Vid meddelande av föreskrifter som avser systemet ska Myndigheten för digital förvaltning samråda med Myndigheten för samhällsskydd och beredskap.

Kravet på erkännande gäller endast om det aktuella medlet för elektronisk identifiering har samma tillitsnivå eller högre än den nivå som krävs för åtkomst till nättjänsten.

Statliga myndigheter som tillhandahåller nättjänster som omfattas av kravet på erkännande ska ansluta till systemet.

Skälen för utredningens förslag

System för erkännande

En grundläggande förutsättning för att e-tjänstelegitimationer ska kunna användas över organisationsgränserna är att det finns tillit mellan parterna och till de e-tjänstelegitimationer som används. För att uppnå detta behöver det skapas en nationell identitetsfederation med bl.a. krav, policys, teknisk infrastruktur samt en process för godkännande av e-tjänstelegitimationer. De grundläggande förutsättningarna för denna federation ska anges i den föreslagna lagen och förordningen. I syfte att hålla bestämmelserna mer neutralt utformade har vi emellertid valt att använda begreppet system i stället för identitetsfederation.

DIGG har enligt 3 § 1 i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning som uppgift att ansvara för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering. Vi föreslår därför att systemet ska tillhandahållas och administreras av DIGG. DIGG kommer därmed i systemet att i praktiken ha rollen som federationsoperatör. Merparten av den reglering som skapandet av systemet kräver är av sådan art att de lämpligen fastställs i myndighetsföreskrifter. Vi föreslår därför att DIGG ska ges ett bemyndigande om att meddela föreskrifter vad avser krav på de e-tjänstelegitimationer som får ingå i systemet samt de förlitande parter som ansluts.

Informationssäkerhet

Det föreslagna systemet skulle bli en central del av den offentliga förvaltningens gemensamma digitala infrastruktur. Av detta följer att det är av central betydelse att säkerheten i systemet blir hög och att en hög nivå av informationssäkerhet säkerställs. På så sätt skapas förutsättningar för ett robust system där tilliten är hög inom och för systemet. Systemet måste fungera även i ett läge av störda elektroniska kommunikationer eller störningar i de e-tjänstelegitimationer som används eller i stödsystem kring dessa. Systemet behöver därför byggas robust och redundant så att det kan stå emot störningar. Vidare behöver såväl identitetsintygsutfärdare som e-tjänster och metadatatjänster vara tillräckligt skyddade ur ett tillgänglighets-, riktighets- och konfidentialitetsperspektiv.

MSB har ett särskilt ansvar inom svensk förvaltning vad gäller informationssäkerhet och myndigheten har bl.a. enligt 11 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap i uppgift att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och regioner samt företag och organisationer. Vi anser att det är lämpligt att MSB bidrar med sin expertkunskap på området när kraven avseende systemet utformas. Det ska därför anges i förordningen att DIGG ska samråda med MSB innan föreskrifter om systemet utfärdas.

Det bör också noteras att oavsett vilka e-tjänstelegitimationer som används behöver myndigheter säkerställa, utöver att systemet är tillräckligt säkert, att de e-tjänstelegitimationer de tillhandahåller till anställda och uppdragstagare uppfyller verksamhetens behov av informationssäkerhet, robusthet och uthållighet. Dessa behov ser olika ut mellan myndigheter och påverkas av den enskilda myndighetens verksamhetsområde och den information myndigheten hanterar. Faktorer som kan påverka är t.ex. om säkerhetsskyddslagen (2018:585) blir tillämplig eller behovet av totalförsvarsplanering. Uthålligheten kan byggas genom att flera e-tjänstelegitimationer stöds men även genom kontinuitetsplaner med alternativa arbetssätt för de fall att e-tjänstelegitimationerna inte kan användas.

Ytterligare informationssäkerhetsaspekter berörs i avsnitt 9.4.8 vad avser undantag på krav om erkännande vid allvarliga säkerhetsrisker samt i avsnitt 9.4.9 när det gäller hantering av säkerhetsincidenter.

Medlet för elektronisk identifiering ska uppfylla samma tillitsnivå eller högre än den nivå som krävs för åtkomst till e-tjänsten

Det är som huvudregel upp till varje tillhandahållare av en e-tjänst att själv bedöma vilka krav på säkerhet tjänsten måste leva upp till även om det i vissa fall kan uppställas sådana krav i författning (se avsnitt 4.3). Det kan t.ex. bero på vilken information som hanteras i tjänsten eller hur tjänsten tekniskt är beskaffad. Vidare är det som huvudregel upp till den som tillhandahåller en e-tjänst som kräver autentisering via e-legitimation att avgöra vilka krav e-legitimationen ska leva upp till för att en användare ska få tillgång till den aktuella e-tjänsten. Som framgår av avsnitt 4.2.3 och 6.3.2 används i Sverige och EU tillitsnivåer för att tydliggöra vilka krav en e-legitimation lever upp till.

eIDAS-förordningen utgår från principen att medlemsstaterna endast behöver erkänna e-legitimationer som är på samma tillitsnivå, eller högre, som den som krävs för den aktuella tjänsten. En e-legitimation på tillitsnivå väsentlig behöver alltså endast erkännas för en tjänst som kräver tillitsnivå väsentlig, däremot inte i en tjänst som kräver tillitsnivå hög.

Kravet på erkännande av e-tjänstelegitimationer i den föreslagna lagen ska gälla endast under förutsättning att den e-tjänstelegitimation som används har samma tillitsnivå, eller högre, som den som krävs för autentisering i den aktuella e-tjänsten. Statliga myndigheter kommer alltså, precis som i dag, att behöva bedöma och fastställa vilken tillitsnivå de ska kräva för att användare ska kunna autentisera sig och få tillgång till myndigheternas e-tjänster. Begreppen tillitsnivåer är enligt vår uppfattning vedertagna inom e-legitimationsområdet både i Sverige och inom EU. Att fortsätta att använda detta begrepp faller sig därför naturligt. Vilket tillitsramverk och vilka tillitsnivåer som ska gälla i systemet kommer att styras av de föreskrifter DIGG utfärdar avseende krav på de e-tjänstelegitimationer som ingår i systemet.

Anslutning av förlitande parters e-tjänster

När e-tjänstelegitimationer används av offentliga aktörer gentemot e-tjänster som tillhandahålls av statliga myndigheter bör användningen ske genom systemet. Statliga myndigheter skulle visserligen som nämnts tidigare kunna erkänna e-legitimationerna genom exempelvis bilaterala avtal med olika offentliga aktörer, eller genom andra lösningar. I syfte att systemet ska leda till så stora effektivitetsvinster som möjligt föreslår vi en uttrycklig bestämmelse om att statliga myndigheter som tillhandahåller e-tjänster som omfattas av kravet på erkännande ska ansluta till systemet.

Aktörer som inte är statliga myndigheter omfattas inte av kravet på att ansluta e-tjänster till systemet. Den föreslagna regleringen uppställer emellertid inga hinder för att även andra aktörer som vill ansluta sig till systemet i egenskap av förlitande parter kan göra det. Om DIGG ser behov av att meddela föreskrifter för villkoren eller förfarandet för anslutningen av dessa aktörer bedömer vi att det faller inom ramen för bemyndigandet att meddela föreskrifter om krav på e-tjänstelegitimationer i systemet.

9.4.6 Granskning och godkännande av e-tjänstelegitimationer

Utredningens förslag: Statliga myndigheter ska erkänna e-tjänstelegitimationer som är godkända av Myndigheten för digital förvaltning för användning i systemet.

Myndigheten för digital förvaltning får meddela föreskrifter om ansöknings- och granskningsförfarandet.

Myndigheten för digital förvaltning ska kunna ta ut avgift för granskningen av de medel för elektronisk identifiering som ansluts till systemet.

Skälen för utredningens förslag

Myndigheten för digital förvaltning ska granska och godkänna e-tjänstelegitimationer

Som framgår av avsnitt 9.4.5 är en grundläggande förutsättning för att e-tjänstelegitimationer ska kunna användas över organisationsgränserna att det finns tillit mellan parterna och till de e-tjänstelegitimationer som används. Vår kartläggning visar att förekomsten av krav att förhålla sig till inte per automatik skapar tillit vid organisationsöverskridande användning av e-legitimationer. Att enbart förlita sig på organisationstillit förenat med någon form av självdeklaration bedömer vi därför inte vara tillräckligt (se mer om organisationstillit i avsnitt 3.16). I synnerhet inte för ett system till vilket det föreslås obligatorisk anslutning.

DIGG granskar i dagsläget att e-legitimationer lever upp till kraven i myndighetens tillitsramverk och därigenom får använda kvalitetsmärket Svensk e-legitimation. Syftet med granskningen av e-legitimationerna är att varje förlitande part inte själv ska behöva granska och bedöma en e-legitimation. Användarna ska också känna sig trygga med att det är en säker e-legitimation.

Samma behov föreligger för det föreslagna systemet. Det behövs ett tydligt tillitsramverk och förlitande parter behöver kunna lita på att de e-tjänstelegitimationer som används i systemet uppfyller kraven de ställer för åtkomst till sina e-tjänster. De offentliga aktörer som anskaffar e-tjänstelegitimationer behöver även veta att de kan användas i systemet. Av detta följer att det i lagen ska föreskrivas att det endast är de e-tjänstelegitimationer som är godkända för använd-

ning i systemet som statliga myndigheter har ett krav på sig att erkänna.

Mot bakgrund av att DIGG ska tillhandahålla systemet och därtill har erfarenhet av granskning av e-legitimationer föreslår vi att myndigheten får i uppgift att granska och godkänna e-tjänstelegitimationer inom ramen för det föreslagna systemet. DIGG kommer genom sin granskning att bedöma om den aktuella e-tjänstelegitimationen lever upp till de krav som ställs. För att granskning ska inledas ska utfärdaren av e-tjänstelegitimationen ansöka om godkännande. I syfte att skapa tillit hos förlitande parter bör granskningen också omfatta eventuella andra relevanta underleverantörer eller avtalsparter med koppling till e-tjänstelegitimationen, såsom exempelvis en extern identitetsintygsutfärdare.[34]

Som framgår av avsnitt 9.4.5 föreslår vi att DIGG ges ett bemyndigande att meddela föreskrifter om krav på e-tjänstelegitimationer som ingår i systemet. Det finns redan i dag ett antal e-tjänstelegitimationer som är granskade av DIGG (se avsnitt 6.4.2). Det är upp till DIGG att avgöra huruvida dessa behöver granskas på nytt eller om redan granskade e-tjänstelegitimationer på denna grund kan godkännas för användning i systemet. E-legitimationer som lever upp till kraven ska godkännas genom beslut av DIGG. Om DIGG bedömer att en e-tjänstelegitimation inte lever upp till kraven ska myndigheten genom beslut avslå ansökan (se avsnitt 9.4.11 om överklagande).

För att statliga myndigheter ska känna tillit till granskningsprocessen är det viktigt att granskningen håller hög kvalitet och att den är transparent i det avseendet att aktörer inom den offentliga förvaltningen får en inblick i vad som granskas och hur. Vidare bör DIGG få ett bemyndigande att efter samråd med MSB genom föreskrifter närmare fastställa hur ansökan ska lämnas, vad den ska innehålla samt vad som gäller för granskningen och förfarandet i övrigt.

Utfärdare av e-tjänstelegitimationer bör meddela DIGG om förändringar görs som påverkar de delar av verksamheten eller e-tjänstelegitimationen som omfattas av granskningen. Byten av eventuella underleverantörer kan t.ex. vara en sådan förändring. I syfte att säkerställa en hög säkerhetsnivå samt främja tillit inom och för syste-

[34] DIGG, *eID för medarbetare – Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte* (dnr 2019-582), 14 december 2020, s. 17.

met bör dessutom uppföljningar av granskningarna göras återkommande.[35] Det bör vara upp till DIGG att bestämma hur ofta och på vilket sätt uppföljningarna ska göras.

Det ska vidare vara möjligt för DIGG att ta ut avgift av utfärdaren för den granskning som genomförs, i syfte att täcka hela eller delar av kostnaden för granskningen. Vi föreslår att förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning ändras för att möjliggöra sådant avgiftsuttag.

9.4.7 Ej godkända e-tjänstelegitimationer

Utredningens förslag: Medel för elektronisk identifiering som inte är godkända får ingå i systemet för erkännande för medel för elektronisk identifiering men det är frivilligt för förlitande parter att erkänna sådana medel.

Myndigheten för digital förvaltning får meddela föreskrifter om förfarandet för anmälan och anslutning, av medel som inte är godkända, till systemet.

Skälen för utredningens förslag

Som framgår av avsnitt 9.4.6 utgör granskning och godkännande av e-tjänstelegitimationer en viktig komponent i att skapa tillit vid organisationsöverskridande åtkomst inom ramen för det föreslagna systemet. Det finns dock aktörer inom förvaltningen som inte ser behov av, eller ser sig förhindrade, att använda sådana medel för elektronisk identifiering som i dag granskas och godkänns av DIGG. Det finns exempelvis aktörer inom förvaltningen som tillhandahåller identifieringslösningar till sina anställda som rent tekniskt skulle kunna användas över organisationsgränser.

Även om tillit är centralt anses i många fall organisationstilliten inom den offentliga förvaltningen vara tillräcklig.

[35] Jfr artikel 20.1 i eIDAS-förordningen där det föreskrivs att kvalificerade tillhandahållare av betrodda tjänster minst en gång vartannat år och på egen bekostnad ska granskas av ett organ för bedömning av överensstämmelse, i syfte de samt de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i förordningen.

Eftersom erkännande enligt den föreslagna lagen är obligatorisk anser vi att det förfarande med granskning och godkännande som behandlas i avsnitt 9.4.6 är nödvändig för systemet som helhet. Den infrastruktur som systemet innebär bör dock också vara möjlig att använda även för erkännande av e-tjänstelegitimationer som inte godkänts. Det ska dock inte finnas något krav om att erkänna dessa medel i de e-tjänster som omfattas av lagen. Om en myndighet som tillhandahåller en e-tjänst på frivillig basis vill erkänna sådana e-tjänstelegitimationer från en eller flera offentliga aktörer ska det dock inte krävas en uppbyggnad av olika bilaterala lösningar för att åstadkomma detta.

Det ska därför vara möjligt även för e-tjänstelegitimationer som inte är godkända att vara med i systemet. För att de ska få vara med i systemet måste dock utfärdaren genom självskattning bedöma om e-tjänstelegitimationen lever upp till kraven. Om bedömningen av utfärdare är att legitimationen lever upp till kraven ska utfärdaren anmäla till DIGG att den ska vara med i systemet. Först efter det att anmälan är inlämnad till DIGG får den vara med i systemet. När DIGG har fått in en anmälan ska myndigheten offentliggöra att den aktuella e-tjänstelegitimationen ingår i systemet, exempelvis genom att publicera informationen på myndighetens webbplats. Det bör tydligt framgå att e-tjänstelegitimationen inte är godkänd av DIGG, i syfte att minska risken för missförstånd i det avseendet. Utfärdaren ska på begäran lämna ut de uppgifter som ligger till grund för bedömningen om överensstämmelse till förlitande parter och till DIGG. Det primära syftet med att uppgifter ska lämnas ut är att upprätthålla tilliten till systemet. Det är emellertid som ovan framgått upp till varje förlitande part att välja att tillåta användning av dessa e-tjänstelegitimationer i respektive e-tjänst som är ansluten till systemet.

Det kan behövas bestämmelser om förfarandet för anmälan av e-tjänstelegitimationer till DIGG samt om hur de kan anslutas till systemet. Det rör sig om bestämmelser som är på en detaljnivå som lämpar sig bäst i myndighetsföreskrifter. DIGG bör därför bemyndigas att efter samråd med MSB utfärda föreskrifter med sådant innehåll.

9.4.8 Undantag från kravet på erkännande

Utredningens förslag: Regeringen får meddela föreskrifter om undantag från kravet på erkännande.

Statliga myndigheter behöver inte erkänna medel för elektronisk identifiering om erkännande innebär allvarliga säkerhetsrisker.

Kravet på erkännande av e-tjänstelegitimationer gäller inte för e-tjänster som endast riktar sig till enskilda.

En statlig myndighet behöver inte erkänna medel för elektronisk identifiering om den aktuella nättjänsten redan är ansluten till ett sektorspecifikt system för erkännande av medel för elektronisk identifiering.

Skälen för utredningens förslag

Regeringen får meddela undantag från kravet på erkännande

Då vi föreslår obligatorisk anslutning till systemet bör det även finnas utrymme för att meddela undantag från de krav på erkännande som det föreslagna regelverket medför. Då den obligatoriska anslutningen gäller statliga myndigheter och då skäl för undantag längre fram kan uppstå som vi i dag inte kan förutse föreslår vi att regeringen ska bemyndigas att meddela föreskrifter om undantag från kravet på erkännande. Nedan lämnar vi förslag om tre undantag. Det kan emellertid övervägas om även vissa specifika myndigheter bör undantas från de krav som föreslås.

Undantag om erkännande medför allvarliga säkerhetsrisker

Kravet att statliga myndigheter ska erkänna godkända e-tjänstelegitimationer syftar till att göra det möjligt för offentliga aktörer att kunna använda e-tjänster som tillhandahålls av myndigheterna. För att det ska finnas tillit till och inom systemet är det viktigt att säkerhet upprätthålls i systemet som helhet, oavsett vilken tillitsnivå som används. Det är emellertid i slutändan primärt den statliga myndighet som tillhandahåller en e-tjänst som riskerar att drabbas om en e-tjänstelegitimation har bristande säkerhet. Det kan t.ex. röra sig om tekniska brister och svagheter eller brister kopplade till den ursprung-

liga identifieringen av användaren. Det kan i sin tur öka risken för intrång med hjälp av e-legitimationen eller att en icke behörig person utför handlingar i en e-tjänst.

Det bör därför vara möjligt för statliga myndigheter att välja att inte erkänna e-tjänstelegitimationer om erkännande skulle innebära allvarliga säkerhetsrisker. Riskerna är att anse som allvarliga om eventuella skador t.ex. kan leda till att enskilda drabbas, om brottsliga handlingar kan företas eller om e-tjänsten eller myndighetens it-miljö i övrigt kan skadas.

Det är viktigt att ta i beaktande att de e-tjänstelegitimationer som statliga myndigheter måste erkänna ska vara godkända av DIGG. Det innebär att en enskild statlig myndighet som tillhandahåller e-tjänster som omfattas av kravet på erkännande inte ska behöva göra en egen granskning av legitimationerna. Det kan emellertid inte uteslutas att det uppstår situationer där riskerna med ett erkännande är så pass allvarliga att ett erkännande framstår som olämpligt. I ett sådant läge bör det vara möjligt för den aktuella myndigheten att välja att inte erkänna legitimationen. Undantaget från kravet bör enligt vår uppfattning kunna tillämpas på grupper av e-tjänstelegitimationer från samma utfärdare eller alla e-tjänstelegitimationer från samma utfärdare. Med grupper avses t.ex. e-legitimationer som har utfärdats till anställda och uppdragstagare vid en och samma organisation.

Säkerhetsrisken eller riskerna ska vara konkreta för att undantaget ska kunna tillämpas. Det kan vara konsekvenser av en incident eller sårbarhet för den enskilda myndigheten. Det ska alltså inte gå att slentrianmässigt tillämpa undantaget.

En statlig myndighet som väljer att inte erkänna en e-tjänstelegitimation som är godkänd i systemet ska utan dröjsmål rapportera det till DIGG. Myndigheten ska i samband med rapporteringen också ange skälen till att den inte erkänner e-tjänstelegitimationen. Syftet är att ge DIGG en överblick över om systemet fungerar som avsett eller om det finns anledning att vidta åtgärder, exempelvis i form av att förändra kraven i systemet eller genom att vidta åtgärder gentemot en viss e-legitimationsutfärdare.

Undantag för e-tjänster som endast riktar sig till enskilda

Till följd av att de e-tjänstelegitimationer som omfattas av kravet på erkännande endast ska användas i tjänsten ska detta krav inte gälla för e-tjänster som endast riktar sig till enskilda personer, dvs. e-tjänster som enbart är avsedda för användning av en enskild i egenskap av privatperson. För sådana tjänster bör det enligt vår bedömning inte finnas något behov av ett krav på att erkänna e-tjänstelegitimationer eftersom legitimationerna inte är avsedda för sådan användning. En statlig myndighet kan givetvis, i egenskap av förlitande part, välja att erkänna e-tjänstelegitimationer även för sådana e-tjänster, men en sådan e-tjänst ska inte omfattas av kravet på erkännande.

Undantag för e-tjänster som är anslutna till sektorsspecifika identitetsfederationer

Det finns i dagsläget redan ett antal identitetsfederationer i Sverige som skapar förutsättningar för organisationsöverskridande åtkomst inom vissa sektorer, såsom hälso- och sjukvårdsområdet och skolområdet (se avsnitt 6.6). Det har under vårt kartläggningsarbete framhållits att det för aktörer som är med i flera olika federationer blir ett merarbete att förhålla sig till olika regelverk. Med beaktande av tekniska aspekter samt de attributprofiler och andra sektorsspecifika behov som kan behöva beaktas finns det enligt vår bedömning i dagsläget ett fortsatt behov av dessa identitetsfederationer.

Vi anser att det på sikt vore önskvärt om både det i betänkandet föreslagna systemet och de befintliga identitetsfederationerna rörde sig mot att ha enhetliga tillitsregelverk. Om det föreslagna systemet och federationerna på sikt rör sig mot enhetliga regelverk kan en interfederation vara en möjlighet för att ytterligare uppnå en mer sammanhållen lösning för organisationsöverskridande elektronisk identifiering. Om befintliga identitetsfederationer längre fram ser fördelar med att uppgå i det föreslagna systemet bör detta även vara ett alternativ. Vi ser emellertid att detta, samt en eventuell interfedering bör ske på frivillig basis.

För statliga myndigheter vars e-tjänster är anslutna till befintliga identitetsfederationer finns det inte heller någon uppenbar anledning att även kräva obligatorisk anslutning till det föreslagna systemet. E-tjänster som omfattas av den föreslagna lagen och som är

anslutna till en sådan federation ska därför undantas från kravet om att erkänna e-tjänstelegitimationer. Det finns emellertid inga hinder mot att en statlig myndighet låter en e-tjänst vara ansluten både till det nu aktuella systemet och en annan identitetsfederation.

9.4.9 Hantering av säkerhetsincidenter

Utredningens förslag: Utfärdare av medel för elektronisk identifiering ska rapportera säkerhetsincidenter till Myndigheten för digital förvaltning samt till förlitande parter som påverkas av incidenten.

Myndigheten för digital förvaltning kan besluta om det godkända medel för elektronisk identifiering en säkerhetsincident avser, tills vidare eller under en begränsad period, inte längre är godkänt. Myndigheten för digital förvaltning kan besluta att det medel för elektronisk identifiering som inte är godkänt för systemet som en säkerhetsincident avser tills vidare eller under en begränsad period inte längre ingår i systemet.

Vid allvarliga säkerhetsincidenter ska Myndigheten för digital förvaltning kunna besluta att medlet för elektronisk identifiering inte längre ska ingå i systemet.

Skälen för utredningens förslag

I syfte att upprätthålla tillit för systemet är det viktigt att eventuella säkerhetsincidenter rapporteras och hanteras. Denna incidentrapportering kan i vissa fall sammanfalla med annan rapporteringsskyldighet som följer av andra författningar eller avtal.[36] Det bör poängteras att rapporteringsskyldighet då ska fullföljas enligt alla de regelverk som en uppkommen incident omfattas av.

Säkerhetsincidenter avseende en e-tjänstelegitimation som ingår i det system vi föreslår ska anmälas av utfärdaren till DIGG. Det gäller oavsett om e-legitimationen är godkänd av DIGG eller inte. Säkerhetincidenter även rapporteras till förlitande parter som påverkas av incidenterna. Det går inte att formulera en uttömmande lista över vad som utgör säkerhetsincidenter. Det är incidenter som

[36] Jfr t.ex. https://swedenconnect.se/incident.html (hämtad 2021-06-13).

påverkar e-tjänstelegitimationernas eller systemet för erkännande av medel för elektronisk identifierings tillgänglighet, riktighet eller konfidentialitet. Det kan röra sig om exempelvis tekniska sårbarheter eller andra sårbarheter, faktiska intrång eller att någon av de organisationer som använder den aktuella e-tjänstelegitimationen inte hanterar dem på ett tillförlitligt sätt. En säkerhetsincident kan föreligga även när sårbarheten är teoretisk. Det krävs således inte att en sårbarhet ska ha utnyttjats av någon. Det faktum att sårbarheten finns kan räcka för att det anses vara en säkerhetsincident som ska rapporteras.

När en säkerhetsincident rapporteras behöver DIGG skyndsamt bedöma hur allvarlig incidenten är eller hur allvarlig den kan komma att bli, för att sedan besluta om vilka åtgärder som ska vidtas. DIGG kan komma överens med utfärdaren om vilka åtgärder som måste vidtas. För godkända e-tjänstelegitimationer gäller vidare att DIGG får besluta att e-tjänstelegitimationer tillfälligt eller tills vidare inte längre är godkända för användning i systemet. Ett sådant beslut kan avse grupper av e-tjänstelegitimationer från samma utfärdare eller alla e-tjänstelegitimationer från samma utfärdare fram till dess att incidenten anses åtgärdad. Grupper av e-tjänstelegitimationer kan exempelvis vara legitimationer för användare vid en viss offentlig aktör där bristande säkerhet har identifierats eller en grupp användare för vilka attribut hämtas från ett register där säkerhetsbrister eller felaktigheter har identifierats. För e-tjänstelegitimationer som ingår i systemet men som inte är godkända får DIGG fatta beslut sådana e-tjänstelegitimationer tillfälligt eller tills vidare inte får ingå i systemet. Även ett sådant beslut kan avse grupper av e-tjänstelegitimationer från samma utfärdare eller alla e-tjänstelegitimationer från samma utfärdare. Beroende på säkerhetsincidentens art samt hur den hanteras kan DIGG behöva vidta åtgärder i de tekniska komponenter som finns i systemet för att hindra användningen av berörda e-tjänstelegitimationer i systemet. Om incidenten bedöms som allvarlig får DIGG besluta att e-tjänstelegitimationer inte längre får ingå i systemet. Om e-tjänstelegitimationen är godkänd av DIGG för användning i systemet ska myndigheten återkalla godkännandet (se avsnitt 9.4.12 vad gäller överklagande av beslut).

Det kan krävas bestämmelser om hur säkerhetsincidenter ska hanteras och hur de ska rapporteras. Sådana bestämmelser bedömer vi kommer vara på en sådan detaljerad nivå att de lämpar sig bäst i

myndighetsföreskrifter. DIGG bör därför bemyndigas att efter samråd med MSB meddela sådana föreskrifter.

Det är viktigt att den som förlitar sig på e-tjänstelegitimationerna har planerat för hur de hanterar sådana fall. Det kan handla om att, om det sker internt, ha alternativa sätt för att autentisera sina medarbetare och om det rör extern användning, att de medarbetare som verkligen behöver det kan anskaffa alternativa e-tjänstelegitimationer eller lösa arbetsuppgiften med andra metoder.

För att förlitande parter ska kunna veta om de sårbarheter och de incidenter som inträffar behöver det finnas en informationsdelning mellan de parter som ingår i federationen. Informationen om incidenter och sårbarheter kan vara säkerhetskänslig och därför svår att dela. Det kan därför behöva skapas ett arrangemang kring hur informationsdelningen kan gå till. DIGG bör därför skapa ett sådant arrangemang. Om det krävs föreskrifter om arrangemanget kan de meddelas med stöd av det bemyndigande som redogörs för ovan.

9.4.10 Hantering av personnummer

Utredningens förslag: Personnummer får endast överföras i systemet om krav på användning av personnummer föreskrivs i lag eller i annan författning eller om användning av annan identitetsbeteckning inte är möjlig.

Skälen för utredningens förslag

Inom ramen för vår kartläggning har det av många framförts att de ser fördelar med att deras anställda eller uppdragstagare inte behöver använda sina personnummer vid organisationsöverskridande användning av e-legitimationer. Det kan i vissa fall vara direkt olämpligt eller otillåtet att använda personnummer (jfr avsnitt 9.2.1). En anställd eller uppdragstagare som använder en e-tjänst inom ramen för sin anställning eller sitt uppdrag gör det dessutom på den offentliga aktörens vägnar. Vi anser att personnummer som huvudregel inte bör överföras i systemet vid organisationsöverskridande användning av e-tjänstelegitimationer. En annan unik personidentifieringsuppgift som är bestående över tid i form av exempelvis tjänsteidentiteter bör

i stället användas. Om behov finns att fastställa hur en sådan personidentifieringsuppgift bör vara uppbyggd och vad den bör innehålla föreskrivs det lämpligen i myndighetsföreskrifter som avser krav på e-tjänstelegitimationer i systemet.

Det bör vara ovanligt att de åtgärder en anställd eller uppdragstagare vidtar i en e-tjänst är förknippat med att förlitande part måste veta personens personnummer. En nättjänst kan visserligen vara byggd så att personnummer används, men det bör vara ovanligt att det förfarande tjänsten används till, i sig kräver personnummer. Det kan emellertid finnas sådana krav. Vidare kan det finns situationer där det inte går att använda en annan identitetsbeteckning än personnummer. Det kan således finnas behov av undantag från huvudregeln att personnummer inte ska överföras i systemet.

Undantag bör gälla för det fall krav på användning av personnummer föreskrivs i lag eller annan författning, exempelvis om det förfarande e-tjänsten används för är reglerat på ett sådant sätt att det krävs personnummer. Det andra undantaget ska avse situationer då det inte är möjligt att använda en annan identitetsbeteckning än personnummer. En sådan situation kan t.ex. vara att det uppstår tekniska problem för vissa e-tjänstelegitimationer eller i systemet som innebär att andra beteckningar inte kan användas. Undantaget är avsett att endast omfatta situationer då användningen rent faktiskt inte är möjlig och ska inte tillämpas på situationer då en e-tjänst eller ett bakomliggande system är skapade på ett sådant sätt att de endast kan hantera personnummer.

9.4.11 Behandling av personuppgifter i systemet

Utredningens förslag: Stöd för nödvändig behandling av personuppgifter i systemet av Myndigheten för digital förvaltning ska föreskrivas i författning.

Skälen för utredningens förslag

Systemet för erkännande av medel för elektronisk identifiering kommer medföra behandling av personuppgifter. Behandlingen är nödvändig för att systemet ska kunna användas för erkännande av e-tjänste-

legitimationer. Utfärdare av e-legitimationerna måste säkerställa att de har stöd för personuppgiftsbehandlingen, likaså förlitande parter. Det går ännu inte att fastslå hur systemet kommer att vara uppbyggt eller hur det i detalj kommer att fungera då detta enligt förslaget ska beslutas av DIGG. Det är dock troligt att DIGG kommer att tillhandahålla tekniska komponenter som används när en person ska identifieras elektroniskt. Att myndigheten ska tillhandahålla systemet kommer att föreskrivas i författning. Behandlingen är vidare nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Något som enligt artikel 6.1 e i dataskyddsförordningen utgör en rättslig grund för behandling.

I dataskyddslagen tydliggörs i 2 kap. 2 § att en uppgift av allmänt intresse utgör en rättslig grund för behandling av personuppgifter enligt artikel 6.1 e i dataskyddsförordningen om uppgiften följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning eller är ett led i den personuppgiftsansvariges myndighetsutövning om myndighetsutövningen sker enligt lag eller annan författning.

I förarbetena till dataskyddslagen uttalas att den verksamhet som en statlig eller kommunal myndighet bedriver inom ramen för sin befogenhet är av allmänt intresse och att det vanligen är den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen som bör tillämpas av myndigheter. Detta utesluter dock inte att andra rättsliga grunder samtidigt kan vara tillämpliga i vissa fall.[37]

När DIGG kommer att behandla personuppgifter inom ramen för sitt uppdrag att tillhandahålla systemet för erkännande av medel för elektronisk identifiering kommer detta således att ske för att utföra uppgifter av allmänt intresse som följer av lag eller annan författning. Vi anser emellertid att det för tydlighetens skull bör föreskrivas i lagen att personuppgifter får behandlas av den myndighet som tillhandahåller systemet, dvs. DIGG. Sådan behandling får ske om den är ett nödvändigt led i att identifiera användare elektroniskt. Sådan behandling kan avse personuppgifter kopplade till en enskild e-tjänstelegitimation men det kan också vara nödvändigt för DIGG att behandla personuppgifter med koppling till den administrativa hanteringen av systemet. Den författningsreglering vi föreslår avser

[37] Prop. 2017/18:105 s. 56 f.

endast den eventuella personuppgiftsbehandling DIGG kommer att utföra och inte andra aktörers användning av systemet.

9.4.12 Överklagande m.m.

Utredningens förslag: Om DIGG genom sin granskning bedömer att medlet för elektronisk identifiering inte lever upp till kraven ska myndigheten genom beslut avslå ansökan om godkännande. Ett sådant beslut ska kunna överklagas till allmän förvaltningsdomstol.

Beslut om att medel för elektronisk identifiering som tillfälligt eller tills vidare inte är godkända för användning i systemet samt beslut om att medel inte får ingå i systemet, får överklagas till allmän förvaltningsdomstol.

DIGG får bestämma att beslut enligt ovan ska gälla omedelbart.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Skälen för utredningens förslag

I avsnitt 9.4.6 redogörs för våra förslag avseende granskning och godkännande av e-tjänstelegitimationer. Om en utfärdare av en e-tjänstelegitimation ansöker om att få den godkänd av DIGG för användning i systemet ska DIGG granska legitimationen. För det fall DIGG bedömer att den inte lever upp till de krav som ställs ska myndigheten avslå ansökan. Ett sådant beslut ska kunna överklagas till allmän förvaltningsdomstol.

Av avsnitt 9.4.9 framgår att vi föreslår att DIGG, om det uppstår säkerhetsincidenter, ska kunna besluta att e-tjänstelegitimationer som är godkända tillfälligt eller tills vidare inte är godkända samt att myndigheten ska kunna besluta att legitimationer som inte är godkända, men som ingår i systemet, tillfälligt eller tills vidare inte ingår i systemet. Vidare föreslår vi att DIGG vid allvarliga säkerhetsincidenter kan besluta att en e-tjänstelegitimation inte längre ska ingå i systemet. Om e-tjänstelegitimationen är godkänd för användning i systemet ska godkännandet återkallas. Även dessa beslut ska kunna överklagas till allmän förvaltningsdomstol.

Myndigheten får bestämma att besluten ska gälla omedelbart eftersom vissa säkerhetsincidenter kan vara av en sådan karaktär att det innebär stora risker att låta det vara möjligt att fortsatt använda e-tjänstelegitimationerna.

I likhet med vad som är huvudregeln för överklagande av förvaltningsbeslut bör prövningstillstånd krävas för överprövning i kammarrätten.

9.5 En samverkande infrastruktur mellan offentlig och privat sektor

Utredningens bedömning: Systemet för erkännande av e-tjänstelegitimationer bör utvecklas till att även omfatta privat sektor och denna fråga bör utredas vidare.

Skälen för utredningens bedömning

Utredningens uppdrag är begränsat till användning av e-legitimation i tjänsten i den offentliga förvaltningen. Inom den offentliga förvaltningen finns emellertid behov av åtkomst med e-tjänstelegitimationer till tjänster som tillhandahålls av privata aktörer och det finns även behov av sådan åtkomst mellan aktörer i privat sektor samt från en privat aktör mot e-tjänster som tillhandahållas inom den offentliga sektorn.

Utredningen om bildande av en e-legitimationsnämnd lämnade förslag om en infrastruktur för den offentliga sektorn men påtalade samtidigt vikten av att E-legitimationsnämnden verkade för att en motsvarande och samverkande infrastruktur etablerades även för den privata sektorn. Utredningen framförde bl.a. följande.

> (E)-legitimationer som godtas inom Infrastrukturen för Svensk e-legitimation (ska inte) begränsas så att de får användas endast för e-tjänster inom offentlig sektor. Det är i stället, såsom inom dagens system för e-legitimationer, väsentligt och centralt att en ny infrastruktur resulterar i motsvarande lösning för den privata sektorn.
>
> Detta bör kunna uppnås genom att det bildas två samverkande infrastrukturer för identifiering – en för den offentliga sektorn och en för den privata – som i princip använder sig av samma regelverk. Dessa två

> samverkande infrastrukturer bör från ett användarperspektiv uppfattas som enhetliga. Hit hör rent praktiska frågor som att samma e-legitimationer, användargränssnitt och transaktionsmönster bör införas. Härigenom kan sådana för informationssamhället grundläggande funktioner som elektronisk legitimering hanteras enhetligt. En sådan samordning är viktig även från juridiska utgångspunkter. Enskildas behov av rättssäkerhet och persondataskydd måste tillgodoses enhetligt och det samma gäller för tolknings- och tillämpningsfrågor. Genom en sådan samordning kan det säkerställas att det uppkommer samverkande lösningar i stället för parallella icke samverkande lösningar. Utredningen har därför i olika avseende sökt lösningar för att åstadkomma samverkande infrastrukturer. Bland annat har det föreslagna regelverket för Infrastrukturen för Svensk e-legitimation utformats så att det ska kunna fungera inom både offentlig och privat sektor och stödja samverkande infrastrukturer. Detsamma gäller för de framtagna tekniska specifikationerna och tillitsramverket. En identitetsutfärdare som godkänts inom en ny infrastruktur för offentlig sektor bör, med samma e-legitimationer och identitetsintyg, kunna verka inom en infrastruktur för privat sektor.[38]

Vi delar utredningens bedömning och ser det som viktigt för både digitaliseringen av offentlig sektor som samhällets digitalisering i stort att det skapas förutsättningar för en samverkande infrastruktur mellan offentlig och privat sektor vad gäller elektronisk identifiering. Då detta är en fråga som ligger utanför utredningens uppdrag lämnar vi emellertid inga förslag i denna del utöver att vi anser att denna fråga bör utredas vidare.

9.6 Översyn av det svenska tillitsramverket

Utredningens förslag: Regeringen ska ge Myndigheten för digital förvaltning i uppdrag att se över det svenska tillitsramverket med beaktande av den behovsbild som föreligger för e-tjänstelegitimationer.

[38] *E-legitimationsnämnden och Svensk e-legitimation* (SOU 2010:104), s. 145 f.

Skälen för utredningens förslag

Som konstaterats i avsnitt 6.7 är ett tillitsramverk av central betydelse för att bl.a. skapa tillit och gemensamma referensramar inom e-legitimationsområdet. Med beaktande av de skäl som anges nedan vad gäller behovet av harmonisering med eIDAS-förordningens tillitsnivåer samt om andra krav på kontroll av en användares identitet bör gälla för e-tjänstelegitimationer anser vi att regeringen ska ge DIGG i uppdrag att göra en översyn av tillitsramverket.

Harmonisering med eIDAS-förordningens tillitsnivåer

I dagsläget finns det i Sverige två generella ramverk som existerar parallellt i form av DIGG:s tillitsramverk (se avsnitt 6.3) och eIDAS-förordningens tillitsnivåer (se avsnitt 4.2.3). Båda bygger på samma internationella standard (ISO/IEC 29115) och består av tre tillitsnivåer: 2, 3 och 4 respektive låg, väsentlig och hög. Även om kraven i stora delar överensstämmer för respektive nivå finns det emellertid vissa skillnader mellan nivåerna i DIGG:s tillitramverk och nivåerna i eIDAS-förordningen. Eftersom det enligt förordningen finns en skyldighet för svenska offentliga e-tjänster att erkänna anmälda utländska e-legitimationer på tillitsnivå väsentlig och hög måste myndigheter som tillhandahåller sådana tjänster förhålla sig till båda ramverk.

Den svenska tillitsnivån 3 bedöms överensstämma med nivån väsentlig i eIDAS-förordningen. Dock ställer den svenska tillitsnivån 4 högre krav på e-legitimationen än nivån hög i eIDAS-förordningen, detta eftersom nivå 4 kräver personlig inställelse vid utfärdande eller förnyande vart femte år. Något som är möjligt att genomföra på distans för nivå hög i eIDAS-förordningen.

E-legitimationsnämnden framförde 2016 i en rapport att det i och med de högre kraven i den svenska nivå 4 finns en säkerhetsventil för offentliga myndigheter som har tjänster med behov av den nivån.[39] DIGG har emellertid angett att om en e-tjänst kräver svenska e-legitimationer på tillitsnivå 3 eller 4, måste e-tjänsten också acceptera utländska e-legitimationer som har tillitsnivå väsentlig eller hög.[40]

[39] E-legitimationsnämnden, *Fortsatt försörjning av tjänster för e-legitimering och e-underskrift* (Dnr: 131 645711-15/9513), 25 oktober 2016, s. 23.
[40] www.digg.se/digital-identitet/e-legitimering/offentlig-aktor/internationell-e-legitimering (hämtad 2021-06-14).

Som vi tidigare bedömt är det möjligt för medlemsstaterna att ha nationella tillitsramverk (se avsnitt 4.2.3). Det är emellertid tillitsnivåerna i eIDAS-förordningen som styr vid gränsöverskridande användning av e-legitimationer. En svensk myndighet är mot bakgrund av det förhindrad att ställa ett högre krav på en enligt förordningen anmäld e-legitimation än nivå hög. Att kräva den svenska nivån 4 vid gränsöverskridande användning är enligt vår bedömning inte förenligt med eIDAS-förordningen då det saknas stöd för ett sådant undantag för erkännande.

Det finns e-legitimationer i Sverige som är godkända utifrån tillitsnivå 4 i det svenska ramverket. Vi har däremot under kartläggningsarbetet inte sett något exempel på en e-tjänst inom den offentliga förvaltningen som kräver att autentisering sker med en e-legitimation som är godkänd enligt tillitsnivå 4. Vidare kan vissa krav, såsom krav på personlig inställelse, försvåra för utövandet av den fria rörligheten för personer som befinner sig i andra länder än Sverige.[41]

Sammantaget framstår behovet av tillitsnivå 4 som högst oklar då det argument som tidigare framförts av E-legitimationsnämnden om att denna nivå skulle kunna nyttjas som en ”säkerhetsventil” vid gränsöverskridande användning inte är förenlig med eIDAS-förordningen.

Det är värt att i detta sammanhang notera att 2017 års ID-kortsutredning gjorde bedömningen att den statliga e-legitimationen som enligt utredningens förslag, efter ansökan, skulle finnas på det statliga identitetskortet skulle uppfylla kraven enligt tillitsnivå 4 och att utfärdandet skulle ske vid ett personligt besök.[42] Även om kravet på personlig inställelse i tillitsnivå 4 skulle tas bort från tillitsramverket hade det inte hindrat att en kommande svensk statlig e-legitimation endast hade utfärdats efter personlig inställelse. Detta eftersom godkännande enligt en viss tillitsnivå endast innebär att e-legitimationen uppfyller de krav som den är granskad och godkänd utifrån. Det finns därmed inget hinder mot att en e-legitimation utfärdas på ett sätt som går utöver dessa krav.

Ytterligare ett skäl till varför det svenska tillitsramverket bör harmoniseras med förordningens tillitsnivåer är att det under vårt kartläggningsarbete framkommit att det bl.a. inom e-hälsa pågår arbete på EU-nivå som syftar till att underlätta det digitala gränsöverskridande samarbetet genom gemensamma krav på vilken tillitsnivå som

[41] Deloitte, *Looking ahead – The user experience of eIDAS-based eID*, s. 24.
[42] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 319 ff.

ska krävas till uppgifter om hälsa. Eftersom det rör sig om EU-samarbeten är det naturligt att dessa utgår från eIDAS-förordningens tillitsnivåer. Att tillämpa ett annat ramverk med andra nivåer som ställer andra krav kan försvåra sådana samarbeten och den praktiska användningen av e-legitimationerna.

EU:s förordning om en gemensam digital ingång ställer därtill krav på att medlemsstaterna säkerställer att e-tjänster finns för vissa förfaranden, t.ex. att lämna in en inkomstskattedeklaration, och att dessa tjänster kan nås digitalt av invånare i andra medlemsstater. Förordningen har antagits med utgångspunkt i att individen ska identifiera sig med stöd av den tekniska infrastruktur som upprättats med anledning av eIDAS-förordningen.

Det kan även noteras att det av kommissionen nyligen lämnade förslaget om ändringar i eIDAS-förordningen anger att en digital identitetsplånbok ska uppfylla kraven för ”hög” enligt förordningens tillitsnivå. De svenska förlitande parter vars e-tjänster omfattas av förslaget kommer därmed vara skyldiga att låta användare med en sådan plånbok nyttja dessa tjänster. I skäl 14 i eIDAS-förordningen i dess nuvarande lydelse förtydligas att principen om ömsesidigt erkännande endast avser autentisering för en nättjänst och att den inte ger en rätt till åtkomst till tjänsten. Åtkomsten till tjänsterna och deras slutliga leverans till den sökande är kopplad till rätten att ta emot sådana tjänster enligt villkoren i nationell lagstiftning. Varje offentligt organ får inom ramen för den tillämpliga nationella lagstiftningen avgöra vilka krav som ska ställas för åtkomst till tjänsterna. I det förslag som nu lämnats är ansatsen från kommissionens sida dock tydlig i att EU-medborgare med e-identitetsplånboken utöver autentiseringen även ska kunna använda de berörda e-tjänsterna.

Vårt kartläggningsarbete har visat att det är en utbredd uppfattning bland både aktörer inom den offentliga förvaltningen och utfärdare att det är förvirrande med två parallella begreppsapparater för vad som i grunden är samma sak. Flera är därför av uppfattningen att det svenska ramverket bör harmoniseras med tillitsnivåerna i eIDAS-förordningen. Med beaktande av de omständigheter som anges ovan delar vi denna bedömning.

Krav på personnummer uppställer hinder för vissa arbets- och uppdragstagare

Det svenska tillitsramverket ställer för tillitsnivå 3 och 4 krav som medför att användaren måste ha ett svenskt personnummer, eller samordningsnummer som bygger på styrkt identitet, för att kunna få en e-legitimation som är godkänd på dessa nivåer eftersom en kontroll måste göras mot ett officiellt register. Det är e-legitimationsutfärdaren som ska visa för DIGG att utfärdandet görs baserat på tillräcklig grundidentifiering. Till följd av svårigheter med att identifiera personer med samordningsnummer krävs det oftast i praktiken personnummer.

Avsaknad av personnummer skapar utanförskap för olika grupper i samhället. Detta kan gälla både nyanlända och unionsmedborgare. Vad gäller unionsmedborgare har Sverige återkommande fått kritik för de hinder för den fria rörligheten som de ofta förekommande kraven på personnummer skapar.[43] Mot bakgrund av klagomålen har kommissionen i ett s.k. EU-pilotärende ställt ett antal frågor till svenska myndigheter.[44] Regeringen har med anledning av detta åtagit sig att utreda vilka möjligheter det finns att bättre säkerställa att unionsmedborgare hanteras i enlighet med bestämmelserna om fri rörlighet. Inom ramen för ett annat EU-pilotärende har kommissionen även ställt liknande frågor rörande tredjelandsmedborgare.[45]

Kommerskollegium har i en rapport om hinder för den fria rörligheten för EU-medborgare funnit att digitaliseringen av samhällstjänster förstärker personnumrets betydelse eftersom det lett till att personnumret efterfrågas i allt fler sammanhang. Myndigheten lyfter även den ökade användningen av e-legitimationer som kräver personnummer som ett hinder.[46] Något som även bekräftas av vår kartläggning där det framgår att detta skapar problem då anställda utan personnummer inte kan få tillgång till för tjänsten centrala e-tjänster som kräver autentisering med en e-legitimation (se mer om detta i avsnitt 7.6.4).

---

[43] Se bl.a. Europaparlamentet, Genereldirektoratet för intern politik, *Hinder för rätten att fritt röra sig och att fritt uppehålla sig för unionsmedborgare och deras familjer: Landsrapport för Sverige*, 15 juni 2016, s. 15 ff. och Skatteverket, *Regler och rutiner i folkbokföringsärenden*, 26 februari 2018, s. 8 f.
[44] Fi2016/03726/S3.
[45] Fi2019/03178/S3.
[46] Kommerskollegium, *Att flytta till Sverige – hinder för den fria rörligheten för EU-medborgare* (2013:8), december 2013, s. 13.

Nuvarande tillitsramverk gäller för både privata e-legitimationer och e-tjänstelegitimationer och någon åtskillnad görs inte mellan vilken typ av e-legitimation det rör sig om.

Vad gäller utfärdande av giltiga fysiska id-handlingar godtas exempelvis pass utfärdade av andra EU-länder samt Island, Liechtenstein, Norge och Schweiz som identitetshandling både vid utfärdande av identitetskort för folkbokförda i Sverige samt i samband med förarprov som är den identifiering som sker inför utfärdande av körkort. Även pass från Förenade kungariket godtas vid förarprov.[47] I fråga om tjänstekort som utfärdas av statliga eller kommunala myndigheter framgår av 7 § PMFS 2020:4 att sökanden bl.a. kan styrka sin identitet med EU-pass eller pass utfärdat av Island, Liechtenstein, Norge eller Schweiz.

Både vid utfärdande av vissa svenska identitetshandlingar samt statliga eller kommunala myndigheters tjänstekort godtas således identifiering med pass utfärdade av andra EU-länder samt Island, Liechtenstein, Norge eller Schweiz. Krav på koppling till officiella register som indirekt innebär krav om innehav av personnummer kan vara befogat vad gäller privata e-legitimationer. Vad gäller e-tjänstelegitimationer har dessa emellertid ett mycket mer begränsat användningsområde vilket minskar riskerna för missbruk avsevärt i motsats till privata e-legitimationer. Vi anser därför att det kan ifrågasättas om inte identifiering vid utfärdande likt ovan angivna exempel åtminstone borde godta EU-pass samt pass utfärdat av Island, Liechtenstein, Norge eller Schweiz och att någon annan unik personidentifieringsuppgift med koppling till ett register (t.ex. hos arbetsgivaren) hade kunnat användas i stället för personnummer. Detta hade även undanröjt ett befintligt hinder mot den fria rörligheten för EU-medborgare som tillitsramverkets krav på personnummer i dagsläget medför.

Av kartläggningsarbetet har framgått att behoven även gäller personer som inte är medborgare i antingen ett EU-land respektive Island, Liechtenstein, Norge eller Schweiz. Det bör därför utredas om även andra utländska passhandlingar bör godtas under förutsättning att de bedöms tillförlitliga.[48]

[47] 4 § Skatteverkets föreskrifter om identitetskort (SKVFS 2009:14) och 2 kap. 2 § Transportstyrelsens föreskrifter och allmänna råd om förarprov, gemensamma bestämmelser (TSFS 2012:41).
[48] Vad gäller tillförlitlighet se t.ex. www.migrationsverket.se/Privatpersoner/Bli-svensk-medborgare/Medborgarskap-for-vuxna/Styrkt-identitet/Migrationsverkets-bedomning-av-identitetsdokument.html (hämtad 2021-06-13).

9.7 En framtida lösning för attributshantering

Utredningens bedömning: En framtida lösning för attributshantering bör i huvudsak bygga på att attributen med behörighetsinformation tillhandahålls av arbets- eller uppdragsgivaren.

Skälen för utredningens bedömning

I flertalet e-tjänster räcker det inte med att en användare autentiserar sig utan det kan även krävas vissa andra attribut för att tillgång till tjänsten ska ges. Attributen kan vara sådana som framkommer direkt av identitetsintyget, som personnummer för privatpersoner eller koppling till arbetsgivare eller anställd respektive uppdragstagare vid användning i tjänsten. Det har under vårt kartläggningsarbete framkommit att förlitande parter inom förvaltningen, när e-tjänstelegitimationer används, har det gemensamma behovet att få information om både användaren och organisationen som denne företräder. Utöver den informationen är det däremot svårare att identifiera om och i så fall vad förlitande part behöver för information om användaren av en e-tjänst. Vissa har angett att person och organisation räcker medan andra har indikerat att de behöver mer information än så, exempelvis mer specifik information om var i en organisation personen är anställd. För att e-tjänstelegitimationer ska kunna möta behoven hos förlitande parter kan de därmed behöva förenas med ytterligare attribut.

Det finns olika möjliga sätt att lösa attributs- och behörighetshanteringen. Det kan ske genom centrala register, lokala register i respektive e-tjänst eller genom att användarens uppdragsgivare tillhandahåller informationen. Vi anser att den sistnämnda lösningen är den önskvärda. Det finns sektorer med centrala register såsom hälso- och sjukvården via HSA-katalogen. Det finns även vissa attribut där det kan vara lämpligt att dessa tillhandahålls på nationell nivå, exempelvis uppgifter om firmatecknare.

För att hanteringen av attribut ska bli så enhetlig och effektiv som möjligt kan det vara nödvändigt att närmare reglera hanteringen och lösningen i föreskrifter. DIGG kan meddela sådana föreskrifter med stöd av bemyndigandet avseende krav på e-tjänstelegitimationer i systemet och krav avseende förlitande parter. Det är enligt vår upp-

fattning generellt olämpligt att skapa stora nationella register över anställda och deras roller, såväl ur säkerhetssynpunkt som utifrån skyddet av den personliga integriteten. Att underhålla behörighetsinformation gällande en organisations anställda och uppdragstagare samt deras respektive roller är därtill ett omfattande arbete som kräver regelbundna uppdateringar. Det är därför olämpligt att sprida ut behörighetsinformationen i flera register och källor som behöver underhållas, särskilt då de finns hos andra organisationer. Behörighetsinformation är en färskvara som behöver underhållas av den organisation som en anställd eller uppdragstagare företräder. Därför bedömer vi att behörighetsinformation och attribut bäst tillhandahålles av arbetsgivaren eller uppdragsgivaren.

För att detta ska fungera behöver det finnas en infrastruktur för att tillhandahålla attribut och för att en förlitande part ska kunna ta emot och använda attributen. En sådan lösning kommer också att kräva att varje offentlig aktör som vill att sina anställda eller uppdragstagare ska kunna använda e-tjänstelegitimationer i systemet har en fullgod behörighetshantering.

Det framtida arbetat på området behöver vidare beakta den utveckling som sker inom EU. I kommissionens förslag till ändringar i eIDAS-förordningen föreslås en ny betrodd tjänst, elektronisk attestering av attribut (”electronic attestation of attributes”).[49] Tjänsten är enligt förslaget tänkt att användas tillsammans med den föreslagna digitala identitetsplånboken (se mer om förslaget i avsnitt 4.2.5).

Enligt förslaget ska attribut kunna hämtas för att användas tillsammans med den digitala identitetsplånboken. Kvalificerade betrodda tjänster för elektronisk attestering av attribut ska på förfrågan från användare kunna verifiera attributen som ska kunna hämtas elektroniskt från en autentisk källa på nationell nivå som tillhandahålls av offentlig förvaltning eller via en utsedd källa, som t.ex. folkbokföringsregistret. De attribut som ska kunna tillhandahållas på detta sätt listas i bilaga VI till förslaget och inkluderar bl.a. adress, ålder, kön, nationalitet, professionella- och utbildningskvalifikationer, titlar och licenser m.m.

[49] COM(2021) 281 final.

9.8 Ökat stöd avseende användning av e-tjänstelegitimationer

Utredningens bedömning: Det bör ges mer stöd till den offentliga förvaltningen vad avser användning av e-tjänstelegitimationer.

Skälen för utredningens bedömning

Som framgår av avsnitt 7.6.8 finns det ett behov av ökat stöd inom e-tjänstelegitimationsområdet. Det stöd som behövs gäller i huvudsak grundläggande vägledning med koppling till både tekniska och juridiska frågor. Det är vidare framför allt mindre aktörer inom den offentliga förvaltningen som har behov av sådant stöd.

DIGG har redan i dag enligt 3 § 2 förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning i uppgift att främja användningen av elektronisk identifiering och underskrift. Vi har i delbetänkandet föreslagit att DIGG ska få en utökad roll vad avser att främja användningen av betrodda tjänster.[50] För det stöd som avser de tekniska aspekterna rörande betrodda tjänster bedömde vi att myndighetens anslag, genom tillskott via reformutrymmet, behövde ökas med motsvarande två årsarbetskrafter eller tre miljoner kronor.[51] DIGG:s anslag ökades även med fem miljoner kronor från och med 2021 för att finansiera att myndigheten ska ge ett rättsligt stöd till den offentliga förvaltningen.[52]

Utifrån DIGG:s befintliga uppgift att främja användningen av elektronisk identifiering och då tekniska frågor rörande e-tjänstelegitimationer ofta är sammankopplade med användning av elektroniska underskrifter bedömer vi att DIGG, med de ökade anslag vi föreslår i delbetänkandet, bör kunna möta upp det behov av ökat stöd som finns vad gäller de tekniska aspekterna. De juridiska frågorna bör därtill kunna hanteras inom ramen för det ökade rättsliga stöd DIGG nu ska erbjuda. Mot denna bakgrund lämnar vi inget förslag vad gäller ökat stöd.

[50] *Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9), s. 199 ff.
[51] A.a. s. 249 f.
[52] Prop. 2020/21:1 Utgiftsområde 22 s. 117.

9.9 Bättre förutsättningar för id-växling

Utredningens bedömning: En statlig e-legitimation som kan användas för id-växling bör i enlighet med förslaget från 2017 års ID-kortsutredning införas för att skapa förutsättningar för enklare och billigare utfärdande av e-tjänstelegitimationer samt en mer diversifierad marknad.

Skälen för utredningens bedömning

Som framgår av avsnitt 5.6 föreslog 2017 års ID-kortsutredning att Polismyndigheten skulle ha ansvaret för grundidentifiering och utfärdande av statliga fysiska identitetshandlingar, dvs. pass och statligt identitetskort. Utredningen föreslog även att Polismyndigheten skulle utföra grundidentifiering samt utfärdande av den statliga e-legitimationen som enligt utredningens förslag, efter ansökan, skulle finnas på det statliga identitetskortet. Utredningen lyfte även fram att e-legitimationen hade kunnat användas för id-växling.[53] Förslaget bereds för närvarande inom Regeringskansliet.

Det finns i dag begränsade möjligheter att genomföra id-växling då e-legitimationsutfärdaren måste godkänna detta. 2017 års ID-kortsutredning konstaterade att det är både kostsamt och svårt att utföra grundidentifiering. Vi delar denna bedömning och olika utfärdare har också påtalat olika utmaningar vad avser grundidentifiering. Det är även en väldigt kostsam hantering som skapar en hög tröskel för inträde på marknaden för både utfärdare av privata e-legitimationer och e-tjänstelegitimationer.

Att arbetsgivare i förhållande till e-legitimationsutfärdaren kan ikläda sig delansvaret för att grundidentifiera användaren i samband med ansökan om utfärdande av en e-tjänstelegitimation är något vi under kartläggningen stött på frågor kring. E-legitimationsutfärdare har sett ett antal praktiska och juridiska problem med en sådan hantering. Dessa problem innefattade bl.a. möjligheterna att upprätthålla den processmässiga och tekniska standarden över tid, möjligheten att göra brottsregisterutdrag kring den personal som ska utfärda en e-legitimation, att medarbetare utsätts för ökad hotbild samt ansvarsfrågan – det vill säga ifall en offentlig aktör vill lägga

[53] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 321 f.

ansvaret på en enskild medarbetare att utfärda en identitetshandling som kan användas till en lång rad känsliga och värderelaterade ärenden.

Vi ser sammanfattningsvis att en statlig e-legitimation som kunde användas för id-växling avsevärt hade förenklat utfärdandet av e-tjänstelegitimationer och minskat kostnaderna. Det skulle även sänka tröskeln för marknadsinträde för nya utfärdare och därigenom leda till en mer diversifierad marknad än i dagsläget. Det hade därtill väsentligen underlättat utfärdande av e-legitimationer i samband med en sådan situation som nu föreligger under pandemin eftersom utfärdandet hade kunnat ske helt och hållet på distans om id-växling kunnat ske från en statlig e-legitimation.

10 Konsekvenser

10.1 Nollalternativet

Ett nollalternativ innefattar en bedömning av vad som händer om de i betänkandet föreslagna åtgärderna inte genomförs. Både Utredningen om effektiv styrning av nationella digitala tjänster och Digitaliseringsrättsutredningen konstaterade att den digitala utvecklingen har begränsningar vad gäller förutsebarhet.[1] Vi delar denna bedömning. Det är av denna anledning svårt att bedöma påverkan av ett nollalternativ på längre sikt. I synnerhet då det, som framgår av avsnitt 9.1, är så att den önskade utvecklingen inom den offentliga förvaltningen är att röra sig från utbyten som i dag sker genom extern inloggning med e-legitimationer till utbyten som sker från system till system. Detta ligger emellertid framåt i tiden och det är givetvis svårt att med exakthet bedöma hur lång tid detta kommer ta eller om det ens realiseras fullt ut.

Ett nollalternativ skulle troligen innebära en bibehållen eller ökad användning av privata e-legitimationer i tjänsten. Något vi med beaktande av de aspekter det redogörs för i avsnitt 9.2 ser som negativt.

Ett genomförande av förslagen i DIGG:s rapport om eID för medarbetare skulle kunna leda till en ökad användning av e-tjänstelegitimationer.[2] Den avtalsmodell som föreslås i rapporten bygger dock på frivillighet och det riskerar att resultera i en låg anslutningsgrad eller en långsam anslutningstakt som medför att de avsedda effekterna med förslaget inte uppnås.

---

[1] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 433 och *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25), s. 521.

[2] DIGG, *eID för medarbetare – Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte* (dnr 2019-582), 14 december 2020.

Dagens lösningar för att möjliggöra organisationsöverskridande elektronisk kommunikation inom den offentliga förvaltningen är förenad med kostnader. Det rör sig bl.a. om kostnader för tekniska integrationer och för manuell hantering, exempelvis behörighetshantering. Vi har inte haft möjlighet att bilda oss en heltäckande bild av hur stora dessa kostnader är. Dessa kostnader finns inte minst i integrationen mellan respektive myndighets autentiseringslösningar och centrala system som t.ex. sådana system som tillhandahålls av Statens servicecenter där anpassningar mot respektive myndighet som ansluter sker i dag.

Om förslaget från kommissionen om ändringar i eIDAS-förordningen genomförs kan det även leda till att den europeiska digitala identitetsplånboken används för organisationsöverskridande åtkomst i den offentliga förvaltningen (se mer om förslaget i avsnitt 4.2.5).

10.2 Konsekvenser för kommuner och regioner

I 14 kap. 3 § regeringsformen anges att en inskränkning i den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett den. En lagstiftning som ställer upp krav för en kommunal verksamhet minskar generellt sett kommunernas möjligheter att själva göra prioriteringar i sin verksamhet.

Vi bedömer att förslagen i detta betänkande inte får några konsekvenser för den kommunala självstyrelsen. Förslagen i detta betänkande innebär inte heller några kommunalekonomiska konsekvenser som enligt den kommunala finansieringsprincipen ska kompenseras genom anslag på statens budget.

10.3 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

En ökad användning av e-tjänstelegitimationer i stället för enklare former av autentisering kommer leda till ökad informationssäkerhet och kan därigenom ha viss brottsförebyggande effekt.

E-tjänstelegitimationer har vidare inte lika många användningsområden som privata e-legitimationer vilket borde betyda att de är mindre intressanta för kriminella att få åtkomst till än privata e-legitimationer.

En e-tjänstelegitimation kommer även att spärras i samband med att någon avslutar en anställning eller ett uppdrag vilket innebär att den spärrade e-legitimationen inte kan användas för åtkomst till andra organisationers e-tjänster. I dag används ofta privata e-legitimationer tillsammans med för e-tjänsten lokalt lagrad behörighetsinformation vilket innebär att om inte de lokala behörighetsuppgifterna i den externa e-tjänsten ändras kan en tidigare anställd eller uppdragstagare fortfarande komma åt information i dessa e-tjänster och verka i sin då tidigare uppdragsgivares namn.

10.4 Konsekvenser för sysselsättningen

Vi bedömer att förslagen inte får några direkta konsekvenser för sysselsättningen.

10.5 Konsekvenser för offentlig service i olika delar av landet

Vi bedömer att förslagen inte får några direkta konsekvenser för offentlig service i olika delar av landet.

10.6 Konsekvenser för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags samt konsekvenser för företag i stort

Av 15 § i kommittéförordningen (1998:1474) följer att konsekvenserna av förslagen för små företag särskilt ska anges om de har betydelse för denna grupp. Utredningen ska enligt direktiven även särskilt ange konsekvenser för företag i form av kostnader och ökade administrativa bördor. Nedan presenteras konsekvenserna för små företag. Det som anges om kostnader och administrativ börda kan också appliceras på medelstora och stora företag. Givetvis med den skillnaden att kostnader och administrativa bördor får anses vara mindre betungande för dessa företag.

Att som utfärdare av e-tjänstelegitimationer ha med sin e-tjänstelegitimation i det föreslagna systemet kommer sannolikt att vara attraktivt eftersom det troligen kommer uppställas som ett krav från de flesta aktörer i offentlig förvaltning vid anskaffning av e-tjänstelegitimationer.

Även om de krav som kommer att gälla för godkännande inte fastställs i betänkandet kommer det att vara förenat med vissa kostnader då DIGG kommer ges möjlighet att ta ut en avgift för den granskning som krävs och en viss administrativ börda tillkommer även i samband med ett sådant förfarande. Samtidigt bedöms det underlätta marknadsinträde och öppna upp möjligheten för den som är ansluten till systemet att utöka sin kundkrets.

Utöver e-legitimationsutfärdare berörs också andra företag av vårt förslag om ett system för erkännande, eftersom vi föreslår att även privata utförare inom främst utbildnings-, vård- och omsorgssektorerna ska kunna använda systemet. För dessa företag innebär tillgång till systemet en möjlighet att kunna använda de e-tjänster som tillhandahålls av statliga myndigheter utan att anställda eller uppdragstagare behöver använda sig av privata e-legitimationer. Det är enligt vår uppfattning svårt att bedöma exakt hur många företag som omfattas av denna möjlighet. Vi kan emellertid konstatera att det enligt Friskolornas riksförbund finns drygt 4 100 fristående förskolor och skolor i Sverige[3] och att det enligt Vårdföretagarna fanns närmare 15 400 vårdföretag år 2018.[4] Av vårdföretagen hade strax under 90 procent färre än 10 anställda.

Vi bedömer att våra förslag avseende systemet inte omfattas av krav på upphandling i enlighet med lagen (2016:1145) om offentlig upphandling. Däremot behöver de aktörer som omfattas av lagen, såsom statliga myndigheter, kommuner och regioner, beakta och ta ställning till bestämmelserna när de anskaffar e-tjänstelegitimationer till anställda och uppdragstagare.

[3] Friskolornas riksförbund, *Fakta om friskolor (2021)*, s. 6.
[4] Vårdföretagarna, *Privat Vårdfakta 2020*, s. 17.

10.7 Konsekvenser för jämställdheten mellan män och kvinnor

Förslagen bedöms inte få några konsekvenser för jämställdheten mellan män och kvinnor.

10.8 Konsekvenser för att nå de integrationspolitiska målen

Vi bedömer att förslagen inte får några negativa konsekvenser för att nå de integrationspolitiska målen.

10.9 Förslagens överensstämmelse med EU-rätten

Vi bedömer att förslagen är förenliga med EU-rätten. Våra förslag påverkar inte kravet på erkännande av utländska e-legitimationer som föreskrivs i artikel 6 i eIDAS-förordningen. Förslagen står heller in i strid med förordningens bestämmelser. Vidare bedömer vi att förslagen är förenliga med bestämmelserna om fri rörlighet i Fördraget om Europeiska unionens funktionssätt. Förslaget om att tillitsramverket ska ses över med beaktande av bl.a. de svårigheter som finns för individer utan personnummer att få tillgång till e-tjänstelegitimationer bedömer vi därtill kan få en positiv inverkan på möjligheten att utöva den fria rörligheten.

Vi bedömer att våra förslag inte behöver anmälas till kommissionen enligt de procedurer som fastställs i direktiv (EU) 2015/1535 eller i direktiv 2006/123/EG (tjänstedirektivet). Framtida myndighetsföreskrifter kan emellertid omfattas av krav på anmälan i enlighet med dessa direktiv, något som DIGG måste beakta i sitt fortsatta föreskriftsarbete.

10.10 Närmare om konsekvenserna för enskilda förslag

10.10.1 Krav om att statliga myndigheter ska tillhandahålla e-tjänstelegitimationer till sina anställda

I dagsläget finns det enligt Statistiska centralbyråns myndighetsregister sammanlagt 346 statliga myndigheter i Sverige och 205 utlandsmyndigheter fördelade enligt tabellen nedan.[5] Av dessa ligger fem under riksdagen och omfattas således inte av förslaget.

Tabell 10.1 Svenska statliga myndigheter och utlandsmyndigheter

Myndighetsgrupp	Antal
Statliga förvaltningsmyndigheter	249
Myndigheter under riksdagen	5
Statliga affärsverk	3
AP-fonder	6
Sveriges domstolar samt Domstolsverket	83
Svenska utlandsmyndigheter	205

Det är förenat med kostnader för en myndighet att förse anställda och uppdragstagare med e-tjänstelegitimationer. Av kartläggningen framgår att många statliga myndigheter redan i dagsläget tillhandahåller e-tjänstelegitimationer till sina anställda och att vissa har långt framskridna planer om att göra det. Uppgifter saknas emellertid om exakt hur många av de berörda myndigheterna som redan tillhandahåller e-tjänstelegitimationer. Hur kostnadsbilden ser ut beror dock på ett antal faktorer, t.ex. hur många anställda och uppdragstagare myndigheten har samt vilken eller vilka bärare som ska användas. Vidare kan det tillkomma kostnader i form av anpassning av befintliga system och utbildning av de anställda. Exakt vilka kostnader det rör sig om är således förenat med viss osäkerhet och beror dessutom på vilken utfärdare eller vilka leverantörer myndigheten väljer att använda sig av och det pris som myndigheten får betala.

Utifrån våra kontakter med utfärdare av e-tjänstelegitimationer beräknas kostnaden ligga inom spannet 10 kronor till 42 kronor per månad per e-tjänstelegitimation. Det förekommer också att det för

[5] www.myndighetsregistret.scb.se/Myndighet (hämtad 2021-06-15).

större kunder sätts ett tak för hur hög den månatliga kostnaden kan bli oavsett antal användare.

Engångskostnader som startkostnader och anpassningskostnader för ny kund kan också förekomma, även kostnader för fysiska bärare i form av t.ex. smartkort tillkommer om kunden väljer denna lösning.

Berörda myndigheter har redan i dag kostnader för att hantera identiteter och autentiseringsmetoder för sina anställda och uppdragstagare. Kostnaderna för att gå över till användning av e-tjänstelegitimationer för myndigheter som inte i dag har det behöver inte nödvändigtvis vara högre än myndighetens nuvarande kostnader för hantering av identiteter, autentiseringsmetoder eller eventuell administrativ hantering av behörigheter i externa tjänster som kräver autentisering med privat e-legitimation. För vissa myndigheter kan det dock vara mer kostsamt med e-tjänstelegitimationer än en befintlig lösning. Vi bedömer emellertid att finansiering av förslaget kan ske inom ramen för varje myndighets förvaltningsanslag och att det således inte behöver finansieras i särskild ordning.

10.10.2 Förslag om lag om erkännande av medel för elektronisk identifiering

Konsekvenser för statliga myndigheter

Vad gäller kostnaden för anslutning för de statliga myndigheter som tillhandhåller e-tjänster som omfattas av kravet på erkännande av de e-tjänstelegitimationer som är anslutna till systemet kan paralleller dras till det nyligen lämnade förslaget om krav på att statliga myndigheter ska använda tjänster för elektronisk identifiering som tillhandahålls inom auktorisationssystem. I promemorian där förslaget lämnas görs följande bedömning.

> Kostnaderna för teknisk anslutning hänförliga till användningen av de tjänster som tillhandahålls inom nuvarande valfrihetssystem varierar mellan statliga myndigheter och beror på deras befintliga lösning. Det bedöms att drygt hälften av de offentliga aktörerna endast har stöd för en e-legitimationstyp i dag. Dessa myndigheter behöver möjliggöra inloggning med fler e-legitimationer, under förutsättning att de nya auktorisationssystemen har ungefär samma leverantörssammansättning och krav som nuvarande valfrihetssystem. Vidare bedöms att de myndigheter som tar emot en e-legitimation i dag får en startkostnad på ca 25 000 kronor, de som tar emot två e-legitimationer får en startkostnad på ca 10 000 kronor och de som redan i dag erbjuder stöd för tre eller

> fler e-legitimationstyper inte kommer att öka sina startkostnader. Den fasta månadskostnaden antas öka med fem procent per verksamhet till följd av att tjänsteleverantörer administrerar fler typer av e-legitimationer samt, teoretiskt sett, fler transaktioner. En stor del av de myndigheter som behöver göra tekniska anpassningar av sina system för att kunna ta emot nya leverantörer av tjänster för elektronisk identifiering kommer ändå att behöva göra motsvarande anpassningar för att kunna ta emot utländska e-legitimationer, vilket är en skyldighet enligt EU:s förordning om elektronisk identifiering. Sammantaget bedöms därför kostnaderna för teknisk anpassning bli marginella, under förutsättning att den tekniska kravställningen för nya e-legitimationsutfärdare hålls snarlik den kravställning som görs för anslutning till förbindelsepunkterna för gränsöverskridande elektronisk identifiering.[6]

Vi bedömer att de ovan redovisade kostnaderna för anslutning kan användas som utgångspunkt även för det nu aktuella förslaget. Den exakta kostnaden för respektive myndighet är dock svår att beräkna eftersom de har olika förutsättningar. Vidare kan övergången från att använda personlig e-legitimation med behörighetslösning till att använda e-tjänstelegitimationer medföra övergångskostnader samtidigt som kostnadsposter för den tidigare lösningen försvinner. Även dessa kostnader skiljer sig åt för respektive myndighet utifrån de olika förutsättningar som råder.

Eventuella anpassningskostnader bedöms i huvudsak bli en följd av att systemen anpassas till att använda andra personidentifieringsuppgifter än personnummer. Statliga myndigheter omfattas redan av kravet i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning om att personnummer och samordningsnummer endast får behandlas utan samtycke när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Inom det föreslagna systemet kommer personnummer som regel inte användas för att säker identifiering ska kunna ske. Om den berörda myndigheten inte har annat stöd för att behandla personnummer för detta syfte finns således redan genom denna lagstiftning en skyldighet att anpassa systemen för att inte behandla personnummer.

EU:s förordning om en gemensam digital ingång ställer därtill krav på att medlemsstaterna säkerställer att e-tjänster finns för vissa förfaranden, t.ex. att lämna in en inkomstskattedeklaration, och att

[6] Promemoria, *Auktorisationssystem för elektronisk identifiering och för digital post*, s. 51 f.

dessa tjänster kan nås digitalt av invånare i andra medlemsstater.[7] Detta innebär att myndigheter vars tjänster omfattas av bestämmelserna från december 2023 behöver hantera europeiska personidentifieringsuppgifter. Försäkringskassan har bedömt att denna övergång från dagens huvudsakligen personnummerbaserade hantering kommer ha stor påverkan på såväl e-tjänster som interna system. Myndigheten har beräknat att, beroende på hur frågan hanteras nationellt och hos myndigheten, kan innebära kostnader i storleksordningen en eller flera miljarder kronor.[8] Det kan även noteras att det av kommissionen nyligen lämnade förslaget till ändringar i eIDAS-förordningen kommer, om det genomförs, innebära en liknande omställning för en bredare krets aktörer inom offentlig sektor (se avsnitt 9.6).

Med beaktande av ovan redovisade krav i befintlig lagstiftning som påverkar utformningen av berörda myndigheters e-tjänster och interna system samt de beräknade kostnaderna för anslutning bedöms förslaget inte få några konsekvenser för dessa myndigheter som måste finansieras i särskild ordning.

Konsekvenser för DIGG och MSB

Vi föreslår att de närmare detaljerna om hur systemet, vad gäller både granskning och teknisk uppbyggnad, ska vara utformat delegeras till DIGG att besluta om. Det gör det svårt att bedöma de kostnader som uppstår. Detta då det i förlängningen kommer bli en direkt följd av hur DIGG väljer att utforma systemet. Bedömningen får därmed utgå från kostnader för jämförbara processer och tekniska lösningar.

Granskningen av e-tjänstelegitimationer inför anslutning till systemet kommer sannolikt att ske på liknande sätt som den granskning som i dag sker inom ramen för kvalitetsmärket Svensk e-legitimation. Vi bedömer därför att den kostnad för granskning som sker inom ramen för det föreslagna systemet kan förväntas spegla kostnaderna som DIGG har för denna hantering i dag. Flera av de e-tjänstelegitimationer som kan bli aktuella för användning i systemet är dock redan granskade och godkända av DIGG och beroende på vilka krav som av DIGG uppställs för anslutning är det möjligt att någon ny granskning av dessa inte är nödvändig. Viss uppföljande granskning

[7] Regeringen har gett DIGG i uppdrag att ta fram en genomförandeplan för införandet av bevisutbyte enligt engångsprincipen (I2021/01595), som är en central princip i förordningen.
[8] Försäkringskassan, *Budgetunderlag 2022–2024* (Dnr FK 2020/006213), 17 februari 2021, s. 17.

och kontroll av redan godkända e-legitimationer kan emellertid behöva ske. Kostnaderna för en sådan hantering får dock bedömas bli betydligt lägre än för granskning av en helt ny e-tjänstelegitimation.

Vi har därför inhämtat kostnadsuppskattningar från DIGG för granskningen och för att kunna använda det nuvarande systemet för e-legitimationer i enlighet med myndighetens förslag om eID för medarbetare.[9] Vi bedömer att dessa kostnader i stort speglar kostnaderna för att hantera systemet i enlighet med utredningens förslag. Baserat på dessa underlag gör utredningen bedömningen att förslagen ger granskningskostnader om 150 000 till 250 000 kronor per tillkommande e-tjänstelegitimationsutfärdare. Utöver dessa medför förslagen en förnyad granskning eller mindre omfattande kontroll periodiskt som förväntas kosta 75 000 till 100 000 kronor per e-tjänstelegitimationsutfärdare och gång. Vidare medför anpassning av e-legitimationssystemet engångskostnader om ca en miljon kronor.[10] Utöver detta har DIGG löpande kostnader om ca en miljon kronor per år.[11]

E-tjänstelegitimationerna bedöms använda samma tekniska driftmiljö som för det nuvarande e-legitimationssystemet men kan medföra ökade kostnader bl.a. eftersom volymen ökar. Vi bedömer de tillkommande driftskostnaderna till 1–2 miljoner kronor per år. Viss kostnadstäckning kan ske genom förslaget om att DIGG ska kunna ta ut en avgift för den granskning som sker. Den ökade kostnaden för DIGG kommer, utöver eventuell avgiftsfinansiering, behöva finansieras genom ökade anslag via reformutrymmet.

Enligt förslaget ska DIGG samråda med MSB vid framtagande av föreskrifter. Omfattningen av dessa samråd bedöms ha en försumbar påverkan på MSB:s verksamhet. Sådana samråd får även anses falla inom ramen för myndighetens uppgifter enligt förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

[9] DIGG, *eID för medarbetare – Förstudierapport inom byggblock Identitet i regeringsuppdraget Att etablera en förvaltningsgemensam infrastruktur för informationsutbyte* (dnr 2019-582), 14 december 2020.
[10] I kostnaderna ingår bl.a. avtal, föreskrifter, kommunikation, uppdragsledning och expertkunskap.
[11] I kostnaderna ingår bl.a. uppföljning, avtalshantering, förvaltning, tekniska tester och support.

Konsekvenser för domstolarna

Beslut om att inte godkänna ett medel för elektronisk identifiering får överklagas till allmän förvaltningsdomstol. Antalet e-legitimationsutfärdare är som framgår av avsnitt 6.4 i dagsläget relativt begränsat. Rätten att överklaga dessa beslut bör mot denna bakgrund inte generera någon större mängd mål för domstolarna.

DIGG föreslås vidare mot bakgrund av säkerhetsincidenter kunna besluta att e-tjänstelegitimationer tillfälligt eller tills vidare inte ska vara godkända för användning i systemet alternativt inte längre får ingå i systemet. Rätten att överklaga dessa beslut bedöms inte heller generera någon större mängd mål för domstolarna

Sammantaget bedöms förslaget inte få några konsekvenser för de allmänna förvaltningsdomstolarna som måste finansieras i särskild ordning.

10.10.3 Regeringsuppdrag om översyn av tillitsramverket

Konsekvenser för DIGG

Utredningen föreslår att regeringen ger DIGG i uppdrag att göra en översyn av tillitsramverket. Detta uppdrag bedöms falla inom ramen för DIGG:s uppgifter enligt 3 § 1 förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning och ska därmed finansieras inom myndighetens befintliga ram.

11 Ikraftträdande

11.1 Ikraftträdande av lagen om erkännande av medel för elektronisk identifiering samt förordningen om erkännande av medel för elektronisk identifiering

Utredningens förslag: Lagen och förordningen ska träda i kraft den 1 januari 2024.

Skälen för utredningens förslag

Vi bedömer att det är angeläget att de ändringar vi föreslår träder i kraft så snart som möjligt till stöd för organisationsöverskridande användning av e-tjänstelegitimationer.

Med hänsyn till den tid som kan beräknas gå åt för remissförfarande, fortsatt beredning inom Regeringskansliet och riksdagsbehandling samt anpassning av it-system vid berörda myndigheter bör de lag- och förordningsbestämmelser utredningen föreslår tidigast kunna träda i kraft den 1 januari 2024. Förslagen är inte av den arten att de kräver några särskilda övergångsregler.

11.2 Ikraftträdande av förordningsändringar

Utredningens förslag: Förordningsändringarna ska träda i kraft den 1 januari 2024.

Skälen för utredningens förslag

Vi bedömer det angeläget att de föreslagna ändringarna i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte träder i kraft så snart som möjligt.

Med hänsyn till den tid som kan beräknas gå åt för remissförfarande och fortsatt beredning inom Regeringskansliet samt den tid för omställning som krävs för de myndigheter som inte i dagsläget efterlever kraven, bör de ändringar utredningen föreslår kunna träda i kraft den 1 januari 2024. Förslagen är inte av den arten att de kräver några särskilda övergångsregler.

Vad avser föreslagna ändringar i förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning bör de aktuella förordningsändringarna träda i kraft samtidigt som den föreslagna lagen. Förslagen är inte av den arten att de kräver några särskilda övergångsregler.

12 Författningskommentar

12.1 Förslaget till lag om erkännande av medel för elektronisk identifiering

Inledande bestämmelser

1 §

Paragrafen behandlas i avsnitt 9.4.1. Av paragrafen framgår vad lagen innehåller.

2 §

Paragrafen behandlas i avsnitt 9.4.1. I artikel 6.1 i eIDAS-förordningen föreskrivs att medlemsstaterna om vissa förutsättningar är uppfyllda ska erkänna medel för elektronisk identifiering som har utfärdats i andra medlemsstater (s.k. ömsesidigt erkännande, se mer om detta i avsnitt 4.2.4). Av paragrafen framgår att lagen inte påverkar sådant erkännande som följer av eIDAS-förordningen.

Ordförklaringar

3 §

Paragrafen behandlas i avsnitt 9.4.4 och redogör för de rättssubjekt som anses vara offentliga aktörer. Motsvarande bestämmelser finns i 4 och 5 §§ lagen (2018:1937) om tillgänglighet till digital offentlig service. Paragrafen är avsedd att ha samma innebörd som nämnda bestämmelser i den lagen, se prop. 2017/18:299 s. 30 ff. och 86 ff.

4 §

Paragrafen behandlas i avsnitt 9.4.2. Ord och uttryck i lagen som även förekommer i eIDAS-förordningen ska ha samma betydelse i lagen som i förordningen i dess ursprungliga lydelse.

Erkännande av medel för elektronisk identifiering

5 §

Paragrafen behandlas i avsnitt 9.4.3 och 9.4.5. Paragrafen innebär att statliga myndigheter som tillhandahåller nättjänster som kräver autentisering med medel för elektronisk identifiering ska, om förutsättningarna i första stycket är uppfyllda, erkänna sådana medel som offentliga aktörer tillhandahåller till sina anställda eller uppdragstagare. Erkännande innebär att medel för elektronisk identifiering ska accepteras för tillgång till den aktuella nättjänsten. Med hjälp av medlet ska användaren kunna använda tjänsten, under förutsättning att eventuella behörighetskrav är uppfyllda. För det fall medel för elektronisk identifiering krävs för moment utöver autentisering, exempelvis som ett led i att skapa en elektronisk underskrift inom ramen för tjänsten, avser kravet på erkännande även dessa moment.

Enligt *första stycket första punkten* krävs för att kravet på erkännande ska vara tillämpligt att det medel för elektronisk identifiering som ska erkännas är godkänt för användning i det system för erkännande av medel för elektronisk identifiering som framgår av 6 §.

Enligt *första stycket andra punkten* krävs för erkännande vidare att tillitsnivån för medlet för elektronisk identifiering motsvarar, eller är högre än, den tillitsnivå som krävs för att få tillgång till den aktuella nättjänsten. Det är, med beaktande av eventuella författningskrav, den aktör som tillhandahåller en nättjänst som avgör vilken tillitsnivå som ska krävas.

Regeringen får med stöd av *andra stycket* meddela undantag från kravet på erkännande. Undantag kan exempelvis avse vissa nättjänster eller myndigheter. Undantag kan även meddelas för det fall erkännande av medel för elektronisk identifiering som ingår i systemet är förknippat med allvarliga säkerhetsrisker.

System för erkännande av medel för elektronisk identifiering

6 §

Paragrafen behandlas i avsnitt 9.4.5. Enligt *första stycket* ska den myndighet som regeringen bestämmer tillhandahålla ett system för erkännande av medel för elektronisk identifiering (systemet). Med system avses i denna lag en samling av bl.a. krav, policys, teknisk infrastruktur samt en process för godkännande av medel för elektronisk identifiering. Systemet är avsett att i huvudsak ha samma uppbyggnad och funktion som en identitetsfederation (se avsnitt 6.6).

Med stöd av *andra stycket* får regeringen eller den myndighet regeringen bestämmer meddela närmare föreskrifter om systemet och användningen av det. Sådana föreskrifter kan gälla krav på medel för elektronisk identifiering samt granskning och godkännande av sådana medel. Ytterligare exempel är krav gällande de nättjänster som ansluts till systemet, tillitramverk för system, hantering av säkerhetsincidenter samt krav som avser anslutning av för systemet ej godkända medel för elektronisk identifiering.

7 §

Paragrafen behandlas i avsnitt 9.4.11. Den myndighet som tillhandahåller systemet får behandla personuppgifter om det är nödvändigt för erkännande av medel för elektronisk identifiering i anslutna nättjänster. Sådan behandling kan avse personuppgifter kopplade till medel för elektronisk identifiering och dess innehavare, och där behandlingen sker i samband med autentiseringsprocessen. Det kan också röra personuppgifter som behandlas inom ramen för rent administrativ hantering med koppling till systemet.

Kommittédirektiv 2020:27

Ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen

Beslut vid regeringssammanträde den 12 mars 2020

Sammanfattning

En särskild utredare ska utreda förutsättningarna för ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen. Syftet med utredningen är att höja säkerheten och stärka tilliten när betrodda tjänster används.

I utredarens uppdrag ingår att

- kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster,
- lämna förslag på sådana åtgärder, särskilt när det gäller att
  - tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen,
  - kunna validera och bevara elektroniska underskrifter, och
  - kunna använda e-legitimation i tjänsten, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 30 december 2020.

Betrodda tjänster

Betrodda tjänster är sådana tjänster som används för att skapa, kontrollera, validera och bevara elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar och certifikat samt för att autentisera webbplatser och säkra elektroniska leveranser. Sådana tjänster utgör samhällskritisk infrastruktur som är en förutsättning för fortsatt utveckling av digital service till privatpersoner och företag. De är också centrala för att förverkliga EU:s strategi om en digital inre marknad med fri rörlighet av varor och tjänster. För att kunna verka i en digital miljö är en säker identifiering av helt avgörande betydelse vid t.ex. informationsutbyte eller underskrift av handlingar. Säkra betrodda tjänster är också en förutsättning för en fungerande verksamhet hos många offentliga arbetsgivare.

Betrodda tjänster regleras av 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, den s.k. eIDAS-förordningen. Syftet med förordningen är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan privatpersoner, företag och den offentliga förvaltningen. Avsikten är att därigenom öka effektiviteten hos offentliga och privata digitala tjänster, affärsverksamhet och e-handel i unionen.

Förordningen reglerar vad betrodda tjänster är och vilka tekniska och juridiska förutsättningar som gäller för dem. Betrodda tjänster kan under vissa förutsättningar anses vara kvalificerade eller icke-kvalificerade. Kvalificerade betrodda tjänster är giltiga inom hela EES-området. Post- och telestyrelsen (PTS) publicerar teknisk och juridisk information för kvalificerade betrodda tjänster på den svenska förteckningen över kvalificerade tillhandahållare av betrodda tjänster (trusted list). eIDAS-förordningen är för närvarande föremål för översyn. Resultatet av översynen ska publiceras av Europeiska kommissionen senast den 1 juli 2020.

Kompletterande bestämmelser till förordningen finns i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Utredningen om effektiv styrning av nationella digitala tjänster lämnar i betänkandet reboot – omstart för den digitala förvaltningen (SOU 2017:114) förslag på flera åtgärder för ökad styrning av området för elektronisk identifiering och betrodda tjänster.

Regeringen beslutade den 31 oktober 2019 att tillsätta en utredning som ska föreslå de anpassningar och kompletterande författningsbestämmelser som Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) ger anledning till. Utredaren ska också överväga om det finns anledning att införa ytterligare krav för att skydda verksamhet som är av betydelse för Sveriges säkerhet, som krav på certifiering och godkännande av vissa produkter, tjänster och processer (dir. 2019:73). Uppdraget ska redovisas i den del som avser anpassningar med anledning av EU-förordningen senast den 1 juni 2020. I den del som avser regler till skydd för Sveriges säkerhet ska uppdraget redovisas senast den 1 mars 2021.

Behovet av åtgärder för ökad och standardiserad användning av betrodda tjänster

Förordningen anger vissa krav som betrodda tjänster måste uppfylla. Principen är att en tjänst som är godkänd inom en medlemsstat automatiskt ska vara godkänd i alla medlemsstater. Däremot har genomförandeakter för gemensamma standarder inte antagits. Det finns inte heller regler och riktlinjer för gemensamma standarder på nationell nivå. En konsekvens av detta är att det i praktiken är mycket svårt att utan avancerade it-stöd kunna avgöra om ett elektroniskt undertecknat dokument går att lita på.

Ökad och standardiserad användning av elektroniska underskrifter som går att lita på och som är enkla att använda är grundläggande i ett alltmer digitaliserat samhälle. I svenska digitala tjänster används främst underskrifter som i förordningen benämns avancerade elektroniska underskrifter. I kommissionens genomförandebeslut (EU) 2015/1506 av den 8 september 2015 om fastställande av specifikationer rörande format för avancerade elektroniska underskrifter och avancerade elektroniska stämplar i enlighet med artiklarna 27.5 och 37.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014

om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden beskrivs vilka format och metoder som måste erkännas av medlemsstaterna. Det som i eIDAS-förordningen benämns kvalificerade elektroniska underskrifter används endast i begränsad omfattning i Sverige och marknaden för betrodda tjänster har inte utvecklats på det sätt som förutsågs vid förordningens tillkomst. Svensk lagstiftning ställer inte heller krav på användning av kvalificerade elektroniska underskrifter, utan förekommande krav tar sikte på avancerade elektroniska underskrifter. 2017 års ID-kortsutredning föreslår att det ska införas ett nytt statligt identitetskort med en e-legitimation som ska kunna användas för att skapa just avancerade elektroniska underskrifter. Frågan om den statliga e-legitimationen ska kunna användas även för att skapa kvalificerade elektroniska underskrifter lämnas till stor del öppen, se betänkandet Ett säkert statligt ID-kort – med e-legitimation (SOU 2019:14).

Från flera håll i den offentliga förvaltningen har det kommit rapporter om problem kopplade till elektroniska underskrifter. Både juridiska oklarheter och tekniska svårigheter återkommer i beskrivningarna av de utmaningar som finns. Det gäller särskilt validering och bevarande av dokument som skrivits under elektroniskt. Svårigheterna består bl.a. i att kunna godta olika format och underskrifter. Flera myndigheter använder i dag digitala tjänster där hela förfarandet hanteras i ett flöde. Det innebär att tjänsten hämtar information om användaren och dennes behörighet baserat på information från den elektroniska identifieringen som gjordes i samband med inloggningen. Behörigheten kontrolleras sedan direkt när t.ex. en handling skrivs under elektroniskt. Flödet blir då låst till ett enda sätt att hantera elektronisk identifiering och underskrift. Detta gör det svårt att utveckla tjänster som godtar andra elektroniska underskrifter än de som är kopplade till den elektroniska identifieringen. Det gäller särskilt vid gränsöverskridande användning av digitala tjänster. Ett sätt att hantera detta är att använda en fristående underskriftstjänst som utfärdar ett engångscertifikat för underskrift utifrån den använda e-legitimationen. Ett sådant förfarande kan också användas för en utländsk elektronisk underskrift. I digitala tjänster som tar emot elektroniskt underskrivna blanketter blir flödet enklare, eftersom underskriften då är helt separerad från den digitala tjänstens medel för elektronisk identifiering. Här uppstår i stället krav på mottagaren att kunna validera den elektroniska underskriften.

En digital tjänst kan känna igen elektroniska underskrifter som baseras på kvalificerade certifikat. Sådana underskrifter kontrolleras mot uppgifterna i den svenska förteckningen över kvalificerade tillhandahållare av betrodda tjänster. När det gäller avancerade elektroniska underskrifter finns det inte samma detaljreglering som för kvalificerade elektroniska underskrifter. Avancerade elektroniska underskrifter omfattas exempelvis inte av någon anmälningsplikt och det finns inte heller någon motsvarande förteckning. Det innebär bland annat att det saknas möjlighet att validera avancerade elektroniska underskrifter. Det gör det svårt för mottagaren att avgöra om och hur en avancerad underskrift från en okänd tillhandahållare lever upp till kraven på en avancerad elektronisk underskrift. Mot bakgrund av detta föreslås i betänkandet reboot – omstart för den digitala förvaltningen att regeringen ska tillsätta en utredning som ser över behovet av svensk reglering av betrodda tjänster som inte är kvalificerade.

Ett hinder som ofta lyfts fram när det gäller digitaliseringen av offentlig sektor är avsaknaden av standardiserade e-legitimationer för användning vid tjänsteutövning. De elektroniska intyg som i dag skickas mellan parterna vid elektronisk identifiering innehåller uppgifter om användarens identitet, bl.a. personnumret. Däremot saknas vanligen information om vilken organisation användaren företräder och vilken behörighet denne har. Utredningen om effektiv styrning av nationella digitala tjänster beskriver att det för att effektivisera informationsutbytet mellan myndigheter har utvecklats en praxis som innebär att myndigheter litar på varandra, s.k. organisationstillit. Det räcker då att kontrollera att den andra parten företräder den myndighet som uppges. Utredningen konstaterar dock att frågan om behörigheter är komplex och att behörigheter kan bedömas utifrån olika perspektiv. Myndigheten för digital förvaltning lyfter fram behovet av att utveckla tjänster för hantering av behörigheter som en prioriterad åtgärd för att åstadkomma effektivt och säkert informationsutbyte inom den offentliga förvaltningen. Sveriges Kommuner och Regioner påpekar behovet av att staten tar ett övergripande ansvar för en gemensam sektorsövergripande infrastruktur för e-legitimering i tjänsten och att uppdraget för Myndigheten för digital förvaltning måste förtydligas i denna del (SKR:s styrelses ställningstagande Digital identitetshantering, 2019).

För att Sverige ska leva upp till sina förpliktelser enligt EU-rätten krävs även enligt bland annat Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden med tillhörande beslut samt Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 att Sverige i vissa fall gör det möjligt för personer från andra EU-länder att identifiera sig för att ansöka om tillstånd m.m.

Flera medlemsstater arbetar med att vidareutveckla betrodda tjänster för att hantera behörigheter. Det saknas bland annat standarder för utbyte av information om behörigheter vid gränsöverskridande informationsutbyte. Sådana standarder ska användas även nationellt och för att möjliggöra en sådan utveckling även i Sverige finns det behov av att utreda och lämna förslag på åtgärder som främjar en ökad användning av eIDAS-förordningens betrodda tjänster för att möta förvaltningens behov. Det behövs ett enhetligt sätt att hantera e-legitimationer i tjänsten, och förordningen bedöms utgöra en långsiktig och hållbar bas för den fortsatta utvecklingen på området. Standarder är en viktig grund för att skapa långsiktigt hållbara och återanvändbara lösningar.

Mot denna bakgrund ska utredaren utreda förutsättningarna för ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen. Syftet med utredningen är att höja säkerheten och stärka tilliten när betrodda tjänster används.

I uppdraget ingår att

- kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster,
- lämna förslag på sådana åtgärder, särskilt när det gäller att
  - tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen,
  - kunna validera och bevara elektroniska underskrifter, och
  - kunna använda e-legitimation i tjänsten, och
- lämna nödvändiga författningsförslag.

Internationell utblick

Utredaren ska undersöka och översiktligt redovisa hur de frågor som uppdraget omfattar hanteras i andra länder som är jämförbara med Sverige, exempelvis de nordiska länderna.

Konsekvensbeskrivningar

Utredaren ska analysera de samhällsekonomiska effekterna i utredningsarbetets alla delar, från problembeskrivning och syfte till analys av alternativ och motiv till förslag samt bedöma förslagens konsekvenser i enlighet med kommittéförordningen (1998:1474) och förordningen om konsekvensutredning vid regelgivning (2007:1244). Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Om förslagen innebär en inskränkning av den kommunala självstyrelsen, ska en proportionalitetsprövning göras enligt 14 kap. 3 § regeringsformen. De särskilda avvägningar som underbygger förslagen ska redovisas särskilt. Utredaren ska också särskilt ange konsekvenser för företag i form av kostnader och ökade administrativa bördor. Utredaren ska också analysera risker med identitetsrelaterad brottslighet och redovisa konsekvenser för brottsbekämpning och brottsförebyggande arbete.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet, utredningsväsendet, t.ex. utredningen Cybersäkerhet – genomförande av cybersäkerhetsakten och vissa åtgärder till skydd för säkerhetskänslig verksamhet (Fö 2019:01), och EU. Utredaren ska särskilt beakta det arbete som bedrivs hos Myndigheten för digital förvaltning. Vidare ska utredaren inhämta övriga behövliga upplysningar från berörda myndigheter och organisationer.

Uppdraget ska redovisas senast den 30 december 2020.

(Infrastrukturdepartementet)

Kommittédirektiv 2020:135

Tilläggsdirektiv till Utredningen om betrodda tjänster (I 2020:01)

Beslut vid regeringssammanträde den 17 december 2020

Förlängd tid för uppdraget

Regeringen beslutade den 12 mars 2020 kommittédirektiv till en särskild utredare att utreda förutsättningarna för en ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen i syfte att höja säkerheten och stärka tilliten när betrodda tjänster används (dir. 2020:27). I uppdraget ingår en kartläggning och analys av den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster och att lämna förslag på sådana åtgärder. Utredaren ska även lämna nödvändiga författningsförslag. I utredarens uppdrag betonas särskilt följande delområden: tydliggörande av när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen, validering och bevaring av elektroniska underskrifter samt användning av e-legitimation i tjänsten. Utredningen har tagit namnet Utredningen om betrodda tjänster. Uppdraget skulle enligt direktiven slutredovisas senast den 30 december 2020.

Utredningstiden förlängs. Uppdraget ska, med undantag för den delredovisning som ska lämnas den 15 februari 2021, i stället slutredovisas senast den 30 juni 2021.

Redovisning av uppdraget

Den del av uppdraget som avser åtgärder för ökad och standardiserad användning av betrodda tjänster enligt punktuppställningen nedan ska redovisas senast den 15 februari 2021.

I delredovisningen ska följande ingå:

- kartläggning och analys av den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster,
- förslag på sådana åtgärder och nödvändiga författningsförslag, särskilt när det gäller att
  - tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen, och
  - validera och bevara elektroniska underskrifter.

Resterande delar av uppdraget som framgår av dir. 2020:27 ska slutredovisas den 30 juni 2021.

(Infrastrukturdepartementet)

Statens offentliga utredningar 2021

Kronologisk förteckning

1. Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. I.
2. Krav på kunskaper i svenska och samhällskunskap för svenskt medborgarskap. Ju.
3. Skolbibliotek för bildning och utbildning. U.
4. Informationsöverföring inom vård och omsorg. S.
5. Ett förbättrat system för arbetskraftsinvandring. Ju.
6. God och nära vård. Rätt stöd till psykisk hälsa. S.
7. Förstärkt skydd för väljarna vid röstmottagningen. Ju.
8. När behovet får styra – ett tandvårdssystem för en mer jämlik tandhälsa. Vol. 1 & Vol. 2, bilagor + Sammanfattning (häfte). S.
9. Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen. I.
10. Radiologiska skador – skadestånd, säkerheter, skadereglering. M.
11. Bättre möjligheter för elever att nå kunskapskraven – aktivt stöd- och elevhälsoarbete samt stärkt utbildning för elever med intellektuell funktionsnedsättning. U.
12. Andra chans för krisande företag – En ny lag om företagsrekonstruktion. Ju.
13. En teknikneutral grundlagsbestämmelse för regeringsbeslut. Ju.
14. Boende på (o)lika villkor – merkostnader i bostad med särskild service för vuxna enligt LSS. S.
15. Föreningsfrihet och terroristorganisationer. Ju.
16. En väl fungerande ordning för val och beslutsfattande i kommuner och regioner. Fi.
17. Ett moderniserat konsumentskydd. Fi.
18. Bolags rörlighet över gränserna. Volym 1 & 2. Ju.
19. En stärkt försörjningsberedskap för hälso- och sjukvården. Del 1 och 2. S.
20. Ecris-TCN – ett mer effektivt utbyte av brottmålsdomar mot tredjelandsmedborgare. Ju.
21. En klimatanpassad miljöbalk för samtiden och framtiden. M.
22. Hårdare regler för nya nikotinprodukter. S.
23. Stärkt planering för en hållbar utveckling. Fi.
24. Äga avfall – en del av den cirkulära ekonomin. M.
25. Struktur för ökad motståndskraft. Ju.
26. Använd det som fungerar. M.
27. Ett förbud mot rasistiska organisationer. Ju.
28. Immunitet för utställningsföremål. Ku.
29. Ökade möjligheter att förhindra illegal handel via post. I.
30. Kampen om tiden – mer tid till lärande. U.
31. Kontroller på väg. I.
32. Papper, poddar och ... Pliktmateriallagstiftning för ett tryggat källmaterial. U.
33. En tioårig grundskola. Införandet av en ny årskurs 1 i grundskolan, grundsärskolan, specialskolan och sameskolan. U.
34. Börja med barnen! En sammanhållen god och nära vård för barn och unga. S.
35. En stärkt rättsprocess och en ökad lagföring. Ju.

36. Gode män och förvaltare – en översyn. Ju.
37. Stärkt rätt till personlig assistans. Ökad rättssäkerhet för barn, fler grundläggande behov och tryggare sjukvårdande insatser. S.
38. En ny lag om ordningsvakter m.m. Ju.
39. Ombuds tillgång till vård- och omsorgsuppgifter och förenklad behörighetskontroll inom vården. S.
40. Mervärdesskatt vid inhyrd personal för vård och social omsorg. Fi.
41. VAB för vårdåtgärder i skolan. S.
42. Stärkta åtgärder mot penningtvätt och finansiering av terrorism. Fi.
43. Ett förstärkt skydd mot sexuella kränkningar. Ju.
44. Tillgänglighetsdirektivet. S.
45. En EU-anpassad djurläkemedelslagstiftning. Del 1 och 2. N.
46. Snabbare lagföring – ett snabbförfarande i brottmål. Ju.
47. Ett nytt regelverk för bygglov. Del 1 och 2. Fi.
48. I en värld som ställer om. Sverige utan fossila drivmedel 2040. M.
49. Kommuner mot brott. Ju.
50. Fri hyressättning vid nyproduktion. Ju.
51. Skydd av arter – vårt gemensamma ansvar. Vol. 1 och 2. M.
52. Vilja välja vård och omsorg. En hållbar kompetensförsörjning inom vård och omsorg om äldre. S.
53. En rättssäker vindkraftsprövning. M.
54. Ändrade regler i medborgarskapslagen. Ju.
55. Mikroföretagarkonto – schabloniserad inkomstbeskattning för de minsta företagen. Fi.
56. Nya regler om utländska föräldraskap och adoption i vissa fall. Ju.
57. Om folkbokföring, samordningsnummer och identitetsnummer. Fi.
58. Läge och kvalitet i hyressättningen. Ju.
59. Vägen till tillgänglighet – långsiktig, strategisk och i samverkan. S.
60. Förenklingar för mikroföretag och modernisering av bokföringslagen. N.
61. Utvisning på grund av brott – ett skärpt regelverk. Ju.
62. Användning av e-legitimation i tjänsten i den offentliga förvaltningen. I.

Statens offentliga utredningar 2021

Systematisk förteckning

En klimatanpassad miljöbalk för samtiden och framtiden. [21]

Äga avfall
– en del av den cirkulära ekonomin. [24]

Använd det som fungerar. [26]

I en värld som ställer om.
Sverige utan fossila drivmedel 2040. [48]

Skydd av arter – vårt gemensamma ansvar. Vol. 1 och 2. [51]

En rättssäker vindkraftsprövning. [53]

Näringsdepartementet

En EU-anpassad djurläkemedelslagstiftning. Del 1 och 2. [45]

Förenklingar för mikroföretag och modernisering av bokföringslagen. [60]

Socialdepartementet

Informationsöverföring inom vård och omsorg. [4]

God och nära vård. Rätt stöd till psykisk hälsa. [6]

När behovet får styra
– ett tandvårdssystem för en mer jämlik tandhälsa. Vol. 1 & Vol. 2, bilagor + Sammanfattning (häfte). [8]

Boende på (o)lika villkor – merkostnader i bostad med särskild service för vuxna enligt LSS. [14]

En stärkt försörjningsberedskap för hälso- och sjukvården. Del 1 och 2. [19]

Hårdare regler för nya nikotinprodukter. [22]

Börja med barnen! En sammanhållen god och nära vård för barn och unga. [34]

Stärkt rätt till personlig assistans. Ökad rättssäkerhet för barn, fler grundläggande behov och tryggare sjukvårdande insatser. [37]

Ombuds tillgång till vård- och omsorgsuppgifter och förenklad behörighetskontroll inom vården. [39]

VAB för vårdåtgärder i skolan. [41]

Tillgänglighetsdirektivet. [44]

Vilja välja vård och omsorg.
En hållbar kompetensförsörjning inom vård och omsorg om äldre. [52]

Vägen till ökad tillgänglighet – långsiktig, strategisk och i samverkan. [59]

Utbildningsdepartementet

Skolbibliotek för bildning och utbildning. [3]

Bättre möjligheter för elever att nå kunskapskraven – aktivt stöd- och elevhälsoarbete samt stärkt utbildning för elever med intellektuell funktionsnedsättning. [11]

Kampen om tiden
– mer tid till lärande. [30]

Papper, poddar och ...
Pliktmateriallagstiftning för ett tryggat källmaterial. [32]

En tioårig grundskola. Införandet av en ny årskurs 1 i grundskolan, grundsärskolan, specialskolan och sameskolan. [33]

Regeringskansliet

103 33 Stockholm Växel 08-405 10 00 www.regeringen.se

ISBN 978-91-525-0173-3 ISSN 0375-250X

Omslag: Elanders Sverige AB
Bild: Agneta S Öberg