Finansdepartementet

103 33 Stockholm

Framställning om ändring i förordningen (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post

Innehållsförteckning

Sammanfattning

Försäkringskassan föreslår att regeringen undantar Försäkringskassan från skyldigheten att använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem enligt lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Syftet med förslaget är att Försäkringskassan ska kunna tillhandahålla säkra och robusta tjänster för enskilda och myndigheter samt skydda den egna verksamheten. Detta är särskilt viktigt mot bakgrund av Försäkringskassans ansvar som beredskapsmyndighet och sektorsansvarig myndighet för ekonomisk säkerhet.

1 Författningsförslag

Försäkringskassan har följande förslag till förordningstext.

1.1 Förslag till förordning om ändring i förordningen (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post

Regeringen föreskriver att 3 § förordningen (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post ska ha följande lydelse.

Nuvarande lydelse	Föreslagen lydelse
3 § En statlig myndighet under regeringen som kräver elektronisk identifiering av enskilda för åtkomst till myndighetens digitala tjänster ska använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem enligt lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Tjänsterna behöver dock inte användas av Inspektionen för strategiska produkter, Regeringskansliet, Säkerhetspolisen eller myndigheter som hör till Försvarsdepartementet.	3 § En statlig myndighet under regeringen som kräver elektronisk identifiering av enskilda för åtkomst till myndighetens digitala tjänster ska använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem enligt lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Tjänsterna behöver dock inte användas av *Försäkringskassan,* Inspektionen för strategiska produkter, Regeringskansliet, Säkerhetspolisen eller myndigheter som hör till Försvarsdepartementet.

Denna förordning träder i kraft den x.

2 Bakgrund och gällande rätt

Lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (förkortad lagen om auktorisationssystem) reglerar såväl auktorisationssystem för elektronisk identifiering som för digital post. Samma sak gäller den till lagen knutna förordningen (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (förkortad förordningen om auktorisationssystem).

Det finns för närvarande ett auktorisationssystem för elektronisk identifiering och ett sådant system för digital post. Nedan beskriver Försäkringskassan auktorisationssystemet för elektronisk identifiering, vilket är det system som är föremål för denna framställan. Vi beskriver också de motiv som låg till grund för lagstiftningen och de problem som vi har identifierat med auktorisationssystemet.

2.1 Auktorisationssystem för elektronisk identifiering

Ett auktorisationssystem är ett system där

1. den myndighet som tillhandahåller systemet godkänner att leverantörer av tjänster för elektronisk identifiering av enskilda eller för digital post får ingå ett avtal inom systemet och ingår avtal med var och en av de godkända leverantörerna om utförande av sådana tjänster,
2. en enskild har rätt att välja den leverantör som ska utföra tjänsterna för den enskildes räkning, och
3. en offentlig aktör kan använda tjänsterna i sin verksamhet enligt avtal med den tillhandahållande myndigheten.[1]

Tillämpningen av auktorisationssystem är ett annat sätt för offentliga aktörer att anskaffa tjänster än genom offentlig upphandling.[2] Ett auktorisationssystem är alltså inte någon teknisk lösning, utan ett alternativ till offentlig upphandling.

Myndigheten för digital förvaltning (Digg) är *tillhandahållande myndighet* för auktorisationssystemet för elektronisk identifiering. Utöver att tillhandahålla systemet ingår det i Diggs uppgifter att ta ut en avgift från de offentliga aktörerna och att betala ut ersättning till de godkända leverantörerna i enlighet med de villkor som ställts upp vid inrättandet av auktorisationssystemet.[3]

I lagen om auktorisationssystem saknas definitioner av uttrycken *leverantör* respektive *enskild*. Som exempel på leverantörer kan nämnas de aktörer som tillhandahåller inloggningstjänster för elektronisk identifiering för enskilda. Hur uttrycket enskild ska förstås inom ramen för auktorisationssystemet är mer komplicerat och kommer att utvecklas nedan.[4]

Försäkringskassan är i egenskap av *offentlig aktör* skyldig att använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i systemet.[5]

Inspektionen för strategiska produkter, Regeringskansliet, Säkerhetspolisen och myndigheter som hör till Försvarsdepartementet är undantagna från skyldigheten att

[1] Jämför 2 § lagen om auktorisationssystem.
[2] Se propositionen Auktorisationssystem i fråga om tjänster för elektronisk identifiering och digital post (prop. 2023/24:6) s. 33.
[3] Se prop. 2023/24:6 s. 23.
[4] Se avsnitt 2.4.1.
[5] Se 4 § 1 lagen om auktorisationssystem och 3 § 1 st. förordningen om auktorisationssystem.

använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i systemet.[6]

Digg har med stöd av bemyndiganden i förordningen om auktorisationssystem möjlighet att utfärda föreskrifter. Det finns bland annat en föreskriftsreglerad möjlighet att hos Digg ansöka om tidsbegränsat undantag från kravet på att använda tjänster för elektronisk identifiering som ingår i auktorisationssystem.[7]

De närmare villkoren för leverantörers och offentliga aktörers anslutning till auktorisationssystemet framgår av de avtal som Digg tagit fram.[8] Av villkoren framgår bland annat att anslutna leverantörer ska vara godkända enligt Tillitsramverket för Svensk e-legitimation för aktuell tillitsnivå.[9]

Försäkringskassan har inte anslutit sig till auktorisationssystemet för elektronisk identifiering. Myndigheten är skyldig att senast den 1 oktober 2026 ingå avtal med Digg och därigenom ansluta sig till systemet.[10] Försäkringskassan har svarat på remisser och fört en dialog med Digg sedan auktorisationssystemet för elektronisk identifiering inrättades.

2.2 Samordnad och säker statlig it-drift

Försäkringskassan är tillsammans med Lantmäteriet, Skatteverket och Trafikverket leverantörsmyndigheter enligt 5 § förordningen (2024:1005) om samordnad och säker statlig it-drift. Försäkringskassan är även samordnande myndighet enligt 4 § samma förordning.

Som samordnande myndighet ska Försäkringskassan samordna arbetet enligt förordningen. Myndigheten ska också, i samverkan med övriga leverantörsmyndigheter, fortlöpande föra en förteckning över de it-driftstjänster som ingår i det statliga tjänsteutbudet. Leverantörsmyndigheterna ska tillhandahålla det samordnade statliga tjänsteutbudet och stödja myndigheter under regeringen vid valet av it-driftslösning. Vid utformningen av de it-driftstjänster som erbjuds ska totalförsvarets behov beaktas.

Lantmäteriet har ingått avtal med Digg och anslutit sig till auktorisationssystemet för elektronisk identifiering. Övriga leverantörsmyndigheter har inte ingått avtal med Digg.

---

[6] Se 3 § 2 st. förordningen om auktorisationssystem.
[7] Se 4 § Diggs föreskrifter om fullgörande av, avvikelser och ansökan om undantag från kravet på anslutning till auktorisationssystem för elektronisk identifiering (MDFFS 2025:3).
[8] Se Anslutningsavtal för Auktorisationssystem för elektronisk identifiering – leverantör https://www.digg.se/digitala-tjanster/e-legitimering/bli-godkand-utfardare-av-svensk-e-legitimation/leverera-elektronisk-identifiering-inom-auktorisationssystemet/auktorisationssystem-for-elektronisk-identifiering---administrativa-foreskrifter/anslutningsavtal-for-auktorisationssystem-for-elektronisk-identifiering---leverantor
Se Anslutningsavtal för Auktorisationssystem för elektronisk identifiering – offentlig aktör https://www.digg.se/digitala-tjanster/e-legitimering/erbjud-inloggning-med-svenska-e-legitimationer/anslut-till-auktorisationssystem-for-elektronisk-identifiering/teckna-avtal-inom-auktorisationssystem-for-elektronisk-identifiering/anslutningsavtal-for-auktorisationssystem-for-elektronisk-identifiering---offentlig-aktor
Båda sidorna hämtade 2026-05-29.
[9] Se avsnitt 5.6 Anslutningsavtal för Auktorisationssystem för elektronisk identifiering – leverantör.
[10] Se 3 § MDFFS 2025:3.

2.3 Skälen för att införa auktorisationssystem för elektronisk identifiering

I den proposition som låg till grund för lagen om auktorisationssystem uttalade regeringen bland annat följande om det allmänna behovet av förvaltningsgemensamma digitala lösningar. Sådana lösningar behövdes för att underlätta elektronisk hantering av ärenden och kontakter med enskilda. Myndighetsspecifika lösningar, som skiljde sig från varandra, har resulterat i en ineffektiv ordning för den offentliga sektorn som helhet. Det var viktigt med en robust digital infrastruktur mot bakgrund av det rådande säkerhetspolitiska läget. Tjänsterna måste uppfylla högt ställda krav på säkerhet och skydd för den personliga integriteten. Genom att tydliggöra ansvarsfördelningen och öka standardiseringen kunde styrningen och samordningen stärkas. [11]

Skälen för att införa ett auktorisationssystem för elektronisk identifiering var i huvudsak följande. Systemet skulle öka konkurrensen på marknaden för tjänster för elektronisk identifiering.[12] Vidare ansågs ett sådant system, med ett enhetligt sätt för offentliga myndigheter att anskaffa en funktion för elektronisk identifiering, kunna bidra till att effektivisera processer och arbetssätt inom den offentliga sektorn. Av det skälet reglerade regeringen i förordning att statliga myndigheter under regeringen som huvudregel ska använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem om de kräver elektronisk identifiering av enskilda för åtkomst till myndighetens digitala tjänster.[13] I och med att offentliga aktörer får använda tjänsterna, bedömdes förslaget också leda till bättre förutsättningar för privata utförare av offentligt finansierade uppgifter att utföra dessa på lika villkor.[14]

2.4 Problem med auktorisationssystemet för elektronisk identifiering

Försäkringskassan har identifierat ett antal problem med auktorisationssystemet och redogör nedan för dessa.

2.4.1 Auktorisationssystemets tillämpningsområde

Auktorisationssystemet för elektronisk identifiering omfattar inte alla former av elektronisk verifiering som sker i Försäkringskassans verksamhet. Systemet omfattar inte heller alla tjänster för elektronisk identifiering som finns att tillgå på marknaden och som Försäkringskassan har, eller kan komma att ha, behov av att använda. Nedan beskriver vi auktorisationssystemets tillämpningsområde och de problem som myndigheten ställs inför vid en anslutning till auktorisationssystemet.

Uttrycket enskild
Som framgår av lagtexten omfattar auktorisationssystemet endast elektronisk identifiering som görs av enskilda. Varken i förarbetena eller i de avtal som Digg tagit fram vid inrättande av auktorisationssystemet för elektronisk identifiering lämnas förtydliganden av uttryckets innebörd. Att det saknas en definition av uttrycket är inte unikt för auktorisationssystemet som sådant, snarare förhåller det sig på det viset att uttrycket enskild inte definieras i lag.

Uttrycket enskild får i stället förstås utifrån det sammanhang i vilket begreppet används. Vanligtvis kan uttrycket kontrasteras mot det offentliga och normalt sett anses såväl fysiska som juridiska personer kunna vara ”enskilda”.

[11] Jämför prop. 2023/24:6 s. 16.
[12] Se prop. 2023/24:6 s. 44.
[13] Se prop. 2023/24:6 s. 46.
[14] Se prop. 2023/24:6 s. 48.

Enligt den information som Försäkringskassan har fått från Digg ska uttrycket enskild, inom ramen för elektronisk identifiering, förstås som privatpersoner som ska nå offentlig sektor i sina ärenden.[15] Med tjänster för elektronisk identifiering av enskilda avses enligt Diggs tolkning dels de situationer där en individ använder en privat e-legitimation för att identifiera sig själv i en digital tjänst, dels situationer där en individ använder en privat e-legitimation för att identifiera sig som en representant för ett företag i en digital tjänst. Digg har vidare angett att en enskild avser en person eller ett företag som agerar i förhållande till det allmänna, till skillnad från staten, kommuner eller andra offentliga organ och dess verksamhet. Den efterföljande bedömningen av vilka som i detta sammanhang ska anses vara enskilda i förhållande till den specifika offentliga aktören behöver enligt Digg avgöras av den offentliga aktören.

Det är alltså inte samtliga fall av elektronisk identifiering som omfattas av auktorisationssystemet. Exempel på identifieringar som faller utanför tillämpningsområdet är sådana som görs av företrädare för offentliga aktörer, till exempel när en företrädare för en kommun, region eller statlig myndighet loggar in i en digital tjänst som tillhandahålls av Försäkringskassan eller av någon annan myndighet.

Eftersom inte alla fall av elektronisk identifiering omfattas av auktorisationssystemet måste Försäkringskassan, även efter eventuell anslutning till systemet, upphandla samma tjänster som tillhandahålls inom auktorisationssystemet, för sådan identifiering som görs utanför systemets tillämpningsområde.

Det innebär att auktorisationssystemet inte ersätter Försäkringskassans behov av egna avtal eller andra anskaffningslösningar för elektronisk identifiering. För offentliga aktörer leder systemet därmed inte till en effektivisering av processer och arbetssätt som annars skulle kunna förväntas av en förvaltningsgemensam lösning. Offentliga aktörer som både behöver erbjuda elektronisk identifiering för enskilda och för andra än enskilda kommer fortsatt att behöva upphandla tjänster och ha leverantörsrelationer utanför auktorisationssystemet.

Därutöver behöver Försäkringskassan kunna särskilja de identifieringar som omfattas av auktorisationssystemet från sådana som faller utanför systemets tillämpningsområde. Det är nödvändigt för att myndigheten ska kunna betala avgifter till Digg inom ramen för auktorisationssystemet och ersättning till leverantörer för tjänster som tillhandahålls vid sidan av systemet.

Detta innebär också att leverantörer som tillhandahåller tjänster både inom och utanför auktorisationssystemet kan behöva särskilja identifieringar utifrån om de omfattas av auktorisationssystemet eller inte.

Övriga tjänster för elektronisk identifiering
Även andra tjänster kan falla utanför auktorisationssystemet. Leverantörer kan inom auktorisationssystemet erbjuda tjänster för personer med samordningsnummer.[16] Tjänsten kan alltså tillhandahållas av leverantörer i systemet, men det är för närvarande inte någon leverantör som erbjuder den. Tjänsten måste därför upphandlas separat av Försäkringskassan och andra offentliga aktörer som har behov av tjänsten. Detsamma gäller de övriga tjänster som tillhandahålls på marknaden för elektronisk identifiering men som inte omfattas av tjänsteutbudet inom auktorisationssystemet. Det kan till exempel handla om säkerhetstjänster som erbjuds i syfte att motverka identitetsmissbruk.

[15] Se Diggs promemoria Återkoppling till Försäkringskassan avseende auktorisationssystem för elektronisk identifiering, FK 2026/005921.
[16] Se avsnitt 7.1.2 Anslutningsavtal för Auktorisationssystem för elektronisk identifiering – offentlig aktör.

2.4.2 Egen rådighet

Auktorisationssystemet utgör inte en heltäckande reglering av hela den tekniska och operativa kedjan för elektronisk identifiering. Vidare står delar av avtals- och leverantörskedjan utom Försäkringskassans direkta kontroll.

Det ovan sagda är inte enbart problematiskt för Försäkringskassans roll som ansvarig för samhällsviktig verksamhet, utan även i vår funktion enligt förordningen om samordnad och säker statlig it-drift samt som sektorsansvarig beredskapsmyndighet.

När delar av avtals- och leverantörskedjan hanteras utanför Försäkringskassan direkta kontroll, samtidigt som ansvar för drift, integration, informationssäkerhet, kontinuitet och samhällsviktiga funktioner ligger kvar hos myndigheten, uppstår en förskjutning av rådighet utan motsvarande överföring av ansvar. Det innebär att Försäkringskassan fortsatt ansvarar för helheten men får sämre möjligheter att styra alla delar som påverkar verksamhetens säkerhet och robusthet. Försäkringskassan har som leverantörsmyndighet ett ansvar för att tillhandahålla samordnade och säkra it-tjänster till anslutna myndigheter, vilket förstärker behovet av faktisk rådighet över kritiska delar av identitets- och åtkomstkedjan.

Behovet av rådighet aktualiseras även genom cybersäkerhetslagen (2025:1506), som genomför NIS 2-direktivet i svensk rätt. Regleringen syftar till att uppnå en hög nivå av cybersäkerhet i samhället och innebär skärpta krav på bland annat riskhanteringsåtgärder, ledningsansvar, incidentrapportering och säkerhet i leveranskedjan för verksamhetsutövare.[17] Försäkringskassan omfattas i egenskap av beredskapsmyndighet av bestämmelserna i cybersäkerhetslagen.[18] I detta sammanhang är det särskilt viktigt att myndigheter med ansvar för samhällsviktig verksamhet och sektorsansvar också har faktisk rådighet över de delar av kedjan som är avgörande för säker elektronisk identifiering, kontinuitet och operativ kontroll. För Försäkringskassan handlar det till exempel om att kunna ställa och följa upp säkerhetskrav, hantera incidenter och störningar och säkerställa alternativa lösningar för åtkomst till myndighetens digitala tjänster om en inloggningslösning inte fungerar som avsett.

Försäkringskassan har i remissvar vid Diggs framtagande av föreskrifter och avtal kopplade till auktorisationssystemet, framhållit att myndigheter som är anslutna till systemet måste kunna agera skyndsamt om en leverantör bedöms innebära en säkerhetsrisk.[19] Om Försäkringskassan identifierar hot eller risker hos en leverantör behöver myndigheten ha möjlighet att omgående kunna stänga av eller avbryta den tekniska anslutningen till leverantören för att skydda den egna verksamheten. Denna möjlighet saknas i auktorisationssystemets regelverk.

Försäkringskassans konstaterar att auktorisationssystemet förskjuter rådigheten över delar av avtals- och leverantörskedjan från myndigheten till Digg, samtidigt som myndigheten fortsatt ansvarar för teknisk anslutning, integration, informationssäkerhet, verksamhetsrisker och konsekvenser i den egna verksamheten.

2.4.3 Säkerhetskrav och aktiv kontrollförmåga

Det är av stor vikt att den tillhandahållande myndigheten särskilt ser till att ställa höga krav på säkerhet och genom en aktiv och kontinuerlig uppföljning ser till att kraven

[17] Se 1 § och 2 kap. 3–8 §§ cybersäkerhetslagen.
[18] Jfr 4 § cybersäkerhetsförordningen (2025:1507).
[19] Jfr Försäkringskassans remissvar Förslag till föreskrifter och anslutningsavtal avseende auktorisationssystem för elektronisk identifiering och digital post, FK 2025/006275.

uppfylls.[20] Säkerhetsfrågorna är därmed inte en sidofråga i systemet, utan en bärande förutsättning för att konstruktionen ska fungera.

Leverantörer inom auktorisationssystemet ska som nämnts ovan vara godkända enligt Tillitsramverket för Svensk e-legitimation för aktuell tillitsnivå och följa de krav som gäller enligt ramverket. Tillitsramverket innehåller bland annat krav på informationssäkerhetsarbete, riskhantering, incidenthantering, kontinuitetsplanering, underleverantörer och internrevision.[21] Av anslutningsavtalet för leverantörer följer att leverantören årligen ska skicka en revisionsrapport till Digg efter avslutad internrevision.[22] Digg anger att myndigheten har egna avtal med leverantörer och regelbundet kontrollerar att leverantörerna uppfyller kraven i både auktorisationssystemet och Tillitsramverket för Svensk e-legitimation.[23] I regelverken och Diggs offentliga information klargörs inte i vilken utsträckning kontrollen är proaktiv, hur den utövas i praktiken, hur risker identifieras innan skada uppstår eller hur kontrollen omfattar underleverantörer, förändrade ägarförhållanden och andra riskdrivande förändringar.[24]

Frågan om säkerhetskrav och aktiv kontrollförmåga är särskilt viktig ur ett beredskaps- och säkerhetsperspektiv. Elektronisk identifiering är en grundläggande förutsättning för åtkomst till digitala tjänster och därmed en del av den funktionalitet som måste vara robust även vid störningar, antagonistiska angrepp och andra säkerhetshot.[25] För myndigheter med ansvar för samhällsviktig verksamhet är det därför avgörande att kontrollen av godkända leverantörer inte enbart sker i efterhand, när brister redan har uppstått eller risker har realiserats.

Om uppföljningen i huvudsak bygger på leverantörernas egenkontroll, internrevision och efterföljande rapportering finns en risk att kontrollmodellen blir mer reaktiv än proaktiv. Det ligger inte i linje med utgångspunkten att säkerhetskraven ska upprätthållas genom aktiv och kontinuerlig uppföljning under hela avtalsperioden.[26]

Försäkringskassan anser att auktorisationssystemet inte når upp till de krav på säkerhet som förutsattes i förarbetena till lagstiftningen om auktorisationssystemet och som Försäkringskassan är beroende av.[27] Mot bakgrund av Försäkringskassans ansvar som sektorsansvarig beredskapsmyndighet och som ansvarig för samhällsviktig verksamhet är behovet av tydlig, löpande och förebyggande kontroll särskilt starkt. Detta behov förstärks ytterligare av de skärpta krav på riskhantering, ledningsansvar och incidentrapportering som följer av den nya cybersäkerhetsregleringen.

---

[20] Se prop. 2023/24:6 s. 45.
[21] Se avsnitt 5.1.2 och 5.1.3 Anslutningsavtal för Auktorisationssystem för elektronisk identifiering – leverantör. Se även avsnitt 5.6 Auktorisationssystem för elektronisk identifiering – administrativa föreskrifter samt bl.a. K2.4–K2.6 och K2.9 Tillitsramverk för Svensk e-legitimation.
[22] Se avsnitt 8.16.1 Anslutningsavtal för Auktorisationssystem för elektronisk identifiering – leverantör.
[23] Se https://www.digg.se/digitala-tjanster/e-legitimering/erbjud-inloggning-med-svenska-e-legitimationer/anslut-till-auktorisationssystem-for-elektronisk-identifiering, hämtad 2026-05-29.
[24] Se Diggs promemoria Återkoppling till Försäkringskassan avseende auktorisationssystem för elektronisk identifiering, FK 2026/005921.
[25] Se Försäkringskassans remissvar Förslag till föreskrifter och anslutningsavtal avseende auktorisationssystem för elektronisk identifiering och digital post, FK 2025/006275.
[26] Se prop. 2023/24:6 s. 31 och 45.
[27] Jfr även Försäkringskassans remissvar på promemorian Auktorisationssystem för elektronisk identifiering och för digital post (dnr I2020/03269), FK 2020/006064.

3 Överväganden och förslag

3.1 Inledning

Med hänsyn till de problem som Försäkringskassan identifierat med auktorisationssystemet för elektronisk identifiering är vårt förslag att myndigheten ska undantas från skyldigheten att använda de tjänster som tillhandahålls av leverantörer i systemet.

3.2 Förslaget

Försäkringskassans förslag: Försäkringskassan föreslår att regeringen undantar Försäkringskassan från skyldigheten att använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem enligt lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Skälen för förslaget:
Av de anledningar som Försäkringskassan fört fram i avsnitt 2.4 anser myndigheten att det finns tungt vägande skäl för att myndigheten inte ska vara ansluten till auktorisationssystemet för elektronisk identifiering. Detta då myndigheten, vid en anslutning till systemet, inte anser sig kunna tillhandahålla säkra tjänster för elektronisk identifiering för enskilda och myndigheter.

I förordningen om auktorisationssystem finns en bestämmelse som är utformad på så sätt att tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystemet inte behöver användas av de i bestämmelsen uppräknade myndigheterna. Försäkringskassan föreslår inte någon annan ändring än att Försäkringskassan inkluderas i denna uppräkning.

De föreslagna bestämmelserna bör träda i kraft så snart som möjligt. Försäkringskassan är skyldig att ingå avtal med Digg och därigenom ansluta sig till auktorisationssystemet för elektronisk identifiering senast den 1 oktober 2026. Med hänsyn till detta måste de föreslagna bestämmelserna träda i kraft senast den 1 oktober 2026.

Försäkringskassan bedömer att det inte finns något behov av övergångsbestämmelser.

4 Konsekvensutredning

4.1 Syftet med förslaget

Försäkringskassan har vid sin analys av auktorisationssystemet identifierat risker kopplade till systemets säkerhet. Genom att myndigheten undantas från skyldigheten att använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem, uppnår Försäkringskassan samma nivå av säkerhet i sina tjänster som myndigheten upprätthåller idag. Detta är av vikt inte bara för Försäkringskassan utan även från ett beredskaps- och robusthetsperspektiv och därmed samhället i stort, inte minst under rådande säkerhetsläge.

4.2 Alternativa lösningar

Om nuvarande reglering består måste Försäkringskassan ansluta sig till auktorisationssystemet, trots de problem som har beskrivits ovan. Detta löser inte den grundläggande konflikt som finns mellan auktorisationssystemets utformning och de krav som följer av Försäkringskassans verksamhet. Det innebär inte heller att den enkelhet och enhetlighet som systemet var avsett att skapa uppnås i praktiken, eftersom myndigheten även fortsatt kan behöva hantera kringtjänster, kompletterande avtal och egna tekniska lösningar utanför systemet.

Ett alternativ till Försäkringskassans förslag skulle kunna vara att utvidga auktorisationssystemets tillämpningsområde ytterligare, på så sätt att systemet innefattar identifiering även av andra än enskilda. Om tillämpningsområdet skulle utvidgas på detta vis, skulle det inte längre behövas göras någon skillnad mellan identifiering som görs av en företrädare för ett offentligt organ och privata aktörer. Det skulle dock inte lösa problemen kopplade till rådighet, säkerhet och proaktiv kontrollförmåga av leverantörer. Det skulle inte heller innebära någon skillnad i förhållande till de lösningar som inte erbjuds inom ramen för auktorisationssystemet, till exempel för personer med samordningsnummer, eftersom dessa tjänster fortsatt skulle behöva upphandlas separat. Konsekvenserna av en sådan ordning, där tillämpningsområdet utvidgas på så sätt att systemet innefattar identifiering även av andra än enskilda, blir även svåröverblickbara. I denna del kan nämnas att tillämpningen av 3 § förordningen om auktorisationssystem skulle medföra problem för myndigheter som använder sig av andra lösningar för identifiering och underskrift, såsom tjänstelegitimationer. Om endast de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem får användas vid åtkomst till en myndighets digitala tjänster, kan inte en tjänstelegitimation användas för att komma åt en sådan digital tjänst.

Ett annat alternativ är att lägga tjänster för elektronisk identifiering inom ramen för det samordnade tjänsteutbudet enligt förordningen om samordnad och säker statlig it-drift. En sådan lösning skulle kunna ge offentliga aktörer tillgång till gemensamma tjänster för elektronisk identifiering inom en struktur där säkerhet, robusthet och faktisk rådighet är bärande utgångspunkter. Det skulle också minska behovet av parallella anskaffningar av avtal och kompletterande lösningar utanför systemet. Detta alternativ kan också övervägas istället för att myndigheter med särskilda krav på säkerhet, robusthet och rådighet ska omfattas av en skyldighet att använda auktorisationssystemet. En sådan lösning skulle kunna vara mer ändamålsenlig och på så sätt bidra till att effektivisera processer och arbetssätt inom den offentliga sektorn. Denna lösning medför dock större konsekvenser för själva infrastrukturen för elektronisk identifiering, eftersom den innebär att det inte finns något behov av auktorisationssystemet för elektronisk identifiering. Det skulle också kräva en noggrann analys av om det är möjligt och lämpligt att ansluta offentliga aktörer till det samordnade statliga tjänsteutbudet.

4.3 Ekonomiska konsekvenser

4.3.1 Konsekvenser för Försäkringskassan

Förslaget bedöms kunna medföra minskade kostnader för Försäkringskassan jämfört med en ordning där myndigheten fullt ut skulle behöva anpassa befintliga lösningar till auktorisationssystemet. Förslaget minskar också behovet av parallella avtals- och leverantörslösningar, särskild statistikuppdelning, kostnadsuppföljning och ytterligare teknisk anpassning. Därigenom kan myndighetens kostnader för utveckling, förvaltning och styrning begränsas.

Förslaget innebär samtidigt att Försäkringskassan även fortsättningsvis behöver bära kostnader för anskaffning, utveckling och förvaltning av tjänster för elektronisk identifiering. Dessa kostnader bedöms dock, liksom idag, vara förutsägbara och förenliga med myndighetens behov av rådighet, säkerhet och långsiktig planering till skillnad från de kostnader som följer av en ordning där ansvar och rådighet delas upp mellan flera aktörer.

4.3.2 Konsekvenser för andra myndigheter

Förslaget kan få konsekvenser för andra myndigheter, särskilt Digg, och de offentliga aktörer som omfattas av auktorisationssystemet.

Om Försäkringskassan undantas från skyldigheten att använda auktorisationssystemet bedöms konsekvenserna för övriga myndigheter och offentliga aktörer bli begränsade. Förslaget påverkar inte offentliga aktörers möjligheter att ansluta till eller använda auktorisationssystemet. Det påverkar inte heller Diggs möjlighet att fortsatt tillhandahålla systemet för andra offentliga aktörer.

För Digg innebär förslaget minskade intäkter från avgifter inom auktorisationssystemet, om färre offentliga aktörer omfattas av skyldigheten att använda systemet eller om transaktionsvolymerna inom systemet blir lägre.

För offentliga aktörer som är anslutna till systemet kan förslaget medföra ökade kostnader. Samtidigt bör det noteras att Försäkringskassan inte heller i dagsläget är ansluten till auktorisationssystemet.

4.3.3 Konsekvenser för försäkringsutgifterna

Förslaget rör inte utbetalningar av socialförsäkringsförmåner och har därför inga konsekvenser för försäkringsutgifterna.

4.3.4 Konsekvenser för enskilda

Förslaget innebär att Försäkringskassan behöver upphandla tjänster för elektronisk identifiering, på samma sätt som gäller idag. Konsekvenserna för företag bedöms därför vara begränsade.

Förslaget bedöms inte få några övriga ekonomiska konsekvenser för enskilda.

4.4 Andra konsekvenser

Konsekvenser för enskilda
För enskilda kan förslaget innebära att Försäkringskassans lösningar i vissa delar avviker från den ordning som gäller inom auktorisationssystemet. Förslaget bedöms dock inte i sig medföra några negativa konsekvenser för enskilda. Syftet är istället att säkerställa att tillgången till säkra och fungerande inloggningslösningar kan upprätthållas även över tid och vid störningar.

Förslaget innebär inte att enskilda får en sämre möjlighet att använda elektronisk identifiering i Försäkringskassan digitala tjänster. Tvärtom är avsikten att myndigheten ska kunna säkerställa att de lösningar som används uppfyller de krav som följer av verksamhetens behov, inklusive krav på säkerhet, tillgänglighet, kontinuitet och skydd mot missbruk.

Konsekvenser för företag
För privata aktörer som är anslutna till auktorisationssystemet kan förslaget innebära att Försäkringskassan inte kommer att utgöra en del av det kundunderlag som annars skulle ha funnits inom systemet. För dessa aktörer kan det samtidigt innebära ökad tydlighet i avtalsförhållandena.

Övriga konsekvenser
Förslaget innebär inte några konsekvenser för auktorisationssystemet för digital post.

Förslaget medför inte heller några samhällsekonomiska, sociala eller miljömässiga konsekvenser. Förslaget får inte någon påverkan på brottsligheten eller på jämställdheten mellan kvinnor och män.

4.5 Stämmer regleringen med eventuella EU-krav?

Förslaget överensstämmer med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen.

5 Ikraftträdande- och övergångsbestämmelser

De föreslagna bestämmelserna bör träda i kraft så snart som möjligt. Försäkringskassan är skyldig att ingå avtal med Digg och därigenom ansluta sig till auktorisationssystemet för elektronisk identifiering senast den 1 oktober 2026. Med hänsyn till detta måste de föreslagna bestämmelserna träda i kraft senast den 1 oktober 2026.

Försäkringskassan bedömer att det inte finns något behov av övergångsbestämmelser.

Beslut i detta ärende har fattats av generaldirektör Nils Öberg i närvaro av rättschef Ingrid Utne, avdelningschef Peter Haglind och rättslig expert Marcus Lundén samt verksamhetsutvecklare Azize Cuydur, de senare som föredragande.

Nils Öberg

Marcus Lundén
Azize Cuydur