Skatteverket

PROMEMORIA

Datum
2026-07-03

Dnr
8-208500-2026

Undantag från obligatorisk anslutning till auktorisationssystemet i fråga om tjänster för elektronisk identifiering

Postadress: 205 30 MALMÖ **Telefon**: 0771-567 567
Mejl via "Kontakta oss" på www.skatteverket.se

Innehållsförteckning

Sammanfattning

Bestämmelsen i 3 § första stycket förordningen (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post innebär att det, sedan den 1 januari 2026, är obligatoriskt för myndigheter att ansluta till auktorisationssystemet och att därmed även använda de tjänster som tillhandahålls genom auktorisationssystemet.

Skatteverket har analyserat huruvida de tjänster för elektronisk identifiering som tillhandahålls genom auktorisationssystemet kan användas utifrån de olika uppdrag som Skatteverket har. Skatteverket har konstaterat att tjänsteutbudet inte täcker de behov som Skatteverket har när det gäller elektronisk identifiering. Skatteverket bedömer att en anslutning till auktorisationssystemet skulle medföra ett stort antal praktiska och säkerhetsmässiga problem för Skatteverket. I promemorian föreslås därför att Skatteverket ska få undantag från anslutning till auktorisationssystemet. Därigenom undviks de problem som Skatteverket identifierat.

Skatteverkets förslag överensstämmer i sak med Försäkringskassans förslag om författningsändring i skrivelsen Framställning om ändring i förordningen (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post, som Försäkringskassan lämnade till regeringen den 29 maj 2026, Försäkringskassans dnr FK 2026/013860.

Ändringen föreslår träda i kraft den 1 oktober 2026.

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

Härigenom föreskrivs 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.	Tjänsterna behöver dock inte användas av Inspektionen för strategiska produkter, Regeringskansliet, *Skatteverket,* Säkerhetspolisen eller myndigheter som hör till Försvarsdepartementet.

Denna lag träder i kraft den 1 oktober 2026.

2 Auktorisationssystemet i fråga om tjänster för elektronisk identifiering och för digital post

2.1 Den offentliga sektorns tillgång till digitala tjänster

Digitala tjänster ska, så långt det är möjligt och där det är relevant, vara förstahandsval i den offentliga sektorns kontakter med medborgare, organisationer och företag (prop. 2015/16:1 utg.omr. 22 s. 120).

Förvaltningsgemensamma digitala lösningar behövs för att underlätta elektronisk hantering av ärenden och kontakter med enskilda. Bristen på förvaltningsgemensamma digitala lösningar har lett till myndighetsspecifika lösningar, som skiljer sig från varandra. Detta har resulterat i en ineffektiv ordning för den offentliga sektorn som helhet. Den snabba digitala utvecklingen innebär att komplexiteten tilltar samtidigt som en robust digital infrastruktur är viktigt mot bakgrund av det rådande säkerhetspolitiska läget. Det finns behov av att stärka styrningen och samordningen genom att tydliggöra ansvarsfördelningen och öka standardiseringen (prop. 2023/24:6 s. 16).

Bakgrunden till auktorisationssystemet

Bestämmelserna syftar till att ge alla utförare av offentligt finansierad verksamhet möjlighet att erbjuda service med hjälp av digitala tjänster på lika villkor genom att en myndighet ska tillhandahålla auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Enskilda ska få välja vilken leverantör som ska utföra tjänsten för deras räkning (prop. 2023/24:6).

Myndigheten för digital förvaltning (Digg), som är den tillhandahållande myndigheten, bör bl.a. bestämma vilka säkerhetskrav som ska gälla inom auktorisationssystemen. Detta innebär också att den tillhandahållande myndigheten, till skillnad från vad som gäller i dag, bör ansvara för att bestämmelserna i lagen följs och att de ställda säkerhetskraven upprätthålls (jfr prop. 2012/13:123 s. 51 och 52). I övrigt bör ansvarsförhållandena framgå av de avtal som Digg ingår med de offentliga aktörerna och leverantörerna (prop. 2023/24:6 s. 24). En samlad lag om auktorisationssystem i fråga om tjänster både för elektronisk identifiering och för digital post ger dessutom bättre förutsättningar för ytterligare utvidgning av lagstiftningen till andra liknande förvaltningsgemensamma digitala tjänster (prop. 2023/24:6 s. 30).

2.2 Gällande rätt

Reglering

Bestämmelserna om auktorisationssystem för tjänster för elektronisk identifiering regleras i lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (förkortad lagen om auktorisationssystem) och förordningen (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (förkortad förordningen om auktorisationssystem).

Digg har i föreskrift reglerat fullgörande av, avvikelser och ansökan om undantag från kravet på anslutning till auktorisationssystem för elektronisk identifiering (MDFFS 2025:3). Föreskriften innehåller bestämmelser om

fullgörande av, avvikelser och ansökan om undantag från 3 § första stycket förordningen om auktorisationssystem (1 § MDFFS 2025:3).

Auktorisationssystem, tillhandahållande myndighet och finansiering

Med ett auktorisationssystem avses 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 ingå 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 (2 § lagen om auktorisationssystem).

Digg ska vara den tillhandahållande myndigheten enligt lagen om auktorisationssystem (2 § förordningen om auktorisationssystem). Digg ska ta ut en avgift för användningen av tjänster inom ett auktorisationssystem. Myndigheten får meddela de närmare föreskrifter som behövs för verkställigheten av uttaget av avgifterna och disponera avgiftsinkomsterna (7 § förordningen om auktorisationssystem).

Elektronisk identifiering

Med elektronisk identifiering avses detsamma som i 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 (3 § lagen om auktorisationssystem).

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 om auktorisationssystem (3 § första stycket förordningen om auktorisationssystem). Kravet på användningen av tjänster regleras i 2 § MDFFS 2025:3. Skyldigheten enligt 3 § första stycket förordningen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post ska fullgöras genom att tjänster för elektronisk identifiering ska användas inom tre månader från det att dessa tjänster finns tillgängliga i auktorisationssystem.

Tillfälligt anstånd för samtliga myndigheter att ansluta sig till auktorisationssystemet

Digg har meddelat föreskrifter som innebär att samtliga myndigheter som enligt lagen om auktorisationssystem är tvungna att ansluta sig till auktorisationssystemet får anstånd med att göra det till den 1 oktober 2026.

Anståndet regleras i 3 § MDFFS 2025:3 och innebär att om en myndighet har avtal eller andra förhållande som medför att användning av tjänster för elektronisk identifiering inom den tid som anges 2 § MDFFS 2025:3 medför oskäliga kostnader eller andra oskäliga konsekvenser, ska användning av tjänsterna i stället ske så snart förhållandena medger detta eller senast nio månader från det att dessa tjänster finns tillgängliga i auktorisationssystem. Bestämmelsen upphör att gälla den 1 oktober 2026.

Undantag från kravet på anslutning till auktorisationssystem

Myndigheter som kräver elektronisk identifiering av enskilda för åtkomst till myndighetens digitala tjänster kan få undantag från kravet i 3 § första stycket

förordningen om auktorisationssystem att använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörerna i auktorisationssystemet. Undantaget kan medges genom förordning eller genom ett särskilt undantag som är tidsbegränsat.

Inspektionen för strategiska produkter, Regeringskansliet, Säkerhetspolisen och myndigheter som hör till Försvarsdepartementet är enligt 3 § andra stycket förordningen om auktorisationssystem undantagna från skyldigheten att använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i systemet. Försäkringskassan har i sin skrivelse till regeringen föreslagit att undantaget ska utvidgas till att även omfatta Försäkringskassan (Framställning om ändring i förordningen [2023:709] om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post, 2026-05-29, dnr FK 2026/013860).

Digg får i enskilda fall besluta om tidsbegränsade undantag från skyldigheten enligt 3 § första stycket förordningen om auktorisationssystem (4 § förordningen om auktorisationssystem). Möjligheten att medge tidsbegränsade undantag har införts för att säkerställa nödvändig flexibilitet (prop. 2023/24:6 s. 45).

Möjligheten till ansökan om enskilt undantag från kravet på att använda tjänster för elektronisk identifiering som ingår i auktorisationssystem regleras i 4 § MDFFS 2025:3 (numreras 3 § från den 1 oktober 2026). En ansökan om ett särskilt undantag som är tidsbegränsat enligt 4 § förordningen om auktorisationssystem ska göras skriftligen minst en månad innan önskad tidpunkt från undantaget. Ansökan ska innehålla en beskrivning av grunderna för undantaget och av de kostnader eller andra olägenheter som uppkommer för myndigheter om undantaget inte ges, samt ange tidsperioden för undantaget.

2.3 Vilka som kan använda auktorisationssystemets tjänster för elektronisk identifiering

Den primära målgruppen för de tjänster som finns i auktorisationssystemet när det gäller elektronisk identifiering är personer som är folkbokförda i Sverige och som har svenskt personnummer. Dessa personer förväntas i regel ha tillgång till en svensk e-legitimation som uppfyller kraven i auktorisationssystemet. Personer som inte är folkbokförda i Sverige kan i vissa fall använda tjänsterna. Det gäller t.ex. personer som har samordningsnummer som kan omfattas i den utsträckning deras identitet är tillräckligt styrkt enligt gällande regelverk.

Vissa personer kan dock falla utanför auktorisationssystemets tillämpnings-område. För att dessa personer ändå ska kunna använda sig av e-tjänster som en myndighet tillhandahåller måste den enskilda myndigheten tillhandahålla en elektronisk inloggning som är tillräckligt säker utifrån syftet med e-tjänsten.

3 Skatteverkets möjligheter att ansluta sig till auktorisationssystemet för elektronisk identifiering

3.1 Skatteverkets uppdrag

3.1.1 Förordningen (2017:154) med instruktion för Skatteverket

Regeringens uppdrag till Skatteverket regleras i förordningen (2017:154) med instruktion för Skatteverket (förkortad instruktionen).

Skatteverket ska fastställa och ta ut skatter, socialavgifter och andra avgifter så att en riktig uppbörd kan säkerställas och ska fastställa rättvisande taxeringsvärden på fastigheter så att korrekt underlag finns för skatteberäkning och andra ändamål. Skatteverket ansvarar för frågor om folkbokföring och personnamn och ska utfärda identitetskort för folkbokförda i Sverige. Skatteverket ansvarar för registrering av boupptecknin gar och handläggning av ärenden enligt 16 kap. ärvdabalken och ansvarar för äktenskapsregistret och för registreringsärenden enligt 16 kap. äktenskapsbalken. Skatteverket ansvarar dessutom för utbetalning av garantibelopp och därmed sammanhängande uppgifter enligt lönegarantilagen (1992:497) och lönegarantiförordningen (2024:1329) (jfr 1–5 och 12 b §§ instruktionen). Skatteverket är värdmyndighet åt Valmyndigheten och ansvarar för Statens personadressregister, SPAR, som utgör en egen verksamhetsgren inom Skatteverket.

Skatteverket ska samverka med Kronofogdemyndigheten och Utbetalningsmyndigheten samt ingå serviceavtal med Statens servicecenter om att Statens servicecenter ska utföra uppgifter enligt lagen (2019:212) om viss gemensam offentlig service för Skatteverkets räkning (15–15 b §§ instruktionen).

3.1.2 Samordnad och säker statlig it-drift

Förordningen (2024:1005) om samordnad och säker statlig it-drift innehåller bestämmelser om ett samordnat statligt tjänsteutbud för it-drift (1 § förordningen om samordnad och säker statlig it-drift). Med myndighet avses i förordningen en myndighet under regeringen. Med samordnat statligt tjänsteutbud avses i förordningen it-driftstjänster som tillhandahålls myndigheter av en leverantörsmyndighet eller på uppdrag av en sådan myndighet (3 § förordningen om samordnad och säker statlig it-drift). Försäkringskassan, Lantmäteriet, Skatteverket och Trafikverket är leverantörsmyndigheter enligt förordningen (5 § första stycket förordningen om samordnad och säker statlig it-drift).

Försäkringskassan, Lantmäteriet, Skatteverket och Trafikverket ska som leverantörsmyndigheter bestämma vilka it-driftstjänster som ska erbjudas inom det samordnade statliga tjänsteutbudet och hur tjänstebeskrivningarna för tjänsterna ska utformas. Leverantörsmyndigheterna ska tillhandahålla det samordnade statliga tjänsteutbudet och stödja myndigheterna vid valet av it-driftslösning. Vid utformningen av de it-driftstjänster som erbjuds ska totalförsvarets behov beaktas (5 § andra och tredje stycket förordningen om samordnad och säker statlig it-drift). En leverantörsmyndighet får endast tillhandahålla it-driftstjänster som baseras på den myndighetens it-drift, om inte något annat är föreskrivet (6 § förordningen om samordnad och säker statlig it-drift).

I dagsläget har Trafikverket ingått överenskommelse med Skatteverket om att nyttja de tjänster för e-legitimering och digitala underskrifter som Skatteverket

tillhandahåller inom ramen för samordnad och säker statlig it-drift. Skatteverket har även en långt gången dialog med Lantmäteriet och överenskommelse om att Skatteverket ska tillhandahålla it-drift till Lantmäteriet kommer ingås i närtid.

3.1.3 Beredskapsmyndighet och sektorsansvarig myndighet

Förordningen (2022:524) om statliga myndigheters beredskap innehåller bestämmelser om uppgifter som statliga myndigheter under regeringen har inför och vid fredstida krissituationer och höjd beredskap.

Syftet med förordningen är att statliga myndigheter under regeringen genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter vid fredstida krissituationer och höjd beredskap. Statliga myndigheter med ansvar inom en eller flera viktiga samhällsfunktioner och vars verksamhet har särskild betydelse för samhällets krisberedskap och totalförsvaret ska vara beredskapsmyndigheter (1 och 18 §§ förordningen om statliga myndigheters beredskap). Skatteverket är beredskapsmyndighet och sektorsansvarig myndighet enligt förordningen om statliga myndigheters beredskap (12 a § instruktionen för Skatteverket samt bilaga 1 till förordningen om statliga myndigheters beredskap).

Som exempel bygger Skatteverkets hantering av inkomstdeklarationer, moms och arbetsgivaravgifter, folkbokföring, adressändring m.m. på att den uppgiftsskyldiga personen kan lämna uppgifter digitalt. Detta måste även gälla under kriser och krig. För att den uppgiftsskyldiga personen ska kunna använda Skatteverkets e-tjänster måste Skatteverket säkerställa att myndigheten kan tillhandahålla robusta tjänster för elektronisk identifiering.

3.2 Bedömning av om auktorisationssystemets tjänster för elektronisk identifiering motsvarar Skatteverkets behov

3.2.1 Allmänna överväganden

Som framgår av avsnitt 3.1 har Skatteverket ett omfattande uppdrag som riktar sig till privatpersoner och företag samt till myndigheter och andra samhällsaktörer. Skatteverket tillhandahåller ett stort antal elektroniska tjänster för att underlätta både för de enskilda personerna och för Skatteverket.

Skatteverket är i egenskap av offentlig aktör skyldig att använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i systemet (jfr 4 § 1 lagen om auktorisationssystem och 3 § första stycket förordningen om auktorisationssystem). Skatteverket har, liksom övriga myndigheter som är skyldiga att ansluta sig till auktorisationssystemet, anstånd med att ansluta sig till den 1 oktober 2026. Myndigheter är dock skyldig att senast den 1 oktober 2026 ingå avtal med Digg och därigenom ansluta sig till auktorisationssystemet, såvida de inte söker och får ett särskilt undantag (se avsnitt 2.2).

Skatteverket har i tidigare remissvar varit positiv till att regeringen tar ett samlat grepp om styrningen av förvaltningsgemensam infrastruktur men samtidigt lyft fram risker kopplade till obligatorisk anslutning, ökade kostnader, administrativ börda samt minskad operativ rådighet, se bl.a. Skatteverkets remissvar (2021-03-17 dnr 8-663317) till Infrastrukturdepartementet avseende promemorian Auktorisationssystem för elektronisk identifiering och för digital post (I2020/03269).

Försvarets materielverk har i sitt remissvar (2017-06-16 dnr 17FMV341 l-2:1) på betänkandet digitalforvaltning.nu (SOU 2017:23) lyft fram att utredningen har haft sitt fokus på myndigheter som har som uppdrag att ge service till allmänheten och att det är en svaghet att resonemang saknas om myndigheter som har annat uppdrag. Skatteverket vill i detta sammanhang lyfta fram att en närliggande svaghet är att det även saknas resonemang om myndigheter som har ett komplext uppdrag som täcker såväl service till allmänheten som annan verksamhet såsom it-service till andra myndigheter eller uppdrag som avser skydd och beredskap. Betänkandet digitalforvaltning.nu remitterades i mars 2017 och promemorian Auktorisationssystem för elektronisk identifiering och för digital post remitterades 2021. Regeringen har efter 2021 gett Skatteverket nya uppdrag, bl.a. som ansvarig för statlig it-drift och som beredskapsmyndighet, se avsnitt 3.2.3–3.2.5. Effekterna av dessa uppdrag skulle ha behövt analyseras utifrån att Skatteverket samtidigt ska ansluta till auktorisationssystemet. Till detta kommer att omvärldsläget sedan remitteringen av auktorisationssystemet har förändrats i grunden. Det kraftigt försämrade säkerhetsläget sedan 2022 har inneburit skärpta krav på Skatteverkets förmåga att upprätthålla robusthet, kontinuitet och kontroll i egenskap av beredskapsmyndighet och sektorsansvarig myndighet. Mot denna bakgrund speglar de bedömningar och ställningstaganden som låg till grund för det remitterade förslaget inte fullt ut de säkerhetsmässiga förutsättningar och krav som gäller idag.

Skatteverket har analyserat huruvida de tjänster för elektronisk identifiering som tillhandahålls genom auktorisationssystemet kan användas utifrån de olika uppdrag som Skatteverket har. Skatteverket har konstaterat att tjänsteutbudet i auktorisationssystemet inte täcker det behov som Skatteverket har när det gäller elektronisk identifiering, samt att en anslutning till auktorisationssystemet skulle medföra ett stort antal praktiska och säkerhetsmässiga problem för Skatteverket. Dessa beskrivs närmare i följande avsnitt.

3.2.2 Auktorisationssystemet täcker inte alla situationer då en person behöver identifiera sig elektroniskt när denna använder en e-tjänst som Skatteverket tillhandahåller

Försäkringskassan har i sin skrivelse (s. 7–8) till regeringen (se avsnitt 2.2) konstaterat att auktorisationssystemet inte täcker alla situationer då en person behöver identifiera sig elektroniskt när denna använder en e-tjänst som Försäkringskassan tillhandahåller. Skatteverket har konstaterat att samma problem även gäller för möjligheten för enskilda och företrädare för företag, organisationer och myndigheter att identifiera sig elektroniskt i en e-tjänst som Skatteverket tillhandahåller.

Av Försäkringskassans skrivelse framgår bl.a. följande: 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. 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. Samtliga fall av elektronisk identifiering omfattas således inte 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 en myndighet.

Skatteverket har konstaterat att det finns ett stort antal situationer där olika målgrupper av olika anledningar inte kan få en svensk e-legitimation, t.ex. pga. att personen inte har ett svenskt personnummer. Dessa användargrupper kan dock få andra e-legitimationslösningar som inte omfattas av auktorisationssystemet. För att möjliggöra att alla målgrupper som behöver använda Skatteverkets e-tjänster ska kunna göra det, måste Skatteverket upphandla sådana e-legitimationslösningar separat. De tekniska lösningarna för elektronisk identifiering som Skatteverket tillhandahåller de personer som ska logga in i Skatteverkets e-tjänster omfattas alltså av två olika avtalsmodeller: auktorisationssystemet respektive Skatteverkets avtal direkt med leverantören. Problemet med att ha två olika affärsmässiga avtal för en tjänst som tillhandahålls av samma leverantör kommer även att innebära problem när det gäller ansvaret och gränsdragningar vid incidenter, kontroll osv. Skatteverkets bedömning är att det inte är praktiskt genomförbart med parallella tjänsteleveranser för samma tjänster från samma leverantör men som är upphandlade eller tillhandahålls genom två olika avtal med olika avtalsparter (egen upphandlad lösning och auktorisationssystemet).

3.2.3 Krav på säkerhet och möjligheten att motverka identitetsmissbruk

Leverantörer inom auktorisationssystemet ska 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. Regeringen har konstaterat att 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 uppfylls (prop. 2023/24:6 s. 45). Säkerhetsfrågorna är därmed inte en sidofråga i systemet, utan en bärande förutsättning för att konstruktionen ska fungera.

Av anslutningsavtalet för leverantörer följer att leverantören årligen ska skicka en revisionsrapport till Digg efter avslutad internrevision. 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. I regelverken och Diggs offentliga information klargörs dock 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.

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. 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 väsentlig 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 (jfr prop. 2023/24:6 s. 31 och 45). Skatteverket delar Försäkringskassans uppfattning (se s. 9–10 i Försäkringskassans skrivelse) att auktorisationssystemet inte når upp till de krav på säkerhet som förutsattes i förarbetena till lagstiftningen om auktorisationssystemet och som myndigheterna är beroende av.

3.2.4 Skatteverkets uppdrag inom ramen för samordnad och säker statlig it-drift

Försäkringskassan har i sin skrivelse (s. 7–10) till regeringen redogjort för de problem som myndigheter ser när det gäller att myndigheten dels har ett uppdrag att tillhandahålla tjänster till andra myndigheter inom ramen för förordningen om samordnad och säker statlig it-drift, dels är skyldig att ansluta sig till auktorisationssystemet.

Skatteverkets uppdrag som leverantörsmyndighet för statlig it-drift innebär att myndigheten behöver upprätthålla och tillhandahålla en standardiserad, stabil och säker driftmiljö för ett antal anslutande myndigheter. Driftsmiljön måste bl.a. säkerställa att de krav som ställs när det gäller totalförsvarets behov och i cybersäkerhetslagen uppfylls.

Auktorisationssystemet för elektronisk identifiering innebär att ytterligare krav på tillitskedjor uppkommer när Digg blir en part i kedjan.

Skatteverkets uppdrag som leverantörsmyndighet för statlig it-drift, samtidigt som Skatteverket förväntas tillämpa auktorisationssystemet, ger upphov till både tekniska och organisatoriska utmaningar bl.a. när det gäller ansvarsfördelning, arkitekturprinciper och säkerhetskrav. Skatteverkets bedömning är därför att en anslutning till auktorisationssystemet väsentligt försvårar Skatteverkets möjlighet att tillhandahålla tjänsterna för e-legitimering och digitala underskrifter inom ramen för Skatteverkets uppdrag som leverantörsmyndighet för statlig it-drift.

3.2.5 Skatteverket behöver ha egen rådighet över centrala digitala funktioner såsom elektronisk identifiering

Skatteverkets behov av att upprätthålla egen rådighet över centrala digitala funktioner, såsom elektronisk identifiering, följer av flera författningar som ställer krav på säkerhet, kontinuitet och robusthet i samhällsviktig verksamhet.

Lagen (1992:1403) om totalförsvar och höjd beredskap

Enligt lagen om totalförsvar och höjd beredskap samt tillhörande förordningar ska statliga myndigheter säkerställa att verksamhet av betydelse för totalförsvaret kan upprätthållas även vid allvarliga störningar och under höjd beredskap. I ett samhälle där centrala samhällsfunktioner i hög grad är beroende av digitala system innebär detta att även sådana system utgör en integrerad del av den verksamhet som ska upprätthållas.

Förordningen (2022:524) om statliga myndigheters beredskap

Enligt 1 § förordningen om statliga myndigheters beredskap ska statliga myndigheter genom sin verksamhet bidra till att minska sårbarheten i samhället samt upprätthålla en god förmåga att fullgöra sina uppgifter vid fredstida krissituationer och höjd beredskap. Av 7 § samma förordning följer att myndigheter ska identifiera samhällsviktig verksamhet, analysera risker och sårbarheter samt vidta de åtgärder som krävs för att upprätthålla verksamhetens

kontinuitet. Vidare anges i 13 § att varje myndighet ansvarar för att de egna informationshanteringssystemen uppfyller nödvändiga säkerhetskrav.

Ovan angivna bestämmelser innebär att ansvaret för verksamhetens funktion och säkerhet vilar på den enskilda myndigheten. För Skatteverket, som också är beredskapsmyndighet enligt 18 § samma förordning, krävs därför att myndigheten faktiskt råder över de system och funktioner som är avgörande för att myndigheten ska kunna genomföra sin verksamhet på det sätt och enligt de krav som ställs i förordningen om statliga myndigheters beredskap.

Säkerhetsskyddsförordningen (2021:955)

Av 2 kap. 4 § säkerhetsskyddsförordningen följer att myndigheter ska vidta de åtgärder som krävs för att skydda säkerhetskänslig verksamhet, vilket innefattar kontroll över informationssystem och hantering av risker hänförliga till externa leverantörer. Säkerhetsskyddsförordningen är särskilt viktig för Skatteverket såsom värdmyndighet för Valmyndigheten. Säkerhetskyddsförordningen är också särskilt viktig när det gäller den löpande driften och de dagliga uppdateringarna av Skatteverkets system Navet, som är en del av folkbokföringsdatabasen. Krav på incidentrapportering och säker hantering av it-relaterade händelser framgår även av 14 § förordningen om statliga myndigheters beredskap.

Cybersäkerhetslagen (2025:1506)

Av 1 kap. 1 § cybersäkerhetslagen följer att verksamhetsutövare ska säkerställa en hög nivå av cybersäkerhet i nätverks- och informationssystem. Regelverket förutsätter att verksamhetsutövaren vidtar lämpliga och proportionerliga tekniska och organisatoriska åtgärder för att hantera risker samt att denne har förmåga att förebygga, upptäcka och hantera incidenter. Kraven omfattar även leverantörskedjan och innebär att verksamhetsutövaren ska kunna utöva styrning och kontroll över de komponenter som påverkar systemens säkerhet.

Elektronisk identifiering är förutsättningsskapande för elektroniska underskrifter som utgör en betrodd tjänst i den mening som avses i eIDAS-förordningen, se även definitionerna i 1 kap. 2 § cybersäkerhetslagen. Sådana tjänster utgör en grundläggande komponent i tilliten till digitala transaktioner och är därmed att betrakta som säkerhetskritiska funktioner i samhällsviktig verksamhet.

För en myndighet som Skatteverket, som i sin verksamhet utfärdar eller tillhandahåller funktioner med motsvarande egenskaper som betrodda tjänster – såsom identitetskontroll, autentisering och elektroniska underskrifter – innebär detta att kraven på säkerhet och tillförlitlighet är särskilt långtgående. Dessa krav omfattar de externa aktörer och tekniska komponenter som ingår i den samlade tillits- och åtkomstkedjan.

Mot denna bakgrund förutsätter tillämpningen av cybersäkerhetslagen att Skatteverket har faktisk möjlighet att utöva styrning och kontroll över hela denna kedja. För beredskapsmyndigheter med ansvar för samhällsviktig verksamhet innebär detta att en tillräcklig grad av operativ rådighet över säkerhetskritiska funktioner, inklusive sådana som motsvarar betrodda tjänster, måste kunna säkerställas.

Skatteverkets sammantagna bedömning

Skatteverket konstaterar att gällande rätt inte enbart ställer krav på att myndigheter ansvarar för säkerheten och funktionen i sina informationssystem, utan även förutsätter att myndigheterna har faktisk rådighet över de tekniska och organisatoriska förutsättningar som krävs för att uppfylla detta ansvar. En ordning

där centrala delar av den digitala infrastrukturen ligger utanför myndighetens direkta kontroll, samtidigt som ansvaret kvarstår, riskerar att försvåra möjligheterna att uppfylla de skyldigheter som följer av beredskaps-, totalförsvars- och cybersäkerhetslagstiftningen.

Skatteverket bedömer mot denna bakgrund att egen rådighet över tjänster för elektronisk identifiering utgör en nödvändig förutsättning för att säkerställa att myndigheten kan uppfylla sina rättsliga skyldigheter avseende säkerhet, robusthet och kontinuitet i samhällsviktig verksamhet. En anslutning till auktorisationssystemet för elektronisk identifiering innebär att Skatteverket förlorar rådigheten över centrala digitala funktioner såsom elektronisk identifiering och innebär därför ett hinder för myndigheten att fullgöra sitt uppdrag.

3.3 Ett permanent undantag behövs från kravet för anslutning till auktorisationssystemet när det gäller tjänsterna för elektronisk identifiering

Förslag

Skatteverket undantas 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

Undantaget från att använda tjänsterna för elektronisk identifiering i auktorisationssystemet ska även omfatta Skatteverket

Skatteverkets bedömning är att auktorisationssystemet för elektronisk identifiering kan fungera bra för myndigheter som har ett avgränsat uppdrag.

Som framgår av avsnitt 3.2.2–3.2.5 bedömer Skatteverket att de tjänster för elektronisk identifiering som tillhandahålls inom ramen för auktorisationssystemet inte motsvarar det behov som Skatteverket har. Eftersom de tjänster som tillhandahålls avseende elektronisk identifiering inom ramen för auktorisationssystemet inte kommer att vara tillräckligt för Skatteverkets behov, kommer Skatteverket vara tvungen att upphandla tjänster för elektronisk identifiering. Om Skatteverket skulle vara tvungen att ansluta sig till auktorisationssystemet skulle det skapa betydande svårigheter och ökade kostnader för myndigheten att fullgöra sina uppdrag.

En anslutning till auktorisationssystem för elektronisk identifiering är inte ändamålsenlig utifrån Skatteverkets behov. 3 § andra stycket förordningen om auktorisationssystem bör därför ändras så att Skatteverket räknas upp bland de myndigheter som omfattas av undantaget från 3 § första stycket förordningen om auktorisationssystem.

Fler myndigheter kan behöva omfattas av undantaget

Skatteverkets bedömning är att de problem som Skatteverket och Försäkringskassan har konstaterat när den gäller anslutningen till auktorisationssystemet för elektronisk identifiering sannolikt även gäller övriga beredskapsmyndigheter. Skatteverket har därför övervägt om det är lämpligt att utvidga undantaget i 3 § andra stycket förordningen om auktorisationssystem så att det omfattar samtliga beredskapsmyndigheter. Det kan även finnas ett behov av att undantaget utvidgas

till att omfatta myndigheter som Skatteverket kommer att tillhandahålla it-drift till inom ramen för uppdraget om samordnad och säker statlig it-drift.

Skatteverket konstaterar att ett förslag med en sådan inriktning skulle kräva en mer omfattande utredning av hur olika myndigheter påverkas, vilket inte ligger inom Skatteverkets mandat eller förmåga att genomföra. Skatteverket har därför inte utrett den frågan vidare.

Författningsförslag

Förslaget innebär ändring i 3 § förordningen om auktorisationssystem.

4 Ikraftträdandebestämmelser

Förslag

Författningsändringen ska träda i kraft den 1 oktober 2026.

Skälen för förslaget

Författningsändringen bör senast träda i kraft i samband med att det tillfälliga anståndet för samtliga myndigheter att ansluta sig till auktorisationssystemet upphör att gälla, vilket är den 1 oktober 2026 (se avsnitt 2.2). Om ändringen träder i kraft efter det datumet måste Skatteverket begära att ett särskilt undantag enligt 4 § förordningen om auktorisationssystem medges.

Skatteverket bedömer att det inte finns något behov av övergångsbestämmelser.

5 Konsekvensanalys

I detta avsnitt redogörs för konsekvenserna av det lämnade förslaget i den omfattning som bedöms lämpligt. Konsekvensanalysen är upprättad i enlighet med förordning (2024:183) om konsekvensutredningar. Förslaget är förenligt med EU-rätten. Förslagets konsekvenser bedöms inte vara av sådan omfattning att en utvärdering är nödvändig.

5.1 Syfte, alternativa lösningar och effekter av utebliven ändring

Enligt gällande regler ska Skatteverket senast den 1 oktober 2026 ansluta till auktorisationssystemet för elektronisk identifiering som Myndigheten för digital förvaltnings (Digg) ansvarar för. Förslaget i avsnitt 3.3 innebär att Skatteverket undantas från skyldigheten att använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem enligt lagen om auktorisationssystem.

Skatteverket har analyserat huruvida de tjänster för elektronisk identifiering och digital post som tillhandahålls genom auktorisationssystemet kan användas utifrån de olika uppdrag som Skatteverket har. Skatteverket konstaterar att tjänsteutbudet inte täcker det behov som Skatteverket har när det gäller elektronisk identifiering, samt att en anslutning till auktorisationssystemet skulle medföra ett stort antal praktiska problem för Skatteverket. Skatteverket har identifierat risker rörande systemet kopplade till bl.a. rådighet, säkerhet och proaktiv kontrollförmåga av leverantörer (avsnitt 3.2). Skatteverket bedömer att dessa problem är så allvarliga att myndigheten inte bör ansluta till systemet. I denna promemoria föreslår Skatteverket därför att Skatteverket ska undantas från skyldigheten att ansluta till auktorisationssystemet. Därigenom uppnår Skatteverket samma nivå av säkerhet i sina tjänster som myndigheten upprätthåller idag. Detta är av vikt inte bara för Skatteverket, utan även för samhället i stort sett utifrån ett beredskaps- och robusthetsperspektiv, inte minst under rådande säkerhetsläge. Om nuvarande reglering består måste Skatteverket använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystemet, trots de identifierade problemen.

Skatteverket har också konstaterat att det finns målgrupper som av olika anledningar inte kan få en svensk e-legitimation, men som kan få andra e-legitimationslösningar som inte omfattas av auktorisationssystemet. Nuvarande reglering innebär därför att Skatteverket kommer att behöva upphandla sådana e-legitimationslösningar separat för att möjliggöra att alla målgrupper som behöver använda Skatteverkets e-tjänster ska kunna göra det även i fortsättningen. De tekniska lösningarna för elektronisk identifiering som Skatteverket tillhandahåller kommer därför att omfattas av två olika avtalsmodeller: auktorisationssystemet respektive Skatteverkets avtal direkt med leverantören. Dessa problem undviks om Skatteverkets förslag genomförs.

Som ett alternativ till förslaget skulle Skatteverket i stället kunna ansöka om tidsbegränsade undantag. Det skulle dock vara en tillfällig lösning som endast skjuter problemet på framtiden. Ett tidsbegränsat undantag löser inte det grundläggande problemet med att auktorisationssystemets utformning inte uppfyller de säkerhetskrav som Skatteverket har behov av, vilket bedöms vara ett bestående problem över tid.

Se vidare avsnitt 3.3 för en närmare redogörelse av skälen för förslaget samt alternativa lösningar.

5.2 Effekter för Skatteverket

Skatteverket bedömer att en anslutning till auktorisationssystemet för elektronisk identifiering inte är ändamålsenligt sett till Skatteverkets behov. Om Skatteverket ska ansluta till auktorisationssystemet kvarstår behov av att upphandla tjänster även utanför det systemet. Detta medför att Skatteverkets kostnader för administration av avtalen kommer att öka eftersom myndigheten kommer att behöva ha flera avtal för tjänster som tillhandahålls av samma leverantör och hålla isär inloggningar som sker i respektive system. Digg tar också ut avgifter från myndigheterna, och Skatteverket har beräknat att kostnaden per år kommer att uppgå till 10 miljoner kronor beräknat utifrån den kostnadsnivå som beräknas gälla från 2027. Eftersom Skatteverket även fortsatt kommer att behöva upphandla tjänster utöver det utbud som finns i auktorisationssystemet, kommer anslutningen till Digg att innebära en kostnadsökning för Skatteverket som inte motsvarar nyttan.

Att Skatteverket ska nyttja samma tjänst från samma leverantör både inom auktorisationssystemet och utanför systemet innebär också att det uppkommer ett behov av att särskilja vilka inloggningar som sker med respektive avtal, eftersom avgifterna ska betalas till Digg om inloggningen görs inom systemet men direkt till leverantören om inloggningen sker utanför. Skatteverkets bedömning är att det inte är praktiskt genomförbart med parallella tjänsteleveranser från samma leverantör men med två olika avtal med olika avtalsparter för samma tjänster (egen upphandlad lösning och auktorisationssystemet).

En anslutning till systemet medför därför stora administrativa och tekniska svårigheter för Skatteverket. En anslutning kommer även att innebära problem när det gäller ansvar och gränsdragningar vid incidenter och kontroll. Dessa konsekvenser för Skatteverket uppkommer inte om förslaget genomförs.

En anslutning till auktorisationssystemet påverkar också Skatteverkets möjligheter att tillhandahålla de tjänster för e-legitimering och digitala underskrifter till andra myndigheter som omfattas av Skatteverkets uppdrag som leverantörs-myndighet inom ramen för förordningen om samordnad och säker statlig it-drift. Om Skatteverket förväntas tillämpa auktorisationssystemet ger detta upphov till både tekniska och organisatoriska utmaningar gällande bl.a. ansvarsfördelning, arkitekturprinciper och säkerhetskrav. Dessa effekter undviks om förslaget genomförs.

5.3 Effekter för andra myndigheter

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

Om Skatteverket 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 tillhandahålla systemet för andra offentliga aktörer. Om färre offentliga aktörer omfattas av skyldigheten att använda systemet eller om transaktionsvolymerna inom systemet blir lägre påverkas dock Diggs intäkter från avgifter för systemet. För offentliga aktörer som är anslutna till systemet kan förslaget därför medföra

ökade kostnader. Samtidigt bör det noteras att Skatteverket inte heller i dagsläget är ansluten till tjänster för elektronisk identifiering i auktorisationssystemet.

5.4 Effekter för företag och enskilda

Förslaget innebär att Skatteverket kan fortsätta upphandla tjänster för elektronisk identifiering på motsvarande sätt som görs i dag. Förslagets konsekvenser för företag bedöms därför vara begränsade.

För enskilda kan förslaget innebära att Skatteverkets lösningar i vissa delar avviker från den ordning som gäller inom auktorisationssystemet. Den enskilde användaren kommer dock inte att uppleva någon skillnad i praktiken eftersom Skatteverket även fortsättningsvis kommer att erbjuda samma inloggningsmetoder som de som följer med auktorisationssystemet. Skatteverket kommer dessutom erbjuda ytterligare lösningar. Syftet med förslaget är att säkerställa att tillgången till säkra och fungerande inloggningslösningar kan upprätthållas även över tid och vid störningar.

Förslaget bedöms inte få några övriga ekonomiska konsekvenser för företag eller enskilda.

5.5 Effekter på det brottsförebyggande arbetet

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. 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.

Försäkringskassan har i sin skrivelse (FK 2026/013860) till regeringen konstaterat att myndigheten har behov av mer långtgående tjänster för att motverka identitetsmissbruk än vad som erbjuds inom ramen för auktorisationssystemet. Skatteverket delar Försäkringskassans uppfattning att auktorisationssystemet inte når upp till de krav på säkerhet som förutsattes i förarbetena till lagstiftningen om auktorisationssystemet och som myndigheterna är beroende av. Skatteverket har också behov av att upprätthålla egen rådighet över centrala digitala funktioner, såsom elektronisk identifiering, vilket följer av flera författningar som ställer krav på säkerhet, kontinuitet och robusthet i samhällsviktig verksamhet (avsnitt 3.2.5). Som framgår av avsnitt 3.2.2 uppfyller auktorisationssystemet inte det behov som Skatteverket har när det gäller tjänster för elektronisk identifiering.

Genom förslaget att undanta Skatteverket från skyldigheten att använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem, uppnår Skatteverket samma nivå av säkerhet i sina tjänster som myndigheten upprätthåller idag.