Regeringen

Dir. 2020:27

Kommittédirektiv

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)