Informationsklass	Datum	Diarienummer
Öppen	2026-04-24	FK 2026/008258

Svar på regeringsuppdrag

Delrapport –Tillhandahålla teknisk lösning för uppkoppling till e-Codex för andra aktörer än myndigheter - Ju2025/02279

Försäkringskassan

Datum: 2026-04-24

Version Beslutad

Innehåll

Sammanfattning

Delrapporten beskriver analys, dokumentation och nödvändig reglering av tekniska och säkerhetsmässiga krav på tjänsteleverantörer som omfattas av e-bevisförordningen[1]. Dessa tjänsteleverantörer åläggs att ansluta till den tekniska lösning som Försäkringskassan har regeringsuppdrag att tillhandahålla

Uppdraget

Regeringen gav 30 oktober 2025 Försäkringskassan uppdraget att inrätta, drifta och förvalta en teknisk lösning som möjliggör för av tjänsteleverantörer utsedda verksamhetsställen och rättsliga ombud, (i denna framställning kallade tjänsteleverantörer), att kunna ansluta sig och få åtkomst till det decentraliserade IT-systemet e-Codex i enlighet med artikel 19 i e-bevisförordningen.

Anslutningen ska ske via ett webbaserat gränssnitt eller via applikationsgränssnitt mot en s.k. referensimplementation som tillhandahålls av EU-kommissionen och ska vara tillgänglig från 18 augusti 2026.

I uppdraget ingår att Försäkringskassan ska genomföra en analys av vilka specifika tekniska och säkerhetsmässiga krav som ska ställas på tjänsteleverantörer. Försäkringskassan ska även lämna förslag på hur dessa krav ska dokumenteras och regleras och vid behov lämna förslag till författningsändringar. En delredovisning avseende analys, dokumentation och reglering av tekniska och säkerhetsmässiga krav som ska ställas på de aktörer som önskar koppla en intern IT-lösning för utbyte av information med den nationella åtkomstpunkten ska lämnas senast den 1 maj 2026. Denna rapport utgör delredovisningen.

Vidare ger regeringen Försäkringskassan i uppdrag att möjliggöra även för andra aktörer än myndigheter som agerar som behörig myndighet enligt EU-rättsliga instrument och har en rättslig skyldighet att ansluta sig till IT-systemet e-Codex, t.ex. privata aktörer, att tekniskt kunna ansluta sig och få åtkomst till det decentraliserade IT-systemet e-Codex via ett webbaserat gränssnitt och applikationsgränssnitt eller på annat lämpligt sätt. En slutredovisning av uppdraget ska lämnas till Regeringskansliet (Justitiedepartementet) senast den 1 september 2027.

Uppdraget ska genomföras i samråd med Post- och Telestyrelsen (PTS) och Myndigheten för digital förvaltning (Digg). Synpunkter ska inhämtas på lämpligt sätt från Åklagarmyndigheten.

Analys av de tekniska och säkerhetsmässiga kraven

Delredovisningen ska enligt uppdraget omfatta analys, dokumentation och reglering av tekniska och säkerhetsmässiga krav som ska ställas på de aktörer som önskar koppla en intern IT-lösning för utbyte av information med den nationella åtkomstpunkten.

Enligt e-bevisförordningen har tjänsteleverantörer möjlighet att ansluta sig via ett applikationsgränssnitt (motsvarande ”koppla en intern IT-lösning för utbyte av information”) eller ett webbaserat gränssnitt. Försäkringskassan utgår från att delredovisningen ska omfatta båda dessa alternativ vad gäller analys, dokumentation och reglering av tekniska och säkerhetsmässiga krav.

[1] Europaparlamentets och rådets förordning (EU) 2023/1543 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (e-bevisförordningen)

Rättslig utgångspunkt för tekniska och säkerhetsmässiga krav

Av artikel 19 i e-bevisförordningen framgår att tjänsteleverantörer är skyldiga att vara anslutna till det decentraliserade it-systemet. Vidare ska de, enligt artikel 13.4 samma förordning, vidta de senaste operativa och tekniska åtgärder som krävs för att säkerställa konfidentialitet, sekretess och integritet vid överföring av uppgifter.

Av artikel 25 samma förordning framgår att EU-kommissionen ska anta genomförandeakter för att bl.a. fastställa målen för informationssäkerhet och relevanta tekniska åtgärder som säkerställer minimistandarder för informationssäkerhet och en hög cybersäkerhet.

I genomförandeförordningen[2] specificeras kraven för ett antal olika funktioner, såsom metoder för elektronisk kommunikation, kommunikationsprotokoll och informationssäkerhetsmål. I punkt 5 i bilagan till genomförandeförordningen framgår vilka tekniska åtgärder som ska vidtas för att säkerställa efterlevnad av minimistandarder för it-säkerhet i samband med utbyte av information via det decentraliserade it-systemet.

Den tekniska lösningen baseras på en referensprogramvara från EU-kommissionen

Försäkringskassan har valt att basera den tekniska lösningen på en referensimplementation som tillhandahålls av EU-kommissionen enligt artikel 22 i e-bevisförordningen. Av artikeln framgår att:

Kommissionen ska ansvara för skapandet, underhållet och utvecklingen av en referensprogramvara som medlemsstaterna får välja att använda som sitt backendsystem i stället för ett nationellt it-system. Skapandet, underhållet och utvecklingen av referensprogramvaran ska finansieras genom unionens allmänna budget.

Av skäl 4 i genomförandeförordningen framgår att:

För att säkerställa interoperabilitet bör både nationella it-system och referensprogramvaran omfattas av samma tekniska specifikationer och krav som fastställs i denna förordning.

Referensprogramvara från EU-kommissionen ska därmed uppfylla de funktionella, tekniska och säkerhetsmässiga krav som specificeras i e-bevisförordningen och genomförandeförordningen. Som ansvarig för den svenska implementationen har Försäkringskassan analyserat eventuella behov av att kunna ställa tekniska och säkerhetsmässiga krav på de tjänsteleverantörer som ansluter till lösningen.

Tekniska och säkerhetsmässiga krav

Nedan följer en sammanställning av de specifika, tekniska och säkerhetsmässiga krav som ska ställas på tjänsteleverantörer för anslutning till Försäkringskassans tjänst för åtkomst till systemet e-Codex, samt den rättsliga grunden för kraven. Dessa krav kommer att kommuniceras enligt de former Försäkringskassan och PTS finner lämpligt.

[2] Kommissionens genomförandeförordning (EU) 2025/1550 av den 28 juli 2025 om fastställande av tekniska specifikationer och andra krav för det decentraliserade it-system som avses i Europaparlamentets och rådets förordning (EU) 2023/1543 (genomförandeförordningen)

Tekniska och säkerhetsmässiga krav		Motiv och spårbarhet till rättslig grund
Supporterade webb-läsare	För åtkomst till webbgränssnittet ska tjänsteleverantören använda en webbläsare med aktiverat JavaScript och cookies som stödjer aktuella säkerhetsprotokoll och kryptografiska standarder, inklusive TLS 1.2 eller senare version. Webbläsaren ska vara säkerhetsuppdaterad och stödja funktioner som krävs för säker autentisering och kommunikation enligt punkterna 4–6 i bilagan till genomförandeförordningen.	Säkerställer tekniska förutsättningar för säker anslutning och autentisering. Punkten 4.7 i bilagan till genomförandeförordningen
Uppdaterad användar- och behörighetsinformation	Anslutande organisation ansvarar för att administrera, uppdatera och livscykelhantera sina användare och deras behörigheter i tjänsten. Detta inkluderar att säkerställa att endast behöriga personer har åtkomst, att åtkomst tas bort när den inte längre är motiverad samt att användarinformation hålls korrekt och aktuell. Administrationen ska utföras via det tillhandahållna gränssnittet för behörighetsadministration. Organisationen bär fullt ansvar för konsekvenser av felaktigt hanterade behörigheter.	Säkerställer att korrekt behörighet för användare av tjänsten upprätthålls. Punkten 5.1 c- och f i bilagan till genomförandeförordningen
Autentisering	Åtkomst till tjänsten kräver stark autentisering. Vid användning av webbaserad e-tjänst krävs tvåfaktorsautentisering (2FA) genom godkänd svensk e-legitimation. Vid anslutning via applikationsgränssnitt (API) krävs ömsesidig TLS-autentisering (mTLS). Åtkomst utan uppfyllda autentiseringskrav medges inte.	Säkerställer hög tillitsnivå vid åtkomst till tjänsten Punkten 5.1 c- och f i bilagan till genomförandeförordningen
Utgående IP-adresser	Anslutning till applikationsgränssnitt får endast ske från IP-adresser eller IP-områden som i förväg har registrerats och godkänts av organisationen. Endast trafik från dessa kända och verifierade IP-	Säkerställer hög säkerhet och motverkar risk för påverkan. Punkten 5.3 i bilagan till genomförandeförordningen

	intervall tillåts genom tjänstens IP-filtrering. Eventuella förändringar av användarens adressrymder ska anmälas och godkännas innan åtkomst kan medges.	
Klientcertifikat (mTLS)	Anslutning till applikationsgränssnitt (API) kräver ömsesidig TLS-autentisering (mTLS). Vid anslutning via API ska klienten autentiseras med certifikatbaserad mutual TLS där både klient och server identifierar varandra med certifikat utfärdade av betrodd certifikatutfärdare där tjänsteleverantörerna kan identifieras via organisationsnummer i certifikatet.	Säkerställer säkerhetsnivå i kommunikationsprotokoll och autentisering mot API. Punkterna 4.7, 5.1f, och 5.2 i bilagan till genomförandeförordningen
Tekniska specifikationer	Tjänsteleverantörer som ansluter egna system till den nationella e-bevisplattformen via applikationsgränssnitt (API) ska följa de tekniska specifikationer som Europeiska kommissionen fastställer. Tjänsteleverantörer ska särskilt säkerställa att anslutna system följer de schema-definitioner och informationsstrukturer som gäller för utbyte av EPOC, EPOC-PR samt tillhörande svar och metadata. API är baserat på Etsi TS 104 144 (Interface definition for the e-Evidence Regulation (EU) 2023/1543 for National Authorities and Service Providers).	Säkerställer följsamhet mot specifikationer. Artikel 19 i e-bevisförordningen Punkterna 4.3 och 4.6 i bilagan till genomförandeförordningen
Versionshantering	Tjänsteleverantörer som ansluter egna system via applikationsgränssnittet ska säkerställa att anslutna system är kompatibla med de versioner av applikationsgränssnittet som tillhandahålls. Tjänsteleverantörer ansvarar för att inom kommunicerade tidsramar anpassa sina system till ändringar i applikationsgränssnittets funktionalitet, säkerhetsmekanismer,	Säkerställer följsamhet mot specifikationer. Punkten 4.6 i bilagan till genomförandeförordningen

	informationsstrukturer och schema-definitioner.	

Reglering och dokumentation av de tekniska och säkerhetsmässiga kraven

Försäkringskassan har fått i uppdrag att inrätta en säker och tillgänglig lösning i enlighet med e-bevisförordningen och genomförandeförordningen. Således har Försäkringskassan ansvar för att tjänsten är säker och tillgänglig och för eventuella skador som uppstår i systemet. Därför behöver Försäkringskassan kunna ställa krav på tjänsteleverantörer att vidta nödvändiga operativa och tekniska åtgärder i samband med deras anslutning till och användning av tjänsten. Försäkringskassan har övervägt olika sätt att dokumentera och förmedla krav. Den regleringsform som framstår som mest lämplig är föreskrifter. Fördelarna med att uppställa krav i föreskriftsform är att reglerna blir allmänt tillgängliga på Försäkringskassans webbplats (lagrummet.forsakringskassan.se) och att det blir transparent för alla berörda vilka krav som gäller. Försäkringskassan kan också vid behov relativt enkelt ändra de krav som regleras genom föreskrifterna.

I arbetet med detta uppdrag har Försäkringskassan identifierat flera olika författningsbehov för att kunna tillhandahålla den aktuella tekniska lösningen för uppkoppling till e-Codex. En framställning rörande detta har lämnats in till regeringskansliet den 13 april 2026.[3] Försäkringskassan föreslår i framställningen en förordning om den tekniska lösningen för åtkomst till det decentraliserade it-systemet i enlighet med EU:s förordning om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis. I framställningen föreslås att Försäkringskassan får ett bemyndigande att utfärda föreskrifter om vilka operativa och tekniska krav som tjänsteleverantörer ska uppfylla i samband med anslutning till och användning av den tekniska lösningen. Detta bemyndigande är en förutsättning för att Försäkringskassan ska kunna ställa de krav på anslutande tjänsteleverantörer som behövs för att myndigheten ska kunna tillhandahålla tjänsten.[4]

De föreskrifter som beslutas kommer att kungöras på sedvanligt sätt genom tryck och publicering på Försäkringskassan webbplats, men innehållet kommer också att förmedlas till berörda aktörer på andra sätt. Post- och telestyrelsen kommer som centralmyndighet att ha kontakter med tjänsteleverantörer som ska ansluta till systemet. De kommer då att ha möjlighet att hänvisa till kommunikationsmaterial som informerar om krav för anslutning.

[3] E-bevis – Försäkringskassans behov av författningsreglering av vissa frågor rörande tillhandahållande av teknisk lösning, FK dnr 2026/006976
[4] Se ovanstående framställning, sid 3, 14 och 15

Beslut i detta ärende har fattats av avdelningschef Peter Haglind i närvaro av rättschef Ingrid Utne samt områdeschef Maria Danielsson och IT-Arkitekt Jan-Erik Bergström, de två senare som föredragande.

Peter Haglind

Jan-Erik Bergström

Maria Danielsson